U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

APPENDIX 7.1-C GUIDANCE FOR EVALUATION OF CONFORMANCE TO IEEE Std 603

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

Review Note: The revision numbers of Regulatory Guides (RG) and the years of endorsed industry standards referenced in this Standard Review Plan (SRP) section are centrally maintained in SRP Section 7.1-T (Table 7-1). Therefore, the individual revision numbers of RGs (except RG 1.97) and years of endorsed industry standards are not shown in this section. References to industry standards incorporated by reference into regulation (IEEE Std 279-1971 and IEEE Std 603-1991) and industry standards that are not endorsed by the agency do include the associated year in this section. See Table 7-1 to ensure that the appropriate RGs and endorsed industry standards are used for the review.

1. AREAS OF REVIEW

For nuclear plants with construction permits issued before January 1, 1971, Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h), “Protection and Safety Systems,” requires that

protection systems must be consistent with their licensing basis or may meet the requirements of
the Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999, 10 CFR 50.55a(h) requires that protection systems must meet the requirements stated in either IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Applications filed on or after May 13, 1999 for design approvals, design certifications, construction permits, operating licenses, and combined licenses (COL) that do not reference a final design approval or DC, must meet the requirements for safety systems in IEEE Std 603-1991 and the correction sheet dated January 30, 1995 Although required by U.S. Nuclear Regulatory Commission (NRC) regulations only for safety systems, the criteria of IEEE Std 603-1991 address considerations such as design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and test may be used as review guidance, where appropriate, for any instrumentation and control (I&C) system, as elaborated in SRP Sections 7.2 through 7.9. Therefore, for I&C systems that are not a part of a safety system, but having a high degree of importance to safety, the reviewer may use the concepts in IEEE Std 603-1991 as a starting point for the review of these systems.

This appendix discusses the guidance of IEEE Std 603-1991 as it is used in the review of safety systems to determine that these systems meet NRC regulations. This appendix is not a stand-alone discussion of IEEE Std 603-1991. Each subsection of this appendix relates directly to one or more clauses of IEEE Std 603-1991.

SRP Appendix 7.1-B contains guidance on the application of the requirements of IEEE Std 279-1971.

IEEE Std 603-1991 does not directly discuss digital computer-based systems. RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," provides guidance on applying the safety system criteria to digital computer-based systems. Applications involving digital computer-based safety systems should be reviewed using SRP Appendix 7.1-D.

Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC). For DC and COL reviews, the staff reviews the applicant's proposed ITAAC associated with the structures, systems, and components (SSCs) related to this SRP section in accordance with SRP Section 14.3, "Inspections, Tests, Analyses, and Acceptance Criteria." The staff recognizes that the review of ITAAC cannot be completed until after the rest of this portion of the application has been reviewed against acceptance criteria contained in this SRP section. Furthermore, the staff reviews the ITAAC to ensure that all SSCs in this area of review are identified and addressed as appropriate in accordance with SRP Section 14.3.

COL Action Items and Certification Requirements and Restrictions. For a DC application, the review will also address COL action items and requirements and restrictions (e.g., interface requirements and site parameters).

For a COL application referencing a DC, a COL applicant must address COL action items (referred to as COL license information in certain DCs) included in the referenced DC.

Additionally, a COL applicant must address requirements and restrictions (e.g., interface requirements and site parameters) included in the referenced DC.

2. SCOPE

The scope of IEEE Std 603-1991 includes all I&C safety systems, which are the systems covered in Sections 7.2 through 7.6 of the safety analysis report (SAR). Except for the requirements for independence between control systems and safety systems, IEEE Std 603-1991 does not directly apply to the nonsafety systems such as the control systems and diverse I&C systems described in SAR Sections 7.7 and 7.8, respectively. Although intended only for safety systems, the criteria for IEEE Std 603-1991 are applicable to any I&C system. Therefore, for nonsafety I&C systems that have a high-degree of importance to safety, the reviewer may use the concepts of IEEE Std 603-1991 for the review of these systems. Applicable considerations include design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing. Digital data communications systems as described in SRP Section 7.9 are support systems for other I&C systems. As such, they inherit the applicable requirements and guidance that apply to the supported systems. Consequently, the guidance of IEEE Std 603-1991 is directly applicable to those parts of data communications systems that support safety system functions.

An I&C review of safety systems that follows the guidance of IEEE Std. 603-1991 should be coordinated with other organizations as appropriate to address the following considerations:

- Many of the auxiliary supporting features and other auxiliary features defined in IEEE Std 603-1991 are described in Chapters 4, 5, 6, 8, 9, 10, 12, 15, 18, and 19 of the SAR. I&C reviewers should coordinate with the reviewers of these sections to ensure auxiliary supporting features and other auxiliary features are appropriately addressed by the review.

- The site characteristics, systems (both physical and administrative), and analyses described in the other sections of the SAR may impose requirements on the I&C systems. The I&C reviewers should coordinate with the reviewers of these sections to ensure that the I&C systems appropriately address these requirements.

- I&C systems may impose requirements upon other plant systems and analyses. I&C reviewers should coordinate with the reviewers of the affected systems to ensure that the reviewers are aware of these requirements.

- Other plant systems will impose requirements on the I&C systems. The I&C reviewers should coordinate with the reviewers of the interfacing systems to ensure that these requirements are considered in the review.

IEEE Std 603-1991 provides the following operational elements as examples of auxiliary supporting features and other auxiliary features: Room Temperature Sensors, Component Temperature Sensors, Pressure Switches and Regulators, Potential Transformers, Undervoltage Relays, Diesel Start Logic and Load Sequencing Logic, Limit Switches, Control Circuitry, Heating Ventilation and Air Conditioning Fans and Filters, Lube Pumps, Component Cooling Pumps, Breakers, Starters, and Motors, Diesel Start Solenoid, Crank Motors, Air Compressors and Receivers, Batteries, Diesel Generators, Invertors, Transformers, Electric Buses, and Distribution Panels. Figure 3, “Examples of Equipment Fitted to Safety System Scope Diagram,” of IEEE Std 603-1991 provides a matrix with an extensive list of auxiliary supporting features and other auxiliary features.

IEEE Std 603-1991, Appendix A, “Illustration of Some Basic Concepts for Developing the Scope of a Safety System,” also provides examples of the elements of a safety system needed to achieve a safety function.

The coordination review needed for each I&C system is discussed in Subsection 5 of SRP Section 7.0.

3. DEFINITIONS

This SRP appendix does not provide any additional definitions other than those provided in IEEE Std 603-1991.

4. SAFETY SYSTEM DESIGNATION (IEEE Std 603-1991, Clause 4)

Clause 4 of IEEE Std 603-1991 requires in part that a specific basis be established for the design of each safety system. The design basis should be reviewed to confirm that it has the following characteristics:

- Completeness - The design basis should address all system functions necessary to fulfill the system's safety intent. For safety systems, the design basis should be shown to address the requirements of 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities,” Appendix A, “General Design Criteria for Nuclear Power Plants,” General Design Criterion (GDC) 20, “Protection System Functions.” Information provided for each design basis item should be sufficient to enable the detailed design of the I&C system to be carried out. All functional requirements for the I&C system and the operational environment for the I&C system should be described. As a minimum, each of the design basis aspects identified in IEEE Std 603-1991, Clauses 4.1 through 4.12 should be addressed.

- Consistency - The information provided in the design basis should be analyzed to demonstrate its consistency with the plant safety analysis, including the design basis event analysis of Chapter 15 of the SAR; the mechanical and electrical system designs; and other plant system designs.

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

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

- Unambiguity - The information provided for the design basis items, taken alone and in combination, should have one and only one interpretation.

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

In addition to these characteristics, the following should be noted about the parts of IEEE Std 603-1991, Clause 4.

Clause 4.1 of IEEE Std 603-1991 requires in part the identification of the design basis events applicable to each mode of operation. This information should be consistent with the analysis provided in Chapter 15 of the SAR. SRP branch technical position (BTP) 7-4 provides specific guidance on the failures and malfunctions that should be considered in identification of design basis-events for systems that initiate and control auxiliary feedwater systems. SRP BTP 7-5 provides specific guidance on the reactivity control malfunctions that should be considered in the identification of design-basis events. The malfunctions assumed should be consistent with the control system failure modes described in Section 7.7 of the SAR and the reactivity control interlock functions described in Section 7.6 of the SAR.

Clause 4.4 of IEEE Std 603-1991 requires in part the identification of variables that are monitored in order to provide protective action. The tables in Sections 7.2 and 7.3 of the SAR should provide this information. Performance requirements - including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action - should also be identified in the system designation. The applicant's or licensee's analysis, including the applicable portion provided in Chapter 15, should confirm that the system performance requirements are adequate to ensure completion of protective actions. Clause 4.4 also requires in part the identification of the analytical limit associated with each variable. Review considerations in confirming that an adequate margin exists between analytical limits and setpoints are discussed in Subsection 6.8 below.

Clause 4.5 of IEEE Std 603-1991 describes the minimum criteria under which manual initiation and control of protective actions may be allowed. SRP BTP 7-6 provides specific guidance on determination if the timing margins for changeover from injection to recirculation mode are sufficient to allow manual initiation of the transition.

Clause 4.6 of IEEE Std 603-1991 requires in part the identification of the minimum number and location of sensors for those variables in Clause 4.4 of IEEE Std 603-1991 that have a spatial dependence. The applicant's or licensee's analysis should demonstrate that the number and location of sensors are adequate. Subsection 5.1 below discusses the consideration of the single failure criterion in the evaluation of this analysis.

Clause 4.7 of IEEE Std 603-1991 requires in part that the range of transient and steady-state conditions be identified for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. This information is used in subsequent evaluations.

Clause 4.8 of IEEE Std 603-1991 requires in part the identification of conditions having the potential for causing functional degradation of safety system performance, and for which provisions must be incorporated to retain necessary protective action. This information is used in subsequent evaluations, with special attention given to Clause 5.4 of IEEE Std 603-1991.

Clause 4.9 of IEEE Std 603-1991 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design, and the identification of the methods used to verify that any qualitative or quantitative reliability goals imposed on the system design have been met. The staff's acceptance of system reliability is based on deterministic criteria described in IEEE Std 603-1991 and IEEE Std 7-4.3.2, rather than on quantitative reliability goals. Therefore, the system design basis should discuss the methods used to confirm that these deterministic criteria have been met.

The NRC staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the NRC's regulations for reliability of safety systems. 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 I&C system.

For safety systems that include digital computers, both hardware and software reliability should be considered. Software failures that are not the consequence of hardware failures are caused by design errors and, therefore, do not follow the random failure behavior used for hardware reliability analysis. Consequently, different methodologies may need to be used to assess the unreliability introduced by hardware and by software. For example, reliability of hardware components might be demonstrated by an evaluation of system redundancy and quantitative reliability modeling. Reliability of software might be demonstrated by evaluation of the development process combined with testing under a wide range of input conditions.

5. SAFETY SYSTEM CRITERIA (IEEE Std 603-1991, Clause 5)

Clause 5 of IEEE Std 603-1991 requires that the safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established by design-basis events. The applicant's or licensee's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met. The evaluation should confirm that the general functional requirements have been appropriately allocated to the various system components. The I&C review in this regard should confirm that the system design fulfills the system design-basis requirements established. Confirming the adequacy of system design-basis requirements and verifying that the system meets these requirements will normally be a substantial portion of the I&C review.

The subsections of Section 5, and Sections 6, 7, and 8 (discussed below) deal with specific guidance that safety systems should meet as part of fulfilling the design-basis requirements. Most of these items identify deterministic criteria that, if met, will normally provide the level of reliability needed for safety systems. These criteria may be relevant for both individual system elements, as well as the system as a whole.

5.1 Single-Failure Criterion (IEEE Std 603-1991, Clause 5.1)

This subsection requires that any single failure within the safety system shall not prevent proper protective action at the system level when required. The applicant or licensee's analysis should confirm that the requirements of the single-failure criterion are satisfied. Guidance in the application of the single-failure criterion is provided in RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," which endorses IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

Where it is determined that the spatial dependence of a parameter requires several sensor channels to ensure plant protection, the redundancy requirements are determined for the individual case. In certain designs, for example, adequate monitoring of core power requires a minimum number of sensors arranged in a given configuration to provide adequate protection. This aspect of redundancy is dealt with in coordination with the organization responsible for reviewing reactor designs to establish redundancy requirements.

Components and systems not qualified for seismic events or accident environments and nonsafety-grade components and systems are assumed to fail to function if failure adversely affects safety system performance. These components and systems are assumed to function if functioning adversely affects safety system performance. All failures in the safety system that can be predicted as a result of an event for which the safety system is designed to provide a protective function are assumed to occur if the failure adversely affects the safety system

performance. In general, the lack of equipment qualification may serve as a basis for the assumption of certain failures. After assuming the failures of nonsafety-grade, non-qualified equipment and those failures caused by a specific event, a random single failure is arbitrarily assumed. With these failures assumed, the safety system must be capable of performing the protective functions required to mitigate the consequences of the specific event.

Digital computer-based I&C systems share data, data transmission, functions, and process equipment to a greater degree than analog systems. Although this sharing forms the basis for many of the advantages of digital systems, it also raises a key concern with respect to I&C system vulnerability to a different type of failure. The concern is that a design using shared databases and process equipment has the potential to propagate a common-cause failure of redundant equipment. Another concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the NRC staff has placed significant emphasis on defense-in-depth against common-cause failures within and between functions. The principle of defense-in-depth is to provide several levels or echelons of defense to challenges to plant safety, such that failures in equipment and human errors will not result in an undue threat to public safety.

A detailed diversity and defense-in-depth study should address common-cause failures in digital computer-based systems. The NRC's position for providing defense against common-cause failures in digital I&C systems for future light-water reactors is given in the Staff Requirements Memorandum (SRM) on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," (specifically in Point 18: II Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems"). SRP BTP 7-19 provides guidance for addressing the potential of common-cause failures.

5.2 Completion of Protective Action (IEEE Std 603-1991, Clause 5.2)

The staff's review of this item should include review of functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion.

5.3 Quality (IEEE Std 603-1991, Clause 5.3)

The applicant or licensee should confirm that quality assurance provisions of 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to are applicable to the safety system. The evaluation of the adequacy of the quality assurance program is addressed in the review of Chapter 17 of the SAR.

For digital computer-based systems, the applicant or licensee should address the quality requirements described in Clause 5.3 of IEEE Std 7-4.3.2. Additional guidance is provided in SRP Appendix 7.1-D, Subsection 5.3.

5.4 Equipment Qualification (IEEE Std 603-1991, Clause 5.4)

The applicant or licensee should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located, as identified by Clauses 4.7 and 4.8 of IEEE Std 603-1991.

I&C reviews mild environment qualification and electromagnetic interference (EMI) qualification of safety system I&C equipment, and consults with other organizations to confirm qualification for harsh environments and seismic loads. The review of harsh environment qualification is coordinated with the organization responsible for reviewing electrical systems. The review of

seismic qualification is coordinated with the organization responsible for the review of seismic designs.

RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," provides guidance for mild environment qualification. Additionally, the applicant or licensee should confirm that a single failure within the environmental control system, for any area in which safety system equipment is located, will not result in conditions that could result in damage to the safety system equipment, nor 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 is treated as a single failure that should not prevent the safety system from accomplishing its safety functions.

Because the loss of environmental control systems does not usually result in prompt changes in environmental conditions, the design-bases may rely upon monitoring environmental conditions and taking appropriate action to ensure that extremes in environmental conditions are maintained within non-damage limits until the environmental control systems are returned to normal operation. If such bases are used, the applicant or licensee should confirm that there is independence between environmental control systems and sensing systems that would indicate the failure or malfunctioning of environmental control systems.

Review of mild environment qualification should also include confirmation that the environmental protection of instrument sensing lines conforms to the guidance of RG 1.151, "Instrument Sensing Lines."

EMI qualification in accordance with the guidance of RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," is an acceptable means of meeting the qualification requirements for EMI and electrostatic discharge.

Lightning protection should be addressed as part of the review of electromagnetic compatibility. Lightning protection features should conform to the guidance of RG 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants."

The organizations responsible for the review of equipment qualification to harsh environments and seismic events will perform the evaluation of conformance to the requirements of General Design Criterion 2, "Design Bases for Protection Against Natural Phenomena," General Design Criterion 4, " Environmental and Dynamic Effects Design Bases," and 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important To Safety For Nuclear Power Plants," to ensure the requirements for equipment qualification to harsh environments and seismic events are met. Guidance for the review of this equipment qualification is given in SRP Sections 3.10 and 3.11.

SRP Appendix 7.1-D, Subsection 5.4 provides additional guidance on environmental qualification of digital computers for use in safety systems.

5.5 System Integrity (IEEE Std 603-1991, Clause 5.5)

Information provided in Clauses 4.7 and 4.8 of IEEE Std 603-1991 is reviewed to confirm that the design includes the qualification of equipment for the conditions identified in the design-bases. Failures may not be credited to protect the integrity of other equipment. The review should confirm that tests have been conducted on safety system equipment components and the system racks and panels as a whole to demonstrate that the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady-

state conditions of both the energy supply and the environment. Where tests have not been conducted, the applicant or licensee should confirm that the safety system components are conservatively designed to operate over the range of service conditions.

A special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the critical points of time identified as required by Clause 4.10 of IEEE Std 603-1991. SRP BTP 7-21 provides supplemental guidance on evaluating response time for digital computer-based systems, and discusses design constraints that allow greater confidence in the results analyses or prototype testing to determine real-time performance.

IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," indicates that design for computer system integrity and design for test and calibration should be addressed as part of safety system integrity. Evaluation of computer system hardware integrity should be included in the evaluation against the requirements of IEEE Std 603-1991. Computer system software integrity (including the effects of hardware-software interaction) should be demonstrated by the applicant's or licensee's software safety analysis activities. Subsection B3.1.9 of SRP BTP 7-14 describes the acceptable characteristics of software safety plans. Subsection B3.2.1 of SRP BTP 7-14 describes the characteristics of acceptable software safety analyses.

Evaluation of computer system design for test and calibration is covered in subsection 5.7 below.

The review of system integrity should confirm that the design provides for 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 energy, or adverse environments, are experienced. This aspect is typically evaluated through evaluation of the applicant's or licensee's failure modes and effects analysis. The analysis should justify the acceptability of each failure effect. Reactor trip system (RTS) functions should typically fail in the tripped state. Engineered safety feature actuation system (ESFAS) functions should fail to a predefined safe state. For many ESFAS functions this predefined safe state will be that the actuated component remains as-is.

Computer-based safety systems should, upon detection of inoperable input instruments, 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), unless the operator has already placed the affected channel in a bypass mode (this would change a two-out-of-four logic to a two-out-of-three logic). Hardware or software failures detected by self-diagnostics should also place a protective function into a safe state or leave the protective function in an existing safe state. Failure of computer system hardware or software should not inhibit manual initiation of protective functions or the operator performance of preplanned emergency or recovery actions. During either partial or full system initialization or shutdown after a loss of power, control output to the safety system actuators should fail to a predefined, preferred failure state. A system restart upon restoration of power should not automatically transfer the actuators out of the predefined failure state. Changes to the state of plant equipment from the predefined state following restart and re-initialization (other than changes in response to valid safety system signals) should be under the control of the operator in accordance with appropriate plant procedures.

5.6 <u>Independence</u> (IEEE Std 603-1991, Clause 5.6)

This subsection requires in part independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design-basis events, and (3) safety systems and

other systems. Three aspects of independence should be addressed in each case:

- Physical independence
- Electrical independence
- Communications independence

Guidance for evaluation of physical and electrical independence is provided in RG 1.75, "Criteria for Independence of Electrical Safety Systems," which endorses IEEE Std 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The applicant or licensee should confirm that the safety system design precludes the use of components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features which could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. The organization responsible for the review of electrical systems reviews power source requirements. I&C reviewers should coordinate with the electrical systems reviewers to confirm that I&C safety system power sources are adequate. Transmission of signals between independent channels should be through isolation devices.

SRP BTP 7-11 provides guidance for the application and qualification of isolation devices.

SRP Appendix 7.0-A and SRP Section 7.9 provide guidance on communications independence. The review of communications independence should include confirmation that the routing of signals related to safety maintains (1) proper channeling through the communications systems, and (2) proper data isolation between redundant channels or alternatively, some form of data communications such that data from one channel cannot adversely affect to operation of another channel.

Where data communications exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portion(s). If a digital computer system used in a safety system is connected to a digital computer system used in a nonsafety system, the review should confirm that a logical or software malfunction of the nonsafety system cannot affect the functions of the safety system.

5.7 **Capability for Test and Calibration** (IEEE Std 603-1991, Clause 5.7)

Guidance on periodic testing of the safety system is provided in RG 1.22, "Periodic Testing of Protection System Actuation Functions," and in RG 1.118, "Periodic Testing of Electric Power and Protection Systems," which endorses American National Standards Institute (ANSI)/IEEE Std 338, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems." 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. Periodic testing should duplicate, as closely as practical, the overall performance required of the safety system. The test should confirm operability of both the automatic and manual circuitry. The capability 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 require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation.

For digital computer-based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup. SRP BTP 7-17 describes additional considerations in the evaluation of test provisions in digital computer-based systems.

The review of test and calibration provisions should be coordinated with the organization responsible for reviewing technical specification format and content to confirm that the 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. SRP BTP 7-17 discusses considerations in performing this evaluation for digital computer-based systems.

5.8 Information Displays (IEEE Std 603-1991, Clause 5.8)

The review of information displays should be coordinated with the organization responsible for reviewing reactor designs to confirm that the information displayed and the characteristics of the displays (e.g., location, range, type, and resolution) support operator awareness of system and plant status and will allow plant operators to make appropriate decisions.

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

Safety system bypass and inoperable status indication should conform with the guidance of RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

5.9 Control of Access (IEEE Std 603-1991, Clause 5.9)

Administrative control is acceptable to ensure that the access to the means for bypassing safety system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access.

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

Review of digital computer-based systems should consider controls over electronic access to safety system software and data. Controls should address access via network connections, and via maintenance equipment. SRP Appendix 7.1-D provides specific guidance on applying the safety system criteria to computer-based safety systems.

5.10 Repair (IEEE Std 603-1991, Clause 5.10)

Digital safety systems may include self-diagnostic capabilities to aid in troubleshooting. SRP BTP 7-17 describes characteristics that digital computer-based diagnostic systems should exhibit. 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.

5.11 Identification (IEEE Std 603-1991, Clause 5.11)

Guidance on identification is provided in RG 1.75, which endorses IEEE Std 384. The preferred identification method is color coding of components, cables, and cabinets.

Configuration management is an important process for maintaining the identification of computer software. SRP BTP 7-14 discusses the review of software configuration management. SRP Appendix 7.1-D, Subsection 5.11 provides guidance on identification in computer systems.

5.12 Auxiliary Features (IEEE Std 603-1991, Clause 5.12)

SRP BTP 7-9 provides specific guidance for the review of anticipatory trips that are auxiliary features of a reactor protection system.

5.13 Multi-Unit Stations (IEEE Std 603-1991, Clause 5.13)

The review of shared displays and controls 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.

5.14 Human Factors Considerations (IEEE Std 603-1991, Clause 5.14)

Safety system human factors design should be consistent with the applicant's or licensee's commitments documented in Chapter 18 of the SAR. The review of human-factors considerations should be coordinated with the organization responsible for reviewing human factors.

5.15 Reliability (IEEE Std 603-1991, Clause 5.15)

The applicant or licensee should justify 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.

For computer systems, both hardware and software reliability should be analyzed. SRP Appendix 7.1-D describes the staff's position on software reliability determination. SRP BTP 7-14 provides guidance for software development processes that are expected to produce reliable software. Software that complies with the quality criteria of Subsection 5.3 above and that is used in safety systems that provide measures for defense against common-cause failures as described in Subsection 5.1 above are considered by the staff to comply with the fundamental reliability requirements of General Design Criterion 21, "Protection System Reliability and Testability," IEEE Std 279-1971, and IEEE Std 603-1991.

The 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. Hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communications systems. Hard failures, transient failures, sustained failures, and partial failures should be considered. Software failure conditions to be considered should include, as appropriate, software common-cause failures, cascading failures, and undetected failures.

SRP Appendix 7.1-D indicates that the concept of quantitative reliability goals is not sufficient as a sole means of meeting the NRC's regulations for the reliability of digital computers used in safety systems. This is discussed in more detail as part of Subsection 4 above.

6. SENSE AND COMMAND FEATURES - FUNCTIONAL AND DESIGN REQUIREMENTS (IEEE Std 603-1991, Clause 6)

This subsection provides requirements for sensors and command features.

6.1 Automatic Control (IEEE Std 603-1991, Clause 6.1)

The safety system should, with precision and reliability, automatically initiate and execute protective action for the range of conditions and performance except as justified in Clause 4.5 of IEEE Std 603-1991. The applicant or licensee's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met. The evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. SRP BTP 7-12 discusses considerations for the review of the process for establishing instrument setpoints.

For digital computer-based systems, the evaluation should confirm that the functional requirements have been appropriately allocated into hardware and software requirements. The evaluation should also confirm that the system's real-time performance is deterministic and known. SRP BTP 7-21 provides guidance for this evaluation.

6.2 Manual Control (IEEE Std 603-1991, Clause 6.2)

Features for manual initiation of protective action should conform with RG 1.62, “Manual Initiation of Protection Action.”

The review of manual controls should be coordinated with the organization responsible for reviewing human factors to confirm that the functions controlled and the characteristics of the controls (e.g., location, range, type, and resolution) allow plant operators to take appropriate manual actions.

The review of manual controls should include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified), accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary.

6.3 Interaction Between the Sense and Command Features and Other Systems (IEEE Std 603-1991, Clause 6.3)

The reviewer should confirm that nonsafety system interactions with safety systems are limited such that the requirements of 10 CFR Part 50, Appendix A, General Design Criterion 24, “Separation of Protection and Control Systems,” are met.

Where the event of concern is simple failure of a sensing channel shared between control and protection functions, previously accepted approaches have included:

- Isolating the safety system from channel failure by providing additional redundancy.

- Isolating the control system from channel failure by using data validation techniques to select a valid control input.

6.4 Derivation of System Inputs (IEEE Std 603-1991, Clause 6.4)

As stated in Clause 6.4 of IEEE Std 603-1991, 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. A safety system that requires loss of flow protection would, for example, normally derive its signal from flow sensors. A design might use an indirect parameter such as a pressure signal or pump speed. However, the applicant or licensee should verify that any indirect parameter is a valid representation of the desired direct parameter for all events.

Even a directly measured variable should be reviewed and its response to postulated events compared with the credit taken for the parameter in the events for which it provides protection.

For both direct and indirect parameters, the applicant or licensee should verify that the characteristics (e.g., range, accuracy, resolution, response time, sample rate) of the instruments that produce the safety system inputs are consistent with the analysis provided in Chapter 15 of the SAR.

6.5 Capability for Testing and Calibration (IEEE Std 603-1991, Clause 6.5)

Means shall be provided for checking the operational availability of each sensor required for a safety function. This may be accomplished by perturbing the monitored variable, by varying the input to the sensor within the constraints of Clause 6.5 of IEEE Std 603-1991, or by cross checking between redundant channels. 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 applicant or licensee should state the basis used to ensure that an operator will not take incorrect action when the two channel readouts differ. The applicant or licensee should state the method to be used for checking the operational availability of non-indicating sensors. SRP BTP 7-17 discusses issues that should be considered in sensor check and surveillance test provisions for digital computer I&C systems.

6.6 Operating Bypasses (IEEE Std 603-1991, Clause 6.6)

The requirement for automatic removal of operational bypasses means that the reactor operator shall have no role in such removal. The operator may take action to prevent the unnecessary initiation of a protective action.

6.7 Maintenance Bypass (IEEE Std 603-1991, Clause 6.7)

The review of bypass and removal from operations should be coordinated with the organization responsible for reviewing technical specification format and content to confirm that the provisions for this bypass are consistent with the required actions of the proposed plant technical specifications.

6.8 Setpoints (IEEE Std 603-1991, Clause 6.8)

The applicant or licensee's analysis should confirm that an adequate margin exists between operating limits and setpoints, such that there is a low probability for inadvertent actuation of the system. The applicant’s or licensee's analysis should confirm that an adequate margin exists between setpoints and safety limits, such that the system initiates protective actions before

safety limits are exceeded. RG 1.105, "Instrument Setpoints for Safety Systems," and SRP BTP 7-12 provides guidance on the establishment of instrument setpoints.

Where it is necessary to provide multiple setpoints as discussed in Clause 6.8.2 of IEEE Std 603-1991, the staff's interpretation of "positive means" is that automatic action is provided to ensure that the more restrictive setpoint is used when required. SRP BTP 7-3 provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

7. Execute Features - Functional and Design Requirements
(IEEE Std 603-1991, Clause 7)

This subsection provides requirements for actuators and other execute features.

7.1 Automatic Control (IEEE Std 603-1991, Clause 7.1)

The safety system should, with precision and reliability, automatically initiate and execute protective action for the range of conditions and performance requirements except as justified in Clause 4.5 of IEEE Std 603-1991. The applicant's or licensee's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met. The evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. SRP BTP 7-12 discusses considerations for the review of the process for establishing safety system setpoints.

For digital computer-based systems, the evaluation should confirm that the functional requirements have been appropriately allocated into hardware and software requirements. The evaluation should also confirm that the system's real-time performance is deterministic and known. SRP BTP 7-21 provides guidance for this evaluation.

7.2 Manual Control (IEEE Std 603-1991, Clause 7.2)

Features for manual initiation of protective action should conform with RG 1.62, "Manual Initiation of Protection Action."

The review of manual controls should be coordinated with the organization responsible for reviewing human factors to confirm that the functions controlled and the characteristics of the controls (e.g., location, range, type, and resolution) allow plant operators to take appropriate manual actions.

The review of manual controls should include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified), and accessible within the time required of the operator during plant conditions under which manual actions may be necessary.

7.3 Completion of Protective Action (IEEE Std 603-1991, Clause 7.3)

The staff's review of this item should include review of functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion. The seal-in feature may incorporate a time delay as appropriate for the safety function. Additionally, the seal-in feature need not function until it is confirmed that a valid protective command has been received, provided the system meets response time requirements.

7.4 **Operating Bypasses** (IEEE Std 603-1991, Clause 7.4)

The requirement for automatic removal of operational bypasses means that the reactor operator shall have no role in such removal. The operator may take action to prevent the unnecessary initiation of a protective action.

7.5 **Maintenance Bypass** (IEEE Std 603-1991, Clause 7.5)

The review of bypass and removal from operations should be coordinated with the organization responsible for reviewing technical specification format and content to confirm that the provisions for this bypass are consistent with the required actions of the proposed plant technical specifications.

8. POWER SOURCE REQUIREMENTS (IEEE Std 603-1991, Clause 8)

The organization responsible for reviewing electrical systems reviews power source requirements. I&C reviewers should coordinate with the electrical systems reviewers to confirm that I&C safety system power sources are adequate.

9. REFERENCES

1. ANSI/IEEE Std 338, “Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems.”

2. IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations.”

3. IEEE Std 379, “Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.”

4. IEEE Std 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.”

5. IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

6. IEEE Std 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

7. RG 1.22, “Periodic Testing of Protection System Actuation Functions.”

8. RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems.”

9. RG 1.53, “Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems”

10. RG 1.62, “Manual Initiation of Protection Action.”

11. RG 1.75, “Criteria for Independence of Electrical Safety Systems.”

12. RG 1.105, “Setpoints for Safety-Related Instrumentation.”

13. RG 1.118, “Periodic Testing of Electric Power and Protection Systems.”

14. RG 1.151, “Instrument Sensing Lines.”

15. RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.”

16. RG 1.153, “Criteria for Safety Systems.”

17. RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems.”

18. RG 1.204, “Guidelines for Lightning Protection of Nuclear Power Plants.”

19. RG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants.”

20. Safety Evaluation by the Office of Nuclear Reactor Regulation, “EPRI Topical Report TR 106439, Guidance on the Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” May 1997.

21. SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” April 2, 1993.

22. Staff Requirements Memorandum on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” July 21, 1993.

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in the SRP are covered by the requirements of 10 CFR Part 50 and 10 CFR Part 52, and were approved by the Office of Management and Budget, approval number 3150-0011 and 3150-0151.

PUBLIC PROTECTION NOTIFICATION

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

APPENDIX 7.1-C
Description of Changes

APPENDIX 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"

This Appendix 7.1-C Section affirms the technical accuracy and adequacy of the guidance previously provided in Appendix 7.1-C, Revision 5, dated March 2007. See ADAMS Accession Number ML070550088.

The main purpose of this update is to incorporate the revised software Regulatory Guides and the associated endorsed standards. For organizational purposes, the revision number of each Regulatory Guide and year of each endorsed standard is now listed in one place, Table 7-1. As a result, revisions of Regulatory Guides and years of endorsed standards were removed from this section, if applicable. For standards that are incorporated by reference into regulation (IEEE Std 279-1971 and IEEE Std 603-1991) and standards that have not been endorsed by the agency, the associated revision number or year is still listed in the discussion.

Added Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants." to the list of applicable regulatory guides for reviews under this SRP section, and to the discussion of equipment qualification for mild environments.

Part of 10 CFR was reorganized due to a rulemaking in the fall of 2014. Quality requirement discussions in the former 10 CFR 50.55a(a)(1) were moved to 10 CFR 50.54(jj) and 10 CFR 50.55(i). The incorporation by reference language in the former 10 CFR 50.55a(h)(1) was moved to 10 CFR 50.55a(a)(2). There were no changes either to 10 CFR 50.55a(h)(2) or 10 CFR 50.55a(h)(3).

Additional changes were editorial.