U. S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR mPower™ iPWR DESIGN

7.2 INSTRUMENTATION AND CONTROLS – SYSTEM CHARACTERISTICS

REVIEW RESPONSIBILITIES

Primary—Organization responsible for the review of I&C

Secondary—None

This design-specific review standard (DSRS) Section provides guidance associated with instrumentation and control (I&C) safety system characteristics contained in Sections 5, 6, and 7 of Institute of Electrical and Electronics Engineers, Inc. (IEEE) 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[1] 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.

[1] 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 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.

ADAMS Accession No. ML12314A201

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 non-safety related systems, the reviewer will verify that the application describes how the quality measures applied to I&C systems that are not safety 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, General Design Criterion (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 set forth below. The DSRS is not a substitute for the NRC's regulations, and compliance with it is not required. Identifying the differences between this DSRS section and the design features, analytical techniques, and procedural measures proposed for the facility, and discussing how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria, is sufficient to meet the requirements in 10 CFR 52.47(a)(9), "Contents of applications; technical information." The same approach may be used to meet the requirements of 10 CFR 52.79(a)(41) for COL applications.

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, "IEEE Standard for Software Verification and Validation," and IEEE Std. 1028-1997, "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, 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, 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, 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, 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.

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 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.

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 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 lifecycle 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 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 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.

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.

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.
vi. The software design should demonstrate adequate coverage of all software requirements and should not contain any unnecessary functions.
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.
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, 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.
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 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

i. An operations 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 operations 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 operations 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 operations 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 operations 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

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.
iii. 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.
iv. 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.
v. Configuration management and control activities should be conducted to document any proposed or actual changes to the I&C safety system.

M. I&C System Retirement

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 Clause 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 Clause 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 Clause 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, Clause 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 cycle. IEEE Std. 7-4.3.2, Clause 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 (V&V) 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, Clauses 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, Clause 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 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 SRP 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. 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 mPower^{TM}-specific DC, or COL, 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 mPower^{TM} 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 SMR reviews including the associated pre-application activities, the staff has developed the content of this DSRS section as an alternative method for evaluation of an mPower^{TM} -specific DC application submitted pursuant to 10 CFR Part 52 to comply with 10 CFR 52.47(a)(9), “Contents of applications; technical information.”

This regulation states, in part, that the application must contain "an evaluation of the standard plant design against the 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 10 CFR 52.47(a)(9) as long as the mPower^{TM} design control document (DCD) FSAR does not deviate significantly from the design assumptions made by the NRC staff while preparing this DSRS section. 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 by 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.

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 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, App. 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 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

   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 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 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 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, App. 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^{TM} 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 Clauses 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 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 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 and software failures 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 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 Clause 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 Section 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 Clauses 5.15, 5.5, and 5.2 of IEEE Std. 7-4.3.2, and the requirements of Section 5.15, 5.5, 5.2 and 7.3 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower^{TM} 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 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 Section 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 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 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^{TM} 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 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 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 nonsafety loop, such as within each subsystem of the component cooling water system, an interlock should be provided to automatically isolate the safety loop from nonsafety 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^{TM} 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 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 meet the requirements of 10 CFR 50.36. Additional information related to setpoint technical specifications 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, GDC 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^{TM} 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, 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 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 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 descriptions 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 Clauses 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 Section 5.9, 5.11, and 5.10 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 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 failure criteria contained in IEEE Std. 379, “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 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 and the requirements of Section 5.13 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower^{TM} 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 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^{TM} 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 (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 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 Clauses 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 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 provides additional guidance on conformance with this requirement.

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

   The reviewer should confirm that AFW 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^{TM} 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^{TM} 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. 10 CFR 50.34(f)(2)(xxii) requires perform 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 Clauses 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. 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. 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." 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. 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 failure criterion. Any failure that is not detectable must be considered concurrently with any random postulated, detectable, single failure. Guidance on the 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 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 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 Clauses 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 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 reference RTD to laboratory calibration 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 Clauses 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.

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.