U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR B&W mPOWER™ SMR 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~~of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth (D3). 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 designs. In addition, the areas most

significant to safety are discussed first. The current SRP guidance is system-based; 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[1] has been considered in the design of the digital I&C system. Although, there are no specific 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 nonsafety-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

[1] On October 14, 2008, in Volume 73 of the *Federal Register* (FR), pages 60612-60616 (73 FR 60612-60616), the Commission issued a policy statement on the regulation of advanced reactors [NRC-2008-0237].

systems that are ~~not~~ nonsafety-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., 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 anticipated operational occurrences (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~~D3.

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~~ 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, 17, 18, and ~~18~~19). The review of these systems is coordinated (as described above) with the organizations that have primary review responsibility for the supported systems.

4. For DC and combined license (COL) reviews, the staff reviews the applicant's proposed inspections, tests, analyses, and acceptance criteria (ITAAC) associated with the structures, systems and components (SSCs) related to this 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 and applicable guidance 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 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 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 (Chapter 15).

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 (Chapter 5).

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 (Chapter 9).

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 (Chapter 6).

~~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 Chapter 7 also applies to any protective device, such as a circuit breaker or relay with digital logic built into it. The guidance of DSRS Chapter

7 also applies to any grounding paths from an I&C element in a safety system to a ground through the electrical power network (Chapter 8).

~~6.~~

~~7.~~5. ~~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 (Chapter 3).~~

~~8.~~6. 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 (Chapter 3).

7. 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 (Chapter 3).

~~9.~~8. 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 (Chapter ~~3~~18).

~~10.~~9. The organization responsible for the review of quality assurance reviews general quality assurance programs (Chapter 17).

~~11.~~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 (Chapter 19).

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, "Resolution of Generic Safety Issues (Formerly entitled "A Prioritization of Generic Safety Issues")," 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 Three Mile Island (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

Specific DSRS acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are as follows for review described in this DSRS section. 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 DC design, COL facility, or early site permit (ESP)~~ site)~~, 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 intent of the regulations (in 10 CFR 52.47(a)(9), 10 CFR 52.79(a)(41), or 10 CFR 52.17(a)(1)(xii), as applicable).

3. Level of Review Applied ~~To~~ 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 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~~DC and ~~combined license~~COL 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[2], 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.
      - 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.

   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

[2] 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.

conditions, as defined in SECY 95-13294-084 "Policy and Technical Issues Associated with the Regulatory Treatment of Non-safety Systems in Passive Plant Designs (SECY 94-084)," -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 rcreditedcredited for accident mitigation.

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 (SAR). 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 B1 systems 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. The I&C review scope

includes the diverse actuation system 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 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 of less than $1x10^{-4}$ each reactor year and a large release frequency 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 nonsafety-related systems to confirm that any nonsafety-related design features or functional capabilities relied upon to prevent nonsafety-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 are 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~~D3 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 occurrence~~AOOs.

- 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 occurrence~~AOOs 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 occurrence~~AOOs 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 nonsafety-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 Quality Assurance (QA) program to I&C systems that are nonsafety-related. In any case, the development of a software-based I&C system that is nonsafety-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, GUIDANCE 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,	7.2.3 Reliability, Integrity, and Completion of	Full

Regulations	Location in DSRS	Review Responsibilities
"System Integrity"	Protective Action	
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

Regulations	Location in DSRS	Review Responsibilities
IEEE Std. 603-1991, Section 6.5, "Capability for Testing and Calibration"	7.2.15 Capability for Test and Calibration	Full
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

Regulations	Location in DSRS	Review Responsibilities
IEEE Std. 603-1991, Section 7.5, "Maintenance Bypass"	7.2.4 Operating and Maintenance Bypasses	Full
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"	7.1.1 Safety System Design Basis Coordinated with Chapter ~~15~~ 4 of the DSRS	Partial, [5]
GDC 13, "Instrumentation and control"	Sections 7.1 and 7.2 of the DSRS	Full, [6]

Regulations	Location in DSRS	Review Responsibilities
GDC 15, "Reactor coolant system design"	7.1.1 Safety System Design Basis Coordinated with Chapter ~~1~~5 of the DSRS	Partial, [7]
GDC 16, "Containment design"	7.1.1 Safety System Design Basis Coordinated with Chapter 6 of the DSRS	Partial, [8]
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 7.2.15 Capability for Test and Calibration	Full, [11]
GDC 22, "Protection System	7.1.2 Independence	Full, [12]

Regulations	Location in DSRS	Review Responsibilities
Independence"	7.1.5 Diversity and Defense-in-Depth	
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]
GDC 25, "Protection system requirements for reactivity control malfunctions"	Coordinated with Chapter ~~15~~ 4 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~~ Addresses ~~Three Mile Island (~~TMI~~)~~ ~~requirements~~ Requirements		

Regulations	Location in DSRS	Review Responsibilities
10 CFR 50.34(f)(2)(iv) (Safety Parameter Display Console)	7.1.5 Diversity and Defense-in-Depth 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]
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]

Regulations	Location in DSRS	Review Responsibilities
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
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

Regulations	Location in DSRS	Review Responsibilities
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]
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

Regulations	Location in DSRS	Review Responsibilities
10 CFR 52.47(b)(1) (ITAAC)	DSRS Section 14.3.5	Full
10 CFR 52.80(a) (COL ITAAC)	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]

Guidance	Location in DSRS	Review Responsibilities
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	

Guidance	Location in DSRS	Review Responsibilities
RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems"	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	
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	

Guidance	Location in DSRS	Review Responsibilities
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	
RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"	7.2.1 Quality	
RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"	7.2.1 Quality	
RG 1.170, "Software Test Documentation for Digital	7.2.1 Quality	

Guidance	Location in DSRS	Review Responsibilities
Computer Software Used in Safety Systems of Nuclear Power Plants"		
RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"	7.2.1 Quality	
RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"	7.2.1 Quality	
RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"	7.2.1 Quality	
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]

Guidance	Location in DSRS	Review Responsibilities
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. Probabilistic reliability assessments may be performed by the NRC staff to provide a basis for development of deterministic criteria for specific 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.

U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR B&W mPOWER™ SMR DESIGN

7.1 INSTRUMENTATION AND CONTROLS - FUNDAMENTAL DESIGN PRINCIPLES

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls (I&C)

Secondary - None

The organization responsible for the review of I&C should ensure that the application contains sufficiently detailed functional diagrams and explanations to demonstrate that the hardware and software for I&C architectures incorporate the fundamental design principles, namely independence; redundancy; predictability and repeatability; diversity and defense-in-depth (D3).

The reviewer must read Section 7.0 of this design-specific review standard (DSRS) to understand the I&C review scope, applicable regulatory requirements, DSRS acceptance criteria, and interfaces with other DSRS Chapters.

7.1.1 SAFETY SYSTEM DESIGN BASIS

I. AREAS OF REVIEW

The review will evaluate the specific design basis of each I&C safety system and ensure that the information provided for each design basis item is sufficient to enable the detailed design of the I&C system. The review will also verify that the I&C design is consistent with the credit taken in the safety analysis for the I&C system, including design basis, postulated design basis events (DBE) analyses, design descriptions, and operational characteristics of the safety systems.

Review Interfaces

The design basis information may be located in different chapters or sections of the application. The organization responsible for review of I&C safety systems should coordinate with the applicable U.S. Nuclear Regulatory Commission (NRC) technical organizations, as identified in the review procedures section below, in proper identification of the design basis, postulated DBE analysis, system description, system operational characteristics, and the I&C requirements[3] for each safety system.

[3] The design of digital I&C systems is governed by the legal requirements set forth in NRC regulations, including those in several of the ~~(~~GDC~~)~~ in 10 CFR Part 50, Appendix A and 10 CFR 50.55a(h), which incorporates by reference IEEE Std. 603-1991. NRC guidance endorses other IEEE standards, and these IEEE standards, as well as IEEE Std. 603-1991, are written in terms of so-called system, functional, performance, design, and other "requirements." These terms are well-understood in the I&C technical community, but, except as used in IEEE Std.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with Institute for the Institute of Electrical and Electronics Engineers, Inc.(IEEE) Standard (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 paragraphs of Title 10 of the Code of Federal Regulations (10 CFR) 50.55a(h)(2) and (3). This standard includes Section 4, "Safety System Designation." This section requires, in part, that a specific basis be established for the design of each safety system. In accordance with 10 CFR 50.55a(a)(3), an applicant can propose alternatives to the requirements of paragraph (h) of this section, 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.

2. General Design Criteria (GDC) 10, "Reactor Design," requires the reactor core and associated coolant, control, and protection systems be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences (AOOs).

3. GDC 15, "Reactor coolant system design," requires that the reactor coolant system and associated auxiliary, control, and protection systems be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including AOOs.

4. GDC 16, "Containment Design," requires reactor containment and associated systems 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.

5. GDC 19, "Control Room," requires, in part, that equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain

---

603-1991, are not legal requirements. To avoid confusion, this DSRS section will use the "requirements" terminology of the IEEE standards that are not incorporated into NRC regulations in connection with references to such standards. These "requirements," as referenced in this DSRS section, should be understood as recommendations that the NRC staff considers adequate to satisfy portions of NRC regulatory requirements, but which are not the only acceptable methods of compliance. The system, functional, performance, design, and other requirements of IEEE Std. 603-1991, which are legal requirements, will be explicitly identified as originating from IEEE Std. 603-1991.

the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

6. GDC 20, "Protection System Functions," requires protection system be designed to: (1) initiate automatically the operation of appropriate systems, including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of AOOs, and (2) sense accident conditions and to initiate the operation of systems and components important to safety.

DSRS Acceptance Criteria

Specific DSRS acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are as follows for review described in this DSRS section. 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 DC design, COL facility, or ESP site), 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 intent of the regulations (in 10 CFR 52.47(a)(9), 10 CFR 52.79(a)(41), or 10 CFR 52.17(a)(1)(xii), as applicable).

III. REVIEW PROCEDURES

The reviewer should confirm that the design bases, system design descriptions, system operation characteristics, postulated DBE analyses, and other information set forth in the application for each of the I&C safety systems satisfy~~ies~~ the requirements of GDCs 10, 15, 16, 19, 20, and Section 4 of IEEE Std. 603-1991. Many of the system characteristics contained in Section 7.2 of the DSRS are directly associated with the design bases documentation prescribed in IEEE Std. 603-1991, Section 4. These characteristics include, for example, identification of the I&C systems' safety functions and corresponding protective actions, all monitored variables used to control each protective action, the minimum number and location of sensors required for protective purposes, critical points in time or plant conditions, and the range of transient and steady-state conditions throughout which the safety systems shall perform, including conditions having the potential for functional degradation of safety system performance.

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer will confirm that the application contains information sufficient to demonstrate that the requirements contained in Section 4 of IEEE Std. 603-1991 are satisfied. In addition, the reviewer will confirm that the design basis descriptions have the following characteristics:

1. Completeness - The design basis descriptions should address all system functions necessary to fulfill the system's safety purpose.

2. Consistency - The information provided in the design basis descriptions should be analyzed to confirm its conformance with the plant safety analysis, including the DBE

analysis of Chapter 15 of the application, the mechanical and electrical system designs, and other plant system designs.

3. Correctness - The information provided for the design basis items should be technically accurate.

4. Traceability - It should be possible to trace the information in each design basis item to the safety analyses, plant system design documents, regulatory requirements, application commitments, or other plant documents.

5. Unambiguity - The information provided for the design basis items, taken alone and in combination should have one and only one interpretation. The design bases should not contain contradictory statements.

6. Verifiability - The information provided for the design basis items should be stated or provided in such a way as to facilitate the establishment of verification criteria and the performance of analyses and reviews of the various safety systems.

Additional Considerations in the Review of Design Basis Information

The reviewer will confirm that the application contains a description of all functional requirements for the I&C systems and the operational environment for the I&C systems. The information provided for each design basis item should be sufficient to enable the detailed design of the I&C system to be carried out. As a minimum, each of the design basis aspects identified in IEEE Std. 603-1991, Sections 4.1 through 4.12, should be addressed. The following should be noted about Section 4 of IEEE Std. 603-1991:

1. Section 4.1 of IEEE Std. 603-1991 requires, in part, the identification of the DBEs applicable to each mode of operation along with the initial conditions and allowable limits of plant conditions for each such event. The reviewer should confirm that this information conforms to the analysis provided in Chapter 15 of the application. This includes a review of the DBEs that are examined, the selection of plant variables that are used to initiate protective action, and functional and performance requirements for systems and components. Although DBEs and corresponding safety functions are discussed in Chapter 15 of the application, the reviewer will gain an understanding of the DBEs considered and the initiating events that are analyzed to identify safety functions and protective actions of the execute features.

2. Section 4.2 of IEEE Std. 603-1991 requires, in part, the identification of safety functions and corresponding protective actions of the execute features for each DBE. Additional information to address this requirement is derived from Section 4.4 of IEEE Std. 603-1991, which addresses the identification of variables that are monitored in order to provide protective action.

3. Section 4.3 of IEEE Std. 603-1991 requires, in part, the identification of the permissive conditions for each operating bypass capability that is to be provided. Permissive signals are used to enable, disable, or modify the operation of actuation functions based on plant conditions. The reviewer should confirm that the application contains information sufficient to identify permissive conditions for each operating bypass capability that is provided in the design. The reviewer should consider Section 6.6 of IEEE Std. 603-1991, which provides requirements for operating bypasses applicable to sense and command features, and Section 7.4 of IEEE Std. 603-1991, which provides requirements for operating bypasses applicable to execute features. Additionally, Section 5.8.3 of IEEE 603-1991 requires the indication of bypasses.

4. Section 4.4 of IEEE Std. 603-1991 requires, in part, the identification of variables that are monitored in order to provide protective action. Performance requirements, including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action, should be identified in the system designation. The reviewer should confirm that the application includes analyses, including the applicable portion provided in Chapter 15 of the application, demonstrating that system performance requirements are adequate to ensure completion of the protective actions. Additionally, variables that control each protective action by automatic means must be identified and documented using the criteria in Sections 6.1 and 7.1 of IEEE 603-1991. Section 4.4 also requires, in part, the identification of the analytical limit associated with each variable. The reviewer should confirm that an adequate margin exists between the analytical limits and the setpoints. In this context, adequate margin means the proper allowance for instrument uncertainties between 1) the device setpoint and the process analytical limit such that the system initiates protective actions before safety limits are exceeded, and 2) operating limits and setpoints such that there is a low probability for inadvertent actuation of the system. Additional information on setpoint requirements is in Section 6.8 of IEEE 603-1991, and setpoint guidance is contained Section 7.2.7 of this DSRS.

5. Section 4.5 of IEEE Std. 603-1991 describes the minimum criteria for determining whether manual initiation and control of protective actions are allowed. Specifically, the reviewer will confirm that the application describes:

   A. The points in time and plant conditions during which manual control is allowed. Section 4.10 of IEEE Std. 603-1991 requires the identification of critical points in time or the plant conditions for which safety system actuation is credited.

   B. The justification for permitting initiation or control subsequent to initiation solely by manual means.

   C. The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations shall be performed.

D. The variables in Section 4.4 of IEEE Std. 603-1998 that shall be displayed for the operator to use in taking manual action. The reviewer should consider Section 5.8.1 of IEEE Std. 603-1991, which requires the display of manually controlled actions credited for the safety systems to accomplish their safety functions.

Criteria for manual control of sense and command features are provided in Section 6.2 of IEEE Std. 603-1991, and criteria for manual control of execute features is provided in Section 7.2 of IEEE Std. 603-1991.

6. Section 4.6 of IEEE Std. 603-1991 requires, in part, the identification of the minimum number and location of sensors for those variables identified in Section 4.4 of IEEE Std. 603-1991 that have a spatial dependence. The reviewer should confirm that the application's analysis demonstrates that the number and location of sensors are adequate.

7. Section 4.7 of IEEE Std. 603-1991 requires that the design basis documentation include the range and steady-state transient conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform. The reviewer should confirm that the application provides information sufficient to address the range and steady-state transient conditions during normal, abnormal, and accident conditions stated above.

8. Section 4.8 of IEEE Std. 603-1991 requires, in part, identification of the conditions having the potential for functional degradation of safety system performance (including missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in nonsafety-related systems, etc.). The application should contain information sufficient to identify conditions having the potential for functional degradation of safety system performance as well as the provisions that are incorporated in the design to maintain each system's capability for performing its safety functions. The reviewer should confirm that the application complies with the independence criteria contained in Section 5.6 of IEEE Std. 603-1991 and the criteria for interactions between sense and command features and other systems contained in Section 6.3 of IEEE Std. 603-1991.

9. Section 4.9 of IEEE Std. 603-1991 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design, and the identification of the methods used to verify that any qualitative or quantitative reliability goals imposed on the system design have been met. The reviewer will determine the acceptability of system reliability based on the criteria described in IEEE Std. 603-1991 and IEEE Std. 7-4.3.2. The reviewer should also confirm that the application complies with the single-failure criterion requirements of Section 5.1 of IEEE

Std. 603-1991 and the reliability criteria contained in Section 5.15 of IEEE Std. 603-1991.

10. Section 4.10 of IEEE Std. 603-1991 requires identification of the critical points in time or plant conditions after the onset of a design basis event including: (1) the point in time or plant conditions for which the protective actions of the safety system shall be initiated, (2) the point in time or plant conditions that define the proper completion of the safety function, (3) the point in time or the plant conditions that require automatic control of protective actions, and (4) the point in time or the plant conditions that allow return of a safety system to normal. The reviewer should confirm that the application contains sufficient information to address the critical points in time or plant conditions outlined in Items 1-4. Requirements for automatic and manual initiation and control of protective actions for sense and command features are set forth in Sections 6.1 and 6.2 of IEEE Std. 603-1991, respectively. Requirements for automatic and manual initiation and control of protective actions for execute features are set forth in Sections 7.1 and 7.2 of IEEE Std. 603-1991, respectively.

11. Section 4.11 of IEEE Std. 603-1991 requires documentation of equipment protective provisions that prevent the safety systems from accomplishing their safety functions. The safety-related systems must be designed to accomplish their safety-related functions in accordance with the single-failure criterion in Section 5.1 of IEEE Std. 603. The reviewer should also consider the system's capability for test and calibration and the hazard analyses performed on the system as part of this finding. Additional guidance related for test and calibration and hazard analyses is contained in Section 7.2.15 and Appendix A of this DSRS.

12. Section 4.12 of IEEE Std. 603-1991 requires the documentation of any other special design basis that may be imposed on the system design, such as diversity, interlocks, or regulatory agency guidance criteria. These could include other necessary permissive signals that maintain safety-related interlocks, interlocks associated with plant operating modes, or interlocks that provide status and control signals to other systems and alarms.

Remote Shutdown Capability[4]

[4] Shutdown remote from the control room is not an event analyzed in the accident analysis in Chapter 15 of this DSRS. Specific scenarios have not been specified upon which the adequacy of shutdown capability remote from the control room is evaluated. However, smoke due to a fire in the control room has long been recognized as the type of event that could force the evacuation of the control room and result in a need to shut down remote from the control room. Regulatory Guide (RG) 1.189, "Fire Protection for Operating Nuclear Power Plants," establishes the bases for safe shutdown with respect to fire protection. Specifically, fire damage limits as they impact on safe shutdown have been established therein. These limits do not call for consideration of an additional, random, single failure in the evaluation of the capability to safely shut down as a consequence of-fires. The evaluation of conformance to R G 1.189 is addressed in SRP Section 9.5.1. Therefore, the application of the single-failure criterion to remote shutdown is only applicable for other events that could cause the control room to become uninhabitable. These events would not result in consequential damage or unavailability of systems credited for safe shutdown.

To the extent that the engineered safety feature (ESF) systems are used to achieve and maintain safe shutdown, the review of these systems in this section is limited to those features that are unique to safe shutdown and not directly related to accident mitigation. The features within the scope below may involve individual component control for safe shutdown versus system-level actuation for accident mitigation, or system-level controls used to achieve and maintain safe shutdown but not used for accident mitigation. System-level controls used for accident mitigation may also need to be reviewed below if the safe shutdown functions of these controls involve features or operating modes that are unique to their safe shutdown functions. This DSRS section also addresses the review of those systems credited for safe shutdown that are not classified as ESF systems.

During safe shutdown, reactivity control systems must maintain a subcritical condition of the core, and residual heat removal systems must operate to maintain adequate cooling of the core. For definitions of plant-specific shutdown conditions, see Chapter 16 in the applicant's safety analysis report.

1. The design should provide for control in locations removed from the main control room that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. This control equipment should be capable of operating independently of (i.e., without interaction with) the equipment in the main control room. This equipment may include the remote shutdown station and other local controls.

2. Equipment in the remote shutdown stations should be designed in accordance with the same standards as the corresponding equipment in the main control room.

3. Remote shutdown station control transfer devices should be located remote from the main control room and their use should initiate an alarm in the control room.

4. In the event that control functions are transferred from the control room to the remote shutdown station, the design should display parameter indications in the remote shutdown station such that the operators have access to the same parameter indications that they would have relied upon in the control room. Section 7.2.13 of this DSRS provides guidance associated with the typical parameters that should be displayed to monitor the plant status of a prompt hot shutdown of the reactor, maintaining the unit in a safe condition during hot shutdown, and for subsequent cold shutdown.

5. The location should be consistent with the guidance used for the design of remote, alternative, and dedicated shutdown equipment, as appropriate.

6. Access to remote shutdown stations should be under strict administrative controls. (See DSRS Section 7.2.9)

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, including the coordination with those having primary review responsibility for the accident analysis, the staff can conclude that the application provides information sufficient to: 1) demonstrate that a documented design basis is established for the design of each I&C safety system of the nuclear power generating station, and 2) the proposed I&C design conforms to with the safety systems' I&C requirements, including design basis, postulated DBE analyses, design descriptions, and operational characteristics of the safety systems. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the applicable requirements of GDCs 10, 15, 16, 19, 20, and Section 4 of IEEE Std. 603-1991.

V. IMPLEMENTATION

The staff will use this DSRS section in performing safety evaluations of B&W mPower specific design certification (DC), combined license (COL), or early site permit (ESP) applications submitted by applicants pursuant to 10 CFR Part 52. The staff will use the method described herein to evaluate conformance with Commission regulations.

Because of the numerous design differences between the B&W mPower and large light-water nuclear reactor power plants, and in accordance with the direction given by the Commission in SRM-COMGBJ-10-0004/COMGEA-10-0001, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews," dated August 31, 2010 (ML102510405), to develop risk-informed licensing review plans for each of the small modular reactor (SMR) reviews including the associated pre-application activities, the staff has developed the content of this DSRS section as an alternative method for the evaluation of a B&W mPower-specific DC, COL, or ESP application submitted pursuant to 10 CFR Part 52.

NRC regulations state, in part, that the DC, COL, or ESP application must contain an evaluation (of the design, facility, or site, respectively) against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application. The content of this DSRS section has been accepted as an alternative method for complying with those regulations (10 CFR 52.47(a)(9), 10 CFR 52.79(a)(41), or 10 CFR 52.17(a)(1)(xii), as applicable) as long as the B&W mPower DCD FSAR does not deviate significantly from the design/facility/site assumptions made by the NRC staff while preparing this DSRS section.

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in ppendix D of this Chapter.

7.1.2 INDEPENDENCE

I. AREAS OF REVIEW

The review will evaluate the methods described in the application used to demonstrate independence of the I&C systems: (1) between redundant portions of a safety system, (2) between safety systems and the effects of a DBE, and (3) between safety systems and other systems, as required by 10 CFR 50.55a(h). The review addresses the concepts of physical independence, electrical independence, communications independence, and functional independence.

Review Interfaces

Other fundamental design principles, such as redundancy, ~~diversity and defense-in-depth~~D3, and predictability and repeatability, inform the review of independence. In addition, the appendices to DSRS Chapter 7 provide additional guidance describing how the reviewer should consider the architectural description, simplicity, and hazard analysis techniques, and how they inform the staff's review of the system's independence.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.6, "Independence." This section requires physical, electrical, and communication independence between redundant portions of safety systems, safety systems and the effects of DBEs, and safety systems and other systems.

2. GDC 13, "Instrumentation and Control," requires in part that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operations, for AOOs, and for accident conditions as appropriate to assure adequate safety. Appropriate controls should be provided to maintain these variables and systems within prescribed operating ranges.

3. GDC 21, "Protection System Reliability and Testability," requires, in part, that the redundancy and independence designed into the protection system shall be sufficient to assure that no single failure results in loss of the protection function.

4. GDC 22, "Protection System Independence," requires, in part, that the protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis.

5. GDC 24, "Separation of Protection and Control Systems," 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.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for independence are as follows:

1. The reviewer should confirm that the I&C systems conform to the guidance in the version of RG 1.75 in place 6 months before the docket date of the application. Currently, RG 1.75 endorses IEEE Std. 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits," with identified exceptions and clarifications. The applicant should examine the version of RG 1.75 that applies to its application to identify the applicable standards.

   The relevant guidance includes electrical isolation criteria for circuits and electrical equipment that comprise or are associated with safety systems. Note that the evaluation of physical separation of electrical cables and power source independence is part of Chapter 8 of the DSRS and is not documented in this chapter. In addition, the reviewer should evaluate the following when assessing electrical independence:

   A. The reviewer should confirm that the design provides for the use of redundant power sources.

   B. The reviewer should verify that isolation devices are used for interfaces between (1) independent divisions and (2) safety systems and other systems. Isolation devices should be classified as part of the safety system and powered in accordance with IEEE Std. 603-1991 and the guidelines contained in the version of RG 1.75 in place 6 months before the docket date of the application. Accordingly, the reviewer should verify that each isolation device is powered by a ~~safety~~ ~~safety-~~related power source.

2. The system should conform to the communication independence guidance in the version of RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," in place 6 months before the docket date of the application. Currently, RG 1.152 endorses IEEE Std. 7-4.3.2-2003, with identified exceptions and clarifications. The applicant should examine the version of RG 1.152 that applies to its application to identify the applicable standards.

III. REVIEW PROCEDURES

The reviewer will evaluate the I&C system design described in the application to confirm that it meets the independence requirements of GDCs 13, 21, 22, 24, and Section 5.6 of IEEE Std. 603-1991. Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer will confirm that the proposed design exhibits independence between: (1) redundant portions of a safety system, (2) safety systems and the effects of DBEs, and (3) safety systems and other systems. For each of these areas, the review should evaluate, at a minimum, the following:

1. Physical independence
2. Electrical independence
3. Communications independence
4. Functional independence

Physical Independence

Physical independence is attained by physical separation and physical barriers. The reviewer should consider whether the application contains sufficient information to demonstrate the separation of (1) redundant portions of the safety system and (2) safety (protection) and nonsafety-related (control) systems to confirm that all interfaces among redundant portions of the safety system and between safety systems and nonsafety systems have been properly identified and addressed. The reviewer should confirm that the I&C systems conform to the physical independence guidance in the version of RG 1.75 in place 6 months before the docket date of the application. The relevant guidance includes physical separation criteria for circuits and electrical equipment that comprise or are associated with safety systems. Note that the review of physical separation of electrical cables is part of Chapter 8 of the DSRS and is not documented in this chapter.

Electrical Independence

The reviewer should confirm that the I&C systems conform to the electrical independence guidance in the version of RG 1.75 in place 6 months before the docket date of the application. The relevant guidance includes electrical isolation criteria for circuits and electrical equipment that comprise or are associated with safety systems. In addition, the reviewer should evaluate the following when assessing electrical independence:

1. The I&C evaluation of electrical independence is limited to the review of components and electrical wiring inside racks, panels, and control boards for safety systems. Note that the evaluation of physical separation of electrical cables is part of Chapter 8 of the DSRS and is not documented in this chapter.

2. The reviewer should confirm the use of redundant power sources. Note that the evaluation of power source independence is part of Chapter 8 of the DSRS and is not documented in this chapter.

3. The reviewer should verify that isolation devices are used to transmit signals between independent divisions and/or from safety to other systems. Isolation devices should be

classified as part of the safety system and powered in accordance with IEEE Std. 603-1991 and the guidelines contained in the version of RG 1.75 in place 6 months before the docket date of the application. The reviewer should also verify that each isolation device is powered by a safety-related power source.

Communications Independence

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer will confirm that the proposed design exhibits communication independence between: (1) redundant portions of the safety system, and (2) between safety and nonsafety systems. The reviewer should confirm that the design of the data communication meets the requirements of IEEE Std. 603-1991, Section 5.6. The reviewer should also confirm that data communication conforms to the guidance for the separation and isolation of data processing functions of interconnected computers contained in IEEE Std. 7-4.3.2, ~~Clause~~ Section 5.6, as endorsed by RG 1.152. The reviewer should consider the following:

1. The application should provide detailed information to demonstrate that the safety function of each safety division is protected from adverse influence from outside the division. For the I&C architecture proposed by the applicant, the reviewer should evaluate the signal path of redundant channels from sensors to final actuation devices to confirm division independence.

2. A safety division should not be dependent upon any information or resource originating or residing outside its own division to accomplish its safety function. Each safety division should receive plant data only from sensors dedicated to that division and that data should not be shared among divisions. Data flows between redundant portions of safety systems should be limited to those credited for coincidence logic voting for actuation and interlocks used for the performance of safety functions.

3. For designs that implement sharing of data between trip processing units and voting unit processors, or among voting unit processors, the reviewer should confirm that the proposed design includes provisions to cope with a trip processing unit or voting unit processor experiencing a lock-up condition (also known as hang or freeze), whether the processor controls a reactor trip or engineered safeguards system function. Such design provisions should include the following:

   A. Any voting unit processor or trip processing unit experiencing a lock-up condition will produce an alarm in the main control room and send a trip signal to all voting unit processors or trip processor units for that channel/division.

   B. If any two or more voting unit processors or trip processing units experience a simultaneous lock-up condition, an alarm will be displayed in the main control room and a reactor trip will result.

   C. The means used for ensuring that a trip signal is produced from either a trip

processing unit or voting unit processor that experiences a lock-up condition should be completely independent among safety divisions, should be hardware-based, and completely independent of software.

These design provisions apply to microprocessor-based technology as well as other forms of complex logic such as programmable logic devices (e.g. Field Programmable Gate Arrays (FPGAs)).

4. Communication processing faults in one safety division should not adversely affect performance of the safety function in other divisions.

5. Functions that are not necessary for safety should be executed outside the safety system.

6. The application should identify communications methods, including communications protocols, memory allocation methods, and message formatting methodology. The following should be evaluated.

   A. The protocol selected for the data communication is adequate to support performance of all safety function of the supported systems.

   B. Vital communication should be point-to-point by means of a dedicated medium. Vital communications include communications that are needed to support a safety function. Failure of vital communications could inhibit the performance of the safety function. The most common implementation of vital communications is the distribution of channel trip information to other divisions for the purpose of voting.

   C. Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. Error-correcting methods, if used, should be shown to reconstruct the original message exactly or designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

   D. The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory that is dedicated exclusively to this exchange of information. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a predictable and repeatable~~deterministic~~ manner (consistent with section 7.1.4 of this DSRS).

E. The safety function processor should not perform communication handshaking, as well as using acknowledgment signals and should not accept interrupts from outside its own safety division.

F. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. Guidance for reviewing cycle time is provided in Subsection 7.1.4, "Predictability and Repeatability~~Determinism~~," of this DSRS.

G. Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor.

H. Only desired data in predefined address, fixed format, fixed length, and structure should be accepted and processed by the receiving system. Unrecognized messages and data should be identified and discarded by the receiving system.

I. The effects of data communication equipment malfunction or failure that generates erroneous signals should be examined. Corrupted messages, missing messages and duplicate messages should be detected and handled, as appropriate~~ and repaired~~. Communications equipment failures and message errors that result in alarms should be identified.

7. All safety functions should be performed without interruption by any other signals, regardless of whether these signals are valid or erroneous.

8. Communication faults should not adversely affect the performance of required safety functions. The potential hazards to and from the data communication equipment should be reviewed. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

9. Priority modules should be safety-related. A command initiating a safety function should have the highest priority and should override lower priority commands. All requirements that apply to safety software should also apply to priority module software. The priority module software should be stored in the nonvolatile memories to prevent online alteration.

Functional Independence

Functional independence provides additional assurance regarding the isolation of a safety system from other safety systems. Functional independence seeks to prevent safety function failures by ensuring that physically and electrically independent portions of safety systems (with the exception of coincidence voting) do not depend on information from other independent portions of the safety system. The concept of functional diversity (using different parameters, different technologies, different logic or algorithms, or different actuation means to provide

several ways of detecting and responding to a significant event) helps accomplish functional independence, but does not totally address it.

Consideration of functional independence in the I&C system design helps demonstrate that successful completion of the system's safety functions is not dependent upon any behavior, including failures and normal operation of another system, or upon any signals, data, or information derived from the other system. Functional independence could also be used as a means of achieving isolation between redundant systems.

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer should verify that the following criteria related to functional independence are appropriately considered in the design of I&C systems:

1. Functional independence is supported by the architectural design and treatment of data that are shared between functions.

2. In computer systems, one-way, broadcast data communication should be used where computer based systems of a higher safety classification provide data to systems of lower safety classification. Hardware characteristics that enforce the one-direction communication feature (e.g., the use of a link that is connected only to a transmitter in the higher classified system and only to a receiver in the lower classified system) should be considered as the preferred means of ensuring one-directional communication.

   If bi-directional data communication between systems of different safety classifications is included in the design submitted by the applicant, staff may need to consult review guidance outside of the scope of the DSRS.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the proposed I&C systems addressed the fundamental design principle of independence among safety divisions, between redundant portions of a safety system, between safety systems and the effects of a DBE, and between safety systems and other systems. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the guidance contained in RG 1.75, and RG 1.152, ~~and RG 1.53,~~ and independence requirements of GDCs 13, 21, 22, 24, and Section 5.6 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.1. The reviewer must read Section 7.1.1 Safety System Design Basis subsection “V. Implementation”.

VI. REFERENCES

All of the references in this DSRS Chapter 7, “Instrumentation and Controls,” may be found in Appendix D of this chapter.

7.1.3 REDUNDANCY

I. AREAS OF REVIEW

Redundancy is commonly used in I&C safety systems to achieve system reliability goals and conformity with the ~~single~~ single-failure criterion. The application should provide information that describes what level of redundancy is used in the safety system to assure 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. In addition to the redundancy, the application should also describe the means employed in the I&C design for guarding against ~~common~~ common-cause failures.

Review Interfaces

Other fundamental design principles, such as independence, D3, and predictability and repeatability~~determinism~~, inform the review of redundancy. In addition, the appendices to DSRS Chapter 7 provide additional guidance describing how the reviewer should consider the architectural description, simplicity, and hazard analysis techniques, and how they inform the staff's review of the system's redundancy.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.1, "Single-Failure Criterion." This section states, in part, that the safety system must perform all safety functions required for a DBE in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions.

2. GDC 21, "Protection System Reliability and Testability," requires that the protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure 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.

3. GDC 24, "Separation of Protection and Control Systems," requires that "[t]he 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."

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for redundancy are as follows:

The system should conform to the physical and electrical independence guidance contained in the version of RG 1.53, "Application of Single-Failure Criterion to Nuclear Power Plant Protection Systems," in place 6 months before the docket date of the application. Currently, RG 1.53 endorses IEEE Std. 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," with identified exceptions and clarifications. The applicant should examine the version of RG 1.53 that applies to its application to identify the applicable standards.

III. REVIEW PROCEDURES

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer should confirm that the application provides information sufficient to demonstrate that the guidance on the ~~single~~ single-failure criterion in RG 1.53 is satisfied. IEEE Std. 379 provides a detailed discussion of how the safety I&C systems address the ~~single~~ single-failure criterion that the reviewer will consider in the review.

In addition to satisfying the single-failure criterion, suitably implemented redundancy enables system testing without loss of function. Similarly, redundancy enables component bypass or removal from service without loss of function. Additional redundancy may be warranted when protection and control systems share common components.

The reviewer should consider the following when assessing redundancy:

1. The application should provide a single-failure analysis in accordance with IEEE Std. 603-1991, Section 5.1, and IEEE Std. 379. In addition, the I&C architecture description should describe how redundancy is implemented in the I&C system design.

2. The reviewer will confirm that: (1) an evaluation of the effects of each component failure mode on the overall system is performed, (2) any component failure mode that could contribute to a failure of the safety system is identified, (3) the design of a safety system is such that no single failure of a component will result in spurious actuations and (4) necessary action is taken to eliminate, prevent, or control failure modes.

3. The reviewer will confirm that the application provides information sufficient to demonstrate that all structures, systems and components (SSCs) needed for safe shutdown have sufficient redundancy to satisfy the single-failure criterion. The use of data communication systems as single paths for multiple signals or data raises particular concern about extensive consequential failures as the result of a single failure. This review will confirm that channel assignments to individual communication subsystems can ensure that both redundancy and diversity requirements within the supported systems are met. NUREG/CR-6082, "Data Communications," provides additional guidance for issues that need to be considered for single failure when reviewing data communication designs (e.g., layering, encapsulation, protocol, multiplexing, error detection, etc.) and how redundancy may be used to address these issues.

4. The reviewer will confirm that the removal from service of any single safety system component does not result in a loss of the required minimum redundancy unless the reliable operation of the system can be otherwise demonstrated. The application should provide information to demonstrate how redundancy of channels implements the single-failure criteria as required by GDC 24. Channel redundancy should support safe removal of a channel from service (or channel bypass) for testing as prescribed by the technical specification.

The reviewer should also consider the following IEEE Std. 603-1991 requirements in the review of redundancy:

1. Section 5.7, which provides requirements for test and calibration of safety system equipment.

2. Section 6.3, which provides requirements for interactions between sense and command features and other systems.

3. Section 6.5, which provides requirements for test and calibration of sense and command feature sensors during reactor operations.

4. Section 6.7, which provides maintenance bypass requirements for sense and command features.

5. Section 7.5, which provides maintenance bypass requirements for execute features.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the design has sufficient redundancy 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. On such a basis, the reviewer can conclude that the

design of I&C systems satisfies the guidance contained in RG 1.53 and the redundancy requirements contained in GDCs 21, 24, and Section 5.1 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower™ DSRS Section 7.1. The reviewer must read Section 7.1.1 Safety System Design Basis subsection "V. Implementation".

VI. REFERENCES

~~All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this~~ chapter.

7.1.4 PREDICTABILITY AND REPEATABILITY

~~The review will evaluate the methods described in the application to demonstrate that the I&C system output is predictable and repeatable. Predictable and repeatable system behavior refers to the case in which input signals and system characteristics result in output signals through known relationships among the system states and responses to those states. Such a system will produce the same outputs for a given set of input signals (and the sequence of inputs) within well-defined response time limits to allow timely completion of credited actions. I&C safety systems should be designed to operate in such a predictable and repeatable manner, which is also called "deterministic" behavior.~~

I. AREAS OF REVIEW

The review will evaluate the methods described in the application to demonstrate that the I&C safety system output is predictable and repeatable. Predictable and repeatable system behavior refers to the case in which input signals and system characteristics result in output signals through known relationships among the system states and responses to those states. Such a system will produce the same outputs for a given set of input signals (and the sequence of inputs) within well-defined response time limits to allow timely completion of credited actions. I&C safety systems should be designed to operate in such a predictable and repeatable manner, which is also called "deterministic" behavior.

For digital systems, the reviewer will evaluate the predictability and repeatability of the output of digital I&C and data communications systems. The objective of this review is to (1) verify that system timing derived from the analysis of DBEs has been allocated to the I&C system architecture as appropriate and has been satisfied in the I&C system design, (2) confirm that the I&C system design and communication protocols provide features to assure system (or logic) performance in terms of response to inputs and time to produce a response, and (3) confirm that hazards that could challenge predicted behavior have been adequately identified and accounted for in the design.

Review Interfaces

Other fundamental design principles, such as independence, D3, and redundancy, inform the review of I&C system output predictability and repeatability. In addition, the appendices to DSRS Chapter 7 provide additional guidance describing how the reviewer should consider the architectural description, simplicity, and hazard analysis techniques, and how they inform the staff's review of the I&C system output predictability and repeatability.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). IEEE Std. 603-1991 provides requirements related to safety system performance and the timing of safety system response. The standard requires, in part, that safety systems have a documented design basis as follows:

A. Section 4.4 specifies limits, ranges, and rates of change of variables that should be included in the documented design basis.

B. Section 4.10 indicates that the applicant should identify critical points in time after the onset of a DBE that should be specified in the design basis.

In addition, Section 5.5, “System Integrity,” of IEEE Std. 603-1991 requires safety systems be designed to accomplish their safety-related functions under the range of conditions enumerated in the design basis. After initiation by either automatic or manual means, the sequence of protective actions (from receipt of a signal from the sense and command features to the actuated equipment that perform the safety function) shall go to completion in conformance with IEEE Std. 603, Section 5.2, “Completion of Protective Action.”

2. GDC 13, "Instrumentation and Control," requires in part that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operations, for AOOs, and for accident conditions as appropriate to assure adequate safety. Digital instrumentation must respond quickly enough so that the behavior of variables can be ascertained by operators.

3. GDC 21, “Protection System Reliability and Testability,” requires, in part, that the protection system be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.”

4. GDC 29, “Protection against Anticipated Operational Occurrences,” requires that the protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of AOOs.

DSRS Acceptance Criteria

There are no specific DSRS acceptance criteria in this section. However, the guidance provided below should be used to review the acceptability of the I&C system output predictability and repeatability.

III. REVIEW PROCEDURES

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer will confirm that the application conforms to the performance and timing requirements for safety systems contained in IEEE Std. 603-1991.

The timing of specific system responses credited in the safety analysis may affect the system architecture because it may not be possible to obtain sufficient computational performance for a specific function or group of functions from a single processor or the locations where functions are performed may be widely separated. Timing of credited actions may also increase

complexity, either by fragmenting the system into multiple processors or by code tuning, which makes the software product (or logic) harder to understand, verify, and maintain.

The reviewer will confirm that the application provides a detailed timing analysis discussing how the I&C system and supporting communication systems address the concept of predictability and repeatability. Appendix B of this chapter provides guidance on the relationship between the I&C system architecture and predictability and repeatability. The reviewer should also consider the following IEEE Std. 603-1991 sections in the review of predictability and repeatability:

1. Section 4.4, regarding limits, ranges, and rates of change of variables should be included in the documented design basis.

2. Section 4.10, regarding critical points in time should be specified for after the onset of a DBE.

3. Section 5.5, regarding the capability of safety systems to accomplish their safety-related functions under the range of conditions enumerated in the design basis.

4. Section 5.2, regarding the sequence of protective actions (from receipt of a signal from the sense and command features to the actuated equipment that perform the safety function) that will go to completion after initiation by either automatic or manual means.

The reviewer should confirm that the application provides sufficient information (in the form of architectural descriptions, functional block diagrams, descriptions of operation, etc.) to demonstrate that the proposed system's real-time performance is repeatable, predictable, and known at all times.

The review will include the following when assessing predictability and repeatability:

1. Verify that the digital I&C system timing analysis identifies limiting response times, digital computer timing requirements, architecture, and design commitments.

2. The digital I&C system timing analysis should address all system components from signal collection to completion of protective action (e.g., sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, de-multiplexer, computers, memory devices, controls, displays, logic processing, output processing, and voting).

3. Verify that the timing of specific system responses credited in the safety analysis have been allocated to the digital computer portion of the system, as appropriate, and have been satisfied in the digital system architectural design. Hardware and software design specifications should reflect these functional timing requirements.

4. Verify the digital I&C system timing analysis demonstrates that the protection safety functions are achieved within the times assumed in the safety analysis.

5. Verify that design practices that do not implement rigorous real-time and predictable and repeatable performance in digital I&C systems are documented. For those practices identified, verify (1) the methods used for controlling the associated risk have been documented, (2) such practices do not affect safety functions, and (3) the design does not impede any protective action.

6. Verify that data communications system timing is predictable and repeatable. Consider data rates, data bandwidths, and data precision for normal and off-normal operation, including the impact of environmental extremes. The application should make note of any delay that could impair the communication system's predictability and repeatability and provide a basis to conclude that such delays are neither part of any safety function nor can impede any protective action. Excess capacity margins should be sufficient to accommodate likely future increases in data communications system demands or software or hardware changes to equipment attached to the data communications systems. Confirm that the error performance is specified.

7. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed. To ensure predictable behavior, every datum in a message packet should be included in every transmit cycle, whether it has been changed since the previous transmission or not.

8. Verify that the processing cycle is defined, predictable, and repeatable within a specified sample time. In addition, the timing analysis should demonstrate that all safety functions are accomplished in each cycle or within a specific number of cycles. A discussion of why it is acceptable should be included in the application.

9. I&C safety systems that exhibit predictable and repeatable behavior, in general, should not be designed with the capability for unscheduled event-based disruptions or operator-based system functions that would inhibit or prevent the system from accomplishing its safety function. For software-based designs, predictable behavior also includes that the cycle time is repeatable with all safety functions accomplished in each cycle or within a specific number of cycles that is invariant.

10. Confirm that the I&C architecture design does not diminish the design's conformance with the other fundamental design principles.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the design of the I&C and data communication systems adequately address the fundamental design

principle of predictability and repeatability at both the system and component levels as demonstrated in the applicant's timing analysis. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the reliability, predictability, and repeatability requirements of GDCs 13, 21, 29 and Sections 4.4, 4.10, 5.2, and 5.5 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower™ DSRS Section 7.1. The reviewer must read Section 7.1.1 Safety System Design Basis subsection "V. Implementation".

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this Chapter.

7.1.5 DIVERSITY AND DEFENSE-IN-DEPTH

I. AREAS OF REVIEW

The objective of this review is to verify that (1) the I&C safety systems have a level of D3 such that there are two or more redundant systems or components which will be able to perform the safety functions credited in the safety analysis, (2) the different systems or components will have different attributes so as to reduce the likelihood of ~~common~~ common-cause failure (CCF), and (3) the displays and manual controls for critical safety functions initiated by operator action are diverse from digital systems used in the automatic portion of the protection systems. The staff will focus its review of D3 in digital I&C systems on whether the safety functions can be achieved in the event of a postulated CCF in the digital I&C system. Conformance with these objectives is sufficient to demonstrate conformance to the applicable requirements of 10 CFR 50.55a(h). To the extent the application addresses the requirements of 10 CFR 50.62 with respect to equipment used to address anticipated transient without ~~SCRAM~~ scram (ATWS) events, such considerations will be evaluated as part of this DSRS section.

Review Interfaces

1. Other fundamental design principles, such as independence, predictability, repeatability~~determinism~~, and redundancy, inform the review of D3. In addition, the appendices to DSRS Chapter 7 provide additional guidance describing how the reviewer should consider the architectural description, simplicity, and hazard analysis techniques, and how they inform the staff's review of the system's D3.

2. DSRS Chapter 18 defines a methodology, applicable to new reactors, for evaluating manual operator actions as a diverse means of coping with AOOs and postulated accidents ~~(PAs)~~ that are concurrent with a software CCF of the digital I&C protection system. Appendix 18-A of DSRS Chapter 18 offers additional guidance.

3. The review of D3 should be coordinated with the organization responsible for the review of Chapter 15 of the application. The reviewer should confirm with the organization responsible for the review of reactor systems that the analytical basis detailed in the D3 assessment is acceptable and consistent with the Chapter 15 analysis, and that the design of the mechanical systems used for ATWS mitigation is acceptable.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.1, "Single Failure Criteria." This section states, in part, that the safety system must perform all safety functions required for a DBE in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures, (2) all failures caused by the

single failure, and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions.

2. GDC 13, “Instrumentation and Control,” requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operations, for AOOs, and for accident conditions as appropriate to assure adequate safety.

3. GDC 22, “Protective System Independence,” requires in part that 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.

4. GDC 24, “Separation of Protection and Control Systems,” 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.

5. 10 CFR 50.62 requires, in part, automatic initiation of ATWS mitigation systems and equipment that is diverse and independent from the reactor trip system.

6. 10 CFR 50.34(f)(2)(xiv), “Containment Isolation Systems,” requires, in part, that all non-essential systems are isolated automatically by the containment isolation system.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for D3 are as follows:

1. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” issued December 1994, summarizes several D3 analyses performed after 1990 and presents an acceptable method for performing such analyses.

2. Staff’s Requirement Memorandum (SRM) to SECY-93-087 describes the NRC position on defense-in-depth in Item 18.II.Q.

3. Generic Letter (GL) 85-06, “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related,” dated April 16, 1985, provides quality assurance guidance for nonsafety-related ATWS equipment.

4. The system should conform to the guidance in the version of RG 1.53, in place 6 months before the docket date of the application. Currently, RG 1.53 endorses IEEE Std. 379-2000, “Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” with identified exceptions and clarifications. The applicant should

examine the version of RG 1.53 that applies to its application to identify the applicable standards. SectionClause 5.5 of IEEE Std. 379 establishes the relationship between CCF and single failures by defining criteria for CCFs that are not subject to single-failure analysis and identifies defense-in-depth as a technique for addressing CCF.

5. The version of RG 1.62, "Manual Initiation of Protective Actions," in place 6 months before the docket date of the application, includes information on diverse manual initiation of protective action. The applicant should examine the version of RG 1.62 that applies to its application to identify the applicable standards.

6. IEEE Std. 7-4.3.2 provides guidance on performing an engineering evaluation of software CCF for digital-based systems, including use of manual action and nonsafety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the CCF.

III. REVIEW PROCEDURES

The reviewer will confirm that the application has addressed vulnerabilities to CCF in accordance with the NRC position on D3 originating from the SRM, dated July 21, 1993, to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993, and particularly Item 18.II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems."

D3 can assure that a safety task will be accomplished when necessary to mitigate plant AOOs and postualted accidentsPAs, while also providing a defense against CCFs. Defense-in-depth is the principle of providing multiple barriers to any credible failure that would prevent a function from achieving its objective. Diversity, in the context of digital I&C, is the principle of using different technologies, equipment manufacturers, logic processing equipment, signals, logic and algorithms, development teams and personnel, and functions to provide a diverse means of accomplishing a safety function. Diversity complements defense-in-depth by decreasing the probability that a particular function will fail to achieve its objective.

Software-based or software-logic-based digital system development errors are a credible source of CCF. Common software includes software, firmware, and logic developed from software-based development systems. Generally, digital systems cannot be proven to be error free; thus, they are considered susceptible to CCF because identical copies of the software-based logic and architecture are present in redundant divisions of safety-related systems. Since CCF is not classified as a single failure (as defined in RG 1.53), design basis evaluations need not assume that a postulated CCF is a single failure. Consequently, analyses can employ realistic assumptions to evaluate the effect of CCF coincident with DBEs.

For designs that use digital safety systems, the NRC has established a four point position on D3 for new reactor designs and for digital system modifications to operating plants. The staff SRM, dated July 21, 1993, to SECY-93-087, and particularly Item 18.II.Q, forms the foundation of this position.

In the review of D3 assessments, the reviewer will focus on the following ~~four~~ points:

1. D3 Assessment

   The reviewer will confirm that a D3 assessment has been completed for the proposed I&C system and that the assessment demonstrates that vulnerabilities to ~~common~~ common-cause failures have been adequately addressed. The focus of the D3 assessment should be on the protection systems; however, other systems may be included in the D3 assessment to the extent that they are credited as providing diverse functions to protect against CCF in the protection systems.

2. Analysis of DBEs as Part of D3

   The application should contain information sufficient to demonstrate that the D3 assessment analyzes each postulated common-~~mode~~ cause failure for each event that is evaluated in the accident analysis section of the application using best-estimate methods. The application should include the following information:

   A. vulnerabilities to CCF in the I&C system

   B. plant response (calculated using realistic assumptions) demonstrating that any radiation release for each postulated CCF of the events evaluated in Chapter 15 does not exceed 10 percent of the applicable siting dose guideline values in 10 CFR 52.47(a)(2)(iv) or violate the integrity of the primary coolant pressure boundary (the application should (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken)

   C. an evaluation of all elements or signal sources common to two or more system echelons, including identification of all interconnections between the safety systems and nonsafety systems provided for system interlocks, and a justification that functions required by 10 CFR 50.62 are not impaired by the interconnections [In this context, "echelons" *or "echelons of defense," as referred to in NUREG/CR-6303, are specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the control system, the reactor trip or scram system, the Engineered Safety Features actuation system (ESFAS), and the monitoring and indicator system.*]

   D. a demonstration that adequate diversity is provided within the design for each of these events (adequate diversity applies to consideration of the software-based development tools used to develop software for computer-based processors or software-developed logic for digital logic devices)

   E. justification should be provided if vulnerabilities, are not addressed by design modification, refined analyses, or provision of alternate trip, initiation, or mitigation capability~~)~~

3. Diverse System Characteristics

If a postulated CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-~~mode~~ cause failure, should be capable of performing either the same function or a different function that will accomplish the same protection action. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. When a diverse means is needed to be available to replace an automated system used to accomplish a credited safety function as a result of the D3 assessment identifying a potential CCF, the reviewer should confirm that the credited safety function (or a different function that will execute the same desired safety protection) can be accomplished via either an automated system or manual operator actions performed from the main control room. The preferred diverse means is normally an automated system. In this context, the diverse means should be:

A. At the system or division level (depending on the design);

B. Initiated from the control room;

C. Capable of responding with sufficient time available for the operators to determine the need for protective actions even with indicators that may be malfunctioning due to the CCF if credited in the D3 coping analysis;

D. Appropriate for the event;

E. Supported by sufficient instrumentation that indicates:

i. the protective function is needed,
ii. the safety-related automated system did not perform the protective function, and
iii. whether the automated diverse means or manual action is successful in performing the safety function.

The diverse means could be safety-related and part of a safety division, and would then be subject to meet divisional independence and automatic and/or manual control requirements as defined in IEEE Std. 603-1991. The independence requirements of a diverse protection system for a safety protection system (i.e., physical, electrical, and communication separation) are defined in IEEE Std. 603-1991. The diverse means could also be nonsafety-related in which case the IEEE Std. 603-1991 requirements to separate safety-related equipment from not safety-related equipment would still apply and would require independence of the two systems. In either case, the diverse means should be independent of the safety system such that a CCF of the safety system would not affect the diverse system. See Figure 1.

Use of Automation as a Diverse Means

If automation is used ~~in~~ as the diverse means, the reviewer should confirm that the functions are provided by equipment that is not affected by the postulated CCF and are sufficient to maintain plant conditions within recommended acceptance criteria for the particular AOO or postualted accidents~~PA~~. The automated diverse means may be a nonsafety-related system, provided that the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The reviewer should confirm that the automated diverse means is similar in quality to systems required by the ATWS rule (10 CFR 50.62), as described in the enclosure to GL 85-06.

Use of Manual Action as a Diverse Means

The method for actuating the protective safety functions could be via manual operator actions that meet human factors engineering (HFE) acceptability criteria. If manual operator actions are used as the diverse means or as part of the diverse means to accomplish a safety function, the reviewer should confirm that a suitable HFE analysis was performed by the applicant to demonstrate that plant conditions can be maintained within recommended acceptance criteria for the particular AOO or postualted accidents~~PA~~. The acceptability of such actions is to be reviewed by the NRC staff in accordance with DSRS Chapter 18, which provides review criteria for crediting manual operator actions in D3 Analyses.

The following should be considered when reviewing manual actions:

A. If the D3 assessment indicates that a safety-related manual initiation could be subject to the same potential CCF as the automatically initiated protective action, then a diverse manual means of initiating protective action would be needed (i.e., two manual initiation means that are diverse from ~~one another~~each other would be needed).

B. If the safety-related system or division level manual initiation required by IEEE Std. 603-1991 is sufficiently diverse, the diverse (second) manual means would not be necessary (see Figure 1).

C. If credit is taken for a manual actuation method that meets both the IEEE Std. 603-1991, Sections 6.2 and 7.2 requirements and a need for a diverse manual means, then the applicant should demonstrate that such criteria are satisfied and that sufficient diversity exists.

D. The difference between Time Available and Time Required for operator action is a measure of the safety margin. As this difference decreases, uncertainty in the estimate of the difference between these times should be appropriately considered on a case-by-case basis. This uncertainty could reduce the level of assurance in, and potentially invalidate, a conclusion that operators can perform the action reliably within the time available. For complex situations and for actions with limited margin,

such as less than 30 minutes between time available and time required, a more focused staff review will be performed.

E. If the diverse means is nonsafety-related, the reviewer should confirm that the manual diverse means is similar in quality to systems required by the ATWS rule (10 CFR 50.62), as described in the enclosure to GL 85-06. In addition, the reviewer should confirm that IEEE Std. 603-1991, Section 5.6, "Independence," is considered for the independence of the safety systems and the diverse means.

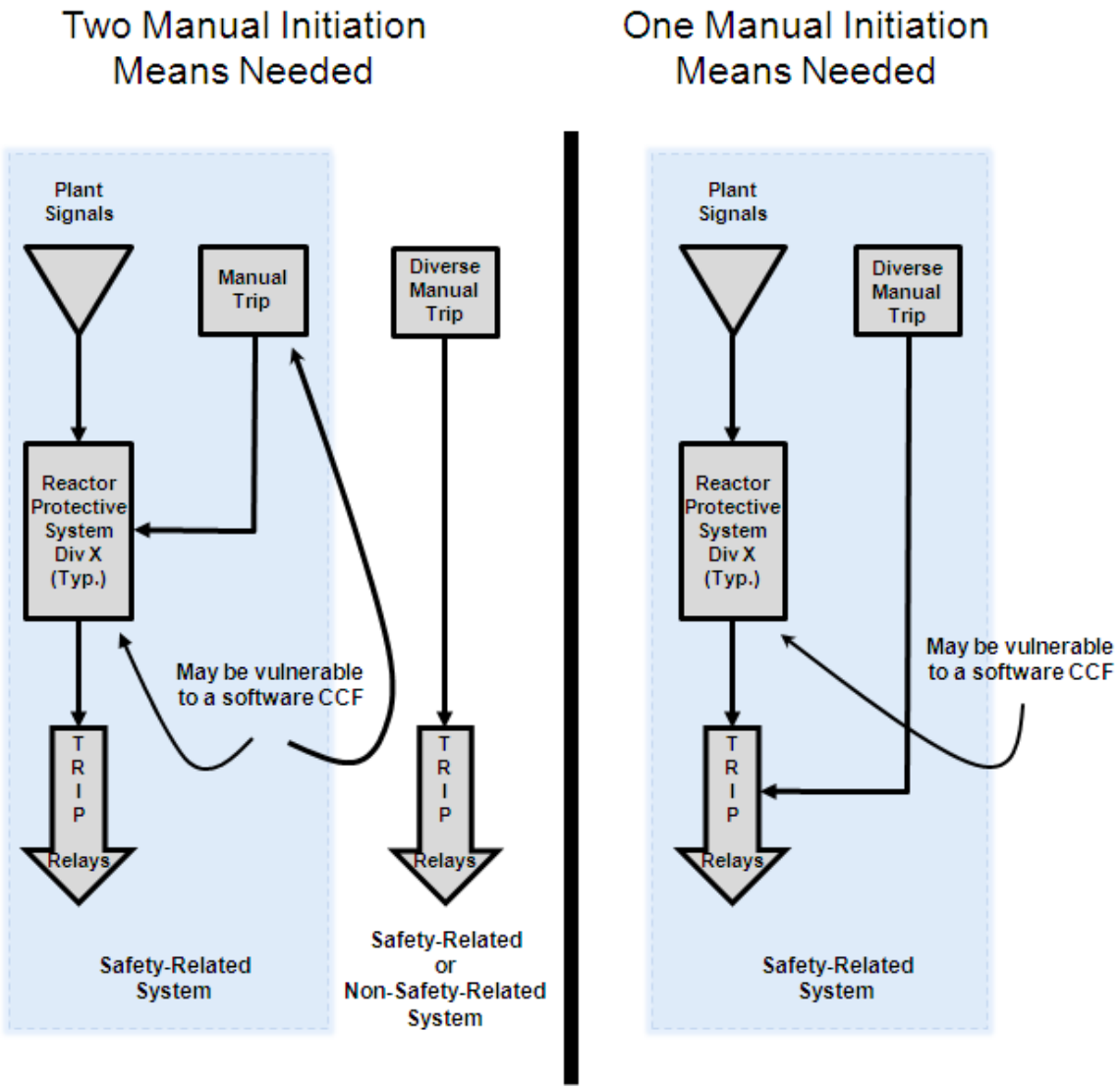

Figure 1. Two Manual Initiation methods versus One Initiation Method

4. Displays and Controls

A set of displays and controls located in the main control room should be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer system identified in Items 1 and 3 above.

Failure of monitoring or display systems should not influence the functioning of the reactor trip system (RTS) or ESF. If a plant monitoring system failure can induce operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that the protection system function will compensate for such operator-induced transients.

5. Additional Considerations for D3 Review

A. Prioritization between safety-related and diverse nonsafety-related systems is necessary to ensure that the credited safety function can be accomplished by either system.

i. Diverse actuation signals should be applied to plant equipment control circuits downstream of the digital system to which they are diverse to ensure that the diverse actuation will be unaffected by digital system failures and malfunctions. Accordingly, the priority modules that combine the diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to CCF.

ii. A command initiating a safety function should have the highest priority and should override lower priority commands. For example, a reactor trip would be considered the safe state and should not be overridden even if generated by a spurious actuation caused by a CCF of the automated protection system. However, in the case of the spurious actuation of engineered safety features actuation system (ESFAS) ~~actuation system (AS)~~ equipment, the design should afford the reactor operator the ability to manually control components in the priority scheme. Many options are available for how the system accomplishes these actions (i.e., through hardwiring or direct network control or through a priority module, etc.).

iii. Commands that originate in a safety-related channel, but which only cancel or enable cancellation of the effect of the safe-state command (i.e., a consequence of a CCF in the primary system that erroneously forces the plant equipment to a state that differs from the designated safe state) and which do not directly support any safety function, should have lower priority and may be overridden by higher priority commands. An example is a postulated CCF that causes the ESFAS to erroneously turn off components credited to perform a safety function. The reviewer should note whether the priority scheme would allow the reactor operator to place such components in

the safe state necessary to support the safety function and how the system accomplishes the operator action.

iv. The analysis of the proposed priority ranking should explain conflicts due to timing and sequencing of signals. The reviewer should refer the proposed priority ranking and its explanation to appropriate systems experts for review.

v. The priority module itself should be shown to apply the commands correctly in order of their priority rankings and should meet all other applicable guidance. The application should demonstrate that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.

B. While the D3 assessment should consider failure of the protection system to actuate a safety function when plant conditions warrant a trip or actuation in response to a CCF of the automated protection system, failures of the automated protection system stemming from a software CCF may cause spurious actuations. The plant design basis should address the effects of certain spurious actuations caused by a software CCF.

i. The overall D3 strategy of a plant should prevent or mitigate the effects of spurious actuations caused by a software CCF that have the potential to place a plant in a configuration that is not bounded by the plant's design basis.

ii. The effects of some postulated spurious actuations caused by a software CCF in the automated protection system may not be evaluated in the design basis accident analyses. In these cases, an analysis should be performed to determine whether these postulated spurious actuations could result in a plant response that results in conditions that do not fall within those established as bounding for plant design. The analysis should also identify whether coping strategies—whether for prevention or mitigation—exist for these postulated spurious actuations (e.g., emergency, normal, and diverse equipment and systems, controls, displays, procedures, and the reactor operations team) and consider the adequacy of such strategies.

iii. If existing coping strategies are not effective for responding to the postulated spurious actuations from software CCFs that result in the plant exceeding its design basis, the application should develop and present additional coping strategies.

iv. The design of a diverse automated or diverse manual actuation system should address how to minimize the potential for a spurious actuation of the protective system caused by the diverse means.

C. In reviewing the D3 assessment using the above acceptance criteria, the reviewer should evaluate whether the analysis of the D3 design features conforms to the guidance of NUREG/CR-6303. In general, several types of diversity should exist, some of which should exhibit the attributes listed in NUREG/CR-6303. The reviewer should be aware of the following when reviewing the D3 assessment:

i. The justification for equipment diversity, or for the diversity of related system logic such as a real-time operating system, should extend to the equipment's components to assure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby incorporating the potential for common failure causes in otherwise different equipment. Claims for diversity on the basis of the difference in manufacturer name are insufficient without consideration of the above.

ii. With respect to computer software and software-based logic diversity, experience indicates that independence may not be achieved in cases in which, for example, multiple versions of software are developed using the same set of software, system, and logic development tools. Other considerations, such as technology, functional and signal diversity that lead to different software, system, and logic requirements form a stronger basis for diversity.

In addition, the evaluation of failure modes as a result of CCF should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate, in accordance with NUREG/CR-6303.

D. Many system design and testing attributes, procedures, and practices can contribute to significantly reducing the probability of CCF. However, there are two design attributes, either of which is sufficient to eliminate consideration of ~~software~~ software-based or ~~software~~ software-~~logic~~ logic-based CCF:

i. Diversity – If sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

ii. Testability – If a system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested), then CCF within the system can be considered to be appropriately addressed without further action.

If a portion or component of a system can be fully tested, then it can be considered not to have a potential for software-based CCF. Fully tested or 100% testing means that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case. Further, in assessing the system states, the guidance provided in IEEE Std. 7-4.3.2, Section~~Clause~~ 5.4.1, "Computer system [equipment qualification] testing," should be addressed. This approach is applicable to microprocessor-based technology as well as other forms of complex logic such as programmable logic devices (e.g. Field Programmable Gate Arrays (FPGAs)).

6. Conformance with 10 CFR 50.62

As defined in 10 CFR 50.62, an ATWS event is an AOO followed by failure of the reactor trip portion of the protection system. Diverse actuation system (DAS) and ATWS mitigation functions may be combined into a single system, or the ATWS mitigation functions may be performed by a completely separate system. For ATWS mitigation systems in pressurized water reactors, 10 CFR 50.62 requires diversity from the sensor output to the final actuation device. The ATWS mitigation systems ~~should include the capability for initiation from the control room and~~ should be testable at power (up to, but not necessarily including, the final actuation device). The ATWS mitigation logic and DAS should be designed such that, once initiated, the mitigation function will go to completion. Logic and actuation device power for the ATWS mitigation system should be from an instrument power supply independent from the power supplies for the existing RTS.

The reviewer should verify that the DAS functions are independent and diverse from the RTS and ESFAS, and that the ATWS mitigation systems are diverse from the RTS. However, interconnections between the RTS and ESFAS (for interlocks providing for reactor trip if certain ESFs are initiated, ESF initiation when a reactor trip occurs, or operating bypass functions) are permitted. RTS and ESFAS may be combined into a single controller or central processing unit. However, the preferred method is to perform the RTS and ESFAS functions in distinct and separate modules, systems, or platforms. Whether distinct or combined, the following criteria are addressed:

A. D3 is adequately addressed to protect against CCF.

B. The interconnections between the RTS and ESFAS (for interlocks providing for reactor trip if certain ESFs are initiated, ESF initiation when a reactor trip occurs, or operating bypass functions) can be demonstrated not to impair the functions required by the ATWS rule (10 CFR 50.62).

C. The ~~fundamental principle~~ concept of simplicity has been adequately addressed.

7. Conformance with 10 CFR 50.34(f)(2)(xiv)

Signal diversity should be provided for the containment isolation function. The containment isolation functions of the ESFAS should be reviewed to confirm that the

ESFAS automatically closes each isolation device on each nonessential penetration. For plants with digital-computer-based ESFAS, signal diversity should be confirmed in the review of the applicant's D3 analysis.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the proposed I&C systems are designed with sufficient diversity to cope with a DBE concurrent with a CCF that disables the safety function. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the guidelines in the SRM to SECY-93-087 and NUREG/CR-6303 with regard to D3, and the D3 requirements contained in GDCs 13, 22, 24, 10 CFR 50.62, 10 CFR 50.34(f)(2)(xiv), and Section 5.1 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.1. The reviewer must read Section 7.1.1 Safety System Design Basis subsection “V. Implementation”.

VI. REFERENCES

All of the references in this DSRS Chapter 7, “Instrumentation and Controls,” may be found in Appendix D of this Chapter.

U. S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR B&W mPOWER™ SMR DESIGN

7.2 INSTRUMENTATION AND CONTROLS – SYSTEM CHARACTERISTICS

REVIEW RESPONSIBILITIES

Primary—Organization responsible for the review of instrument and controls (I&C)

Secondary—None

This design-specific review standard (DSRS) Section provides guidance associated with I&C safety system characteristics contained in Sections 5, 6, and 7 of Institute of Electrical and Electronics Engineers, Inc. (IEEE) Standard (Std.) 603-1991 and IEEE Std. 7-4.3.2, as endorsed by the version of Regulatory Guide (RG) 1.152 in place 6 months before the docket date of the application.

Section 7.1 of this DSRS provides guidance to address major functional and design considerations associated with I&C safety systems, including compliance with relevant regulatory requirements. Guidance associated with additional functional and design considerations contained in Sections 5, 6, and 7 of IEEE Std. 603-1991 and IEEE Std. 7-4.3.2 (for computer-based I&C systems) are addressed in this DSRS section. Some of the characteristics discussed below address specific functional and design requirements[5] for I&C systems, including safety system criteria, sense and command features, and execute features that complement the design principles addressed in DSRS 7.1. To provide for a streamlined review, certain characteristics have been grouped together in this section.

The reviewer must read Section 7.0 of this DSRS to understand the I&C review scope, applicable regulatory requirements, DSRS acceptance criteria, and interfaces with other DSRS Chapters.

[5] The design of digital I&C systems is governed by the legal requirements set forth in NRC regulations, including those in several of the General Design Criteria (GDCs) of Title 10 of the Code of Federal Regulations (10 CFR) Part 50, Appendix A and 10 CFR 50.55a(h), which incorporates by reference IEEE Std. 603-1991. NRC guidance endorses other IEEE standards, and these IEEE standards, as well as IEEE Std. 603-1991, are written in terms of so-called system, functional, performance, design, and other "requirements." These terms are well-understood in the I&C technical community, but, except as used in IEEE Std. 603-1991, are not legal requirements. To avoid confusion, this DSRS section will use the "requirements" terminology of the IEEE standards that are not incorporated into NRC regulations in connection with references to such standards. These "requirements," as referenced in this DSRS section, should be understood as recommendations that the NRC staff considers adequate to satisfy portions of NRC regulatory requirements, but which are not the only acceptable methods of compliance. The system, functional, performance, design, and other requirements of IEEE Std. 603-1991, which are legal requirements, will be explicitly identified as originating from IEEE Std. 603-1991.

7.2.1 QUALITY

I. AREAS OF REVIEW

The application should provide information to confirm that I&C safety system equipment will be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.

The scope of this section covers all I&C safety systems. For nonsafety-related systems, the reviewer will verify that the application describes how the quality measures applied to I&C systems that are nonsafety-related are commensurate with the importance to safety of those systems. Application of the guidance in this section would be adequate for that purpose.

Review Interfaces

The organization responsible for the review of Quality Assurance (QA) evaluates QA program descriptions (QAPDs) submitted by applicants for a design certification (DC). Guidance for the review of QA is provided in DSRS Chapter 17. I&C system development processes (hardware and software) described in this section are to be implemented within a QA program that conforms to applicable regulatory requirements.

The I&C reviewer will assess the framework that will be used to design and develop I&C safety systems with assistance from the organization responsible for the review of QA.

II. ACCEPTANCE CRITERIA

Requirements

1. 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 paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.3, "Quality." Section 5.3 requires that components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. It also requires that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. 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.

2. 10 CFR 50.55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed.

3. 10 CFR Part 50, Appendix A, GDC 1, "Quality Standards and Records," requires, in part, that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.

4. Appendix B to 10 CFR Part 50 establishes QA requirements for the design, manufacture, construction, and operation of safety-related structures, systems, and components.

DSRS Acceptance Criteria

Specific DSRS acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are as follows for review described in this DSRS section. 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 DC design, COL facility, or ESP site), 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 intent of the regulations (in 10 CFR 52.47(a)(9), 10 CFR 52.79(a)(41), or 10 CFR 52.17(a)(1)(xii), as applicable).

The specific DSRS acceptance criteria for quality are as follows:

1. The version of RG 1.28, "Quality Assurance Program Criteria (Design and Construction)," in place 6 months before the docket date of the application. Currently, RG 1.28 endorses ASME NQA-1-2008, "Quality Assurance Requirements for Nuclear Facility Applications," and the ASME NQA-1a-2009 Addenda, "Addenda to ASME NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications," with identified exceptions and clarifications. The applicant should examine the version of RG 1.28 that applies to its application to identify the applicable standards.

2. Digital I&C safety systems should conform to the quality guidance in the version of RG 1.152, ~~"Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,"~~ in place 6 months before the docket date of the application. Currently, RG 1.152 endorses IEEE Std. 7-4.3.2-2003, with identified exceptions and clarifications. The applicant should examine the version of RG 1.152 that applies to its application to identify the applicable standards.

3. Digital I&C safety systems should conform to the guidance in the version of RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," in place 6 months before the docket date of the application. Currently, RG 1.168 endorses IEEE Std. 1012-~~1998~~2004, "IEEE Standard for Software Verification and Validation," and IEEE Std. 1028-~~1997~~2008, "IEEE Standard for Software Reviews and Audits," with identified exceptions and clarifications. The applicant should examine the version of RG 1.168 that applies to its application to identify the applicable standards.

4. Digital I&C safety systems should conform to the guidance in the version of RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," in place 6 months before the docket date of the application. Currently, RG 1.169 endorses IEEE Std. 828-~~1990~~2005, with identified exceptions and clarifications. The applicant should examine the version of RG 1.169 that applies to its application to identify the applicable standards.

5. Digital I&C safety systems should conform to the guidance in the version of RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," in place 6 months before the docket date of the application. Currently, RG 1.170 endorses IEEE Std. ~~IEEE Std.~~ 829-~~1983~~2008, "IEEE Standard for Software Test Documentation,"~~,~~ with identified exceptions and clarifications. The applicant should examine the version of RG 1.170 that applies to its application to identify the applicable standards.

6. Digital I&C safety systems should conform to the guidance in the version of RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," in place 6 months before the docket date of the application. Currently, RG 1.171 endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing," with identified exceptions and clarifications. The applicant should examine the version of RG 1.171 that applies to its application to identify the applicable standards.

7. Digital I&C safety systems should conform to the guidance in the version of RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," in place 6 months before the docket date of the application. Currently, RG 1.172 endorses IEEE Std. 830-~~1993~~1998, "IEEE Recommended Practice for Software Requirements Specifications," with identified exceptions and clarifications. The applicant should examine the version of RG 1.172 that applies to its application to identify the applicable standards.

~~7.~~8. Digital I&C safety systems should conform to the guidance in the version of RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," in place 6 months before the docket date of the application. Currently, RG 1.173 endorses IEEE Std. 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process," with identified exceptions and clarifications. The applicant should examine the version of RG 1.173 that applies to its application to identify the applicable standards. [Note: RG 1.173 is currently focused on software development processes, whereas this section of the DSRS addresses the overall I&C system development, which includes hardware and software components.]

Technical Rationale

I&C systems may be safety-related or not safety-related. Safety-related I&C systems are subject to the requirements of 10 CFR Part 50, Appendix B. While the NRC review of the applicant's entire QA program is documented in Chapter 17 of this DSRS, NRC staff I&C reviewers will evaluate the aspects of the proposed QA measures to the extent that they apply to technical matters unique to I&C safety systems. Specifically, the I&C reviewer will verify that the technical aspects of the applicant's proposed I&C design life-cycle identified in this DSRS section are subject to the applicant's proposed QA program under Appendix B.

The reviewer will consider whether the technical matters described in this section are subject to the activities described in a QA program. In regard to design control under Appendix B, Criterion III, the life-cycle criteria described in this section provide guidance for activities associated with I&C system and software development. In addition, this guidance discusses quality standards for such activities that should be specified in design documents, and the design control measures for verifying or checking the adequacy of the design that are unique to

these I&C activities. ~~In regard to~~ Regarding Criterion V, the life-cycle criteria in this section provide guidance for I&C activities affecting quality that may warrant unique documented procedures and guidance on the control of I&C documents that prescribe activities affecting quality and may involve considerations unique to I&C. In regard to Criterion VII, the life-cycle criteria in this section provide guidance on the unique aspects of measures to assure that procured I&C equipment and services conform to procurement documents. In regard to Criterion XI, the life-cycle criteria in this section provide guidance on the aspects of the testing program unique to I&C. In addition to the foregoing, this section covers unique aspects of I&C project management and organizational processes; software quality assurance (SQA) processes; software verification and validation (V&V) processes; and software configuration management (CM) processes. Note that the Appendix B criteria identified above are not intended to form an exhaustive list.

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. 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.

III. REVIEW PROCEDURES

Appendix B to 10 CFR Part 50 establishes QA requirements for the design, manufacture, construction, and operation of safety-related structures, systems, and components. The guidance in this section provides detailed recommendations for complying with the requirements of 10 CFR 50.55a(a)(1), GDC 1, and Appendix B to 10 CFR Part 50 as they apply to I&C system engineering activities, including design, development, integration, operations, maintenance, and retirement.

The application should describe the methods and practices for the planning, design, development, integration, testing, operation, maintenance, and retirement of I&C safety systems, including those relating to hardware and software engineering. These activities should be coordinated with organizational and project management processes, which include configuration management, reviews/audits, verification and validation, quality assurance and safety plans (In this context quality assurance is limited to those activities associated with software development). Such coordination will assure adherence to appropriate standards and procedures. The reviewer will evaluate the adequacy of the methods and practices that will support the development of I&C safety systems, including hardware and software, using the criteria contained below. This guidance does not recommend new requirements for system, hardware, and software development; many of the attributes outlined in the guidance provided below may be addressed through the applicant's or developer's existing I&C safety system development processes, procedures, and programs.

I&C Safety System Development Processes

The reviewer will confirm that the application provides a discussion of the framework that will be used to design and develop I&C safety systems. This framework should supplement the applicant's overall QAPD with specific system, hardware, and software development activities, including a description of the proposed development life-cycles as well as

management activities that will be implemented in the design and development of I&C safety systems.

The activities during the system life-cycle phases are summarized as follows:

- Create the concepts on which the design of the system will be based.
- Translation of these concepts into system requirements.
- System requirements are allocated to system elements (e.g., software, hardware).
- The design is implemented into hardware and software functions.
- System elements such as software and hardware are integrated.
- Functions are tested to confirm that system requirements have been correctly implemented.
- System is installed and ready to operate.
- Provisions are established for system maintenance and retirement. Note that actual performance of system maintenance and retirement will be the responsibility of the licensee, and those activities may be subject to other NRC regulations.

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. In developing these systems, an applicant should follow a well-defined and documented system development approach that is consistent with the guidance in this section.

Using the acceptance criteria contained below, the reviewer will evaluate whether the proposed framework described in the application is adequate to deliver a high quality I&C safety system. While U.S. Nuclear Regulatory Commission (NRC) regulations set the minimum standards for I&C safety systems, additional detailed acceptance criteria are set forth in NRC regulatory guides and industry standards.

1. System and Software Development Activities

Criterion III of Appendix B requires, in part, that measures be established to assure that applicable regulatory requirements and the design basis for those structures, systems, and components to which Appendix B applies are correctly translated into specifications, drawings, procedures, and instructions. Additionally, Criterion III requires that measures must be established for the identification and control of design interfaces and for coordination among participating design organizations. To confirm that an applicant has described measures that satisfy the requirements of Criterion III of Appendix B, the reviewer will confirm that the application provides a description of input information, life-cycle activities, and output information necessary to develop I&C safety systems, in accordance with applicable regulatory requirements and the design bases, and consistent with industry standards and related guidance.

The development of I&C safety systems should progress according to a defined life-cycle. Without recommending a particular life-cycle model, the reviewer will confirm that the application contains a description of life-cycle activities and tasks, including inputs and outputs, that will be implemented in the development of I&C safety systems. Many different life-cycle models exist for system and software development. Generally, these models differ

in the timing of the various activities and tasks used to produce a high-quality product, but such activities and tasks must be done.

This guidance does not describe the activities listed below in sufficient detail for those activities to be employed in the development of any particular I&C system. The reviewer will confirm that the applicant has described a life-cycle model that includes processes appropriately tailored and relevant to its particular development project to implement the activities listed below. An applicant should select and document a system and software development life-cycle model that includes phase transition criteria for each life-cycle phase.

Although this review guidance does not specify the use of any particular life-cycle model, the reviewer will confirm that the description of system and software development of QA activities includes provisions to address, at a minimum, the following activities:

A. Plant Safety Analyses and I&C System and Software Safety Analyses

i. I&C system design should be bounded by the plant safety analyses and should be conducted during the I&C system requirements phase as required in Section 4 of IEEE Std. 603-1991. Refer to 7.1.1 of this DSRS for further evaluation.

ii. The I&C system, hardware, and software safety analysis should be conducted for each phase of the development life-cycle and should include the identification of hazards associated with the chosen I&C design concept or operation. Subsequent I&C system, hardware, and software safety analyses should identify when software is a potential cause of a hazard or when it is used to support the control of a hazard. Further guidance associated with hazard analyses (HA) is contained in Appendix A.

iii. As part of the software safety analyses, the application should define a software integrity level (SIL) scheme to quantify software criticality, as defined in the endorsed IEEE Std. 1012. A criticality analysis should be performed to determine the SIL level of the software necessary to accomplish each safety function. Functions of lower SIL levels that support a system safety function would have to be reclassified to the highest SIL level for that function. A review of the criticality analysis should be performed during subsequent life-cycle phases to ensure that the SIL classification is preserved or updated as needed.

B. I&C System Requirements

i. An I&C system requirements specification should be developed that describes the identification, development, documentation, review, approval, and maintenance of I&C system requirements.

ii. The I&C system requirements specification should include, at a minimum, the need for system and software safety analyses throughout the ~~life~~ life-cycle; functions and capabilities of the I&C system during operations; system boundaries; safety classification; safety functional properties and

additional features not performing a safety function; customer requested features; safety, security, and human-machine interfaces; operations and maintenance measures, including intended fault identification, test, calibration and repair; design constraints; qualification requirements; results from hazard analyses; and restrictions and constraints placed on the system to ensure compatibility with other plant systems.

iii. All identified system requirements should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management.

iv. ~~A requirements traceability matrix (RTM) should be developed, documented, tracked, and maintained.~~ The RTM should facilitate bi-directional traceability (from requirements to system validation testing) of all system requirements. ~~The RTM should also document and justify the origin and rationale of every system requirement.~~ Where appropriate, the RTM should identify references to analyses and/or supporting documentation that establish the bases for system requirements.

v. Inconsistencies between system requirements and other system-related elements such as hardware and software should be identified and evaluated.

vi. The completed I&C system requirements specification should be used as input to the ongoing I&C system safety analysis activity.

C. I&C System Architecture

i. An I&C system architecture should be developed based on a defined methodology that provides all necessary I&C functions needed to ensure safe plant operation. Additional guidance on I&C system architecture is provided in DSRS Section 7.1, Appendix B.

ii. The I&C system architecture should be documented, baselined, updated as necessary, and placed under configuration management.

iii. The completed I&C system architecture should be used as input to the ongoing I&C system safety analysis activity.

D. I&C System Design

i. A detailed design of the I&C system should be developed and recorded in an I&C system design description, based on the architectural design, and that conforms to the I&C system design basis.

ii. The I&C system design description should identify, at a minimum, system elements such as hardware and software , automatic and manual functions, interrelationship between components, , and interface design, and demonstrate traceability of the system requirements to the design.

iii. I&C system safety analyses should be reviewed to identify any software that has the potential to cause a hazard or is credited to support control of a hazard.

iv. The I&C system design description should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management.

v. Bi-directional traceability should be established between the I&C system design description, the I&C system architecture, and the I&C system requirements.

vi. The completed I&C system design description should be used as input to the ongoing I&C system safety analysis activity.

E. Software Requirements

i. A software requirements specification should be developed to document the basis for the design and implementation of software units of the I&C system, consistent with the guidance in RG 1.172. In this DSRS, a software unit is the highest element in the software hierarchy. Software units are comprised hierarchically of software components and software modules.

ii. The software requirements specification should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management. Software requirements should be baselined prior to initiating software design.

iii. The software requirements specification should be derived from and traceable to the system design, I&C system architecture, and system requirements. Where appropriate, the RTM should identify references to analyses and/or supporting documentation that establish the basis for software requirements.

iv. The completed software requirements specification should be used as input to the ongoing I&C system safety analysis activity.

F. Software Design

i. A software design description should be developed that documents the detailed design for each software element of the system and how the software units are to be constructed.

ii. The software design description should document, at a minimum, the methods by which software units will be refined into lower levels containing software modules to allow coding, compiling, and testing; and the division of the software into a set of interacting units, including the description of those units, their interfaces, and dependencies in a structured fashion.

iii. The design of a software module should be restricted to one clearly identified function that involves only minimum interaction with other functions thus minimizing the impact of changes. The interfaces between the various units should be simple, completely identified, and documented.

iv. The software design and implementation should incorporate applicable software requirements from the previous phase.

v. Each ~~software unit should identify measures for traceability to software modules and design features.~~Traceability between software unit(s) and software module(s) should be established.

vi. The software design should demonstrate adequate coverage of all software requirements and should not contain any unnecessary functions. For pre-developed digital platforms, pre-existing software (e.g., operating system software) may contain features that are not used (or not configured for use) in a specific I&C system. In those instances, the applicant should identify those unused capabilities, evaluate whether those functions may impact performance of the safety function, and identify any compensatory measures taken.

vii. The use of support software and tools (e.g., code generating tools, compilers, assemblers, operating systems, coverage analyzers) should be consistent with the guidance in IEEE Std. 7-4.3.2, as endorsed in RG 1.152.

viii. Code change requests and modifications should be controlled.

ix. The software design description should be analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management.

x. The completed software design description should be used as input to the ongoing I&C system safety analysis activity.

G. Software Implementation

i. A software implementation plan should be developed that documents the criteria for testing each software unit and the test procedures and data for testing each software unit. This should include the criteria for defining software units, software modules, or any other terminology describing software implementation activities.

ii. The software implementation plan should describe the translation of the detailed design into computer code in the selected programming language.

iii. The code should implement the safety design features and methods developed during the software design process.

iv. Analysis should be performed on the code to identify potential hazards in accordance with DSRS Chapter 7, Appendix A.

v. Strict coding rules, methods, standards, and/or criteria should be defined and enforced. For example, use of global variables and dynamic memory allocation should be discouraged.

vi. The code should be designed so as to facilitate analysis, testing and readability.

vii. The correct implementation of software requirements in each software unit should be verified to ensure accuracy and conformance with design requirements.

viii. Software unit testing should be performed as software is developed to ensure it satisfies design requirements, consistent with the guidance in RG 1.170. The primary testing methods and standards, test cases used, and test coverage should be documented.

ix. Test documentation should be consistent with the guidance in RG 1.171.

x. The software implementation plan should be derived from and traceable to the software design, I&C system architecture, and system requirements.

xi. The completed software implementation plan should be used as input to the ongoing I&C system safety analysis activity.

H. Software Integration

i. A software integration plan should be developed to describe the methods for integrating software modules and software components into a software unit. Aggregates of units tested during the unit test phase should be integrated into a software item in accordance with the integration plan.

ii. Critical elements of software integration should include, but are not limited to: identifying software modules and software components for integration; defining and implementing the integration environment; management of interfaces; and item integration sequences.

iii. As-coded software items should reflect the design documentation.

iv. Software qualification testing should be conducted to verify that software requirements have been adequately implemented for this phase of the software life-cycle.

v. The integration plan results should be documented, analyzed, reviewed, approved, updated as necessary, and placed under configuration management.

vi. Discrepancies between actual and expected results should be identified and resolved.

vii. The software integration plan should be derived from and traceable to the software design, I&C system architecture, and I&C system requirements.

viii. The completed software integration plan should be used as input to the ongoing I&C system safety analysis activity.

I. I&C System Testing

i. A system test plan should be developed that documents the integration and testing of all software items, hardware, manual processes, and other system interfaces that constitute the I&C system, consistent with the architectural design.

ii. System testing should consider all of the integrated software components that have successfully passed integration testing and also the software system itself integrated with any applicable hardware systems.

iii. System testing should be conducted on a complete, integrated system to evaluate the system's compliance with the I&C system requirements.

iv. The test plan should include tasks to integrate and test all software and hardware items, prepare the test environment, test cases (inputs, outputs, and test criteria), hardware, and other system interfaces that constitute the system.

v. System testing should detect any inconsistencies between the software units and the hardware.

vi. System test results should be documented. Test results should be analyzed to verify that all I&C system requirements have been satisfied.

vii. Testing should demonstrate that hazards have been eliminated or controlled to an acceptable level of risk. Additional hazardous states identified during testing should undergo analysis prior to software delivery or use.

viii. All test discrepancies should be evaluated and corrected. Provisions should be available for appropriate regression testing following changes made to address discrepancies.

ix. The completed system test results should be used as input to the ongoing I&C system safety analysis activity.

J. I&C System Installation

i. A system installation plan should be developed that documents the methods by which the I&C safety system will be installed and connected to other plant systems.

ii. The system installation plan should describe, at a minimum, procedures for software installation, -combined hardware/software installation, and systems installation; checks to ensure that the computer system is functional, that sensors and actuators are functional, that all cards are present and installed in the correct slots (when applicable), and that the communication system is correctly installed; and measures to confirm that the correct software versions (i.e., consistent with the versions used for final system testing) are installed on the correct I&C system.

iii. Acceptance testing should demonstrate that the installed system will perform its safety function described in the system design basis.

iv. Anomalies discovered during installation should be reported to the developer and resolved prior to placing the system into operation.

v. Software modifications during installation should be controlled.

vi. The completed system installation results should be documented and used as input to the ongoing I&C system safety analysis activity.

K. I&C System Operations [Note: Execution of the system operation plan activities will be the responsibility of the licensee.]

i. An operation~~s~~ plan should be developed that documents the deployment of the I&C safety system to its operational environment with appropriate documentation to support operations, including user manuals, configuration control documents, and other associated documentation.

ii. The operation~~s~~ plan should describe, at a minimum, a general description of the functions that the system is to perform and a general discussion of the means of carrying out those functions; the controls needed over operation activities to prevent unauthorized changes to hardware, software, and system parameters; the monitoring activities needed to detect unauthorized access to the system; and contingency plans needed to ensure appropriate response to control of access issues.

iii. The operation~~s~~ plan should describe the facilities used to operate the delivered software. It should list and describe the software, hardware and associated documentation used to operate the delivered software.

iv. The operation~~s~~ plan should include a description of procedures for executing the software in all operating modes, and procedures for ensuring that the software state is consistent with the plant operating mode at all times.

v. The operations plan should include a description of backup procedures for data and code, and the intervals at which backup should occur.

vi. The operations plan should provide controls for continuously monitoring I&C safety system performance to ensure that it is consistent with pre-established system performance measures.

vii. The operation plan should include a comprehensive list of error messages, a description of the error indication, the probable interpretation of the error indication, and steps to be taken to resolve the situation.

viii. An operations manual should be developed that provides plant personnel and operators with a detailed operational description of the I&C safety system and its associated environment.

ix. System documentation should be provided that contains the details of system design, programs, their coding, system flow, process description, and other pertinent system information.

L. I&C System Maintenance [Note: Execution of the system maintenance plan activities will be the responsibility of the licensee.]

i. A maintenance plan should document the methods for monitoring the system's performance, record problems for analysis, take corrective and preventive actions, and confirm restored capability after servicing.

ii. The maintenance plan should identify the controls needed over maintenance activities and maintenance and test equipment to prevent unauthorized changes to hardware, software and system parameters. At a minimum, the potential for introducing unauthorized changes during repair, testing and calibration should be addressed.~~Maintenance should be limited to the process of modifying a software design output to repair nonconforming items or to implement pre-planned actions necessary to maintain performance. Modifications to improve performance or other attributes or to adapt the design outputs to a modified environment should be considered design changes. When modifications or changes are identified as necessary, the system may reenter the planning phase.~~

~~Maintenance should be limited to the process of modifying a software design output to repair nonconforming items or to implement pre-planned actions necessary to maintain performance. Modifications to improve performance or other attributes or to adapt the design outputs to a modified environment should be considered design changes. When modifications or changes are identified as necessary, the system may reenter the planning phase.~~

iii. The maintenance plan should call for timely evaluation of the effects of reported problems to support equipment operability determinations as required by plant technical specifications.

iv. The maintenance plan should identify that cConfiguration management and control activities should be conducted to document any proposed or actual changes to the I&C safety system. [Note: Activities described in a maintenance plan should be limited to the process of modifying a software design output to repair nonconforming items or to implement pre-planned actions necessary to maintain performance. Modifications to improve performance or other attributes or to adapt the design outputs to a modified environment should be considered design changes. When modifications or changes are identified as necessary, the system may reenter the planning phase.]

M. I&C System Retirement [Note: System retirement and replacement activities will be the responsibility of the licensee; however, the vendor should consider the need for design provisions to support system retirement actions.]

i. Provisions should be in place for the removal of the I&C safety system from its active use either by ceasing its operation or support or by replacing it with a new system or an upgraded version of the existing system.

ii. Retirement activities should ensure the orderly termination of the system and preservation of vital information about the system so that some or all of the information may be reactivated in the future, if necessary.

iii. The information, hardware, and software may be moved to another system, archived, discarded, or destroyed. Retirement controls should include provisions for relating the actions taken and making the transition to a new system.

iv. Particular emphasis should be given to proper preservation of the data processed by the I&C safety system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

2. Project Management and Organizational Processes

The application should provide a description of the project management processes or organizational processes that will be employed by the QA program and used to define the project's organization, planning, execution, monitoring, control, and closure activities of the entire I&C safety system development effort.

The reviewer will confirm that the application provides a description of the organizational and project processes that includes provisions to address, at a minimum, the following:

A. Measures for the creation of plans to control the system development environment, including hardware and software in accordance with Criterion V of Appendix B. The result of the planning process should be a set of documents that will be used to control and oversee the development of system elements, including hardware and software.

B. Controls for the identification of the project scope, estimation of the work involved, determination of deliverables, lines of communication, formal and informal reviews, and interfaces with other internal and external organizations.
C. Provisions for the establishment, documentation, and maintenance of a schedule that considers the overall project as well as interactions of milestones.
D. Provisions for risk management, including problem identification, impact assessment, and development of risk mitigation plans for risks that have the potential to significantly impact system quality goals with appropriate metrics for tracking resolution progress. For software-related project risk activities, additional guidance can be found in Section 5.3.6 of IEEE Std. 7-4.3.2.
E. Establishment of quality metrics throughout the life-cycle to assess whether quality requirements of IEEE Std. 603-1991 are being met. Additional guidance can be found in Section 5.3 of IEEE Std. 7-4.3.2.
F. Adequate control of software tools to support system development and verification and validation (V&V) processes. Additional guidance can be found in Section 5.3.2 of IEEE Std. 7-4.3.2.
G. Provisions for the documentation and resolution of problems and non-conformances found in the system elements.
H. Provisions for effective oversight of all life-cycle related activities.

3. Software Quality Assurance (SQA) Processes

By definition, QA includes software QA. RG 1.152 indicates, in part, that conformance with the recommendations of IEEE Std. 7-4.3.2 is a method acceptable for satisfying high functional reliability and design requirements for computers used in the safety systems of nuclear power plants. IEEE Std. 7-4.3.2, Section 5.3.1, states, in part, that computer software shall be developed, modified, or accepted in accordance with an approved software QA plan.

The application should describe measures to satisfy the applicable requirements of Appendix B to 10 CFR Part 50 with respect to software QA. In particular, the application should describe how the software QA plan will be implemented throughout the software development ~~life~~ life~~-~~cycle. This review will be coordinated with Section 17.5. ~~IEEE Std. 7-4.3.2, SectionClause 5.3.1, states, in part, guidance for developing software QA plans can be found in IEEE Std. 730-1998. RG 1.152 will be used to review processes and activities associated with software QA.~~

4. Software Verification and Validation Processes

RG 1.152 endorses IEEE Std. 7-4.3.2, subject to the positions and modifications identified in the regulatory guide. IEEE Std. 7-4.3.2, Sections 5.3.3 and 5.3.4 contains guidance on V&V activities and independent V&V, respectively.

RG 1.168 endorses IEEE Std. 1012, ~~"IEEE Standard for Software Verification and Validation,"~~ and IEEE Std. 1028, ~~"IEEE Standard for Software Reviews and Audits,"~~ with the exceptions stated in the regulatory positions. IEEE Std. 1012 describes a method acceptable to the NRC staff for complying with the NRC's regulations for promoting high functional reliability and design quality in software used in safety systems. In particular, the method, if correctly applied, will ensure compliance with GDC 1 in Appendix A to 10 CFR Part 50 and the criteria for quality assurance programs in Appendix B, as they

apply to software verification and validation. IEEE Std. 1028 provides guidance acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. RGs 1.152 and 1.168 will be used to review processes and activities associated with software V&V and software reviews.

5. Software Configuration Management (CM) Processes

~~RG 1.152 endorses IEEE Std. 7-4.3.2, subject to the positions and modifications identified in the regulatory guide. IEEE Std. 7-4.3.2,~~ Section 5.3.5, contains guidance on software configuration management. RG 1.169 endorses IEEE Std. 828~~, "IEEE Standard for Software Configuration Management Plans,"~~ subject to the positions and modifications identified in the regulatory guide. IEEE Std. 828 describes methods acceptable to the NRC staff for use in complying with the NRC's regulations for quality standards that promote high functional reliability and design quality in software used in safety systems. In particular, the methods, if correctly applied, will ensure compliance with GDC 1 in Appendix A to 10 CFR Part 50 and the criteria for quality assurance programs in Appendix B to 10 CFR Part 50 as they apply to the maintenance and control of appropriate records of software development activities. RGs 1.152 and 1.169 will be used to review processes and activities associated with software CM processes.

6. Process Improvement Approaches and Assessments

The reviewer will confirm that the proposed development processes for systems and software (when applicable) conform to the guidance and references provided in this subsection. Nevertheless, the NRC recognizes that an applicant (or contractor) may develop and implement processes for the development of hardware or software using the Capability Maturity Model Integration (CMMI) framework.

CMMI is a process improvement approach that can be used to guide process improvement across a project, a division, or an entire organization. CMMI best practices are published in documents called models, each of which addresses a different area of interest. CMMI for Development (CMMI-DEV) is a model that addresses product and service development processes. This model covers the life-cycle of a product from conception through delivery to maintenance, addressing areas like project management, engineering, and supporting functions such as quality assurance. The reviewer should be aware that these process improvement practices could supplement existing guidance related to system and software development.

Further, the Standard CMMI Appraisal Method for Process Improvement (SCAMPI) provides for the examination of one or more processes by a trained team of professionals using an appraisal reference model as the basis for determining strengths and weaknesses of an organization. If an application proposes to use SCAMPI, the reviewer should evaluate how the applicant leverages SCAMPI assessments used to provide benchmark-quality ratings relative to CMMI models as a way to supplement contractor oversight and confirm effective adequate process implementation. Further, the NRC may opt to review SCAMPI assessments to support verification activities as part of inspections, tests, analyses, and acceptance criteria (ITAAC) for system and software development processes.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, and if the review performed in accordance with DSRS Chapter 17 confirms that the application conforms to the guidance identified in those sections, the reviewer can conclude that the design of I&C systems satisfies the guidance contained in RG 1.28, RG 1.152, RG 1.168, RG 1.169, RG 1.170, RG 1.171, RG 1.172, and RG 1.173. On this basis, the staff can conclude that the application provides information sufficient to demonstrate that the QA measures applied to the proposed I&C system and software life-cycle satisfy the applicable quality assurance requirements of GDC 1, 10 CFR 50.55a(a)(1), 10 CFR Part 50 Appendix B, and Section 5.3 of IEEE Std. 603-1991.

V. IMPLEMENTATION

The staff will use this DSRS section in performing safety evaluations of B&W mPower specific design certification (DC), combined license (COL), or early site permit (ESP) applications submitted by applicants pursuant to 10 CFR Part 52. The staff will use the method described herein to evaluate conformance with Commission regulations.

Because of the numerous design differences between the B&W mPower and large light-water nuclear reactor power plants, and in accordance with the direction given by the Commission in SRM–COMGBJ-10-0004/COMGEA-10-0001, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews," dated August 31, 2010 (ML102510405), to develop risk-informed licensing review plans for each of the small modular reactor (SMR) reviews including the associated pre-application activities, the staff has developed the content of this DSRS section as an alternative method for the evaluation of a B&W mPower-specific DC, COL, or ESP application submitted pursuant to 10 CFR Part 52.

NRC regulations state, in part, that the DC, COL, or ESP application must contain an evaluation (of the design, facility, or site, respectively) against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application. The content of this DSRS section has been accepted as an alternative method for complying with those regulations (10 CFR 52.47(a)(9), 10 CFR 52.79(a)(41), or 10 CFR 52.17(a)(1)(xii), as applicable) as long as the B&W mPower DCD FSAR does not deviate significantly from the design/facility/site assumptions made by the NRC staff while preparing this DSRS section.

For a DC application, the application must identify and describe all differences between the standard plant design and this DSRS section, and discuss how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria. If the design assumptions in the DC application deviate significantly from the DSRS, the staff will use the SRP as specified in 10 CFR 52.47(a)(9).

Alternatively, the staff may supplement the DSRS section be adding appropriate criteria in order to address new design assumptions. The same approach may be used to meet the requirements of 10 CFR 52.79(a)(41) for COL applications or 10 CFR 52.17(a)(1)(xii) for ESP applications.

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this Chapter.

7.2.2 EQUIPMENT QUALIFICATION

I. AREAS OF REVIEW

The application should provide information to confirm that I&C safety system equipment is designed to meet the functional performance requirements credited in the safety analysis over the range of environmental conditions postulated for the area in which it is located. This I&C safety system equipment is designed in accordance with GDC 2 and GDC 4. The equipment qualification program includes: 1) seismic qualification in accordance with Criterion III of 10 CFR Part 50, Appendix B, 2) qualification of equipment such as sensors, cables, and certain post-accident monitoring (PAM) equipment located in harsh environments in accordance with 10 CFR 50.49, and 3) qualification of digital I&C equipment located in mild environments under IEEE Std. 603-1991.

The I&C review of equipment qualification is limited to confirmation that: 1) I&C equipment (including isolation devices) located in areas subject to seismic and environmental qualification requirements has been identified and design criteria established (i.e., seismic, environmental) in the application, 2) computer-based I&C system equipment qualification criteria contained in Section 5.4 of IEEE Std. 603-1991 and Section~~Clause~~ 5.4 of IEEE 7-4.3.2, as endorsed by RG 1.152, have been considered as part of the process for the qualification of digital computers, and 3) the I&C system design includes the design and installation of safety-related instrument sensing lines and lightning protection systems. Note that the evaluation of the seismic and environmental qualification programs is part of DSRS Chapter 3, “Design of Structures, Components, Equipment, and Systems,” and is not included in this Chapter.

Review Interfaces

The organization responsible for the review of seismic qualification verifies the methods of test and analysis employed to ensure the functionality of mechanical and electrical equipment (including I&C) under the full range of normal and accident loadings. In addition, the organization responsible for the review of environmental qualification of I&C systems reviews mild and harsh environment qualification. Guidance for the review of seismic and environmental qualification is provided in DSRS Sections 3.10 and 3.11.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR Part 50, Appendix~~.~~ B, Criterion III, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.”

2. 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants."

3. GDC 2, "Design Bases for Protection against Natural Phenomena," requires that components important to safety be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches, without loss of capability to perform their safety function.

4. GDC 4, "Environmental and Dynamic Effects Design Bases," requires that structures, systems, and components important to safety be designed to accommodate the effects of, and be compatible with, the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss of coolant accidents (LOCAs).

5. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.4, “Equipment Qualification,” which requires that safety equipment be qualified by type test, previous operating experience, or analysis, or any combination of these three methods.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for equipment qualification are as follows:

1. Digital I&C safety systems should conform to the guidance in Section~~Clause~~ 5.4 of IEEE Std. 7--4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” as endorsed (with identified exceptions and clarifications) by the version of RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” in place 6 months before the docket date of the application. The applicant should examine the version of RG 1.152 that applies to its application to identify the applicable standards.

2. The safety systems should conform to the environmental qualification guidance contained in the version of RG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants,” in place 6 months before the docket date of the application. Currently, RG 1.209 endorses IEEE Std. 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” with identified exceptions and clarifications. The applicant should examine the version of RG 1.209 that applies to its application to identify the applicable standards.

3. The safety systems should conform to the guidance in the version of RG 1.151, “Instrument Sensing Lines,” in place 6 months before the docket date of the application. Currently, RG 1.151 endorses ANSI/ISA-67.02.01-1999, “Nuclear Safety-Related Instrument-Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants,” with identified exceptions and clarifications. The applicant should examine the version of RG 1.151 that applies to its application to identify the applicable standards.

4. The safety systems should conform to the guidance in the version of RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” in place 6 months before the docket date of the application. The applicant should examine the version of RG 1.180 that applies to its application to identify the applicable standards.

5. The safety systems should conform to the guidance in the version of RG 1.204, “Guidelines for Lightning Protection of Nuclear Power Plants,” in place 6 months before the docket date of the application. The applicant should examine the version of RG 1.204 that applies to its application to identify the applicable standards.

Technical Rationale

The staff determined in RG 1.209 that the practices in IEEE Std. 323 are sufficiently comprehensive to address qualification for the less severe environmental conditions of typical plant locations where safety-related computer-based I&C systems are generally located.

III. REVIEW PROCEDURES

1. Equipment ~~qualification~~Qualification

The I&C technical review will be coordinated with the review of Sections 3.10 and 3.11 of the application. These sections provide a description of the seismic and environmental qualification programs as well as a list of equipment that will be subject to qualification. In addition to the guidance applicable to environmental qualification programs, the review of the environmental qualification program for I&C equipment should be performed in accordance with the guidance provided in RG 1.209. Note that the evaluation of the equipment qualification programs (both seismic and environmental) is part of Chapter 3 of the DSRS and is not documented in this Chapter.

The application should confirm that I&C safety system equipment is designed to meet the functional and performance requirements over the range of normal environmental conditions for the area in which it is located, as identified by Sections 4.7 and 4.8 of IEEE Std. 603-1991. The I&C reviewer will confirm that the I&C equipment (including isolation devices) subject to seismic and environmental qualification requirements have been identified and design criteria established in the application. The I&C reviewer will also confirm that the computer-based I&C system equipment qualification testing criteria contained in Section 5.4 of IEEE Std. 7-4.3.2 has been considered as part of the environmental qualification of digital computers.

2. Instrument Sensing Lines

The reviewer will confirm that instrument sensing lines are designed to conform to the guidance in ANSI/ISA-67.02.01, as endorsed by the version of RG 1.151 in place 6 months before the docket date of the application. This standard establishes acceptance criteria for the design and installation of safety-related instrument sensing lines that provide connections to the reactor coolant system for measuring process variables (e.g., pressure, level, and flow). The guidance provided in ANSI/ISA-67.02.01, as endorsed by RG 1.151, will be used to review instrument sensing lines.

3. Environmental ~~control~~ Control ~~systems~~Systems

If environmental controls systems are used, the application should provide information to confirm that a single failure within the environmental control system will not result in conditions that could result in damage to the safety system equipment or prevent the balance of the safety system not within the area from accomplishing its safety function. In this regard, the loss of an environmental control system in any area in which safety equipment is located is treated as a single failure that should not prevent the safety system from accomplishing its safety functions.

The design bases of environmental control systems may rely upon monitoring environmental conditions and take credit for appropriate action to ensure that environmental conditions are maintained within pre-determined limits within which system or component damage will not occur during the period until the environmental control systems are returned to normal operation. If such bases are used, the application should provide information to confirm that the environmental control systems are independent from the sensing systems credited to indicate the failure or malfunctioning of environmental control systems.

4. Electromagnetic and Radio-Frequency Interference (EMI/RFI)

The I&C reviewer will confirm that EMI qualification is performed in accordance with the guidance contained in RG 1.180~~, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,"~~ which provides an acceptable means of meeting the qualification guidelines for EMI and electrostatic discharge. In addition, lightning protection should be addressed as part of the review of electromagnetic compatibility. The I&C reviewer will confirm that lightning protection features conform to the guidance contained in RG 1.204~~, "Guidelines for Lightning Protection of Nuclear Power Plants."~~.

IV. EVALUATION FINDINGS

If the reviewer confirms the matters described above, and if the review performed in accordance with DSRS Sections 3.10 and 3.11 confirms that the application conforms to the guidance identified in those sections, the staff can conclude that the application provides information sufficient to: (1) identify I&C equipment (including isolation devices) subject to seismic and environmental qualification requirements, (2) demonstrate the seismic and environmental qualification of I&C equipment, (3) demonstrate that specific qualification testing criteria for computer systems recommended by the NRC has been considered as part of environmental qualification, and (4) demonstrate the adequacy of the design of safety-related instrument sensing lines and environmental control systems. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the equipment qualification guidance contained in Section~~Clause~~ 5.4 of IEEE Std. 7-4.3.2, the guidance contained in RG 1.151, RG 1.180, RG 1.204, and RG 1.209, and therefore meets the requirements of 10 CFR Part 50, Appendix~~.~~ B, Criterion III, 10 CFR 50.49, GDCs 2, 4, and Section 5.4 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection "V. Implementation."

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this Chapter.

7.2.3 RELIABILITY, INTEGRITY, AND COMPLETION OF PROTECTIVE ACTION

I. AREAS OF REVIEW

Under this DSRS section, the NRC staff reviews the reliability and integrity of I&C components and systems, and their ability to complete protective action once initiated to confirm that I&C components and systems are sufficiently reliable to accomplish their safety functions.

The NRC staff considers an I&C component or system adequately reliable if there is a high probability that a component or system will be available when needed and remain capable of performing the functions it was designed to achieve. The staff considers an I&C component or system to have adequate integrity if it has the capability to perform all of its intended functions with the accuracy and resulting outputs credited in the safety analyses. The staff considers a safety system to have completed protective action if, upon manual or automatic initiation, the system performs the entire sequence of protective actions or all execute features provided in the design that are necessary to achieve the result credited in the safety analyses.

Review Interfaces

The fundamental design principles described in Section 7.1 as well as the Appendices to Chapter 7 of the DSRS inform the review of reliability and integrity of I&C systems.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.15, “Reliability,” Section 5.5, “System Integrity,” and Sections 5.2 and 7.3, “Completion of Protective Action.” Section 5.15 of IEEE 603-1991 requires that, for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. Section 5.5 states that safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Sections 5.2 and 7.3 require that safety systems and execute features be designed such that, once initiated, the intended sequence of protective actions shall continue to completion.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for reliability, integrity, and completion of protective action are as follows:

1. Digital I&C safety systems should conform to the reliability, integrity, and completion of protective action guidance contained in Section~~Clause~~s ~~5.2,~~ 5.5, and 5.15 of IEEE Std. 7-4.3.2, as endorsed by the version of RG 1.152 in place 6 months before the docket date of the application. The applicant should examine the version of RG 1.152 that applies to its application to identify the applicable standards.

III. REVIEW PROCEDURES

Reliability Characteristics

To determine whether the I&C system satisfies the reliability requirements contained in Section 5.15 of IEEE Std. 603-1991 and the guidance contained in Section~~Clause~~ 5.15 of IEEE Std. 7-4.3.2 (for digital-based I&C safety systems), the review should include the following:

1. The application should demonstrate that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. These characteristics ensure that the I&C systems are capable of functioning over all plant conditions including normal operation, anticipated operational occurrences (AOOs), and accident conditions. Additional information to support I&C system reliability is addressed in Section 7.1 of the application.

2. The reviewer should verify that the quantitative and qualitative reliability goals for I&C systems are defined in the application. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the safety system. However, the concept of quantitative reliability goals is not endorsed as the sole means of meeting the NRC's regulations for reliability of digital computers in safety systems.

   A. For those systems for which either quantitative or qualitative reliability goals have been established, the reviewer should review the application's reliability analysis as well as I&C design documentation to confirm that the quantitative or qualitative reliability goals have been achieved.

3. The reviewer should confirm that, when reliability goals are identified, the proof of meeting such goals should include the software and firmware. The application should describe how the reliability criteria in Section~~Clause~~ 5.15 of IEEE Std. 7-4.3.2 are satisfied. In addition, the reviewer's assessment of reliability should consider the effect of possible hardware failures and software ~~failures~~ errors and the design features provided to prevent or limit the effects of these failures and to ensure the I&C system's capability to perform its safety functions. Additional criteria for failure analysis are contained in the ~~Hazard Analysis (~~HA~~)~~ provided in the application.

System Integrity Characteristics

To determine whether the I&C system satisfies the integrity requirements in Section 5.5 of IEEE Std. 603-1991 and the guidance contained in Section~~Clause~~ 5.5 of IEEE Std. 7-4.3.2 (for computer-based I&C safety systems), the reviewer should consider the HA information contained in the application. In addition, the reviewer's assessment of system integrity should consider the following:

1. The reviewer should confirm that the safety system components are conservatively designed to operate over the range of service conditions established in the I&C system's design bases.

2. Computer system software integrity (including the effects of hardware-software interaction) should be demonstrated by the application's software safety analysis activities over the range of service conditions established in the I&C system's design bases. This analysis is part of the design of I&C safety software.

3. The design for computer integrity, test and calibration, fault detection, and self-diagnostics must be consistent with the guidance in SectionClause 5.5 of IEEE Std. 7-4.3.2.

4. The reviewer should confirm that, for digital computer-based I&C systems, the system's real-time performance is adequate to ensure completion of protective actions within the critical points in time identified in Section 4.10 of IEEE Std. 603-1991. Subsection 7.1.4, "Predictability and Repeatability," provides guidance for reviewing the system's real-time performance.

5. The reviewer should confirm that the design incorporates protective measures that provide for the I&C safety systems to fail in a safe state, or into a state that has been demonstrated to be acceptable on some other defined basis, if conditions such as disconnection of the system, loss of power, or adverse environments, are experienced. Additional information to address I&C system failure modes is contained in the HA provided in the application.

6. Computer-based safety systems should, upon detection of inoperable input instruments, include provisions to automatically place the protective functions associated with the failed instrument(s) into a safe state (e.g., automatically place the affected channel(s) in trip). In such situations, manual operator control of the protective functions may also be considered to place the affected channel(s) in a safe state.

Completion of Protective Action

To determine whether the I&C system satisfies the completion of protective action requirements contained in Sections 5.2 and 7.3 of IEEE Std. 603-1991, the review should include the following:

1. The reviewer should consider information from the functional and logic diagrams to verify whether "seal-in" features are provided in the design to enable system-level protective actions to go to completion (a seal-in feature maintains current flow after a contact has been established and released). If seal-in features are incorporated in the I&C system design, the reviewer should verify the following:

   A. Seal-in features may incorporate a time delay as appropriate for the safety function.

   B. Seal-in features need not function until it is confirmed that a valid protective command has been received, provided the system responds within the time credited in the safety analysis.

2. The reviewer should confirm that deliberate operator action is needed to return the safety systems to normal operation. This IEEE Std. 603-1991 requirement does not preclude the use of any documented equipment protective provisions as required by Section 4.11 of IEEE Std. 603-1991 (Refer to DSRS Section 7.1.1, Item 11 under

"Additional Considerations in the Review of Design Basis Information") or the provision for deliberate operator interventions. Additionally, the reviewer will verify that, when sense and command features reset, the execute features do not automatically return to normal, but that the only way to return these features to their normal states is for the operator to take separate, deliberate action. After the initial protective action has gone to completion, the execute features may be actuated by manual or automatic control (i.e., cycling) of specific equipment to maintain completion of the safety function.

3. The anticipated transient without scram (ATWS) mitigation logic and diverse actuation system should be designed such that, once initiated, the mitigation function will go to completion.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to: (1) demonstrate that I&C components and systems will be reliable and available when needed and remain capable of performing the functions they are designed to achieve, (2) demonstrate that I&C components and systems will have adequate integrity to perform all of their intended functions with the accuracy and resulting outputs credited in the safety analyses, and (3) I&C safety systems will perform the entire sequence of protective actions or all execute features that are necessary to achieve the results credited in the safety analyses. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the reliability, system integrity, and completion of protective action guidance contained in Section~~Clause~~s 5.15, 5.5, and 5.2 of IEEE Std. 7-4.3.2, and the requirements of Sections 5.15, 5.5, 5.2 and 7.3 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection "V. Implementation."

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this Chapter.

7.2.4 OPERATING AND MAINTENANCE BYPASSES

I. AREAS OF REVIEW

The review will evaluate the I&C system's proposed operating bypasses that should be designed to automatically prevent the activation of an operating bypass or, under specified conditions, initiate the appropriate safety function(s) whenever the applicable permissive conditions are not met. In addition, the review will evaluate the I&C system's proposed maintenance bypasses that provide for the capability of a safety system to accomplish its safety function while sense and command and execute features equipment is in maintenance bypass. A bypass is a device that deliberately but temporarily inhibits the functioning of a circuit or system. A maintenance bypass is a bypass of safety system equipment during maintenance, testing or repair. An operational bypass is the bypass of certain protective actions when they are not necessary in a particular mode of plant operation. A permissive is a set of conditions that must be satisfied before a decision is made or an action is taken.

Review Interfaces

The review of operating and maintenance bypasses should be coordinated with the organization responsible for reviewing technical specifications in Chapter 16 of the application to confirm that the provisions for these bypasses are consistent with the required actions of the proposed plant technical specifications.

II. ACCEPTANCE CRITERIA

Requirements

10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Sections 6.6 and 7.4, "Operating Bypasses," and Sections 6.7 and 7.5, "Maintenance Bypass." Sections 6.6 and 6.7 provide requirements for operating and maintenance bypasses applicable to sense and command features. Sections 7.4 and 7.5 provide requirements for operating and maintenance bypasses applicable to execute features.

- 10 CFR 50.34(f)(2)(v), "Additional TMI-Related Requirements," requires automatic indication of the bypassed and operable status of safety systems.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for operating and maintenance bypasses are as follows:

1. The components and system should conform to the version of RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," in place 6 months before the docket date of the application.

III. REVIEW PROCEDURES

Operating Bypasses

The review should focus on evaluating how the I&C system design includes provisions to address operating bypasses. The reviewer should evaluate the following:

1. If the applicable permissive conditions are not met, a safety system must automatically prevent the activation of an operating bypass or initiate the appropriate safety function. Further, if plant conditions change such that an active operating bypass is no longer permissible, the safety system must either remove the appropriate active operating bypass, restore plant conditions to the permissive conditions, or initiate the appropriate safety functions as required in IEEE Std. 603-1991, Sections 6.6 and 7.4. The requirement for automatic removal of active bypasses means that the reactor operator may not have a role in such removal; however, the operator may take action to prevent the unnecessary initiation of a protective action.

2. Automatic indication for bypassed status should be provided in the control room. Features for bypassed and inoperable status indication should conform to the guidance in RG 1.47. Additional guidance can be found in Section 7.2.13 of this DSRS.

Maintenance Bypass

The review should focus on evaluating how the I&C system design includes provisions to address maintenance bypasses. The reviewer should evaluate the following:

1. While sense and command features equipment is in maintenance bypass, the capability of a safety system to accomplish its safety function must be retained and, during such operation, the sense and command features must continue to meet the requirements of IEEE Std. 603-1991, Sections 6.7. Additionally, provisions for a maintenance bypass should be consistent with the technical specification action statements to meet the requirements of IEEE Std. 603-1991, Sections 7.5.~~While sense and command features equipment is in maintenance bypass, the capability of a safety system to accomplish its safety function must be retained and, during such operation, the sense and command features must continue to meet the requirements of IEEE Std. 603-1991, Sections 6.7 and 7.5. Additionally, provisions for a maintenance bypass should be consistent with the technical specification action statements.~~

2. When a portion of the system is placed in maintenance bypass, the remaining portions of the system should be of acceptable reliability.

3. Automatic indication for bypassed status should be provided in the control room. Features for bypassed and inoperable status indication should conform to the guidance in RG 1.47. Additional guidance can be found in Section 7.2.13 of this DSRS.

Technical Specifications

The organization responsible for reviewing technical specifications (TS) in Chapter 16 of the application will review the adequacy ~~if~~ of the format and standard content of the TS. The Chapter 7 reviewer will coordinate with the Chapter 16 organization and confirm that the

provisions for operating and maintenance bypasses are consistent with the required actions of the proposed plant TS.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to: 1) demonstrate that the design of operating and maintenance bypasses ensure the initiation of the appropriate safety function(s) under the conditions described above, 2) demonstrate that the proposed operating and maintenance bypasses are consistent with the required actions of the proposed plant TS, and 3) demonstrate that adequate indication for bypassed status is provided in the control room. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the bypassed and inoperable status indication guidance contained in RG 1.47 and the requirements of Sections 6.6, 6.7, 7.4, and 7.5 of IEEE Std. 603-1991, and 10 CFR 50.34(f)(2)(v).

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection “V. Implementation.”

VI. REFERENCES

All of the references in this DSRS Chapter 7, “Instrumentation and Controls,” may be found in Appendix D of this Chapter.

7.2.5 INTERLOCKS

I. AREAS OF REVIEW

The reviewer will evaluate the acceptability of interlocks that: (1) operate to reduce the probability of occurrence of specific events, (2) maintain variables within the ranges of values specified in the safety analyses, (3) assure proper system alignment during plant operation, or 4) maintain safety systems in a state that assures their availability in an accident. The scope of this review includes mechanical as well as computer-based interlocks.

Review Interfaces

The review of interlocks should be coordinated with the review of Chapter 15 of the application to ensure the design of interlocks is compatible with the functions and performance assumed in the Chapter 15 of the application. Additionally, the reviewer should coordinate with organization responsible for the review of reactor systems and plant systems to confirm the adequacy of all proposed controls and instrumentation associated with mechanical interlocks.

II. ACCEPTANCE CRITERIA

Requirements

1. Interlocks must satisfy the requirements of 10 CFR 50.55a(h), which requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3).

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for interlocks are as follows:

1. For computer-based interlocks, the components and system should conform to the guidance for digital computers in IEEE Std. 7-4.3.2, as endorsed (with identified exceptions and clarifications) by the version of RG 1.152 in place 6 months before the docket date of the application. The applicant should examine the version of RG 1.152 that applies to its application to identify the applicable standards.

III. REVIEW PROCEDURES

I&C Interlocks

The reviewer should evaluate all proposed I&C interlocks to ensure that the applicable requirements of IEEE Std. 603-1991 are met. These requirements include redundancy, independence, satisfaction of the ~~single~~ single-failure criterion, qualification, bypasses, status indication, and testing. For computer-based interlocks, the design should address the guidance provided by IEEE Std. 7-4.3.2 as endorsed by the version of RG 1.152 in place 6 months before the docket date of the application. Several of the design considerations associated with interlocks, including computer-based interlocks, are addressed in Section 7.1 of the DSRS, which provides functional and design criteria for I&C safety systems. The review of interlocks will be performed in accordance with DSRS Section 7.1. Additional design considerations applicable to interlocks that should be addressed in the application are discussed below.

Although the primary I&C review emphasis is on equipment comprising the interlocks, the reviewer should consider the interlock functions at the system level. In addition to evaluating interlocks against the criteria of IEEE Std. 603-1991, the reviewer should coordinate the review of interlocks that are credited in the design bases accident analyses with the review of Chapter 15.

Mechanical Interlocks

The I&C reviewer will coordinate the review of mechanical interlocks with the organization responsible for the review of reactor systems and plant systems. The I&C reviewer will confirm the adequacy of all proposed controls and instrumentation associated with mechanical interlocks. The following are examples of mechanical interlocks that could be described in the application and that should be reviewed:

1. Interlocks to prevent over-pressurization of low-pressure systems.

   The following measures should be incorporated in designs of the interfaces between low-pressure systems and the high-pressure reactor coolant system:

   A. At least two valves in series should be provided to isolate any subsystem whenever the primary system pressure is above the pressure rating of the subsystem.

   B. For system interfaces where both valves are motor-operated, the valves should have independent and diverse interlocks to prevent both from opening unless the primary system pressure is below the subsystem design pressure. Also, the valve operators should receive a signal to close automatically whenever the primary system pressure exceeds the subsystem design pressure.

   C. For those system interfaces where one check valve and one motor-operated valve are provided, the motor-operated valve should be interlocked to prevent the valve from opening whenever the primary pressure is above the subsystem design pressure, and to close automatically whenever the primary system pressure exceeds the subsystem design pressure.

   D. Suitable valve position indication should be provided in the control room for the interface valves.

2. Interlocks to prevent over-pressurization of the primary coolant system during low-temperature operations of the reactor vessel.

   If pressure relief is through a low-pressure system not normally connected to the primary system, interlocks that would isolate the low-pressure system from the primary coolant system should not defeat the overpressure protection function.

3. Interlocks for Emergency Core Cooling System ~~(ECCS)~~ accumulator valves.

   The following features should be incorporated into the design of motor-operated isolation valve ~~(MOIV)~~ systems for safety injection tanks:

A means for automatic opening of the valves should be provided when either primary coolant system pressure exceeds a preselected value (to be specified in the technical specifications), or a safety injection signal (i.e., mPower's emergency core cooling actuation signal) is present. Both primary coolant system pressure and safety injection signals should be provided to the valve operator.

4. Interlocks to isolate safety systems from nonsafety systems.

   If cross-connections exist between a safety loop and a non-safety loop, such as within each subsystem of the component cooling water system, an interlock should be provided to automatically isolate the safety loop from non-safety loop upon the safety system's receipt of an actuation signal credited in the safety analysis.

5. Interlocks to preclude inadvertent inter-ties between redundant or diverse safety systems.

   If inter-ties exist for testing and maintenance purposes between redundant or diverse safety systems, interlocks should be provided to preclude such inter-ties except when the systems are being tested or maintained.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the design incorporates interlocks that: (1) operate to reduce the probability of occurrence of specific events, (2) maintain variables within the ranges of values specified in the safety analyses, (3) assure proper system alignment during plant operation, or (4) maintain safety systems in a state that assures their availability in an accident. On such a basis, the reviewer can conclude that the design of interlocks satisfy the applicable guidance contained in IEEE Std. 7-4.3.2 and the applicable requirements contained in IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection "V. Implementation".

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this Chapter.

7.2.6 DERIVATION OF SYSTEM INPUTS

I. AREAS OF REVIEW

In performing its review, the staff will evaluate the methods described in the application used for the derivation of system inputs to ensure, to the extent feasible and practical, that sense and command feature inputs are derived from signals that are direct measures of the variables specified in the design basis.

Review Interfaces

The review of system inputs should be coordinated with the review of Chapter 15 of the application to ensure that system inputs are direct measures of specified process variables in the design basis, to the extent feasible and practical.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 6.4, “Derivation of System Inputs.” This requirement states that, to the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.

DSRS Acceptance Criteria

There are no specific DSRS acceptance criteria in this section. However, the guidance provided below should be used to review the acceptability of information associated with derivation of system inputs.

III. REVIEW PROCEDURES

1. To determine whether the I&C system satisfies the functional and design criteria contained in Section 6.4 of IEEE Std. 603-1991, the reviewer should focus on examining documentation such as I&C system design basis, I&C architecture, or logic diagrams that show sense and command feature inputs and measured variables for applicable systems. These design considerations are addressed in Section 7.1 of the DSRS, which provides functional and design criteria for I&C safety systems.

2. A safety system that requires protection from loss of flow would, for example, normally derive its signal from flow sensors. The measured variables should be reviewed to confirm that system inputs are, to the extent feasible and practical, derived from signals that are direct measures of the desired variables that reflect the physical processes of interest, as specified by the design bases.

3. A design might use an indirect parameter such as a core exit thermocouples as a surrogate for fuel centerline temperature or pump speed as a surrogate for system flow rate. The reviewer should confirm that if indirect parameters are used, the indirect parameter is a valid representation of the corresponding direct parameter for all events.

In addition, the reviewer should confirm that, for both direct and indirect parameters, the characteristics of the instruments that produce the safety system inputs, such as range, accuracy, resolution, response time, and sample rate, correctly reflect the applicable analyses provided in Chapter 15 of the application.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that sense and command feature inputs are derived from signals that are, to the extent feasible and practical, direct measures of the variables specified in the design basis. On such a basis, the reviewer can conclude that the design of I&C systems satisfy the requirements related to derivation of system inputs contained in Section 6.4 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection "V. Implementation."

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this Chapter.

7.2.7 SETPOINTS

I. AREAS OF REVIEW

Setpoint values are assigned to the I&C devices that perform automatic protective actions, or alarm abnormal plant conditions. The setpoints of concern in this review include 1) setpoints specified for process variables on which safety limits (SLs) have been placed, and 2) setpoints related to process variables associated with safety functions but that do not protect any SLs.

Establishing setpoints involves determination of the proper allowance for uncertainties between the device setpoint and the process analytical limit (AL) or documented nominal process limit. The calculation of device uncertainties is documented and the device setpoint determined using a documented methodology. The setpoint analysis set forth in the setpoint methodology confirms that an adequate margin exists between setpoints and SLs or normal process limits (for variables with no related SL). Furthermore, the analysis should confirm that an adequate margin exists between operating limits and setpoints to avoid inadvertent actuation of the system.

A setpoint methodology developed in accordance with the version of RG 1.105, "Setpoints for Safety-Related Instrumentation," describes a method acceptable to the NRC staff for complying with the NRC's regulations for ensuring that setpoints for safety-related instrumentation are initially within and remain within the TS limits.

Review Interfaces

The reviewer should coordinate the setpoint review with the organization responsible for technical specifications (TS) and basis sections in Chapter 16 of the application, including the setpoint control program, and the organization responsible for accident analysis contained in Chapter 15 of the application. The SLs and ALs are established in Chapter 15 of the application.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 6.8, "Setpoints." In general, IEEE Std. 603-1991 requires that device setpoints be determined using a documented methodology that accounts for uncertainties and that processes which may be subject to multiple setpoints be governed by the more restrictive setpoint.

2. 10 CFR 50.36(c)(1)(ii)(A) requires, in part, that if a limiting safety system setting (LSSS) is specified for a variable on which a safety limit has been placed, the setting be chosen so that automatic protective action will correct the abnormal situation before a safety level is exceeded. LSSSs are settings for automatic protective devices related to variables with significant safety functions. Additionally, 10 CFR 50.36(c)(1)(ii)(A) requires that a licensee take appropriate action if it is determined that the automatic safety system does not function as required.

3. 10 CFR 50.36(c)(3) states that surveillance requirements are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met.

4. GDC 13, “Instrumentation and Control,” requires, in part, that instrumentation be provided to monitor variables and systems and that controls be provided to maintain these variables and systems within prescribed operating ranges.

5. GDC 20, “Protection System Functions,” requires, in part, that the protection system be designed to initiate automatically the operation of appropriate systems to ensure that specified acceptable fuel design limits are not exceeded as a result of AOOs.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for setpoints are as follows:

1. The setpoint methodology should conform to the applicable version of RG 1.105, in place 6 months before the docket date of the application. Currently, RG 1.105 endorses ISA-S67.04-1994, "Setpoints for Nuclear Safety-Related Instrumentation," with identified exceptions and clarifications. The applicant should examine the version of RG 1.105 that applies to its application to identify the applicable standards.

2. NRC Regulatory Issue Summary (RIS) 2006-17, “NRC Staff Position on the Requirements of 10 CFR 50.36, ‘Technical Specifications,' Regarding Limiting Safety System Settings during Periodic Testing and Calibration of Instrument Channels,” discusses issues that could occur during testing of LSSSs and which therefore, may have an adverse effect on equipment operability.

3. Generic Letter (GL) 91-04, "Guidance on Preparation of a Licensee Amendment Request for Changes in Surveillance Intervals to accommodate a 24-Month Fuel Cycle," provides guidance on issues that should be addressed by the setpoint analysis when calibration intervals are extended from 12 or 18 to 24 months.

III. REVIEW PROCEDURES

1. Review of IEEE Std. 603-1991, Section 6.8:

   A. The setpoints identified in the application are to be established using an approved methodology conforming to applicable version of RG 1.105. This reviewer should verify that the setpoints are established using the ALs developed from event analyses models and identified in Chapter 15 of the application, and identified in the technical specifications and limits contained in Chapter 16 of the application. Note that the evaluation of ALs and technical specifications is part of Chapters 15 and 16 and such limits and TS are not reviewed in Chapter 7.

   B. The application identifies some setpoints that are used for a general class of LSSSs related to variables having significant safety functions but which do not protect SLs. For these LSSSs, 10 CFR 50.36(c)(1)(ii)(A) requires that a licensee take appropriate action if it is determined that the automatic safety system does not function as

required. The bases for these setpoint calculations include system or equipment protection. A normal process limit (NPL) should be documented and adjusted for the appropriate margin to establish the setpoint when no AL is established by the accident analysis.

C. The basis for algorithms that may be used in the establishment of safety setpoints are located in the technical specifications and bases provided in Chapter 16 of the application. For algorithms that are different from the standard technical specifications algorithms, this review should confirm that an evaluation of the algorithms has been performed as part of the review of Chapter 15 of the application. Note that the review of setpoints in Chapter 7 does not evaluate the adequacy of the algorithms; instead, the Chapter 7 review evaluates only its application within the setpoint analysis.

D. This review should confirm that where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design provides automatic or manual control to ensure that the more restrictive setpoint is used as credited in the safety analysis. The provisions used to prevent improper use of less restrictive setpoints should be part of the sense and command features and are evaluated in DSRS Section 7.2.12.

2. If a review of Setpoint Methodology is necessary:

A. The objectives of the methodology review are to 1) verify that setpoint calculation methods are adequate to assure that protective actions are initiated before the associated plant process parameters exceed their ALs, 2) verify that setpoint calculation methods are adequate to assure that control and monitoring setpoints are consistent with their system specifications, and 3) confirm that the established calibration intervals and methods are consistent with safety analysis assumptions.

B. If the applicant commits to develop a setpoint methodology in accordance with RG 1.105, the reviewer should confirm conformance with the RG and RIS 2006-17. The areas of review to establish such conformance include:

i. Relationships between the SL, AL, LSSS, the allowable value (if used), the setpoint, the acceptable as-found band, the acceptable as-left band, and the setting tolerance. The methodology should provide a diagram that depicts the relationship for the above.

ii. The setpoint ~~technical specifications~~TS meet the requirements of 10 CFR 50.36. Additional information related to setpoint ~~technical specifications~~TS is provided in RIS 2006-17.

iii. Basis for selection of the trip setpoint.

iv. Uncertainty terms that are addressed.

v. Method used to combine uncertainty terms.

vi. Justification of statistical combination.

vii. Relationship between instrument and process measurement units.

viii. Data used to select the trip setpoint, including the source of the data.

ix. Assumptions used to select the trip setpoint (e.g., ambient temperature limits for equipment calibration and operation, potential for harsh accident environment).

x. Instrument installation details and bias values that could affect the setpoint.

xi. Correction factors used to determine the setpoint (e.g., pressure compensation to account for elevation difference between the trip measurement point and the sensor physical location).

xii. Instrument test, calibration or vendor data, as-found and as-left; each instrument should be demonstrated to have random drift by empirical and field data. Evaluation results should be reflected appropriately in the uncertainty terms, including the setpoint methodology.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to: (1) demonstrate that the setpoint calculation methods are adequate to assure that protective actions are initiated before the associated plant process parameters exceed their analytical limits, (2) demonstrate that the setpoint calculation methods are adequate to assure that control and monitoring setpoints are consistent with their system specifications, and (3) the established calibration intervals and methods are consistent with safety analysis assumptions. On such a basis, the reviewer can conclude that the setpoint methodology satisfies the requirements of 10 CFR Part 50, Appendix A, GDCs 13 and 20, 10 CFR 50.36(c)(1)(ii)(A) and (c)(3), and the requirements of Section 6.8 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection “V. Implementation.”

VI. REFERENCES

All of the references in this DSRS Chapter 7, “Instrumentation and Controls,” may be found in Appendix D of this Chapter.

7.2.8 AUXILIARY FEATURES

I. AREAS OF REVIEW

The review of auxiliary features is divided into two portions: evaluation of auxiliary supporting features and evaluation of other auxiliary features. Auxiliary supporting features are systems or components that provide services upon which safety systems rely in accomplishing their safety functions. Auxiliary supporting features typically include, for example, electric power systems, diesel generator fuel storage and transfer systems, instrument air systems, heating, ventilating, and air conditioning (HVAC) systems, and essential service water and cooling water systems. Other auxiliary features are systems or components that perform a function upon which the safety systems do not rely to accomplish their safety functions, but which cannot be isolated from the safety system and are designated as part of the safety systems by association.

Review Interfaces

The I&C aspects of auxiliary supporting features and other auxiliary features are addressed in the review of those DSRS sections that discuss the systems that provide these features, including electric power systems, diesel generator fuel storage and transfer systems, instrument air systems, HVAC systems, and essential service water and component cooling water systems. I&C reviews of auxiliary features should be coordinated with the organizations responsible for the reviews of these features to ensure that they are appropriately addressed.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.12, “Auxiliary Features.” This Section indicates that auxiliary supporting features shall meet the requirements of IEEE Std. 603-1991, and that other auxiliary features that perform a function upon which the safety systems do not rely to accomplish their safety functions and that are part of the safety systems by association shall be designed so that they do not degrade the safety systems below an acceptable level.

2. 10 CFR 52.47(a)(2) states, in part, that the application shall discuss such items as auxiliary systems insofar as they are pertinent.

3. 10 CFR 50.34(f)(2)(xxiii) requires that applications provide, as part of the reactor protection system, an anticipatory reactor trip that would be actuated on loss of main feedwater and on turbine trip.

DSRS Acceptance Criteria

There are no specific DSRS acceptance criteria in this section. However, the guidance provided below should be used to review the acceptability of information associated with auxiliary features.

III. REVIEW PROCEDURES

The reviewer should evaluate the following when assessing auxiliary features:

1. The application should identify and describe all auxiliary features proposed in the design, which may be described in other Chapters of the application. Identification of auxiliary features will help assure adequate coordination with the respective DSRS sections where these auxiliary supporting features and other auxiliary features are described. Note that the functional performance of auxiliary supporting features and other auxiliary features are reviewed by other branches in accordance with the DSRS sections that address these systems.

2. The scope of the I&C review is limited to those I&C protection systems that provide functionality to auxiliary supporting features and other auxiliary features. The review includes the adequacy of I&C system controls, instrumentation, and signals relied upon for proper operation of auxiliary supporting features, including isolation signals under unusual conditions such as postulated accidents. Auxiliary supporting features must satisfy the requirements of IEEE Std. 603-1991, including reliability, single failure, qualification, and independence. These design considerations associated with auxiliary supporting features are addressed in Section 7.1 of the DSRS, which provides functional and design criteria for I&C safety systems. The review of auxiliary supporting features will be performed in accordance with DSRS Section 7.1.

3. To confirm that the requirements of 10 CFR 50.34(f)(2)(xxiii) are considered, the reviewer will verify that the application provided information to address the design of all reactor trips (including trips that would be actuated on loss of main feedwater and on turbine trips) incorporated in the reactor protection system. Such trip functions should comply with the requirements of IEEE Std. 603-1991. This applies to the entire trip function, from the sensor to the final actuated device. For sensors located in non-seismic areas, the installation (including circuit routing) and design should be such that the effects of credible faults (i.e., grounding, shorting, application of high voltage, or electromagnetic interference) or failures in these areas could not be propagated back to the reactor protection system and thus degrade the reactor protection system performance or reliability. The sensors should be designed to operate in a seismic event, i.e., not fail to initiate a trip for conditions which would cause a trip.

4. The reviewer will confirm that Section 5.12.2 of IEEE Std. 603-1991, which provides criteria for other auxiliary features that: a) perform a function upon which a safety system does not rely in accomplishing its safety function, and b) are part of a safety system by association, is applied in the design of such auxiliary features. The reviewer should confirm that other auxiliary features that need not be operable for the I&C safety systems to perform their functions are designed to meet applicable functional and design criteria in IEEE Std. 603-1991 that ensure that such other auxiliary features do not degrade the functionality of I&C safety systems.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, and if the review performed in accordance with those DSRS Sections that discuss auxiliary features

confirms that the application conforms to the guidance identified in those sections, the staff can conclude that the application provides information sufficient to: 1) demonstrate that auxiliary supporting features are designed consistent with the applicable requirements of IEEE Std. 603-1991, 2) demonstrate that other auxiliary features are designed such that they do not degrade safety systems below an acceptable level, 3) demonstrate that the reactor protection system provides an anticipatory reactor trip that would be actuated on loss of main feedwater and on turbine trip. On such a basis, the reviewer can conclude that the design of auxiliary features satisfy the requirements of Section 5.12 of IEEE Std. 603-1991, 10 CFR 52.47(a)(2), and 10 CFR 50.34(f)(2)(xxiii).

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection "V. Implementation."

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this Chapter.

7.2.9 CONTROL OF ACCESS, IDENTIFICATION, AND REPAIR

I. AREAS OF REVIEW

The review includes the area of administrative control of the I&C system hardware and software, identification of safety equipment, and equipment repair features. Control of access to I&C system hardware and software allows a licensee to limit access to the means for bypassing safety system functions to qualified plant personnel. "Identification" refers to the naming and labeling of I&C related structures, systems and components (SSCs), and I&C system documentation, software, and firmware to ensure adequate control of safety system equipment. The review also includes evaluation of the capability to repair I&C safety systems.

Review Interfaces

The review of any proposed identification of SSCs in the control room and remote shutdown room should be coordinated with the organization responsible for reviewing human factors. Similarly, the review of any proposed identification concerning the electrical power supply for I&C systems should be coordinated with the organization responsible for electrical engineering.

II. ACCEPTANCE CRITERIA

Requirements

10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.9, "Control of Access," Section 5.11, "Identification," and Section 5.10, "Repair." Section 5.9 of IEEE Std. 603-1991 states, in part, that the design shall permit the administrative control of access to safety system equipment. Section 5.11 contains requirements for the identification of safety system equipment. Section 5.10 requires that safety systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for identification are as follows:

1. Digital I&C safety systems and components should conform to the identification guidance contained in Section~~Clause~~ 5.11 of IEEE Std. 7-4.3.2, as endorsed by the version of RG 1.152 in place 6 months before the docket date of the application. The applicant should examine the version of RG 1.152 that applies to its application to identify the applicable standards.

2. I&C safety systems and components should conform to the identification guidance in IEEE Std. 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," as endorsed (with identified exceptions and clarifications) by the version of RG 1.75 in place 6 months before the docket date of the application. The applicant should examine the version of RG 1.75 that applies to its application to identify the applicable standards.

III. REVIEW PROCEDURES

Control of Access

The reviewer should evaluate how access to I&C safety systems will be controlled and how such controls satisfy the requirements of Section 5.9 of IEEE Std. 603-1991 and the guidance contained in RG 1.152 for digital-based I&C safety systems. The reviewer should confirm that the design allows for the administrative control of access to I&C safety system equipment. These administrative controls should be supported by provisions within the safety systems, by provisions in the generating station design, or by a combination thereof. These administrative controls are more specifically described below.

1. The reviewer should evaluate how design features provide the means to control physical access to safety system equipment, including access to test points and the means for changing setpoints. Typically, access control includes provisions such as alarms and locks on safety system panel doors or control of access to rooms in which I&C safety system equipment is located.

2. For digital-based systems, the reviewer should consider the controls over electronic access to safety system software and data described in the application. Physical and electronic access to digital computer-based control system software and data should be controlled to prevent changes by unauthorized personnel. Controls should address access through network connections and maintenance equipment. Specifically, there should be no access via network connections, and access via maintenance equipment should be limited to those times the maintenance equipment is actually being used for maintenance by persons authorized to do so.

3. The review should evaluate the measures to ensure that I&C systems do not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators. The security of computer-based systems is established through: (a) designing software security features, (b) developing systems that do not contain undocumented codes, and (c) installing and maintaining those systems in accordance with the station administrative procedures and security programs.

4. Features for control of access should conform to the guidance in Regulatory Positions 2.1 through 2.5 of RG 1.152, which provide specific guidance on the establishment of a secure development and operational environment for the protection of digital safety systems against undesirable actions and events that may affect the reliable operation of the system.

Identification

The reviewer should evaluate the description of hardware and software identification controls for I&C safety equipment and how such controls satisfy the guidance contained in RG 1.75 and the requirements of Section 5.11 of IEEE Std. 603-1991 regarding identification of I&C safety systems.

1. The reviewer should confirm that there is or will be a means such that redundant divisions of the I&C safety system components, cables, and cabinets are easily and distinctively identified as by a color code scheme, unique symbols, or other acceptable

means. The preferred identification method is color coding of components, cables, and cabinets.

2. For digital-based I&C safety systems, the reviewer should confirm that the following identification provisions specific to software and firmware systems are met:

   A. Firmware and software identification should be used to assure the correct software version is installed in the correct hardware component.

   B. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

   C. Means should be included in the software program for computers that would identify the program version as well as a means to identify the version after the software has been compiled and loaded onto a computer.

   D. Means should be provide to assure that the correct control parameters and constants are initially installed in the computers and digital devices and that these control parameters and constants are maintained and updated correctly.

   E. The identification scheme and its application should be clear and unambiguous.

   F. The identification should include a unique revision identifier and should be traceable to configuration control documentation that identifies and justifies the changes made by that revision.

   G. The versions of computer hardware, programs, and software should be distinctly identified in accordance with the guidance in Section~~Clause~~ 5.11 of IEEE Std. 7-4.3.2.

   H. The reviewer should confirm that a configuration management plan exists and provides for the identification and configuration baselines for all software and firmware.

Repair

The reviewer should evaluate the applicant's capability to repair I&C safety systems to ensure that the requirements contained in Section 5.10 of IEEE Std. 603-1991 are met. The reviewer should consider the following:

1. The hardware and software description~~s~~ and descriptions of the surveillance testing and self-diagnostics should be sufficient to demonstrate that safety system design facilitates timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

2. The reviewer should confirm that the system design allows for bypass of individual functions in each safety channel to allow for repairs.

3. Digital safety systems may include self-diagnostic capabilities to aid in troubleshooting. However, the use of self-diagnostics does not replace the need for the capability for test

and calibration systems as required by Section~~Clause~~s 5.7 and 6.5 of IEEE Std. 603-1991.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to: 1) demonstrate that the proposed administrative provisions to control access to I&C safety systems and equipment are adequate to prevent unauthorized access and modification to the safety I&C systems, 2) demonstrate that I&C safety system are distinctively marked, versions of hardware are marked accordingly, and configuration management is used for maintaining identification of safety-related software, and 3) demonstrate that demonstrate that safety system design facilitates timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the control of access guidance of RG 1.152, the identification guidance contained in RG 1.75, and the control of access, identification, and repair requirements of Sections 5.9, 5.~~11~~10, and 5.~~10~~ 11 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection “V. Implementation.”

VI. REFERENCES

All of the references in this DSRS Chapter 7, “Instrumentation and Controls,” may be found in Appendix D of this Chapter.

7.2.10 INTERACTION BETWEEN SENSE AND COMMAND FEATURES AND OTHER SYSTEMS

I. AREAS OF REVIEW

The review of this area includes evaluation of the interaction between sense and command features and other systems to confirm that nonsafety system interactions with I&C safety systems are limited and do not adversely affect the I&C safety systems.

Review Interfaces

The fundamental design principles described in Section 7.1 as well as the Appendices to Chapter 7 of the DSRS inform the review of interactions between sense and command features and other systems.

II. ACCEPTANCE CRITERIA

Requirements

10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 6.3, “Interaction between Sense and Command Features and Other Systems.” This Section states that if a single credible event can both cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, either alternate channels not subject to this failure will be provided, or equipment not subject to failure caused by the same single credible event shall be provided.

DSRS Acceptance Criteria

There are no specific DSRS acceptance criteria in this section. However, the guidance provided below should be used to review the acceptability of the information associated with interaction between sense and command features and other systems.

III. REVIEW PROCEDURES

The reviewer should evaluate the controls described in the application to ensure that nonsafety system interactions with safety systems are limited. Section 6.3 of IEEE Std. 603-1991 indicates that if a single credible event can both (1) cause a non-safety system action that results in a condition that needs protective action and (2) concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, either alternate channels not subject to this failure will be provided, or equipment not subject to failure caused by the same single credible event will be provided. Note that where the event of concern is a simple failure of a sensing channel shared between control and protection functions, previously accepted approaches have included the following:

1. Providing additional redundancy to isolate the safety system from channel failure.

2. Using data validation techniques to select a valid control input to isolate the control system from the failed channel.

In addition, the reviewer should evaluate the I&C system design provisions included to satisfy the requirements of Section 6.7 of IEEE Std. 603-1991 if a channel is in maintenance bypass. The reviewer will confirm that the I&C system is designed such that, while sense and command features equipment is in maintenance bypass, the capability of a safety system to accomplish its safety function is retained, and during such operation, the sense and command features continue to meet the ~~single~~ single ~~-~~failure requirements contained in Section 5.1 of IEEE Std. 603-1991 and the requirements for interaction between sense and command features and other systems contained in Section 6.3 of IEEE Std. 603-1991.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that non-safety system interactions with safety systems are limited and do not adversely affect the I&C safety systems. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the requirements related to interactions between the sense and command features and other systems contained in Section 6.3 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection “V. Implementation.”

VI. REFERENCES

All of the references in this DSRS Chapter 7, “Instrumentation and Controls,” may be found in Appendix D of this Chapter.

7.2.11 MULTI-UNIT STATIONS

I. AREAS OF REVIEW

Although SSCs can be shared between nuclear power plant (NPP) units of multi-unit stations (i.e., multiple NPP units located at the same site), the main area of this review is to verify that I&C safety systems are not shared between NPP units in this application. GDC 5 and IEEE Std. 603-1991 allow this sharing provided that the sharing of the SSCs will not impair the performance of the required safety functions in all units. If the application proposes the sharing of I&C safety systems, this review guidance would need to be supplemented.

Review Interfaces

The fundamental principles described in Section 7.1 of the DSRS inform the review of multi-unit stations. In addition, if the application proposes multi-unit shared displays and controls, the review should be coordinated with the organization responsible for reviewing human factors to confirm that shared user interfaces are sufficient to support the operator needs for each of the shared units. The review of any proposed sharing of electrical power in multi-unit NPPs or proposed capability for manual connection for sharing of electrical power should be coordinated with the organization responsible for reviewing electrical engineering.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.13, “Multi-Unit Stations.” This Section states that the sharing of structures, systems, and components between units at multi unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired.

2. GDC 5, “Sharing of structures, systems, and components,” states that structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for multi-unit stations are as follows:

1. I&C systems and components should conform to the application of the ~~single~~ single-failure criteria contained in IEEE Std. 379-2000, “Single Failure Criterion.” The version of RG 1.53, “Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems,” in place 6 months before the docket date of the application, provides additional guidance for the application of this criterion. The applicant should examine the version of RG 1.53 that applies to its application to identify the applicable standards.

III. REVIEW PROCEDURES

1. The review should evaluate the I&C design described in the application to ensure that safety-related SSCs are not shared between units in multi-unit stations. The reviewer should consider the following:

   A. The reviewer should confirm that the I&C architecture and system design meet the regulatory requirements contained in Section 5.13 of IEEE Std. 603-1991 and the guidance contained in IEEE Std. 379-2000 with respect to sharing of safety I&C systems among multi-unit stations.

   B. The reviewer will coordinate the review with the organization responsible for human factors to confirm that, for any proposed shared safety displays and controls, the shared user interfaces are sufficient to support the operator needs for each of the shared units.

2. The reviewer should confirm that any design that proposes sharing of SSCs other than I&C safety systems demonstrates the ability to simultaneously perform credited safety functions in all units as follows:

   A. The I&C systems' ability to actuate a minimum of engineered safety features credited in the safety analysis as available for each design basis event.

   B. The reviewer should coordinate with the organization responsible for review of electrical engineering to confirm that sharing Class 1E power systems does not impair the ability of the I&C systems to perform credited safety functions and also satisfies other requirements such as independence.

   C. Design basis events occurring in one unit do not impair the ability of the I&C systems to perform credited safety functions in the other unit(s).

3. The reviewer should confirm that provisions are included in the I&C design to ensure that single failures or transients within the I&C safety systems of one unit will not adversely affect or propagate to another unit and thereby prevent the shared systems from performing the safety functions credited for the other unit. The reviewer should also confirm that any proposed contingency or emergency plans for temporary sharing of systems (such as electrical power cross ties) will not adversely affect the capability of the I&C safety systems to perform their safety functions.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that, if I&C safety systems are shared at multi-unit stations, such sharing of the SSCs will not impair the performance of the credited safety functions in any unit. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the guidance contained in IEEE Std. 379-2000 and the requirements of Section 5.13 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection “V. Implementation.”

VI. REFERENCES

All of the references in this DSRS Chapter 7, “Instrumentation and Controls,” may be found in Appendix D of this Chapter.

7.2.12 AUTOMATIC AND MANUAL CONTROL

I. AREAS OF REVIEW

The review of this area includes evaluation of automatic and manual initiation of protective actions to ensure that I&C safety systems automatically initiate and execute protective action for the range of conditions and performance specified in the safety analysis. In addition, the review of manual controls should confirm that the controls will be functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary.

Review Interfaces

The review of automatic and manual controls should be coordinated with the organization responsible for the review of human factors to confirm that the functions controlled and the characteristics of the controls allow plant operators to take appropriate manual actions.

II. ACCEPTANCE CRITERIA

Requirements

10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Sections 6.1 and 7.1, “Automatic Control,” and Sections 6.2 and 7.2, “Manual Control.” Sections 6.1 and 7.1 provide requirements for the automatic initiation and control of all protective actions for both sense and command features as well as execute features. Section 6.2 requires, in part, that means be provided to manually initiate protective system actuation at the division level with a minimal number of discrete operator manipulations. Similarly, Section 7.2 requires, in part, that any additional design features in the execute features necessary to accomplish manual controls shall not defeat single failure protection and will support the capability of other safety-related manual controls.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for manual control are as follows:

1. The components and system should conform to the version of RG 1.62, “Manual Initiation of Protection Action,” in place 6 months before the docket date of the application. RG 1.62 also provides guidance that should be considered in the review of manual initiation of ATWS mitigation and diverse actuation system functions. The applicant should examine the version of RG 1.62 that applies to its application to identify the applicable standards.

III. REVIEW PROCEDURES

Automatic Control

Sections 6.1 and 7.1 of IEEE Std. 603-1991 discuss the general functional and design requirements for automatic control. The reviewer will verify that I&C systems provide capability to automatically initiate and control all protective actions, except as justified in accordance with

Section 4.5 of IEEE Std 603-1991. The application should provide information to confirm that I&C safety systems have been designed to demonstrate that the performance specifications are met, and that the evaluation of the precision of the safety system is addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. I&C systems should also be designed with capability in the execute features to receive and act upon automatic control signals from the sense and command features in accordance with Section 4.4 of IEEE Std 603-1991.

For digital computer-based systems, the reviewer should confirm that the functional requirements have been appropriately ~~allocates~~ allocated between hardware and software.

The reviewer should confirm that the system's real-time performance is predictable and repeatable, as described in DSRS section 7.1.4. This includes accounting for response times for all I&C timing delays involved in an instrument channel from sensor to final actuation device. The reviewer should confirm that the proposed response times assure that automatic actuations have an acceptable level of determinism with predictable performance margins when a demand signal is present.

Manual Control

Sections 6.2 and 7.2 of IEEE Std. 603-1991 provide the general functional, design, and executive requirements for manual control. Section 6.2 specifically states that means shall be provided to (1) implement manual initiation at the division level of all automatically initiated protective actions, while maintaining independence between redundant portions of the safety system, (2) implement manual system initiation and control of the protective actions not selected for automatic controls, based on the analysis conducted in accordance with Section 4.5 of IEEE Std 603-1991, and (3) maintain the plant in a safe condition using manual controls after the protective actions are completed. IEEE 603-1991, Section 6.2 provides that the number of discrete operator manipulations to implement manual initiation of protective actions shall be minimized and shall depend on the operation of a minimum amount of equipment. Another acceptable method is the system-level manual initiation of protective actions that results in the actuation of all divisions at once if it meets the independence, single failure, and minimum equipment requirements of IEEE Std 603-1991. Section 7.2 requires, in part, that additional execute features necessary to accomplish manual control of the actuated component shall not defeat the requirements of the single-failure criterion.

RG 1.62 provides an acceptable method for complying with IEEE Std. 603-1991 in regard to the manual initiation of protective actions. The reviewer should:

1. Confirm the organization responsible for human factor reviews has reached a satisfactory conclusion on the subjects contained in Regulatory Position 3. The human factors engineering (HFE) program described in Chapter 18 addresses the following areas (Note that these areas are part of Chapter 18 and are not reviewed in this chapter):

    A. Identification and allocation of functions to automatic control, manual control, or a combination. The allocation process follows criteria that ensure automatic action is used for events that occur too quickly for operator intervention as well as tasks that have a high human error probability.

B. Identification of controls, displays, and alarms needed to monitor the automatic actions and initiate and control the manual actions.

C. If the manual action is risk significant, credited in the accident analysis, or credited in the D3 scoping analysis, a detailed analysis should be performed to ensure the time available to perform the credited manual actions is greater than the time required for the operators to perform the actions. Verification that all necessary controls, displays, and alarms needed to support manual actions are visible from the location of the manual control.

D. Validation that all necessary controls, displays, and alarms needed to support manual actions are available when needed and are unambiguous.

2. The review of manual controls should confirm that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified).

3. The reviewer will verify that the design provides the capability to transfer safety system actuation between automatic and manual control. The reviewer also verifies that the design provides the variables that are to be displayed for the operator to use in taking manual action.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to: 1) demonstrate that I&C systems provide the capability to automatically initiate and control all protective actions for the range of conditions and performance specified in the safety analyses, and 2) demonstrate that manual controls will be functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the manual control guidance contained in RG 1.62, and the automatic and manual control requirements contained in Sections 6.1, 6.2, 7.1, and 7.2 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection “V. Implementation.”

VI. REFERENCES

All of the references in this DSRS Chapter 7, “Instrumentation and Controls,” may be found in Appendix D of this Chapter.

7.2.13 DISPLAYS AND MONITORING

I. AREAS OF REVIEW

The areas of review of this subsection include the review of the display and monitoring systems, which provide information for (1) the safe operation of the plant during normal operation, AOOs, and postulated accidents, (2) supporting manual initiation and control of safety systems, (3) the normal status and the bypassed and inoperable status of safety systems, and (4) satisfying requirements of the 10 CFR 50.34(f), which are sometimes identified as Three Mile Island (TMI) action plan items.

Review Interfaces

The review of information displays should be coordinated with the organization responsible for reviewing:

1. Reactor systems to confirm that the information displays and the characteristics of the displays (e.g., location, range, type, and resolution) support the system design

2. Electrical systems to confirm that the power for pressurizer level indication, block valve position indication, and relief valve position indication should be supplied from a source of emergency power in the event of a loss of offsite power.

3. Chapters 11 and 12 of the application to confirm that the information displays support radiation monitoring.

4. Chapter 15 of the application to confirm information displays conform to the analyses of AOOs and postulated accidents.

5. Chapter 18 of the application to confirm that the information displays incorporate human factors principles.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.8, “Information Displays.” Section 5.8 provides requirements for displays used for manually controlled actions, system status indication, including indication of bypasses, and location of information displays.

2. 10 CFR 50.34(f)(2)(iv) requires a plant safety parameter display console that will display to operators a minimum set of parameters defining the safety status of the plant, capable of displaying a full range of important plant parameters and data trends on demand, and capable of indicating when process limits are being approached or exceeded.

3. 10 CFR 50.34(f)(2)(v) requires automatic indication of the bypassed and operable status of safety systems.

4. 10 CFR 50.34(f)(2)(xi) requires direct indication of relief and safety valve position (open or closed) in the control room.

5. 10 CFR 50.34(f)(2)(xii) requires, in part, that auxiliary feedwater (AFW) system flow indication be provided in the control room.

6. 10 CFR 50.34(f)(2)(xvii) requires instrumentation in the control room to measure, record and readout (A) containment pressure, (B) containment water level, (C) containment hydrogen concentration, (D) containment radiation intensity (high level), and (E) noble gas effluents at all potential, accident release points. Provide for continuous sampling of radioactive iodines and particulates in gaseous effluents from all potential accident release points, and for onsite capability to analyze and measure these samples.

7. 10 CFR 50.34(f)(2)(xviii) requires, in part, that instruments be provided in the control room to provide an unambiguous indication of inadequate core cooling~~, such as primary coolant saturation meters in pressurized water reactors (PWRs),~~ and a suitable combination of signals from indicators of coolant level in the reactor vessel and in-core thermocouples ~~in PWR's~~.

8. 10 CFR 50.34(f)(2)(xix) requires instrumentation adequate for use in monitoring plant conditions following an accident that includes core damage.

9. 10 CFR 50.34(f)(2)(xx) requires power supplies be provided for pressurizer relief valves, block valves, and level indicators such that: (A) Level indicators are powered from vital buses; (B) motive and control power connections to the emergency power sources are through devices qualified in accordance with requirements applicable to systems important to safety and (C) electric power is provided from emergency power sources.

10. GDC 13, “Instrumentation and Control,” requires in part that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

11. GDC 19, “Control Room,” requires in part that a control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for displays and monitoring are as follows:

1. The components and system should conform to the criteria for accident monitoring instrumentation contained in the version of RG 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” in place 6 months before the docket date of the application. Currently, RG 1.97 endorses IEEE Std. 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations,” with identified exceptions and clarifications. The applicant should examine the version of RG 1.97 that applies to its application to identify the applicable standards.

2. The components and system should conform to the version of RG 1.47 in place 6 months before the docket date of the application.

3. The SRM on SECY-93-087, Item II.T, "Control Room Annunciator Alarm Reliability," provides general guidance on the alarm system interface with operator workstations.~~.~~

III. REVIEW PROCEDURES

Conformance to IEEE Std. 603-1991, Section 5.8.1, "Displays for Manually Controlled Actions"

The reviewer should confirm that the I&C systems conform to the requirements associated with display for manual control actions contained in Section 5.8.1 of IEEE Std. 603-1991 using the following guidance:

1. Displays supporting manual actions are a subset of the displays addressed by RG 1.97, which endorses IEEE Std. 497. The review of this acceptance criterion should be coordinated with the reviews performed for Subsection (3B) under Conformance to IEEE Std. 603-1991, Section 5.8.1, below~~Subsection (b) below~~.

2. Minimizing the possibility of ambiguous indications is accomplished within the HFE program described in Chapter 18. In summary, fully trained experienced operators respond to a series of scenarios on a full scope simulator. The scenarios exercise the simulator displays. The operators' performance is observed and recorded. The results are evaluated for any condition that creates operator error or introduces operator confusion that could lead to an operator error.

3. With respect to the IEEE Std. 603-1991 requirement to minimize ambiguous indications, any indication that creates confusion would be identified and the issue would be resolved. In some cases a design change may be necessary. Also, any situations where indications have to be combined or further evaluated before action can be taken are identified and actions are taken to stream-line that process. NUREG-0711, "Human Factors Engineering Program Review Model," contains detailed guidance for these activities. No further evaluation is needed as part of this review.

4. The review of information displays for manually controlled actions should include confirmation that displays are functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary.

Conformance to IEEE Std. 603-1991, Section 5.8.2, "System Status Indication"

The reviewer should confirm that the I&C systems conform to the requirements associated with system status indication contained in Section 5.8.2 of IEEE Std. 603-1991 using the following guidance:

1. Identification of Main Control Room Indications

   A. The Chapter 18 review verifies that the main control room (MCR) indications required by 10 CFR 50.34(f)(2) are included in the application's MCR design. Additionally, the

applicant completes a task analysis that, in part, identifies all controls, alarms and displays needed in the MCR to manage the plant safety functions. Provided the I&C system that processes these indications meets the guidance in the other sections of Chapter 7, no further action is needed for the reviewer to verify that all required information will be available in the MCR. Similarly, ambiguous indications are addressed in Chapter 18 as described above and need no further evaluation in Chapter 7.

2. Identification of Remote Shutdown Station Indications

The design of remote shutdown stations should provide displays associated with the controls necessary (Refer to DSRS Section 7.1.1 under remote shutdown capability) so that the operator can monitor the plant status of a prompt hot shutdown of the reactor, maintaining the unit in a safe condition during hot shutdown, and for subsequent cold shutdown. Examples of typical parameters that should be displayed on remote shutdown station displays include pressurizer pressure, pressurizer level, reactor coolant temperature, steam generator pressure, steam generator level, source-range neutron flux, level indication for tanks involved in shutdown, and shutdown system diagnostic instrumentation.

3. Identification of Accident Monitoring Variables

A. The reviewer should verify that Type A, B, C, D, and E variables have been identified and conform to the definitions of functional and design guidelines in Section~~Clause~~ 4 of IEEE Std. 497, as endorsed by the applicable version of RG 1.97. The review should verify that documentation has been developed and maintained for the selection bases for the accident monitoring variables.

B. The reviewer should verify ~~the~~ that Type A, B, C, D, and E variables conform to the performance, design, and qualification criteria in Section~~Clause~~s 5 through 9 of IEEE Std. 497. Experience shows that this review is best accomplished by an interdisciplinary team consisting of I&C (lead), Probabilistic Risk Assessment (PRA) and Severe Accidents, Reactor Systems, and HFE representatives. In addition to the guidance in IEEE Std. 497, the following attributes should also be reviewed:

i. The ranges for radiation and meteorological instrumentation that are provided in Revision 3 of RG 1.97 are applicable for applications using Revision 4 or later versions of RG 1.97. Applications using Revision 4 or later versions should document differences from the Revision 3 ranges for radiation and meteorological instrumentation.

ii. To the extent practicable, the same instruments should be used for accident monitoring as are used for normal operations of the plant. In cases in which a single display may indicate the reading of more than one instrument, the underlying purpose of this recommendation is met if the same variable and same display are used for accident monitoring even though the sensor providing the signal are different.

iii. Accident monitoring equipment identified as Type A, B, or C in accordance with RG 1.97 should be environmentally qualified as required by 10 CFR

50.49 and seismically qualified in accordance with RG 1.100. Additional guidance can be found in DSRS 7.2.2.

C. 10 CFR 50.34(f)(2)(xix) requires instrumentation for use in monitoring plant conditions following an accident that includes core damage. This requirement is addressed in RG 1.97, Section C(3) which establishes the regulatory position that Type C variables should have expanded ranges and a source term that considers a damaged core. The reviewer should note that this position expands the guidance for Type C variables beyond what is stated in IEEE Std. 497.

The reviewer should contact the organization responsible for reviewing PRA and Severe Accidents for assistance in identifying the necessary instrumentation. The reviewer should consider the following attributes:

i. The variables monitored and the range and accuracy of instrumentation provided to monitor these variables should conform with the severe accident analysis submitted pursuant to 10 CFR Section 52.47(a)(23).

ii. The instrumentation provided for monitoring severe accident conditions should be designed to operate in the severe accident environment for which it is intended and over the time span for which it is needed.

iii. To the extent practicable, the same instruments should be used for accident monitoring as are used for normal operations of the plant. In cases in which a single display may indicate the reading of more than one instrument, the underlying purpose of this recommendation is met if the same variable and same display are used for accident monitoring even though the sensors providing the signal are different.

Conformance to IEEE Std. 603-1991, Section 5.8.3, “Indication of Bypasses”

The reviewer should confirm that the I&C systems conform to the requirements associated with indication of bypasses contained in Section 5.8.3 of IEEE Std. 603-1991 using the following guidance:

1. The display instrumentation for bypasses does not need to be part of a safety system. If the bypass display instrumentation is not part of the safety system, the reviewer should confirm that display instrumentation for bypasses is designed and installed in a manner that precludes the possibility of adverse effects on plant safety systems. Administrative procedures should not call for immediate operator action based solely on bypass indication. If an operator action is based solely on the bypass indications, and this action is credited in the safety analysis to maintain the integrity of the safety systems, then the status indication should be classified as part of a safety system.

A. The reviewer should confirm that indication of a bypass is automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year, and (b) is expected to occur when the affected system is required to be operable.

B. The reviewer should confirm that capability exists in the control room to manually activate the display indication of all bypasses.

C. The reviewer should confirm that the indication equipment is designed and installed in a manner that precludes the possibility of adverse effects on plant safety systems. For example, inadvertent operator actions, such as an unintended touch on a touch sensitive display, should not prevent a safety system from performing a safety function.

D. The reviewer should confirm that failure or bypass of a protective function should not be a credible consequence of one or more failures in the indication equipment, and a bypass indication should not reduce the independence between redundant safety systems.

E. The bypass and inoperable status indication system should include a capability for ensuring its own operable status during normal plant operation to the extent that the indicating and annunciating functions can be verified.

F. The bypass and inoperable status indications should be arranged to enable the operator to determine the status of each safety system and whether continued reactor operation is permissible.

G. When a protective function of a shared system can be bypassed, indication of that bypass condition should be provided in the control room of each affected unit.

H. The means by which the operator can cancel erroneous bypass indications, if provided, should be justified by demonstrating that each postulated case of erroneous indication cannot be eliminated by another practical design.

I. Bypass and inoperable status indicators should be designed and installed in a manner that precludes the possibility of adverse effects on plant safety systems. The reviewer should confirm that unless the indication system is designed in conformance with the criteria established for the safety systems, it should not be used to perform safety functions.

Annunciator Systems

The annunciator system should consist of sets of alarms (which may be displayed on tiles, video display units (VDUs), or other devices) and sound equipment; logic and processing support; and functions to enable operators to silence, acknowledge, reset, and test alarms. The SRM to SECY 93-087, Item II.T identifies the following three design concepts:

1. Hierarchical access to alarms – Historically, alarm systems tended to overwhelm operators during transients because of the many nearly simultaneous annunciator activations, which had varying degrees of relevancy to the operator tasks. Alarm processing and alarm prioritization are two HFE design principles applied to address this challenge. They include the concept of hierarchical access. The HFE design principles are described in detail in NUREG-0700, “Human System Interface Design Review Guidelines” which is referenced by DSRS, Chapter 18. No additional reviews of this concept are needed as part of Chapter 7.

2. The alarm system is nonsafety-related and alarm circuits must be isolated from interfacing Class 1E circuits. This is a design requirement stated in IEEE Std. 603-1991. It is addressed in DSRS, Section 7.1.2.

3. Alarms that are provided for manually controlled actions for which no automatic control is provided and that are relied upon to enable the safety systems to accomplish their safety functions, should meet the applicable requirements for Class 1E equipment and circuits. The reviewer should review the manual actions credited in the design for accomplishing safety functions and corresponding protective action. The applicant provides this information to demonstrate conformity to IEEE Std. 603-1991, Section 4.5. Typically the reviewer should ~~to~~ evaluate whether alarms are directly credited with initiation of these manual actions. Operators are trained and procedures direct that alarms are verified using workstation displays and these displays are used to prompt manual action initiation. The displays are subject to the requirements and guidance listed in part II of this section.

4. If a specialized alarm is proposed for which indication is not available, and the operational direction is to respond directly to the alarm, then the alarm circuit design should implement this guidance.

TMI Action Items

10 CFR 50.34(f) imposes TMI action plan items for I&C systems important to safety. The reviewer should confirm that the application provides sufficient information to demonstrate the I&C system design satisfies the requirements in 10 CFR 50.34(f) using the following guidance.

1. 10 CFR 50.34(f)(2)(iv)

   The reviewer should confirm that the application includes a plant safety parameter display console that will display to operators a minimum set of parameters defining the safety status of the plant, capable of displaying a full range of important plant parameters and data trends on demand, and capable of indicating when process limits are being approached or exceeded.

2. 10 CFR 50.34(f)(2)(v)

   The reviewer should confirm that the bypassed and operable status indication of safety interlocks is automatically provided in the control room. Appropriate bypass indications should be provided to give the operators timely information regarding safety system status so the operators can mitigate the effects of unexpected system unavailability. The bypass indications should satisfy the guidelines of RG 1.47.

3. 10 CFR 50.34(f)(2)(xi)

   The reviewer should confirm that relief and safety valve position indication (both open and closed) is provided in the control room. ~~The indicator should also show valve p~~Position indication should be derived from a reliable valve-position detection device or a reliable indication of flow in the discharge pipe. The valve position indication may be

safety grade. If the indication is not safety grade, a reliable single-channel direct indication powered from a vital instrument bus may be provided if backup methods of determining valve position are available and are discussed in the emergency procedures as an aid to operator diagnosis of an action. The position indication should also be seismically and environmentally qualified. NUREG-0737, "Clarification of TMI Action Plan Requirements," provides additional guidance on conformance with this requirement.

4. 10 CFR 50.34(f)(2)(xii)

   The reviewer should confirm that ~~AFW~~ auxilliary feedwater system flow indication is provided in the control room. NUREG-0737 provides additional guidance on conformance with this requirement.

5. 10 CFR 50.34(f)(2)(xvii)

   The reviewer should confirm that instrumentation is provided in the control room to measure, record, and read out containment pressure, containment water level, containment hydrogen concentration, containment radiation intensity (high-level), and noble gas effluents at all potential accident release points. The accident monitoring instrumentation functions required by 10 CFR 50.34(f)(2)(xvii) should be included in the information systems important to safety. NUREG-0737 provides additional guidance on conformance with this requirement.

6. 10 CFR 50.34(f)(2)(xviii)

   The reviewer should confirm that unambiguous indication for inadequate core cooling is provided in the control room. The indication should provide the operator with sufficient information during accident situations to take planned manual actions, and to determine whether safety systems are operating properly. In addition, the instrumentation should also provide data sufficient for the operator to be able to evaluate the potential for core uncovery and gross breach of protective barriers, including any resulting release of radioactivity to the environment. NUREG-0737 provides additional guidance on conformance with this requirement.

7. 10 CFR 50.34(f)(2)(xix)

   The reviewer should confirm that instrumentation for monitoring plant conditions following an accident that includes core damage is provided. There should be instrumentation of sufficient quantity, range, availability, and reliability to permit adequate monitoring of plant variables and systems during and after an accident. Sufficient information should be provided to the operator for (1) taking planned manual actions to shut the plant down safely; (2) determining whether the reactor trip, ESF systems, and manually initiated safety-related systems are performing their intended safety functions (i.e., reactivity control, core cooling, and maintaining the reactor containment system and containment integrity); and (3) determining the potential for a gross breach of the barriers to radioactivity release (i.e., fuel cladding).

8. 10 CFR 50.34(f)(2)(xx)

The reviewer should confirm that power for pressurizer level indication, block valves, and relief valves is supplied from a source of emergency power in the event of a loss of offsite power. Level indicators must be powered by the vital buses. The power supplies should conform with the guidance of NUREG-0737. However, 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 reviewer should confirm that the application satisfies these requirements with the organization responsible for the review of electrical systems.

Other Information Systems

The reviewer should confirm that the information systems provide sufficient information to allow operators to determine what actions are necessary to mitigate the consequences of AOOs. For the safety parameter display system (SPDS), emergency response facilities (ERF), and emergency response data system (ERDS), the reviewer should limit the review to the system interface with the plant control and safety systems. The adequacy of the independence for these systems is reviewed in DSRS Section 7.1.2. Functional performance and other design aspects of the SPDS, ERF, and ERDS are the subject of other chapters of the application and are not reviewed in connection with Chapter 7.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to: (1) demonstrate that I&C display and monitoring systems provide the necessary information for the safe operation of the plant during normal operation, AOOs, and postulated accidents as described in the safety analyses, (2) demonstrate that I&C displays and monitoring systems will provide the necessary information for manual initiation and control of safety systems, and (3) provide normal status and the bypassed and inoperable status of safety systems. On such a basis, the reviewer can conclude that the design of I&C display and monitoring systems satisfies the reliability, availability and accuracy guidance contained in RG 1.47 and RG 1.97, and the requirements of GDC 64, Section 5.8, IEEE Std. 603-1991, and the I&C related Three Mile Island action items of 10 CFR 50.34(f)(2).

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection "V. Implementation."

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this Chapter.

7.2.14 HUMAN FACTORS CONSIDERATIONS

I. AREAS OF REVIEW

HFE principles and criteria should be applied to the selection and design of the displays and controls. Human performance design objectives should be described and related to the plant safety criteria. Recognized human factors standards should be employed to support the described human performance design objectives. The adequacy of the human factors aspects of the control room design is described in Chapter 18 of the application.

Review Interfaces

Appropriate application of human-factors principles should be confirmed with the organization responsible for reviewing Chapter 18 of the application.

II. ACCEPTANCE CRITERIA

Requirements

10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.14, "Human Factors Considerations." Section 5.14 requires, in part, that human factors be considered throughout the design process

DSRS Acceptance Criteria

There are no specific DSRS acceptance criteria in this section. However, the guidance provided below should be used to review the acceptability of information associated with human factors considerations.

III. REVIEW PROCEDURES

NUREG-0711~~, "Human Factors Engineering Program Review Model,"~~ provides guidance for establishing a program for the application of HFE to systems, equipment, and facilities of nuclear power generating stations. NUREG-0711 contains the review criteria referenced in Standard Review Plan Chapter 18. No additional reviews of HFE are performed as part of Chapter 7.

IV. EVALUATION FINDINGS

The staff findings in regard to the human factors considerations described in the application are set forth in DSRS Chapter 18.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection "V. Implementation."

VI. REFERENCES

All of the references in this DSRS Chapter 7, “Instrumentation and Controls,” may be found in Appendix D of this Chapter.

7.2.15 CAPABILITY FOR TEST AND CALIBRATION

I. AREAS OF REVIEW

The review of this area includes evaluation of the capability for test and calibration of the safety systems. The periodic testing consists of surveillance testing required by TS, including functional tests and checks, calibration verification, and time response measurements, to verify that I&C safety systems perform their safety functions as credited in the safety analysis.

Review Interfaces

The review of test and calibration provisions should be coordinated with the organization responsible for reviewing technical specifications.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Sections 5.7 and 6.5, "Capability for Test and Calibration." These Sections require capability for test and calibration of safety system equipment, while retaining capability of the safety systems to accomplish their safety functions.

2. 10 CFR 50.36(c)(3) states that surveillance requirements are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met.

3. GDC 21, "Protection system reliability and testability," requires that the protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. 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.

~~3.~~4. 10 CFR 50.34(f)(2)(xxii) requires performance of a failure modes and effects analysis of the integrated control system (ICS) to include consideration of failures and effects of input and output signals to the ICS.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for capability for test and calibration are as follows:

1. Digital I&C safety systems and components should conform to the guidance related to capability for test and calibration contained in Section~~Clause~~s 5.7, 5.5.2, and 5.5.3 of IEEE Std. 7-4.3.2, as endorsed by the version of RG 1.152 in place 6 months before the

docket date of the application. The applicant should examine the version of RG 1.152 that applies to its application to identify the applicable standards. ~~To the extent that the applicable version of RG 1.152 endorses additional portions of IEEE Std. 7-4.3.2, the components and system should also conform to the endorsed guidance in IEEE Std. 7-4.3.2.~~

2. ~~The applicant should examine the version of RG 1.~~22 that applies to its application to identify the applicable standards. ~~I&C components and systems should conform to the version of RG 1.22, "Periodic Testing of Protection System Actuation Functions," in place 6 months before the docket date of the application.~~

3. I&C components and systems should conform to the version of RG 1.118, "Periodic Testing of Electric Power and Protection Systems," in place 6 months before the docket date of the application. RG 1.118 endorses IEEE Std. 338, "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems." The applicant should examine the version of RG 1.118 that applies to its application to identify the applicable standards. ~~To the extent that the applicable version of RG 1.118 endorses additional portions of IEEE Std. 338, the components and system should also conform to the endorsed guidance in IEEE Std. 338.~~

III. REVIEW PROCEDURES

The reviewer should confirm that the capability for testing and calibration of I&C safety system equipment is provided without impairing the capability to accomplish the safety functions, consistent with the guidance in RG 1.22 and RG 1.118 and the requirements contained in Section 5.7 of IEEE Std. 603-1991 and GDC 21. The review should consider the following:

1. The reviewer should coordinate with the organization responsible for reviewing technical specifications to confirm that the I&C system design supports the types of testing required by the technical specifications. The system design should also support the compensatory actions required by technical specifications when limiting conditions for operation are not met. Typically, the design should allow for tripping or bypass of individual functions in each safety system channel.

2. The extent of test and calibration capability provided bears heavily on whether the design meets the ~~single~~ single-failure criterion. Any failure that is not detectable must be considered concurrently with any random postulated, detectable, single failure. Guidance on the ~~single~~ single-failure criterion is contained in DSRS Section 7.1.3.

3. Periodic testing should duplicate, as closely as practical, the overall performance of the safety system credited in the safety analysis. The test should confirm operability of both the automatic and manual circuitry. The capability for testing should be provided to permit testing during power operation. When this capability can only be achieved by overlapping tests, the test scheme must be such that the tests do, in fact, overlap from one test segment to another. Test procedures that call for disconnecting wires, installing jumpers, or making other similar modifications to the installed equipment are not acceptable test procedures for use during power operation.

4. For sense and command features, the reviewer should confirm that the application provides a means for checking the operational availability of each sense and command

feature input sensor relied upon for a safety function during reactor operation, in accordance with the requirements in Section 6.5 of IEEE Std. 603-1991. The review should consider the following:

A. Verification of the operational availability of each sensor credited for a safety function could be accomplished in various ways, such as by (a) perturbing the monitored variable, (b) introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, within the constraints of operating bypasses, or (c) cross-checking between channels that bear a known relationship to each other and have readouts available.

B. Cross checking between redundant channels is the most common method used to verify the availability of the input sensors. When only two channels of readout are provided, the application should contain information that establishes the basis used to ensure that an operator will not take incorrect action when the two channel readouts differ. The application should also contain information to describe the method that will be used for checking the operational availability of non-indicating sensors.

5. For digital computer-based systems, the reviewer should confirm that the following provisions contained in IEEE Std. 7-4.3.2 and the following guidance below are addressed in the application:

A. Test and calibration functions do not adversely affect the ability of the computer to perform its safety function, consistent with sub-~~clause~~ section 5.5.2 of IEEE Std. 7-4.3.2.

B. Self-diagnostics used to detect and report computer system faults and failures should be designed consistent with sub-~~clause~~ section 5.5.3 of IEEE Std. 7-4.3.2. The reviewer should confirm that the use of self-diagnostics does not replace the capability for test and calibration as required by Section~~Clause~~s 5.7 and 6.5 of IEEE Std. 603-1991.

C. The amount of resources (cycle time, processing capacity, etc.) that are assigned to self-supervision should be appropriately balanced to ensure that the I&C systems' safety function and performance are not affected.

D. A hardware watchdog timer is critical in the overall diagnostic scheme. The reviewer should confirm that a hardware watchdog timer is provided, since a software watchdog timer will fail to operate if the processor freezes and no instructions are processed. When a hardware watchdog timer is part of the design, the reviewer should verify that the hardware watchdog timer resets the safety processor if the processor does not complete its function. The reviewer should also confirm that a software failure will not cause an inadvertent actuation of the software processor reset subroutine, thereby nullifying the effectiveness of the hardware watchdog timer.

6. For designs utilizing resistance temperature detectors (RTDs), the reviewer should consider the following in reviewing any cross-calibration proposed for the RTDs:

A. The reviewer should examine the safety system design basis to identify the RTD accuracy and time response credited in the safety analysis.

B. The reviewer should examine the cross-calibration method, if used, and calibration and response time data to identify calibration inaccuracies, uncertainties, and errors, and to confirm that the cross-calibration method is adequate.

C. The reviewer should review the programmatic documentation of the cross-calibration process, if used, against the following criteria. This review should confirm that the calibration process is consistent with all setpoint analysis assumptions and the design basis.

i. Supporting Analysis

The reviewer should confirm that analyses and information on the instrument maintenance and calibration program supports the adequacy of the cross-calibration program, if one is used. The analysis should, as a minimum, include the following topics:

- Justification that the cross-calibration program accounts for the characteristics of the RTD sensors, including RTD specifications, range, accuracy, repeatability, dynamic response, installed configuration, environmental qualification, calibration reference, calibration history, and calibration intervals.

- The specific methods or analyses used for signal conditioning or processing (for example, averaging, biasing, failure detection, data quality determination, and error compensation) and the applicant's reasons for choosing these methods or analyses .

- The planned process for cross-calibration and response time determination.

- Justification that the cross-calibration process and testing results ~~verifies~~ verify that instruments are functioning as credited in the safety analysis (i.e., in accordance with design basis).

- The technical basis for the acceptance criteria and values of cross-calibration points monitored in-situ throughout the RTD range, to ensure that the data are adequate for detecting degradation or systematic drift.

D. Traceability of the ~~installed~~ Installed ~~reference~~ Reference RTD to ~~laboratory~~ Laboratory ~~calibration~~ Calibration ~~data~~Data

Laboratory calibration involves measuring an RTD's resistance at several known temperatures. The data are then used to provide a calibration curve for the device. In addition, the RTD response time can be determined under laboratory conditions using controlled temperature baths and a methodology to calculate the RTD response time over the temperature range for which the applicant intends to use the RTD.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to: 1) demonstrate that I&C components and systems are capable of being tested and calibrated while retaining their capability to accomplish their safety functions, both manually and automatically, 2) demonstrate that, for digital-based I&C systems, test and calibration functions (including any self-diagnostics functions) do not adversely affect the ability of the computer to perform its safety function, 3) demonstrate that, for designs using RTDs, appropriate analysis are included in the application for cross-calibration of RTDs. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the guidance related to capability for test and calibration contained in Section~~Clause~~s 5.5.2 and 5.5.3 of IEEE Std. 7-4.3.2, the guidance contained in RG 1.22 and RG 1.118, and the requirements contained in Section 5.7 of IEEE Std. 603-1991 and GDC 21.

V. IMPLEMENTATION

This section is identical throughout this mPower DSRS Section 7.2. The reviewer must read Section 7.2.1 Quality subsection "V. Implementation."

VI. REFERENCES

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D of this Chapter.

U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR B&W mPOWER™ SMR DESIGN

7.0 APPENDIX A INSTRUMENTATION AND CONTROLS - HAZARD ANALYSIS

Introduction

A hazard analysis (HA) is a process for examining an instrumentation and control (I&C) system throughout its development life-cycle to identify hazards (i.e., factors and causes), I&C requirements,[6] and constraints to eliminate, prevent, or control them. Hazard analyses examine ~~safety~~ safety-related I&C systems, subsystems, and components, their interrelationships and their interactions with other systems, subsystems, and components to identify unintended or unwanted I&C system operation including the impairment or loss of the ability to perform a safety function.

This appendix provides an approach to evaluate HAs used in the design of a digital I&C system. Experience with complex systems in general and with digital systems for critical functions in diverse application sectors in particular (including lessons learned from U.S. Nuclear Regulatory Commission (NRC) experience in recent licensing reviews) has revealed that current hazard analysis techniques such as fault tree analysis (FTA) and failure modes and effects analysis (FMEA),~~,~~ by themselves, do not assure the discovery of (or ~~assure~~ absence of) system-internal hazards rooted in system development activities. In contrast, a hazard analysis should facilitate a more focused I&C system review and should help to ensure traceability among regulatory requirements, architectural considerations, and system requirements to enable a more effective, and efficient I&C licensing review.

The application should contain HA information sufficient to ensure that the applicant has identified the hazards of concern, as well as the system requirements and constraints to eliminate, prevent, or control them. These system requirements and constraints help demonstrate that the hardware and software for I&C architectures incorporate the fundamental design principles, namely independence; redundancy; predictability and repeatability; and

[6] The design of digital I&C systems is governed by the legal requirements set forth in NRC regulations, including those in several of the General Design Criteria (GDC) in Title 10 of the *Code of Federal Regulations* (CFR),~~,~~ Part 50, Appendix A and 10 CFR 50.55a(h), which incorporates by reference Institute for Electrical and Electronics Engineers, Inc. (IEEE) ~~IEEE~~ Standard (Std.) 603-1991. NRC guidance endorses other IEEE standards, and these IEEE standards, as well as IEEE Std. 603-1991, are written in terms of so-called system -functional, performance, design, and other "requirements." These terms are well-understood in the I&C technical community, but except as used in IEEE Std. 603-1991, are not legal requirements. To avoid confusion, this DSRS section will use the "requirements" terminology of the IEEE standards that are not incorporated into NRC regulations in connection with references to such standards. These "requirements," as referenced in this DSRS section, should be understood as recommendations that the NRC staff considers adequate to satisfy portions of NRC regulatory requirements, but which are not the only acceptable methods of compliance. The functional, performance, design, and other requirements of IEEE Std. 603-1991, which are legal requirements, will be explicitly identified as originating from IEEE Std. 603-1991.

diversity and defense-in-depth (D3) as described in Section 7.1 of this DSRS. 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.

This appendix does not endorse any particular technique(s) for the development of HA. Rather, the information contained in this appendix provides examples of topics that the reviewer should consider in determining the adequacy and completeness of an HA. The reviewer will evaluate the adequacy of the application of any particular HA technique or combination of techniques to a topic identified below on a case-by-case basis.

HA Scope

This HA review guidance applies to any I&C system or element of a system to which a safety function is allocated, or on which a safety function depends, or which could impair a safety function. Impairment includes:

- not providing the function,
- providing the function when not needed,
- providing the function at the wrong time or for too long a duration or for too short a duration or out of sequence,
- providing the function based on incorrect value of the controlled parameter or variable,
- providing the function erratically, e.g., creating chatter or flutter of the controlled variable or parameter,
- Interfering with another action.

HA of an I&C system or I&C system element includes interaction with both its internal and external environment within the scope of Chapter 7 review areas. An applicant's HA could inform overlapping areas, such as human-machine interface systems, but these are outside the scope of Chapter 7 review of an applicant's HA.

HA is iterative and should be performed at every phase in the system development life-cycle to identify new hazards that could arise as the design is implemented in software and hardware.

HA Information to be Reviewed

The applicant's HA should describe and define each I&C system to be analyzed, identify each loss or impairment of safety function that the I&C system should prevent, and ensure that all safety functions identified in the application are allocated to the appropriate I&C system, whether the system is safety-related or not.

For each system, the reviewer should consider, at a minimum, the areas identified below. For each identified area, the reviewer will confirm whether the applicant performed an HA adequate to identify the hazards that could lead to impairment or loss of a safety function during all modes of operation (such as power operating mode, cooldown mode, hot shutdown mode, refueling mode, etc.). In addition, the reviewer will confirm that the applicant evaluated the impact of each identified hazard on the safety system, its subsystems and components, and their interrelationships. The reviewer will also confirm that the design provides the necessary

hazard restrictions and controls in the form of architectural and environmental constraints, or additional safety features to show that safety functions will be accomplished.

Evaluation Topics

1. I&C system functions and constraints are properly allocated between hardware and software.

   A. There should be no undesirable or unintended functions.

2. System behavior should be completely and correctly understood and specified, and the system should behave in a predictable and repeatable manner.

   A. All states, including failure mode states, safe state regions, and safely recoverable process states, are known.

   B. System is in a known state at all times, e.g., through positive monitoring and indication.

   C. Each transition from a current state (including initial state) to some next state is known.

   D. Analysis of the system should demonstrate that conflicts among shared system resources will not interfere with correct, timely execution of a function.

3. Expected values, type, and range of system inputs and outputs are known, monitored and verified.

4. Conditions such as degradation~~, drift,~~ and unacceptable deviation that could lead to unanalyzed system states should be detectable by the I&C system and appropriate intervention provided before impairment or loss of the safety function.

5. Boundaries of each I&C safety system and the interfaces, interactions, and inter-dependencies with other systems should be specified (including physical, functional, temporal, etc.)

   A. Redundancy should not be compromised through a dependency or interference.

   B. System interactions should be limited to those necessary to accomplish the safety functions.

   C. System interactions and interconnections that preclude complete verification and validation should be avoided, eliminated, or prevented.

D. System independence should be assured across lines of defense-in-depth, redundant divisions, and monitoring and monitored elements of system (e.g., there is no unintended or undesirable communication pathway).

6. The nature of change in a monitored physical phenomenon (such as pressure, temperature, flow, or neutron flux density) is correctly characterized in the I&C systems.

7. Internal hazards that could be generated by the I&C system should be identified. For example, excessive load or demand on resources by the I&C system, such as electric power overload due to a short circuit or communication bus overload.

External hazards such as disruption in I&C system conditions and physical conditions in the environment that may impair a safety function should be identified. For example:

A. Water intrusion.

B. Uncontrolled transfer of energy into the system. Such energy may take various forms, e.g.,~~:~~ heat; light; vibration; radiation; electromagnetic radiation.

C. Interruption of services (primary; secondary; other forms of back-up), e.g., electric power supply.

D. Disturbance in services, propagating to a disturbance in a main signal, e.g., electric power supply; service water; service air.

E. Breaching of isolation barriers, e.g., cable penetration; other duct penetration.

F. Adverse conditions in temperature, pressure, or humidity/moisture, e.g., too high or too low or rapid changes.

HA Information to be Considered for Inspections, Tests, Analyses, and Acceptance Criteria

Inspections, tests, analyses, and acceptance criteria (ITAAC) will be used to verify that the I&C system has been implemented and installed in accordance with the approved design and performs its safety functions. To the extent that system implementation and installation involves HA, the ITAAC will be used to verify that the HA was adequate. Activities in the scope of ITAAC would verify that the constraints through ~~hazard analyses~~HA have been satisfied. Section 14.3.5 of the DSRS will provide specific ITAAC evaluation criteria.

The reviewer should ensure appropriate ITAAC associated with HA are identified by the applicant since hazards that could lead to the impairment or loss of safety function can be generated as the design is implemented. The sections below provide two examples. It is the applicant's responsibility to identify additional contributory hazards and the appropriate ITAAC commitments associated with the implementation of their design.

I&C ~~systems~~ Systems ~~development~~ Development ~~process~~ Process ~~contributory~~ Contributory ~~hazards~~ Hazards

The I&C development process can contribute to hazards that could lead to the impairment or loss of system safety function. For example, the development process may include erroneous, incomplete, or improperly implemented I&C system requirements. The application may provide information associated with contributory hazards as the system is developed, and the reviewer should evaluate this information for adequacy during the review of the application. However, an applicant need only submit the information required by the regulation governing the content of the application. Detailed HA information beyond the level of the final safety analysis report (FSAR) will be reflected in the scope of ITAAC. The reviewer should confirm that the HA information includes the necessary controls for the various contributory hazards and the associated commitments for each phase of the development process. In determining whether a license can be issued, the reviewer will confirm that the application identifies ITAAC for the I&C safety systems that reflect HA during each phase of the development process that is not completely reviewed in either the design certification (DC) or combined license (COL) review.

In the review of information associated with HA during each phase of the development process described in the application, the reviewer will consider hazard controls and commitments associated with life-cycle phases for I&C safety systems. Examples of such controls for contributory hazards are listed below, but this list is not exhaustive and is dependent on the specific design implementation.

1. I&C Requirements are analyzed for completeness. For example:

   A. I&C requirements should be correctly identified and translated into derived constraints on all system elements.

   B. I&C requirements should account for inter-relationships and interactions with the environment in all configurations and modes (including degraded ones), and changes from one to another.

   C. I&C requirements should include time-dependencies, relationships and constraints.

2. I&C requirements should be formulated to maintain the plant in a safe state.

3. I&C requirements and their dependencies with other I&C requirements should be identified, evaluated, and tracked.

4. Each requirement associated with a hazard should be traceable and subject to configuration control.

5. Methods to describe, represent, or specify architectures should support transformations or mappings across architectural descriptions, e.g., transformation from system conceptual or I&C requirements level to system design level to software design level to software implementation level to procedure or subroutine or function level.

6. Methods to describe, represent, or specify architectures should support transformations or mappings across dissimilar elements, e.g., interactions across hardware and software elements.

7. Methods to describe, represent, or specify architectures should support transformations or mappings across elements from different sources or suppliers.

Software ~~related~~ Related ~~contributory~~ Contributory ~~hazards~~ Hazards

The I&C safety software can contribute to hazards that could lead to the impairment or loss of system safety function. For example, the software may use non-deterministic tasks such as interrupts. The applicant may provide information associated with contributory hazards as the software is developed, and the reviewer should evaluate this information for adequacy during the review of the application. However, an applicant need only submit the information required by the regulation governing the content of the application. The adequacy of detailed information beyond the level of the FSAR will be verified in the context of ITAAC. The reviewer should confirm that the HA information includes the necessary controls for the various contributory hazards, including design and implementation constraints, and the associated commitments. The reviewer will confirm the application identifies the appropriate ITAAC for HA during software development that is not completely reviewed in determining whether a license can be issued.

In the review of information associated with HA during software development described in the application, the reviewer will consider hazard controls and commitments. Examples of such controls for contributory hazards are listed below, but this list is not exhaustive and is dependent on the specific software implementation.

1. The behavior of an element (e.g., a software unit) should be a composite of the behaviors of its constituent elements, with well-defined unambiguous rules of composition.

   A. Interfaces of elements are unambiguously specified, including behavior.

   B. Interactions across elements occur only through their specified interfaces, i.e., interactions adhere to principles of encapsulation.

2. The system should be modularized, and thereby avoid unnecessary interdependence.

3. Each element should be internally well-structured. For example:

   A. Each software unit that implements one or more safety functions uses well-defined coding rules and unambiguous coding design.

   B. Paths from inputs to outputs avoid unnecessary coupling.

4. The system design should favor simple approaches and avoid system behavior that increases complexity. For example:

A. Tasks should be executed in a deterministic manner.

B. Tasks in execution should run to completion.

C. Resources such as memory and processor execution time should be allocated statically.

5. Naming conventions and data dictionaries should be established for ease of comprehension and bidirectional traceability.

U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR B&W mPOWER™ SMR DESIGN

7.0 APPENDIX B INSTRUMENTATION AND CONTROLS - SYSTEM ARCHITECTURE

Introduction

The instrumentation and control (I&C) system architecture provides high-level definition of I&C systems, the assignment of I&C functions to these systems, and the communications between I&C systems. The implementation of the defense-in-depth concept for I&C is achieved mostly at the I&C architectural level. This section provides an approach to describe the I&C system architecture and identifies relevant information to assess the design's conformance to the defense-in-depth concept and the relevant regulations (e.g., Title 10 of the *Code of Federal Regulations*, Section 50.55a(h)). 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 design-specific review standard (DSRS) uses the term software to refer to such technology and complex logic.

DSRS Chapter 7 sections on the fundamental design principles discuss more specific areas of staff review that take into account the overall I&C architecture. In addition, the actual system development process typically includes, in part, its development life-cycle and the development of system architecture descriptions. The application should contain sufficient information on architecture, whether or not a specific platform or technology has been selected, to support the staff's determination of reasonable assurance of safety from the perspective of the fundamental design principles: independence, diversity and defense-in-depth (D3), redundancy, and predictability and repeatability.

Experience has shown that the review of an I&C system design that has a high degree of interconnectivity among computer-based equipment is quite challenging. Without the information related to the overall I&C system architecture, the review of the fundamental design principles may take on a more segmented review approach resulting in a less streamlined, more complicated, and more resource-intensive review effort.

Relevant Information to Support Consideration of I&C Architecture during Design Review

Clause Section 4 of the Institute of Electrical and Electronics Engineers, Inc. (IEEE) Standard (Std.) 603-1991 requires, in part, that a specific basis be established for the design of each safety system, including all system functions necessary to fulfill the system's safety intent. The architecture description provides a representation of the I&C system's properties, elements, functions, and the relationship among them. The architectural description should also contain the rationale, justification, or reasoning about architecture decisions that have been made, including potential consequences of such decisions.

The reviewer should consider the I&C system overall architecture in concert with the sections relating to the fundamental design principles. In addition, the reviewer should consider other sections of the DSRS that discuss the I&C system design basis, provide I&C system descriptions, and identify I&C system functions for consistency and additional information.

The reviewer, using engineering judgment that is corroborated in the review of each of the sections of this chapter, should verify that the application contained sufficient information at the architectural level to support a more streamlined review.

The staff should review, as a minimum, the following information, which the application should include:

1. ~~Description of the I&C system architecture~~. The architecture description should demonstrate that the architecture reflects the fundamental design principles of independence, redundancy, D3, and supports predictability and repeatability~~deterministic behavior~~. Regarding safety of the I&C system design, the application should provide sufficient information to demonstrate that the overall architecture proposed is sufficiently robust.
2. All I&C functions that are part of the design basis.
3. Diagrams of the overall architecture.
4. Description of systems necessary to support the defense-in-depth concept of the plant, which provides layers of defensive capabilities to mitigate or prevent potential hazards, including the following:

    A. The I&C systems, including their classification, technologies, boundaries, and interfaces with other systems.

    B. End-to-end signal flows and their descriptions (e.g., signal flow paths from sensor input through signal conditioning, data processing, voting, and actuation).

    C. Key functional blocks that make up the I&C architecture, through which the data (plant process information or command signals) are transmitted and their descriptions.

    D. Simplified logic diagrams.

    E. Signal processing block diagrams and their descriptions.

    F. When a vendor's design includes a prioritization scheme that is used to signal selections, the priority functions, diagrams, and their descriptions.

    G. Interfaces and comparisons of electrical and I&C diagrams.

    H. Specific constraints identified in the I&C design resulting from the general plant safety approach that could affect compliance with regulatory requirements (e.g.,

if plant system(s) specifically addressed in regulations or guidance are used in a different manner, or not used at all, in the reactor design due to the general plant safety approach, those differences and their impact on the overall I&C design should be identified).

U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR B&W mPOWER™ SMR DESIGN

7.0 APPENDIX C INSTRUMENTATION AND CONTROLS – SIMPLICITY

Introduction

Simplicity is considered to be a cross-cutting attribute~~principle~~ that affects the fundamental design principles. For safety instrumentation and control (I&C) systems, designers and regulators are faced with the question of what measures should be in place in order to maintain ~~other~~ design principles such as independence, diversity and defense-in-depth (D3), redundancy, and predictability and repeatability~~and defense-in-depth~~ with reasonable confidence. At a generic level, it is difficult to define and control simplicity/complexity for digital safety I&C systems. When faced with several design options on how to implement a function, from a safety perspective, the more simple design options are those that accomplish the function and address potential hazards with the most confidence and clarity. Additional guidance on hazards is contained in Appendix A, "Hazard Analysis."

This appendix provides an approach to evaluate whether simplicity[7] has been considered in the design of the digital I&C system. Although, there are no specific regulations, standards, or guidance to address the aspect of simplicity for digital I&C systems, recent experience in reviews of light-water reactor applications has shown that complex I&C systems challenge the demonstration of conformance with safety system design criteria such as independence. In this context, the U.S. Nuclear Regulatory Commission (NRC) considers simplicity as supporting all fundamental design principles for developing safety systems with high reliability. The application should contain sufficient information on the simplicity of the design to support the staff's determination of reasonable assurance of safety from the perspective of the fundamental design principles: independence, ~~diversity and defense-in-depth (~~D3~~)~~, redundancy, and predictability and repeatability. The reviewer should verify that the approach described in the application addresses specific effects of simplicity such as testability or proof-of-determinism.

Without the information related to the simplicity of the I&C system, the review of the fundamental design principles may take on a more segmented review approach resulting in a less streamlined, more complicated, and more resource-intensive review effort.

[7] On October 14, 2008, in Volume 73 of the Federal Register (FR), pages 60612-60616 (73 FR 60612-60616), the Commission issued a policy statement on the regulation of advanced reactors [NRC-2008-0237].

Relevant Information to Support Consideration of Simplicity during Design Review

The application should provide sufficient information to demonstrate that the design of the I&C systems has considered simplicity both in the functionality of the system~~, as well as,~~and in its implementation. With this information, the reviewer should confirm that simplicity attributes (e.g., single function, fixed number of inputs and outputs, fewer configuration parameters, high testability, software architecture with no branching and minimal interrupts) are considered and incorporated in the design. These attributes help contribute to simplicity and enable high efficiency in the design. 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 following areas related to the design of a plant's I&C systems should be considered in order to demonstrate that such systems meet the fundamental design concept~~principle~~ of simplicity:

1. I&C system architecture
~~2. Hazards analysis~~
~~3.~~2. Independence
~~4.~~3. Redundancy
~~5.~~4. Predictability and Repeatability
~~6.~~5. D3

The staff should consider whether: (1) the I&C design is as simple as practical, and (2) that any added complexity does not diminish the design's conformance to the fundamental design principles. For those areas that exhibit complexity, the application should provide a full description regarding any complexity added to the I&C system design~~,~~ as well as~~,~~ a justification necessary to directly support the safety function. More complex design alternatives require a more ~~resource~~ resource ~~-~~intensive review by the staff and could potentially lengthen the review.

The reviewer should consider the following items in evaluating simplicity in an I&C system design:

1. This review is concurrent with the other fundamental design principles of redundancy, independence, ~~diversity~~D3, and predictability and repeatability contained in Section 7.1.

2. I&C System Architecture: The I&C architecture information described in Appendix B of Chapter 7 should be carefully considered to determine if the I&C design includes unnecessary or nonessential features that are not part of the safety function. The reviewer should also consider the following:

   A. The application should provide a top-down decomposition of the I&C system. This decomposition facilitates a logical, modular description of interactions, signal flows, helps with the definition of interfaces, and allows a more effective review.

   B. The selected architecture should provide a demonstration of a balance between simplicity in concept and the capacity to satisfy regulatory and performance

requirements. This includes predictable and repeatable~~deterministic~~ behavior, independence, and redundancy.

C. A safety benefit should be independently verifiable and should outweigh any concerns associated with the complexity it may introduce in the design.

D. Digital I&C system ~~and software~~ components should be organized in a manner that promotes design simplicity.

E. After reviewing information related to the I&C system's architecture, the reviewer should consider whether:

i. A structured and modular architecture is applied.

ii. The I&C systems, including hardware and software ~~elements~~, ~~all relationships~~interfaces among them~~, as well as properties of both~~, are fully described and address relevant requirements.

3. Independence: Material from the independence section may be used by the reviewer to identify how simplicity is addressed in the design while considering Institute for Electrical and Electronics Engineers, Inc. (IEEE) Standard (Std.) 603-1991. Specifically, the reviewer should consider the following:

A. Whether inter-channel communications or communications between a safety and a nonsafety system exist in this design.

B. ~~Whether simplicity is implemented to reduce or eliminate inter-divisional communication,~~ or whether physical uni-directional communication in function processing and critical signal paths is implemented~~or implemented physical uni-directional communication in function processing and critical signal paths~~.

C. Whether the design maintains separation or segregation among I&C functions within the circuitry, as it enhances simplicity, verifiability and testability of individual functions.

D. The reviewer should consider whether the application proposed simple design options in the approach to address IEEE Std. 603-1991. The following design attributes support this approach:

i. There is adequate separation or segregation among I&C functions.

ii. There are no unnecessary inter-channel communications.

iii. There are no unnecessary communications between a safety and a nonsafety system.

4. Redundancy: Material from the redundancy section may be used by the reviewer to identify how the design achieved redundancy and avoided unnecessary complexity. Specifically, the reviewer may consider the following areas that could help identify unnecessary complexity:

   A. Ancillary, more complex functions are kept independent of the primary I&C safety functions.

   B. The design provides simple connections between redundant trains.

   C. The proposed design does not ~~consider~~ use unnecessary inter-channel communications.

   D. There are no unnecessary communications between a safety and a nonsafety system.

   E. Through the review of redundancy, the reviewer may:

      i. Consider whether simplicity is factored in the design, particularly for the primary I&C functions.

      ii. Consider whether complex functions are kept independent of the primary I&C safety functions.

5. Predictability and Repeatability: Material from the predictability and repeatability section may be used by the reviewer to identify how simplicity is addressed to demonstrate deterministic behavior. Specifically, the reviewer may consider the following:

   A. Simple algorithms are considered in the design of system modules. In general, simplicity should not be sacrificed to achieve performance that is not required.

   B. I&C systems are designed using a finite state machine approach with all states well-defined.

   C. Through the review of predictability and repeatability, the reviewer may:

      i. Consider whether nonsafety features are segregated from the main safety signal path.

      ii. Consider whether there are interrupt functions that could interfere with the performance of the safety function.

      iii. Consider whether early detection of failures is facilitated by the self-diagnostic functions.

6. D3: Simplicity of a software structure is promoted through simple logic, cyclical execution, static resource usage, and avoidance of external interrupts. Material from the D3 section may be used by the reviewer to identify how simplicity is addressed to demonstrate diversity. Specifically, the reviewer may consider the following:

   A. How potential common-cause failures are addressed and how simplicity is considered to address failures.

   B. If basic software and application software are separated, and if it is implemented in a high level programming language.

   C. If basic software performs only the minimal necessary functions, such as initialization, periodic execution of required functions, and error handling.

   D. If application software is described in a graphically symbolized manner, so that functions can be easily understood, verified and validated.

   E. If the design is proposing dynamic allocation of memory.

   ~~F. Through the review of D3, the reviewer may:~~

      ~~i. Consider whether basic software and application software are separated.~~

      ~~ii. Consider whether basic software is implemented in a high level programming language.~~

      ~~iii. Consider whether basic software performs only the minimal necessary functions, such as initialization, periodic execution of required functions, and error handling.~~

      ~~iv. Consider whether application software is described in a graphically symbolized manner, so that functions can be easily understood, verified and validated.~~

      ~~v. Consider whether there is dynamic allocation of memory.~~

7. The following are examples of possible impact to the existing system resulting from added features that could introduce unnecessary complexity to the I&C design and should also be carefully considered:

   A. Features added that could introduce interrupts to the critical safety system performance.

B. Features added to cope with particular types of hazards that could negatively impact other safety design features. An example includes the introduction of cyber security protective features within the safety system as these could impact matters such as safety time response if not carefully integrated.

C. Provisions for troubleshooting and maintenance, including built-in self-test features, and external testing of circuit boards if necessary. Consider accessibility of test points, need for special test equipment, and coverage of built-in self-testing and diagnostics.

U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR B&W mPOWER^{TM} SMR DESIGN

7.0 APPENDIX D INSTRUMENTATION AND CONTROLS - REFERENCES

1. ANSI/ASME NQA-1-2008, “Quality Assurance Program Requirements for Nuclear Facilities.”

2. ANSI/ASME NQA-1a-2009 Addenda, “Addenda to ANSI/ASME NQA-1-2008, Quality Assurance Program Requirements for Nuclear Facilities.”

3. GL 85-06, “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-related,” April 16, 1986.

4. GL 91-04, “Guidance on Preparation of a Licensee Amendment Request for Changes in Surveillance Intervals to Accommodate a 24 Month Fuel Cycle,” April 2, 1991.

5. IEEE Std. 1008, “IEEE Standard for Software Unit Testing.”

6. IEEE Std. 1012, “IEEE Standard for Software Verification and Validation.”

7. IEEE Std. 1028, “IEEE Standard for Software Reviews.”

~~8. IEEE Std. 1042, “IEEE Standard for Software Reviews, IEEE Guide to Software Configuration Management.”~~

~~9.~~8. IEEE Std. 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations.”

~~10.~~9. IEEE Std. 323, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.”

~~11.~~10. IEEE Std. 338, “Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems.”

~~12.~~11. IEEE Std. 379, “Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems~~,~~.”

~~13.~~12. IEEE Std. 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.”

~~14.~~13. IEEE Std. 497, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations.”

~~15.~~14. IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” including the correction sheet, dated January 30, 1995.

~~16.~~15. IEEE Std. 730, “IEEE Standard for Software Quality Assurance Plans.”

~~17.~~16. IEEE Std. 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

~~18.~~17. IEEE Std. 828, “IEEE Standard for Software Configuration Management Plans.”

~~19.~~18. IEEE Std. 829, “IEEE Standard for Software Test Documentation.”

~~20.~~19. IEEE Std. 830, “IEEE Recommended Practice for Software Requirements Specifications.”

~~21.~~20. ANSI/ISA-67.02.01, “Nuclear Safety-related Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants.”

~~22.~~21. NUREG/CR-6082, “Data Communications,” August 1993.

~~23.~~22. NUREG/CR-6303, “Method for Performing Diversity and Defense in Depth Analyses of Reactor Protection Systems,” 1994.

~~24.~~23. NUREG-0700, “Human System Interface Design Review Guidelines,” May 2002.

~~25.~~24. NUREG-0711, “Human Factors Engineering Program Review Model.”

~~26.~~25. NUREG-0737, “Clarification of TMI Action Plan Requirements,” 1982.

~~27.~~26. NUREG-0737, Supplement 1, “Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability,” 1983.

~~28.~~27. NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition,” 2007.

~~29.~~28. NUREG-0933, “Resolution of Generic Safety Issues (Formerly entitled "A Prioritization of Generic Safety Issues"),” December 2011.

~~30.~~29. RG 1.105, “Setpoints for Safety-related Instrumentation.”

~~31.~~30. RG 1.118, “Periodic Testing of Electric Power and Protection Systems.”

~~32.~~31. RG 1.151, “Instrument Sensing Lines.”

~~33.~~32. RG 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants.”

~~34.~~33. RG 1.168, “Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

~~35.~~34. RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

~~36.~~35. RG 1.170, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

~~37.~~36. RG 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

37. RG 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

38. RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

39. RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio Frequency Interference in Safety-related Instrumentation and Control Systems.”

40. RG 1.189, “Fire Protection for Operating Nuclear Power Plants.”

41. RG 1.204, “Guidelines for Lightning Protection of Nuclear Power Plants.”

42. RG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants.”

43. RG 1.22, “Periodic Testing of Protection System Actuation Functions.”

44. RG 1.28, “Quality Assurance Program Requirements (Design and Construction).”

45. RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems.”

46. RG 1.53, “Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems.”

47. RG 1.62, “Manual Initiation of Protection Action.”

48. RG 1.75, “Criteria for Independence of Electrical Safety Systems.”

49. RG 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants.”

50. RIS 2006-17, “NRC Staff Position on the Requirements of 10 CFR 50.36, A Technical Specifications,' Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels,” August 24, 2006.

51. SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs,” April 2, 1993.

52. SRM SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs,” July 21, 1993.

53. SECY-95-132, “Policy and Technical Issues Associated with The Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs (SECY-94-084).”

~~53. SECY-94-084, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-safety Systems in Passive Plant Designs,” dated March 28, 1994 (ML003708068)~~

54. SECY-11-0024, “Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews,” February 18, 2011.

55. SRM-COMGBJ-10-0004/COMGEA-10-0001, “Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews,” August 31, 2010.