U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

Month Year
Division 1

DRAFT REGULATORY GUIDE

Technical Lead
Michael E. Waterman
904-516-7912

DRAFT REGULATORY GUIDE DG-1251

(Proposed Revision 2 of Regulatory Guide 1.153, dated June 1996)

CRITERIA FOR THE POWER, INSTRUMENTATION, AND CONTROL PORTIONS OF SAFETY SYSTEMS FOR NUCLEAR POWER PLANTS

A. INTRODUCTION

Purpose

This regulatory guide (RG) addresses the criteria for the power, instrumentation, and control portions of safety systems for nuclear power plants as specified in Section 50.55a(h), Title 10, Part 50 of the *Code of Federal Regulations* (10 CFR 50.55a(h)) (Ref. 1). The regulation incorporates by reference Institute of Electrical and Electronics Engineers (IEEE) Standard (IEEE Std) 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems" (Ref. 2), IEEE Std 279-1971, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations" (Ref. 3); IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Ref. 4); "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations Correction Sheet issued January 30, 1995" (Ref. 5); IEEE Std 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Ref. 6), and IEEE Std 603-2009 Correction Sheet dated March 10, 2015, "Errata to IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Ref. 7).

Applicable Regulations

- 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," (Ref. 1) governs the licensing of nuclear power plants and it requires that structures, systems, and components that are important to safety in a nuclear power plant must be designed to remain functional under postulated design-basis events (DBEs).

- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," (GDC) (Ref. 1) contains, in part, requirements for the design, reliability, qualification, and testability of safety systems.

- 10 CFR Part 52 "Licenses, Certifications, and Approvals for Nuclear Power Plants," (Ref. 8) governs the issuance of early site permits, standard design certifications, combined licenses, standard design approvals, and manufacturing licenses for nuclear power facilities licensed under Section 103 of the Atomic Energy Act of 1954, as amended (68 Stat. 919), and Title II of the Energy Reorganization Act of 1974 (88 Stat. 1242).

Related Guidance

- IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," (Ref. 9). This standard provides additional computer specific requirements to supplement the criteria and requirements of IEEE Std 603.

- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," (Ref. 10). This RG describes a method that the NRC staff deems acceptable for complying with NRC regulations for promoting high functional reliability, design quality, and a secure development and operational environment (SDOE) for the use of digital computers in the safety systems of nuclear power plants. In this context, the term "computer" identifies a system that includes computer hardware, software, firmware, and interfaces.

- NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," (Ref. 11). The Standard Review Plan (SRP) is prepared for the guidance of staff reviewers in the Office of Nuclear Reactor Regulation in performing safety reviews of applications to construct or operate nuclear power plants. The principal purpose of the SRP is to assure the quality and uniformity of staff reviews and to present a well-defined base from which to evaluate proposed changes in the scope and requirements of reviews. It is also a purpose of the SRP to make information about regulatory matters widely available and to improve communication and understanding of the staff review process by interested members of the public and the nuclear power industry.

- RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," (Ref. 12). This RG provides guidance to licensees and applicants on methods acceptable to the NRC staff for complying with the NRC's regulations on design, installation, and testing practices for addressing the effects of electromagnetic and radio-frequency interference (EMI/RFI) and power surges on safety-related instrumentation and control (I&C) systems.

- RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," (Ref. 13). This RG provides guidance for satisfying the NRC's regulations with respect to the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.

- IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," (Ref. 14). This standard provides basic requirements for qualifying Class 1E equipment and interfaces used in nuclear power generating stations.

- RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," (Ref. 15). This RG describes a method that the NRC staff considers acceptable for determining the environmental qualification procedures for safety-related computer-based I&C systems for service within nuclear power plants. In so doing, this guide endorses certain practices in the current national standard, and it

incorporates guidance to address specific issues posed by the application of microprocessor-based technology.

- IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," (Ref. 16). This standard gives generic requirements and methods for qualifying Class 1E equipment.

- RG 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," (Ref. 17). This RG describes a method acceptable to the NRC staff for complying with 10 CFR 50.49 with regard to qualification of electric equipment important to safety for service in nuclear power plants to ensure that the equipment can perform its safety function during and after a design basis accident.

- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," (Ref. 18). This report describes a method for analyzing computer-based nuclear reactor protection systems that discovers design vulnerabilities to common-mode failure.

- NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," (Ref. 19). This report presents the technical basis for establishing acceptable mitigating strategies that resolve diversity and defense-in-depth assessment findings.

Purpose of Regulatory Guides

The NRC issues RGs to describe to the public methods that the NRC staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the NRC staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants. RGs are not substitutes for regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the NRC.

Paperwork Reduction Act

This RG contains information collection requirements covered by 10 CFR part 50 and 10 CFR part 52 that the Office of Management and Budget (OMB) approved under OMB control number 3150-0011 and OMB control number 3150-0151, respectively. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number.

B. DISCUSSION

Reason for Change

This revision of RG 1.153 provides the underlying basis of the 10 CFR 50.55a(h) regulation when implementing or modifying safety systems in nuclear power plants. This regulatory guidance was issued to support issuance of the revision to 10 CFR 50.55a(h) that incorporates by reference IEEE Std 279-1971, IEEE Std 603-1991 and the correction sheet dated January 30, 1995, and IEEE Std 603-2009, as discussed in Federal Register Notice (FRN) *xxxxxx* (Ref. 20).

NRC issued RG 1.153, in June 1996 (Ref. 21) to state that conformance with the requirements of IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations" (including the correction sheet dated January 30, 1995) provided a method acceptable to the NRC staff for satisfying the Commission's regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of nuclear power plant safety systems. This regulatory guidance allowed licensees with IEEE Std 279-1971 nuclear power plants licenses to use IEEE Std 603-1991 and the correction sheet dated January 30, 1995, when performing protection system modifications.

Background

The IEEE Std 603 series began with IEEE Std 279-1968, "IEEE Standard: Criteria for Nuclear Power Plant Protection Systems" (Ref. 2), a trial-use standard for protection systems. This was followed by IEEE Std 279-1971, a standard for protection systems, which the IEEE then superseded with IEEE Std 603-1977, "Trial-Use Standard Criteria for Safety Systems to Nuclear Power Generating Stations," issued in 1977 (Ref. 22). IEEE Std 603 was revised and issued in 1980 as IEEE Std 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Ref. 23); in 1987 as IEEE Std 603-1987, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations; Correction Sheet" (Ref. 24); in 1991 as IEEE Std 603-1991, supplemented by the correction sheet dated January 30, 1995 (Ref. 5); and in 1998 as IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Ref. 25). The current revision, IEEE Std 603-2009, provides the current IEEE criteria for safety systems.

The previous edition of 10 CFR 50.55a(h)(2), "Protection systems," required that the protection systems in nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999, meet the requirements stated either in 1) IEEE Std 279, or in 2) IEEE Std 603-1991 and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued before January 1, 1971, 10 CFR 50.55a(h)(2) required that protection systems be consistent with their licensing basis or meet the requirements of IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

The previous edition of 10 CFR 50.55a(h)(3), "Safety systems," required that applications filed on or after May 13, 1999, construction permits and operating licenses under 10 CFR part 50, standard design approvals, standard design certifications, and combined licenses under 10 CFR part 52 meet the requirements for safety systems stated in IEEE Std 603–1991 and the correction sheet dated January 30, 1995.

The IEEE superseded the previous standards with IEEE Std 603-2009 and the correction sheet dated March 10, 2015. The previous version of 10 CFR 50.55a(h) was revised to incorporate by reference IEEE Std 603-2009, and to specify requirements for using IEEE Std 603-2009 or earlier versions of this standard on the basis of license date, construction permit date, and type of protection system or safety system modification. The rule applies to: 1) reactor design applications for a license, construction permit,

design approval, or design certification, and 2) applications for license amendments for nuclear power plants.

Since publication of RG 1.153, Revision 1 in 1996, the IEEE published IEEE Std 603-2009 to:

- address potential safety issues that might arise from incorporating components that use advanced technologies in safety systems;
- provide additional and updated references and exclude references that are no longer in effect;
- provide guidance to address electromagnetic compatibility issues;
- add new guidance for common cause failure;
- provide classification requirements for equipment not credited to perform a safety function but connected to safety-related equipment;
- remove the requirement in section 6.7, "Maintenance bypass," for meeting the single failure criterion during maintenance activities, and
- specifically require electrical isolation and digital communication independence between safety systems and non-safety systems.

Consequently, the NRC updated 10 CFR 50.55a(h) to incorporate by reference IEEE Std 603-2009 and the correction sheet dated March 10, 2015, with conditions, in addition to retaining the incorporation by reference for IEEE Std 279-1968, IEEE Std 279-1971, IEEE Std 603-1991, and the IEEE Std 603-1991 correction sheet dated January 30, 1995.

Harmonization with International Standards

The international standards and guides listed below are generally consistent with the principles in the standards incorporated by reference in 10 CFR 50.55a(h). These international standards and guides provide useful information for implementing safety systems in nuclear power plants and utilization facilities, although they may not provide a one-to-one correlation with the standards incorporated by reference in 10 CFR 50.55a(h). However, the NRC does not endorse these standards and guides and does not recognize these standards and guides as an acceptable means for complying with the requirements of 10 CFR 50.55a(h).

- International Atomic Energy Agency (IAEA) Safety Guide NS-G-1.1, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants Safety Guide," November 2000 (Ref. 26)
- IAEA Safety Guide NS-G-1.3, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants Safety Guide," March 2002 (Ref. 27)
- International Electrotechnical Commission (IEC) 60709, Edition 2.0, "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Separation," November 2004 (Ref. 28)
- IEC 60780, Edition 2.0, "Nuclear Power Plants—Electrical Equipment of the Safety System—Qualification," October 1998 (Ref. 29)

- IEC 60880, Edition 2.0, "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Software Aspects for Computer-Based Systems Performing Category A Functions," May 2006 (Ref. 30)

- IEC 60880-2, Edition 1.0, "Software for Computers Important to Safety for Nuclear Power Plants—Part 2: Software Aspects of Defense against Common Cause Failures, Use of Software Tools and of Pre-Developed Software," December 2000 (Ref. 31)

- IEC 60980, Edition 1.0, "Recommended Practices for Seismic Qualification of Electrical Equipment of the Safety System for Nuclear Generating Stations," June 1989 (Ref. 32)

- IEC 61226, Edition 3.0, "Nuclear Power Plants—Instrumentation and Control Important to Safety—Classification of Instrumentation and Control Functions," July 2009 (Ref. 33)

- IEC 61888, Edition 1.0, "Nuclear Power Plants—Instrumentation Important to Safety—Determination and Maintenance of Trip Setpoints," August 2002 (Ref. 34)

- IEC 62385, Edition 1.0, "Nuclear Power Plants—Instrumentation and Control Important to Safety—Methods for Assessing the Performance of Safety System Instrument Channels," June 2007 (Ref. 35)

Documents Discussed in Staff Regulatory Guidance

This regulatory guidance addresses the use of three standards and two correction sheets developed by the IEEE. These standards contain references to other IEEE standards ("secondary references"). If a secondary reference has itself been incorporated by reference into NRC regulations as a requirement, then licensees and applicants must comply with that standard as set forth in the regulation. If the secondary reference has been endorsed in a RG as an acceptable approach for meeting an NRC requirement, then the standard constitutes a method acceptable to the NRC staff for meeting that regulatory requirement as described in the specific RG. If the secondary reference has neither been incorporated by reference into NRC regulations nor endorsed in a RG, then the secondary reference is neither a legally-binding requirement nor a "generic" NRC approved acceptable approach for meeting an NRC requirement. However, licensees and applicants may consider and use the information in the secondary reference, if appropriately justified, consistent with current regulatory practice, and consistent with applicable NRC requirements.

C. STAFF REGULATORY GUIDANCE

As stated in 10 CFR 50.55a(h), conformance with the requirements in IEEE Std 279-1968, IEEE Std 279-1971, IEEE Std 603-1991 and the correction sheet dated January 30, 1995, IEEE Std 603-2009 and the correction sheet dated March 10, 2015, and the additional requirements specified in 10 CFR 50.55a(h) is required with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants.

In Section 4.g, IEEE Std 603-2009 includes electromagnetic interference as an additional environmental factor in the design basis. The staff guidance on this subject is provided in RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems."

In Section 5.1, IEEE Std 603-2009 states that a single failure could occur prior to, or at any time during a design basis event for which the safety system is required to function. Guidance on applying the single failure criterion is provided in RG 1.53, "Application of the Single-Failure Criterion to Safety Systems."

Section 5.4 in IEEE Std 603-2009 references IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," as this standard is the latest version of the equipment qualification standard. The IEEE Std 323-2003 is endorsed by RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," dated March 2007 (ADAMS Accession No. ML070190294) for providing criteria for computer-based equipment qualification in mild environments. The NRC does not endorse IEEE Std 323-2003 as an acceptable means of meeting regulatory requirements for qualifying equipment for operations in harsh environments. For equipment qualified for harsh environments, the procedures described by IEEE Std 323-1974, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations," are acceptable to the NRC staff for satisfying the NRC's regulations pertaining to the qualification of electric equipment for service in nuclear power plants to ensure that the equipment can perform its safety functions in harsh environments subject to the regulatory positions described in RG 1.89, Revision 1, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," dated June 1984 (ADAMS Accession No. ML003740271).

Staff finds using two RGs to endorse the same IEEE standard to be appropriate because RG 1.209 applies to computer-based equipment operating in mild environments and RG 1.89 applies to equipment operating in harsh environments. The guidance in RG 1.209 (endorsing IEEE Std 323-2003) complements the guidance in RG 1.89 (endorsing IEEE Std 323-1974), which was not changed because the new version of IEEE Std 323-2003 did not change any of the criteria applicable to equipment under the scope of § 50.49. Therefore, it is appropriate to reference IEEE Std 323-1974 via RG 1.89 for qualifying equipment operating in harsh environments. Section 5.8.4 of IEEE Std 603-2009 references IEEE Std 497- 2002, "Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations." RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," provides an acceptable method to meet the regulations for accident monitoring equipment.

Section 5.16 of IEEE Std 603-2009, "Common-cause failure criteria," states that IEEE Std 7-4.3.2-2003 provides guidance on performing an engineering evaluation of software common-cause failures, including the use of manual action and non-safety-related systems, or components, or both, to provide means to accomplish safety functions that would otherwise be defeated by the common-cause failure. RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," provides an acceptable method to meet the regulations for common cause failure evaluations. Additional guidance is provided in Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and

Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," in NUREG-0800, "Standard Review Plan," Section 7, "Instrumentation and Controls," for evaluating the effects of digital system common-cause failures.

The following discussion describes the underlying bases of §§ 50.55a(h)(1) through (8). The guidance provided in the following discussion does not modify the scope of 10 CFR 50.55a(h).

Definitions

Definitions of terms used in this section are provided in the Glossary at the end of this guide.

Paragraph-by-Paragraph Discussion

The following discussion summarizes the Commission's intent for each paragraph of 10 CFR 50.55a(h).

10 CFR 50.55a(h)(1) – Definitions

Paragraph 50.55a(h)(1) provides definitions for the terms "current reactors" and "new reactors" in the context of § 50.55a(h).

10 CFR 50.55a(h)(2) – Issue Date Applicability

Conditions for the use of IEEE Std 279 and versions of IEEE Std 603 are provided in §§ 50.55a(h)(2)(i) through (vii) to clarify for protection systems and safety systems the applicability of IEEE Std 603-2009 and the correction sheet dated March 10, 2015, and earlier standards requirements for operating plants, new plants, and manufacturing licenses on the basis of the issue date of the construction permit, standard design certification, or manufacturing license. The regulatory requirements in § 50.55a(h)(2) reduce uncertainty and improve efficiency by identifying the specific criteria to be addressed for protection systems and safety systems. The following discussion addresses the basis underlying each of the subparagraphs under § 50.55a(h)(2).

Paragraph 50.55a(h)(2)(i) clarifies the requirements for protection systems and safety systems in nuclear power plants with construction permits issued before January 1, 1971. Licensees of plants in this category may retain the licensing basis of their plant protection systems and safety systems (i.e., the plant licensing basis or IEEE Std 603-1991 and the correction sheet dated January 30, 1995). Licensees are not required to modify or replace protection systems or safety systems to meet the requirements in IEEE Std 603-2009 and the correction sheet dated March 10, 2015.

Paragraph 50.55a(h)(2)(i) is not intended to allow licensees to lessen the requirements stated in their existing protection system or safety system licensing basis. For example, a safety system that meets the requirements stated in IEEE Std 603-1991 and the correction sheet dated January 30, 1995, could not be modified such that it met only the requirements stated in its original licensing basis.

By preserving the current licensing basis for the protection systems and safety systems addressed in § 50.55a(h)(2)(i), licensees are not required to modify or replace systems that were approved prior to the effective date of 10 CFR 50.55a(h) to meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015. However, licensees have the option to change the licensing basis of their plant protection systems and safety systems to meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in § 50.55a(h)(3) through (8).

Paragraph 50.55a(h)(2)(ii) clarifies the requirements for protection systems and safety systems in nuclear power plants whose construction permits were issued on or after January 1, 1971, but before May 13, 1999. This paragraph does not apply to combined licenses for standard design certifications. Protection systems and safety systems that are not subject to the requirements of § 50.55a(h)(3) are required to meet the requirements stated in the protection system or safety system licensing basis in effect after the effective date of 10 CFR 50.55a(h) instead of the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015 (i.e., IEEE Std 279-1968, IEEE Std 279-1971, or IEEE Std 603-1991 and the IEEE Std 603-1991 correction sheet dated January 30, 1995).

Paragraph 50.55a(h)(2)(ii) is not intended to allow licensees to lessen the requirements stated in the licensing basis for their protection systems or safety systems. For example, a safety system whose current licensing basis is IEEE Std 603-1991 and the IEEE Std 603-1991 correction sheet dated January 30, 1995, could not be modified such that it met only the protection system requirements stated in IEEE Std 279-1971.

By preserving the current licensing basis for the plant protection systems and safety systems addressed in 10 CFR 50.55a(h)(2)(ii), licensees are not required to modify or replace systems that were approved prior to the effective date of 10 CFR 50.55a(h) to meet the safety system requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015. However, licensees have the option to meet the safety system requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in § 50.55a(h)(3) through (8), when modifying or installing protection systems and safety systems.

Paragraph 50.55a(h)(2)(iii) clarifies the requirements for protection systems and safety systems in standard design certifications issued after January 1, 1971, but before May 13, 1999. Two standard design certifications have been codified in 10 CFR Part 52 between these dates: the U.S. Advanced Boiling Water Reactor (ABWR) (10 CFR Part 52, appendix A) and the System 80+ (10 CFR Part 52, Appendix B). As specified in §§ 52.63, 52.83, 52.98, and 52.171, subject to the requirements stated in § 50.55a(h)(3), the protection systems in these two standard design certifications are required to meet the requirements stated in IEEE Std 279-1971 instead of the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015 regardless of the date a combined license referencing either standard design certification plant is issued. For example, an applicant obtaining a combined license for an ABWR nuclear power plant is required to meet the protection system requirements stated in IEEE Std 279-1971 instead of the safety system requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, even if the combined license would be issued after the effective date of 10 CFR 50.55a(h).

Paragraph 50.55a(h)(2)(iv) clarifies the requirements for safety systems in standard design certifications issued on or after May 13, 1999, but before the effective date of 10 CFR 50.55a(h). As of April 1, 2015, three standard design certifications have been codified in 10 CFR part 52 after May 13, 1999: a 600 MWe advanced pressurized water reactor (the AP600) (10 CFR part 52, Appendix C), a 1,000 MWe advanced pressurized water reactor (the AP1000) (10 CFR part 52, appendix D), and a 1,600 MWe advanced boiling water reactor (the ESBWR) (10 CFR part 52, Appendix E). As specified in §§ 52.63, 52.83, 52.98, and 52.171, subject to the requirements in § 50.55a(h)(3), the safety system designs in these three standard design certifications are required to meet the requirements stated in IEEE Std 603-1991 and the IEEE Std 603-1991 correction sheet dated January 30, 1995, instead of the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015. For example, an applicant applying after the effective date of 10 CFR 50.55a(h) for a combined license for an AP1000 nuclear power plant is required to meet the requirements stated in IEEE Std 603-1991 and the correction sheet dated January 30, 1995, instead of the requirements stated in IEEE Std 603-2009 and the correction

sheet dated March 10, 2015, even if the combined license would be issued after the effective date of 10 CFR 50.55a(h).

Paragraph 50.55a(h)(2)(v) clarifies the safety system requirements for standard design certifications issued after the effective date of 10 CFR 50.55a(h). Safety systems in standard design certifications issued after the effective date of 10 CFR 50.55a(h) are required to meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in §§ 50.55a(h)(4) through (8).

Paragraph 50.55a(h)(2)(vi) clarifies the requirements for protection system designs and safety system designs for nuclear power plants with construction permit applications under 10 CFR Part 50 submitted after the effective date of 10 CFR 50.55a(h). The protection system designs and safety system designs in construction permit applications under 10 CFR part 50 submitted after the effective date of 10 CFR 50.55a(h) are required to meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in §§ 50.55a(h)(3) through (8).

Paragraph 50.55a(h)(2)(vii) clarifies the requirements for safety system designs in nuclear power plant combined licenses and manufacturing licenses under 10 CFR part 52 issued after the effective date of 10 CFR 50.55a(h). Combined licenses and manufacturing licenses that reference a standard design certification issued before the effective date of 10 CFR 50.55a(h) are required to meet the requirements stated in the referenced standard design certification. For example, a safety system design for a combined license issued after the effective date of 10 CFR 50.55a(h) that references a standard design certification issued on or after May 13, 1999, but before the effective date of 10 CFR 50.55a(h) is required to meet the requirements stated in IEEE Std 603-1991 and the IEEE Std 603-1991 correction sheet dated January 30, 1995, instead of meeting the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015. Safety system designs in combined licenses and manufacturing licenses that reference a standard design certification issued after the effective date of 10 CFR 50.55a(h) are required to meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in §§ 50.55a(h)(3) through (8).

Table 1 summarizes the § 50.55a(h)(2) criteria to be met on the basis of the issue date of a plant's construction permit under 10 CFR part 50 and standard design certification, combined license, or manufacturing license under 10 CFR part 52. The standards listed in the "Licensing Basis Standard" column designate the licensing basis standards that are applicable for the corresponding paragraph in 10 CFR 50.55a(h). References to IEEE Std 603-1991 include the IEEE Std 603-1991 correction sheet dated January 30, 1995. References to IEEE Std 603-2009 include the IEEE Std 603-2009 correction sheet dated March 10, 2015.

Table 1 - 10 CFR 50.55a(h)(2) issue date applicability

Construction Permit, Standard Design Certification, Combined License, or Manufacturing License Issue Date	**10 CFR 50.55a Paragraph**	**Standard Applicability[1]**
Nuclear power plant construction permits issued before January 1, 1971	**(h)(2)(i)**	Licensing Basis IEEE Std 603-1991
Nuclear power plant construction permits issued on or after January 1, 1971 and before May 13, 1999	**(h)(2)(ii)**	IEEE Std 279-1968 IEEE Std 279-1971 IEEE Std 603-1991

Table 1 - 10 CFR 50.55a(h)(2) issue date applicability

Construction Permit, Standard Design Certification, Combined License, or Manufacturing License Issue Date	10 CFR 50.55a Paragraph	Standard Applicability[1]
Standard design certifications issued before May 13, 1999	**(h)(2)(iii)**	IEEE Std 279-1971
Standard design certifications issued on or after May 13, 1999, but before the effective date of 10 CFR 50.55a(h)	**(h)(2)(iv)**	IEEE Std 603-1991
Standard design certifications issued after the effective date of 10 CFR 50.55a(h)	**(h)(2)(v)**	IEEE Std 603-2009
Applications submitted after the effective date of 10 CFR 50.55a(h) for nuclear power plant construction permits under 10 CFR part 50.	**(h)(2)(vi)**	
Nuclear power plant combined licenses and manufacturing licenses under 10 CFR part 52 issued after the effective date of 10 CFR 50.55a(h)	**(h)(2)(vii)** Referenced Standard Design Certifications issued before the effective date of 10 CFR 50.55a(h)	IEEE Std 279-1971 IEEE Std 603-1991
	(h)(2)(vii) Referenced Standard Design Certifications issued after the effective date of 10 CFR 50.55a(h)	IEEE Std 603-2009

1. See 10 CFR 50.55a(a)(2)

10 CFR 50.55a(h)(3) – Modifications and Installations of Protection Systems and Safety Systems

Conditions for meeting the criteria stated in IEEE Std 279 and versions of IEEE Std 603 are provided in 10 CFR 50.55a(h)(3) to clarify the applicability of IEEE Std 603-2009 and earlier standards for currently operating plants under 10 CFR Part 50, standard design certifications, combined licenses, and manufacturing licenses under 10 CFR Part 52 for modifications of protection systems and safety systems, and installations of new protection system functions and safety system functions.

Paragraph 50.55a(h)(3) preserves the current licensing basis for plants in which a modification or replacement would not add new functionality, new technology, change the independence strategy, or change the diversity strategy in the existing protection system functions or safety system functions. However, licensees and applicants are required to apply IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in §§ 50.55a(h)(4) through (8), for changes to plant protection systems or safety systems that add new safety functionality, new technology, or change the independence strategy or the diversity strategy in the existing protection system functions or safety system functions.

Paragraph 50.55a(h)(3) assures that the most current requirements will be met for new safety functionality or new technology being added to protection systems and safety systems. In the event the independence strategy for divisions is changed, these changes should be introduced into the protection system or safety system in accordance with the requirements in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in §§ 50.55 (h)(4) through (8). Further, if the system diversity strategy would be changed in a protection system or safety system, the revised system diversity strategy should meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in §§ 50.55a(h)(4) through (8), to assure the revised system diversity strategy addresses regulatory criteria.

Paragraph 50.55a(h)(3) is not intended to allow licensees to use a licensing basis or standard that results in a lessening of the requirements stated in the licensing basis for the protection system or safety system. For example, a safety system whose licensing basis meets the requirements stated in IEEE Std 603-1991 and the correction sheet dated January 30, 1995, could not be modified such that it met only the requirements stated in IEEE Std 279-1971.

Paragraph 50.55a(h)(3) reduces licensing uncertainty by providing consistent licensing criteria for modifications of existing protection systems and safety systems, and installations of protection system functions and safety system functions.

While the requirement in 10 CFR 50.55a(h)(3) is intended to address all cases involving modifications and installations of protection systems and safety systems, there may arise specific cases of modifications or replacements that would not apply. In those cases, § 50.55a(h)(3) requires licensees and applicants to meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in §§ 50.55a(h)(4) through (8), as this is the most conservative approach of the alternatives for specifying protection system and safety system requirements.

The following seven examples, which are summarized in Table 2, illustrate the application of 10 CFR 50.55a(h)(3) for different types of protection system or safety system modifications or replacements. These examples are for illustrative purposes only.

Example 1. In this example a licensee replaces a power supply in a single division with a new power. As part of this modification, the licensee determines that the functionality and technology of the new power supply would not be changed. The licensee determines that independence between the redundant divisions and the power trains would be maintained such that a failure occurring in the new power supply would not cause the redundant division or power train to fail. The licensee determines there would be no potential for a common cause failure to occur in the power supplies of the redundant trains.

In this case, § 50.55a(h)(3) requires that the protection system or safety system requirements stated in a plant's licensing basis be applicable for this modification. In modifications such as this, licensees and applicants are not required to modify or replace an existing protection system or safety system to meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015 because the modification would not affect the licensing basis of the plant.

A requirement to modify or replace a protection system or safety system to meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015 when making modifications that would not change the safety system functionality, technology (including changes to equipment qualification characteristics), independence strategy, and diversity strategy could discourage licensees and applicants from improving the reliability and performance of existing protection systems, safety systems, and safety functions.

Example 2. In this example, a licensee replaces all four divisions of the protection system pressure measurement instrumentation with new pressure measurement instrumentation that has the same function and technology (including equipment qualification characteristics). The licensee ensures the new pressure instrumentation would not change the existing independence between redundant divisions of the protection system, and the diversity strategy would not be changed. In this case, the modification would be required by § 50.55a(h)(3) to meet the requirements in the license basis.

A requirement to modify or replace a protection system or safety system to meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015 when making modifications that would not change the safety system functionality or technology could discourage licensees and applicants from improving the reliability and performance of existing protection systems, safety systems, and safety functions.

Example 3. In this example, a licensee replaces the departure from nucleate boiling ratio (DNBR) reactor trip system function with an improved DNBR reactor trip system function based on the same technology. The DNBR reactor trip system function is a diverse means of protecting the fuel rod cladding from damage caused by overheating when reactor coolant thermodynamic or thermal-hydraulic conditions (e.g., reactor coolant pressure, temperature, or coolant flow rate) become degraded such that the reactor must be shut down to prevent further overheating. This safety function is a diverse means of shutting down the reactor if the protection system fails to detect a coolant condition that could adversely affect the fuel rod cladding. The licensee determines that the proposed change would not change the safety system diversity strategy or independence between redundant divisions of the safety system. The licensee further determines that the proposed DNBR safety function would be implemented with the same system functionality. The licensee, therefore, may implement the new DNBR safety function in conformance with the plant's existing license basis instead of meeting the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015.

Example 4. In this example, a licensee modifies a microprocessor-based DNBR safety function by adding functionality to the DNBR safety function to allow the reactor operator to manually select one of four divisions of input data for each of the four previously independent DNBR divisions. This change in functionality and independence strategy would require the safety function to meet the requirements in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in § 50.55a(h)(4) through (8), because the functionality and independence strategy would be changed.

Example 5. In this example, a licensee replaces an analog-based reactor protection system with a microprocessor-based reactor protection system. Paragraph 50.55a(h)(3) requires that replacement of the protection system with an equivalent protection system implemented with a different technology meet the requirements stated in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in §§ 50.55a(h)(4) through (8). As further clarification of the intent of § 50.55a(h)(3), the new system-level functions and technology include (but are not limited to) sensor input modules, trip bistable and signal processing modules, and communication protocols for redundant divisions or external systems and trip signal voting module processors. Reusing existing components in the protection system (e.g., cables, sensors, field mounted signal conditioning equipment, control room panels, and operator displays) as a part of the system-level protection system modification would not exclude this type of modification from the requirements of IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in § 50.55a (h)(4) through (8).

The intent of § 50.55a(h)(3) is to require licensees and applicants to use the most current system safety requirements available when planning, developing, and implementing new protection systems and safety systems that use functions (including changes to independence) or technology (including changes to equipment qualification characteristics) that are different from the system being replaced.

Example 6. In this example, a licensee proposes to replace a microprocessor-based DNBR safety function with another digital-based DNBR safety function. To improve availability, the licensee proposes to share all four divisions of instrument data between the DNBR safety functions, thereby reducing the independence between redundant divisions. In this example, the diversity strategy is not changed because the diversity arising from use of a DNBR function would be preserved. However, since independence between redundant divisions of the safety system would be decreased by eliminating communication independence, the proposed DNBR modification is required to meet the requirements in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in §§ 50.55a (h)(4) through (8).

Example 7. In this example, a licensee replaces a microprocessor-based main steamline and feedwater isolation subsystem with a field-programmable gate array-based (FPGA-based) subsystem that adds new system functionality and operating characteristics that require different methods for coping with system failure modes (e.g., different common cause failure consequences that change the type of operator response and the timing of operator responses). Since system functionality and diversity strategy would be changed, the licensee is required to meet the requirements in IEEE Std 603-2009 and the correction sheet dated March 10, 2015, subject to the conditions in § 50.55a (h)(4) through (8).

Using the above examples, Table 2 summarizes the 10 CFR 50.55a(h) requirements to be met on the basis of the scope of a modification, replacement, or installation of a protection system, safety system, or safety function. References to IEEE Std 603-2009 include the correction sheet dated March 10, 2015.

Table 2- Examples of modifications and replacements of components, functions, and systems

Example	Modification or Replacement Example	Was Functionality (F), Technology (T), Independence strategy (I), or Diversity strategy (D) changed?				Applicable Standard
		F	T	I	D	
1	Power supply replaced in one power train division	no	no	no	no	Licensing Basis Standard
2	Pressure measurement instrumentation replaced with new pressure measurement instrumentation in all four channels of the protection system	no	no	no	no	
3	DNBR safety function replaced with improved DNBR safety function	no	no	no	no	
4	Added functionality to DNBR safety function to allow manual selection of one of four channels of input data for each DNBR channel	yes	no	yes	no	IEEE Std 603-2009 (subject to the conditions in §§ 50.55a (h)(4) through (8))
5	Modified a protection system with components based on a different technology	no	yes	no	no	
6	Modified channels or divisions such that independence was changed	no	no	yes	no	
7	Modified a safety function such that protection system diversity strategy was changed	yes	no	no	yes	

10 CFR 50.55a(h)(4) – System Integrity Requirements

Paragraph 50.55a(h)(4) amplifies the requirements stated in IEEE Std 603-2009 section 5.5, "System Integrity." Paragraph 50.55a(h)(4) requires that in order to assure the integrity and reliable operation of safety systems, safety functions shall be designed to operate in a predictable and repeatable manner. Predictable and repeatable operation of a system requires that the results of translating input signals to output signals are determined through known relationships among the controlled system states and required responses to those states, and in which a given set of input signals produce the same output signals for the full range of applicable conditions enumerated in the design basis. All signal processing between sensor data input and safety control device actuation should be accomplished in a manner such

that required safety functionality remains assured regardless of responses by redundant portions of the safety system or other external systems.

Predictable and repeatable systems, in general, do not provide the capability for unscheduled event-based interrupts or operator-based system interrupts to meet system safety requirements. Systems that operate in a predictable and repeatable manner, in general, should not be designed with the capability for unscheduled event-based disruptions or operator-based system functions that would inhibit or prevent the system from meeting its safety requirements. Analyses used to demonstrate system predictability and repeatability should be based on analysis of system characteristics (e.g., definitive design and performance criteria) as opposed to probabilistic analysis.

10 CFR 50.55a(h)(5) – Independence Requirements

Paragraph 50.55a(h)(5) amplifies the requirements stated in IEEE Std 603-2009, section 5.6, "Independence." Protection systems and safety systems should implement provisions for protection against identified hazards.

Paragraph 50.55a(h)(5)(i) provides requirements for applicants to address independence among redundant portions of safety systems. Receipt of information from outside a safety division could increase the likelihood of impairing the safety function in that division. Provisions should be included to protect against the potential for impairing the safety function. Redundant portions of safety systems should be sufficiently independent such that those provisions are commensurate with the relative risk posed by any potential hazards identified. The degree of interconnectivity between redundant portions of safety systems should be evaluated to ensure that the potential to introduce pathways for such hazards to propagate is minimized. Applicants should evaluate the hazards introduced by such information sharing.

Paragraph 50.55a(h)(5)(ii) provides requirements for applicants to address independence between safety systems and other systems. Receipt of information from other systems could increase the likelihood of impairing a safety function in the safety system. Provisions should be included to protect against the potential for impairing the safety function. Safety systems should be sufficiently independent from other systems such that those provisions are commensurate with the potential hazards identified. The degree of interconnectivity between safety systems and other systems should be evaluated to ensure that the potential to introduce pathways for such hazards to propagate is minimized. Applicants should evaluate the hazards introduced by such information sharing.

Section 5.6.3.1.a.2.ii and section 5.6.3.1.b in IEEE Std 603-2009 uses the term "digital communications independence." This term excludes consideration for technologies other than digital that could also impair safety. Therefore, communications independence between safety systems and other systems should be applied for all signal technologies.

Paragraph 50.55a(h)(5)(iii) clarifies requirements that apply to section 5.6 of IEEE Std 603-2009. Safety system independence is a design principle that accounts for failures and interdependencies (both known and unknown) between plant systems and helps minimize the propagation of errors. To ensure independence, a safety system should not rely upon the performance or receipt of information from other external safety and/or non-safety systems to perform its safety function.

Communications independence provides a degree of protection against hazards that may impair a safety system. For example, a completely independent safety system would not have any communications link between redundant portions of safety systems or between safety and non-safety systems and therefore would be protected from the effects of communication failures or unexpected behaviors. However, having

the ability to send information to non-safety systems could also be beneficial from a display, indication, diagnostic, and data recording perspective.

The sharing of signals between redundant portions of safety systems typically has been used only for the accomplishment of safety-related functions. Communications links can allow non-safety systems to be used as a means (e.g. online diagnostics) to monitor, and maintain control system parameters of a safety system. Digital technology, including the use of digital communications features may provide additional flexibility and functionality in safety and non-safety functions provided by nuclear power plant I&C systems; however, an integrated and interconnected digital communication system may also introduce additional unique failure modes and unexpected interdependencies.

Except for very simple systems, the performance of verification testing to identify all failure modes and interdependencies (e.g., latent defects) in the digital system development process is impractical, if not impossible, due to the number of input and system states that increase with the level of integration and interconnectivity. These errors and interdependencies may challenge the independence between redundant portions of safety systems and between safety systems and non-safety systems. These failure modes and dependencies may outweigh the benefits offered by the interconnectivity.

Paragraph 50.55a(h)(5)(iii)(A) clarifies that the signal processing portions of the safety system should provide the capability to ensure that degradation or failures of signals exchanged among redundant safety divisions or between safety systems and other systems do not propagate in a manner that results in impairment of the safety functions being performed by the safety system.

Paragraph 50.55a(h)(5)(iii)(B) clarifies that safety systems should be designed with provisions for detecting and mitigating the effects of signal faults or failures received from outside the safety division. Redundant divisions of safety systems should have the capability of tolerating such faults or failures originating from outside the safety division in a manner that does not degrade the ability of the safety division to perform its safety functions.

Paragraph 50.55a(h)(5)(iii)(C) clarifies the requirements in section 5.6, “Independence” of IEEE Std 603-2009, for communications (e.g., either analog or digital signals) between redundant portions of safety systems and between safety and non-safety systems in currently operating nuclear power plant designs.

Specifically, § 50.55a(h)(5)(iii)(C) clarifies that communications or signals received by a safety system from outside the division or system should be limited to only those that support the accomplishment of safety functions or otherwise benefit safety. Although this concept has been expressed in previous NRC guidance, the clarity of the guidance has been such that licensees and applicants have not applied this concept consistently. The safety significance of this concept warranted the need for specific regulatory criteria.

For example, complexity is increased by interconnecting safety divisions or connecting maintenance work stations to the safety system. While sharing information among redundant portions of safety systems and between safety systems and other systems could be considered a means to increase safety system reliability and performance, adding complexity to a safety system has the potential to create additional hazards that should be analyzed and addressed. Analyses should (1) ensure the resulting system meets all the criteria in § 50.55a(h)(5); and (2) evaluate the hazards introduced by the added complexity.

Paragraph 50.55a(h)(5)(iii)(D) clarifies the requirements in section 5.6, “Independence” of IEEE Std 603-2009, for communications (e.g., either analog or digital signals) between redundant portions of safety systems and between safety and non-safety systems in new reactor designs.

Paragraph 50.55a(h)(5)(iii)(D) limits the implementation of communications between redundant portions of safety systems and between safety and non-safety systems to limit failure modes and unexpected behaviors associated with communications, while preserving the benefits of digital technology and allowing functionality that improves reliability and availability.

As a general safety principle, hazards should be eliminated when possible during the design stage; otherwise, hazards should be mitigated. Communications that use programmable means to enforce independence could introduce failure modes associated with design errors. By implementing communication independence in the hardware architectural design, the potential for the propagation of design errors is minimized. Failure modes and unexpected behaviors can be minimized in such a design by implementing redundancy in the I&C system architecture design.

Paragraph 50.55a(h)(5)(iii)(D) applies to design certifications; standard design approvals; manufacturing licenses; and combined licenses not referencing a design certification, standard design approval, or manufacturing license under 10 CFR Part 52 issued on or after the effective date of this rule. Paragraph 50.55a(h)(5)(iii)(D) also applies to construction permits and operating licenses under 10 CFR part 50 issued on or after the effective date of this rule, except for an applicant for an operating license who received a construction permit for that facility before the effective date of this rule. For combined licenses issued before the effective date of the rule, § 50.55a(h)(5)(iii)(D) would only apply if the licensee modifies its data communications independence strategy.

For example, if a combined license holder modified its safety I&C system architecture by adding additional controls of safety related equipment from non-safety systems using data communications, then only the modified portion of the architecture would need to comply with the applicable data communications requirements of § 50.55a(h)(5)(iii)(D) (in this example, the applicable requirement is under § 50.55a(h)(5)(iii)(D)(*3*)).

New reactors licensed under the 10 CFR Part 52 process are not required to provide design implementation details at the time of design certification. As stated in § 52.47, the application must contain a level of design information sufficient to enable the NRC staff to reach a final conclusion on all safety questions associated with the design before the certification is granted. The requirements in 10 CFR 50.55a(h) allow new reactor applicants to demonstrate communications independence with a level of design information at the hardware architecture level without the need to provide detailed design implementation information, which is consistent with the requirements of § 52.47. If a new reactor applicant chooses to implement software-based solutions to enforce communications independence, additional design details and implementation information (e.g., software code, testing data, factory acceptance test results, etc.) may be needed in the licensing basis to demonstrate that the software-based solutions to enforce communications independence are safe. Based on experience of new reactor I&C systems reviews conducted prior to the development of the current version of 10 CFR 50.55a(h), many applications did not have this level of information available during the time of design certification or licensing due to the state of maturity of their designs.

It is preferable from a safety and licensing point of view to design systems to promote elimination of failure modes as opposed to incorporating strategies to mitigate the results of failures. New reactor designs are able to more readily accommodate 10 CFR 50.55a(h) requirements as these designs do not have a current licensing basis for an existing system that may impact the particular design. As such, § 50.55a(h)(5)(iii)(D) does not apply to currently operating nuclear power plant licenses or operating licenses with construction permits issued before the effective date of 10 CFR 50.55a(h).

The independence requirements increase consistency of the regulatory framework for I&C systems in advanced reactors by requiring a simplified means to accomplish safety functions. This

approach is supported by the 2007 National Academy of Science Study, "Software for Dependable Systems: Sufficient Evidence?"(Ref. 36), which linked the issue of complexity to the independence design principle. Specifically, the study noted that "the most important form of simplicity is that produced by independence, in which particular system-level properties are guaranteed by individual components much smaller than the system as a whole, which can preserve these properties despite failures in the rest of the system. Independence can be established in the overall design of the system, with the support of architectural mechanisms."

Non-safety digital I&C systems could have failure modes and behaviors that may not be fully identified or adequately mitigated. Specifically, since non-safety systems may not have been developed using rigorous development activities that are required for safety systems (e.g., independent verification and validation and requirements traceability), there is more potential for the software in these non-safety systems to contain errors and defects. It is this potential for latent software design errors and hardware defects that may create failure modes and/or unexpected behavior within a non-safety system that may propagate to safety systems through the communications links of interconnected systems. Paragraph 50.55a(h)(5)(iii)(D)(*1*) is intended to eliminate or mitigate failure modes and unexpected behaviors associated with communication failures among interconnected I&C systems by restricting use of communication links from non-safety systems to safety systems during specific periods of operation.

A further concern regarding non-safety systems is that some of these systems are not required to operate in a predictable and repeatable manner (e.g., no response time requirements, using event driven interrupts). This situation could potentially increase or introduce unidentified failure modes within these non-safety systems. Although safety-related isolation devices can be used to detect and prevent propagation of failures from non-safety systems to safety systems, these isolation devices may not be capable of addressing the effects of failures originating in non-safety systems because the full set of non-safety system failure modes may not be identified or anticipated. In addition, a safety system's ability to address potential failures (e.g. communications errors) propagated by non-safety systems may not be effective in addressing these failures. This situation may arise when the potential failures occur in a manner different than anticipated, and thus the software features in the safety system may not be able to detect or mitigate an unanticipated failure.

Paragraph 50.55a(h)(5)(iii)(D)(*1*) is intended to ensure that data communication from safety systems to non-safety systems is in one direction while the safety system division or channel is in operation, and the one-way communication is accomplished through hardware means. This will allow information to be transmitted to non-safety systems in a manner that prevents the receiving non-safety system from adversely impacting a safety function. By limiting the implementation of the data communication to one direction (i.e., from the safety system to the non-safety system) while the safety system division or channel is in operation, § 50.55a(h)(5)(iii)(D)(*1*) allows for safety and non-safety systems to take advantage of digital technology without adversely affecting safety system functionality.

For example, § 50.55a(h)(5)(iii)(D)(*1*) allows communication from safety systems to non-safety systems for display, control, recording, and diagnostics. Failure modes may still exist with use of data communications within the design; however, if the communication link is a physical one-way connection (i.e., no hand-shaking signal and only a fiber optic or copper wire connection from a transmit port to a receive port), then the failure modes associated with data communications are more effectively addressed by hardware designed to maintain the communication flow. The use of physical mechanisms (i.e., hardware devices) to prevent non-safety to safety system communication while the safety system division or channel is in operation further reduces reliance on software to maintain safety system independence.

Paragraph 50.55a(h)(5)(iii)(D)(*2*) ensures that transfer of signals between redundant portions of safety systems is only accomplished when the signal transferred is required for the performance of safety-

related functions. Although sharing of signals among redundant portions of safety systems could be considered a means to increase safety system reliability, operational performance, and availability, such sharing of signals has the potential to create additional failure modes and unexpected behaviors. The NRC recognizes that there may exist circumstances in which the sharing of information is necessary to accomplish a safety function. The sharing of inputs to the coincidence logic (i.e., combining the logical results of each division to produce a safety system actuation signal) among otherwise independent redundant portions of the protection system has been found acceptable when this communication is required to accomplish safety-related functions or to perform safety interlock functions.

Paragraph 50.55a(h)(5)(iii)(D)(*3*) ensures that, for functions that require safety systems to receive signals from non-safety systems to ensure diversity and defense-in-depth or to support automatic anticipatory reactor trip functions, the signal transfer method is restricted to means that do not use data communication. For example, diverse back-up systems may require connection to safety components to mitigate the effects of beyond design basis safety system common-cause failures. If the diverse back-up system is a non-safety system, then functionality of this system is limited to mitigating the effects of beyond design basis safety system common-cause failures (e.g., the non-safety system should not have the capability to perform control functions or modify safety-related functions during normal operations). Another example is a nuclear power plant design that implements anticipatory reactor trip functions (e.g., reactor shutdown on turbine trip). In these cases, a signal may need to be sent from a non-safety system to the reactor protection system to initiate the anticipatory reactor trip function.

If a signal is needed to support diversity and automatic anticipatory reactor trip functions as described in the examples above, then independence could be achieved through means other than data communications. These alternative means could be accomplished using Class 1E isolators. As required by § 50.55a(h)(5)(ii), the hazards associated with the transmission of these signals over hardwired connections (e.g., EMI, spurious actuations) must be identified and addressed such that it can be demonstrated that a fault in the non-safety system would not propagate to the safety system. The above requirements limit the transfer of signals from non-safety systems to safety systems to reduce interdependencies between safety systems and non-safety systems.

Paragraph 50.55a(h)(5)(iii)(D)(*3*) limits transmission of signals to safety systems from other systems to only those that are necessary to accomplish defense–in-depth, diversity, and automatic anticipatory reactor trip functions. This paragraph does not allow for control of safety equipment from non-safety systems (e.g., non-safety control systems and a multi-divisional display for controlling safety systems). In addition to the potential for errors in non-safety systems to impact the operation of safety systems, control of plant safety equipment could result in conditions that exceed a plant's safety analysis limits. For example, failures in non-safety systems might result in spurious actuation of safety systems that result in plant conditions that exceed safety analysis limits. Limiting the control of safety equipment from non-safety systems reduces the potential for such spurious actuations.

Paragraph 50.55a(h)(5)(iii)(D)(*4*) addresses the potential communication pathways introduced by an alternative approach to 10 CFR 50.55a(h) between a digital safety system and other systems, such as other safety systems or non-safety systems. This paragraph requires applicants of design certifications, standard design approvals, or manufacturing licenses to identify all direct and indirect communication pathways to safety systems to facilitate the identification of interdependences and failure modes in the design. For example, if a non-safety system is connected to a safety system to provide information on the status of the plant (e.g., either directly connected or indirectly through another non-safety system), then this connection must be identified to ensure that failure modes and unexpected behaviors associated with this connection are addressed.

10 CFR 50.55a(h)(6) – Checking the operational availability

Paragraph 50.55a(h)(6) corrects a reference in IEEE Std 603-2009 section 6.5.1, "Checking the operational availability."

Section 6.5.1.b in IEEE Std 603-2009 references section 6.6, "Operating Bypasses." Section 6.6 requires safety systems to automatically override a safety function bypass condition when plant operating conditions require the safety function to be active, which is not relevant to checking operational availability. Section 6.7, "Maintenance Bypass," requires safety systems to accomplish safety functions while sense and command features equipment is in maintenance bypass, which is relevant to checking operational availability.

Since section 6.5.1 addresses checking operational availability of safety functions, which is a maintenance activity, licensees should reference IEEE Std 603-2009 section 6.7, which addresses system bypasses during maintenance activities, instead of referencing section 6.6.

10 CFR 50.55a(h)(7) – Maintenance Bypasses

Paragraph 50.55a(h)(7) clarifies requirements with regard to the ability of the safety system to continue to perform its required safety functions while redundant portions are in maintenance bypass mode. The paragraph also clarifies the need to demonstrate acceptable reliability of the portions of the safety system that are not in maintenance bypass mode. Section 6.7 in IEEE Std 603-2009 states,

> "…Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features should continue to meet the requirements of 5.1 and 6.3."

The accompanying Note for section 6.7 states,

> "NOTE—For portions of the sense and command features that cannot meet the requirements of 5.1 and 6.3 when in maintenance bypass, acceptable reliability of equipment operation shall be demonstrated (e.g., that the period allowed for removal from service for maintenance bypass is sufficiently short, or additional measures are taken, or both, to ensure there is no significant detrimental effect on overall sense and command feature availability)."

In IEEE standards, Notes provide additional information concerning a particular requirement and do not provide mandatory requirements. A "Note" in the text of a requirement in an IEEE standard is an informative (i.e., non-binding) part of the standard; therefore, the IEEE does not allow important information on safety, health, or the environment in a Note. Therefore, the Note in IEEE Std 603-2009 section 6.7 would not become a regulatory requirement or alternative to the requirement(s) in the referencing section although the IEEE Std 603-2009 would be incorporated by reference in § 50.55a.

In contrast to IEEE Std 603-2009, section 6.7 in IEEE Std 603-1991 states,

> "Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of 5.1 and 6.3."

"EXCEPTION: One-out-of-two portions of the sense and command features are not required to meet [section] 5.1 and [section] 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability)."

Section 6.7 in IEEE Std 603-1991, as compared to section 6.7 in IEEE Std 603-2009, provides a more conservative requirement for placing sense and command features equipment in maintenance bypass. Therefore, § 50.55a(h)(7) requires that licensees and applicants meet the requirements stated in section 6.7 of IEEE Std 603-1991.

10 CFR 50.55a(h)(8) – Documentation Supporting Compliance

Paragraph 50.55a(h)(8) requires that applicants and licensees develop and maintain documentation, analyses, and design details demonstrating compliance with §§ 50.55a(h)(2) through (7) to ensure this documentation is accessible to the NRC staff to support independent NRC evaluations of safety systems.

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[1] may use this guide and information regarding the NRC's plans for using this regulatory guide. In addition, this section describes how the NRC staff complies with 10 CFR 50.109, "Backfitting" and any applicable finality provisions in 10 CFR Part 52 "Licenses, Certifications, and Approvals for Nuclear Power Plants."

Use by Licensees

Licensees may voluntarily[2] use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this regulatory guide may be deemed acceptable if they provide sufficient basis and information for the NRC staff to verify that the proposed alternative demonstrates compliance with the appropriate NRC regulations.

Licensees may use the information in this regulatory guide for actions that do not require NRC review and approval such as changes to a facility design under 10 CFR 50.59, "Changes, Tests, and Experiments." Licensees may use the information in this regulatory guide or applicable parts to resolve regulatory or inspection issues.

Use by NRC Staff

The NRC staff does not intend or approve any imposition or backfitting of the guidance in this regulatory guide. The NRC staff does not expect any existing licensee to use or commit to using the guidance in this regulatory guide, unless the licensee makes a change to its licensing basis. The NRC staff expects licensees to adopt this regulatory guide to resolve generic regulatory issues regarding

1 In this section, "licensees" refers to licensees of nuclear power plants under 10 CFR Parts 50 and 52; and the term "applicants," refers to applicants for licenses and permits for (or relating to) nuclear power plants under 10 CFR Parts 50 and 52, and applicants for standard design approvals and standard design certifications under 10 CFR Part 52.

2 In this section, "voluntary" and "voluntarily" means that the licensee is seeking the action of its own accord, without the force of a legally binding requirement or an NRC representation of further licensing or enforcement action.

10 CFR 50.55a(h) requirements. Since this regulatory guide only describes the underlying bases of 10 CFR 50.55a(h) requirements, the NRC staff does not expect or plan to initiate NRC regulatory action that would require the use of this regulatory guide. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of the regulatory guide, requests for information under 10 CFR 50.54(f) as to whether a licensee intends to commit to use of this RG, generic communication, or promulgation of a rule requiring the use of this regulatory guide without further backfit consideration.

During regulatory discussions on plant specific operational issues, the NRC staff may discuss with licensees various actions consistent with NRC staff positions in this RG regarding underlying NRC regulatory requirements. Such discussions would not ordinarily be considered backfitting even if prior versions of this RG are part of the licensing basis of the facility. However, unless this RG is part of the licensing basis for a facility, the NRC staff may not represent to the licensee that the licensee's failure to comply with the positions in this RG constitutes a violation.

If an existing licensee voluntarily seeks a license amendment or change and (1) the NRC staff's consideration of the request involves a regulatory issue directly relevant to this new or revised regulatory guide and (2) the specific subject matter of this RG is an essential consideration in the NRC staff's determination of the acceptability of the licensee's request, then the NRC staff may request that the licensee either follow the guidance in this RG or provide an equivalent alternative process that demonstrates compliance with the underlying NRC regulatory requirements. This is not considered backfitting as defined in 10 CFR 50.109(a)(1) or a violation of any of the issue finality provisions in 10 CFR Part 52.

If a licensee believes that the NRC is either using this RG or requesting or requiring the licensee to implement the methods or processes in this RG in a manner inconsistent with the discussion in this implementation section, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NUREG-1409, "Backfitting Guidelines," (Ref. 37) and the NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 38).

Glossary

In developing the10 CFR 50.55a(h) regulation, the NRC applied the following definitions to describe the underlying bases of the 10 CFR 50.55a(h) paragraphs.

"Current reactors," in the context of 10 CFR 50.55a(h), is defined as nuclear power plants whose construction permits were issued before May 13, 1999.

"Data communication," in the context of 10 CFR 50.55a(h), is defined as a method of transmitting and receiving information in which the information is encoded in a specific format (e.g., header, data content, and end of message) using software.

"Defense-in-depth," in the context of 10 CFR 50.55a(h), is defined as an approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is relied upon exclusively. The defense-in-depth design approach includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures. More succinctly, "defense-in-depth," in the context of 10 CFR 50.55a(h), is defined as the principle of using different functional barriers to the propagation of faults to compensate for failures in other barriers.

"Diversity," in the context of 10 CFR 50.55a(h), is defined as the use of different means including function, design, principles of operation, and organizational and development strategies to compensate for failures within a safety system.

Protection system and safety system diversity strategies use different means to compensate for failures within the protection system and safety system. Defense-in-depth strategies use different functional barriers (e.g., a non-safety control system and a reactor trip system) to compensate for potential failures in other functional barriers. Implementation of defense-in-depth and diversity strategies assure protection and safety system independence from coincident failures or propagated failures due to the effects of natural phenomena , normal operation, postulated functional barrier failure modes, maintenance, testing, and postulated accident conditions.

"Function," in the context of 10 CFR 50.55a(h), is defined as a specific process, action, or task that a system is to perform. More specifically, the term "function" is the process by which inputs into a structure, system, or component are transferred to outputs from the structure, system or component by some mechanism and that, subject to certain controls, can be identified by a function name and can be modeled as a unique entity. For example, a reactor trip system function consists of the reactor process measurement instrumentation, the reactor trip logic processing components, the reactor trip breakers, and the medium by which the input signals, the logic processing signals, and the output signals are transmitted to components in the safety function process (i.e., inputs, processing, outputs, and actuated devices).

"Functionality," in the context of 10 CFR 50.55a(h), is defined as the set of functions or capabilities associated with software, computer hardware, or a component. These functions include the safety functions needed to actuate safety equipment and supporting features that are not required to perform the safety function, such as self-testing and diagnostic features and human-system interface functions.

"Hardwired connections," in the context of 10 CFR 50.55a(h) is defined as a permanent physical point-to-point connection that is used to transmit signals. Hardwired connections can be implemented using various physical media (e.g., copper wire and optical fiber).

"New reactors," in the context of 10 CFR 50.55a(h) is defined as design certifications; standard design approvals; manufacturing licenses; and combined licenses not referencing a design certification, standard design approval, or manufacturing license under 10 CFR Part 52 issued on or after the effective date of the final rule, construction permits and operating licenses under 10 CFR Part 50 issued on or after the effective date of the final rule, except for an applicant for an operating license that received a construction permit for that facility before the effective date of the final rule, and holders of combined licenses issued under 10 CFR Part 52 before the effective date of the final rule, but only if the combined license holder voluntarily modifies its data communication independence strategy.

"Physical mechanism," in the context of 10 CFR 50.55a(h) is defined as a means to enforce one way communication from safety systems to non-safety systems through a hardware-based method such that no software is used to maintain the direction of data flow.

"Predictable," in the context of 10 CFR 50.55a(h), is defined as the ability to determine the output of a system at any time through known relationships among the controlled system states and required responses to those states, such that a given set of input signals will always produce the same output signals.

"Protective function" is defined in IEEE Std 279-1971 as "the sensing of one or more variables associated with a particular generating station condition, signal processing, and the initiation and completion of the protective action at values of the variables established in the design bases."

"Protection system," in the context of 10 CFR 50.55a(h) encompasses all electric and mechanical devices and circuitry (from sensors to actuation device input terminals) involved in generating those signals associated with the protective function. These signals include those that actuate reactor trips and that, following certain events, actuate engineered safeguards such as containment isolation, core spray, safety injection, pressure reduction, and air cleaning.

"Repeatable," in the context of 10 CFR 50.55a(h), is defined as the output of a system being consistently achieved given the same input and system properties (including internal and external conditions).

"Safety benefit," in the context of 10 CFR 50.55a(h), is defined as a justification for adding safety system functionality that is not necessary to accomplish a safety function, but that contributes to safety (e.g., by increasing safety system availability or increasing the safety of a mechanical, nuclear, or electrical system design).

"Safety function," in the context of 10 CFR 50.55a(h), is defined as one of the processes or conditions (for example, emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event. The functional portion of a safety system consists of those functions of a safety system that must operate correctly for the safety system to accomplish its safety function.

"Safety system," in the context of 10 CFR 50.55a(h), is defined as a minimum set of interconnected components, modules, signal processors, and equipment that is relied upon to accomplish one or more safety functions (e.g., equipment relied upon to remain functional during and following design basis accidents). Safety system is a broad-based and all-encompassing term, embracing the protection system in addition to other electrical systems. Thus, the term "protection system" is not synonymous with the term "safety system," but instead is a subset of "safety systems."

The IEEE Std 603-1991 and IEEE Std 603-2009 use the term "safety system" rather than "protection system." A "safety system" is defined in IEEE Std 603-1991 (and in IEEE Std 603-2009) as:

> [a] system that is relied upon to remain functional during and following design basis events to ensure: (i) the integrity of the reactor coolant pressure boundary, (ii) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (iii) the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR Part 100 guidelines.

"Safety system function," in the context of 10 CFR 50.55a(h), is defined as any function performed by the safety system, including safety functions and other functions.

"Signal," in the context of 10 CFR 50.55a(h), is defined as a detectable and measurable representation of a physical quantity by which messages or information can be transmitted. Signals can either be digital or analog in nature.

"Signal sharing," in the context of 10 CFR 50.55a(h), is defined as the replication or duplication of a signal in one system and subsequent transmission to a different system. Signals can be shared through various media, including copper wires and optical links.

"Support(s) safety," in the context of 10 CFR 50.55a(h)(5)(iii)(C), is defined as activities or functions that are necessary to accomplish a safety function or prevent impairment of a safety function.

"Technology," in the context of 10 CFR 50.55a(h), is defined as the methods, techniques, and materials that are used to develop and implement a protection system function or a safety system function. For example, differences in technology exist in the methods, techniques, and materials for implementing a safety function with analog technology, microprocessor technology, and field programmable gate array (FPGA) technology. These technologies are significantly different from one another in system development processes, format of the function logic (e.g., arrangement of discrete electronic components versus software versus hardware description language, respectively), supporting hardware components, and operating and maintenance characteristics. The safety issues arising from these differences in characteristics between technologies could be sufficiently different that a licensee or applicant could be challenged to address issues such as electromagnetic compatibility (EMC), equipment qualification (EQ), common cause failure (CCF) mitigation, and digital communication independence. Converting an analog-based safety function or system into a microprocessor-based safety function or system, and replacing a microprocessor-based safety function or system with an FPGA-based safety function or system are two examples of technology changes.

REFERENCES[3]

1. *U.S. Code of Federal Regulations*, "Domestic Licensing of Production and Utilization Facilities," Part 50, Title 10, "Energy."

2. Institute of Electrical and Electronics Engineers, IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," Piscataway, NJ.[4]

3. Institute of Electrical and Electronics Engineers, IEEE Std 279-1971, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations" Piscataway, NJ.

4. Institute of Electrical and Electronics Engineers, IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.

5. Institute of Electrical and Electronics Engineers, IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" correction sheet issued January 30, 1995, Piscataway, NJ.

6. Institute of Electrical and Electronics Engineers, IEEE Std 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.

7. Institute of Electrical and Electronics Engineers, IEEE Std 603-2009 Correction Sheet dated March 10, 2015, "Errata to IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.

8. *U.S. Code of Federal Regulations*, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Title 10, "Energy."

9. Institute of Electrical and Electronics Engineers, IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Piscataway, NJ.

10. U.S. Nuclear Regulatory Commission, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152, Washington, DC.

11. U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," NUREG-0800, Washington, DC, Agencywide Document Access and Management System (ADAMS) Accession No. ML070630046.

12. U.S. Nuclear Regulatory Commission, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Regulatory Guide 1.180, Washington, DC.

---

3 Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. The documents can also be viewed on-line or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or (800) 397-4209; fax (301) 415-3548; and e-mail pdr.resource@nrc.gov.

4 Copies of Institute of Electrical and Electronics Engineers (IEEE) documents may be purchased from the Institute of Electrical and Electronics Engineers Service Center, 445 Hoes Lane, PO Box 1331, Piscataway, NJ 08855 or through the IEEE's public Web site at http://www.ieee.org/publications_standards/index.html.

13. U.S. Nuclear Regulatory Commission, "Application of the Single-Failure Criterion to Safety Systems," Regulatory Guide 1.53, Washington, DC.

14. Institute of Electrical and Electronics Engineers, IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Piscataway, NJ.

15. U.S. Nuclear Regulatory Commission, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," Regulatory Guide 1.209, Washington, DC.

16. Institute of Electrical and Electronics Engineers, IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Piscataway, NJ.

17. U.S. Nuclear Regulatory Commission, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," Regulatory Guide 1.89, Washington, DC.

18. U.S. Nuclear Regulatory Commission, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," NUREG/CR-6303, Washington, DC, December 1994, ADAMS Accession No. ML071790509.

19. U.S. Nuclear Regulatory Commission, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," NUREG/CR-7007, Washington, DC, ADAMS Accession No. ML100880143.

20. Office of the Federal Register, "Nuclear Regulatory Commission, 10 CFR Part 50, "Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009, NRC-2011-0089, Federal Register Notice (FRN) *xxxxxx*.

21. U.S. Nuclear Regulatory Commission, "Criteria for Safety Systems," Regulatory Guide 1.153, Revision 1, Washington, DC.

22. Institute of Electrical and Electronics Engineers, IEEE Std 603-1977, "Trial-Use Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.

23. Institute of Electrical and Electronics Engineers, IEEE Std 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.

24. Institute of Electrical and Electronics Engineers, IEEE Std 603-1987 , "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations; Correction Sheet—January 1987," Piscataway, NJ.

25. Institute of Electrical and Electronics Engineers, IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.

26. International Atomic Energy Agency, IAEA Safety Guide NS-G-1.1, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants Safety Guide," Vienna, Austria.[5]

5 Copies of International Atomic Energy Agency (IAEA) documents may be obtained through their Web site: WWW.IAEA.Org/ or at http://iaea.org/Publications and by writing the International Atomic Energy Agency P.O. Box 100 Wagramer Strasse 5, A-1400 Vienna, Austria. Telephone (+431) 2600-0, Fax (+431) 2600-7, or E-Mail at Official.Mail@IAEA.Org

27. International Atomic Energy Agency, IAEA Safety Guide NS-G-1.3, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants Safety Guide," Vienna, Austria.

28. International Electrotechnical Commission, IEC 60709, Edition 2.0, "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Separation," Geneva, Switzerland.[6]

29. International Electrotechnical Commission, Geneva, IEC 60780, Edition 2.0, "Nuclear Power Plants—Electrical Equipment of the Safety System—Qualification," Switzerland.

30. International Electrotechnical Commission, IEC 60880, Edition 2.0, "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Software Aspects for Computer-Based Systems Performing Category A Functions," Geneva, Switzerland.

31. International Electrotechnical Commission, IEC 60880-2, Edition 1.0, "Software for Computers Important to Safety for Nuclear Power Plants—Part 2: Software Aspects of Defense against Common Cause Failures, Use of Software Tools and of Pre-Developed Software," Geneva, Switzerland.

32. International Electrotechnical Commission, IEC 60980, Edition 1.0, "Recommended Practices for Seismic Qualification of Electrical Equipment of the Safety System for Nuclear Generating Stations," Geneva, Switzerland.

33. International Electrotechnical Commission, IEC 61226, Edition 3.0, "Nuclear Power Plants—Instrumentation and Control Important to Safety—Classification of Instrumentation and Control Functions," Geneva, Switzerland.

34. International Electrotechnical Commission, IEC 61888, Edition 1.0, "Nuclear Power Plants—Instrumentation Important to Safety—Determination and Maintenance of Trip Setpoints," Geneva, Switzerland.

35. International Electrotechnical Commission, IEC 62385, Edition 1.0, "Nuclear Power Plants—Instrumentation and Control Important to Safety—Methods for Assessing the Performance of Safety System Instrument Channels," Geneva, Switzerland.

36. National Research Council of the National Academies, "Software for Dependable Systems, Sufficient Evidence?" The National Academies Press, Washington, DC.

37. U.S. Nuclear Regulatory Commission, "Backfitting and Information Collection," NUREG-1409, July 1990, ADAMS Accession No. ML032230247.

38. U.S. Nuclear Regulatory Commission, "Management of Facility-specific Backfitting and Information Collection," NRC Management Directive 8.4.

---

6 Copies of International Electrical Commission (IEC) documents may be obtained through their Web site: http://www.iec.ch/ or http://webstore.iec.ch/ and by writing the IEC Central Office at P.O. Box 131, 3 Rue de Varembé, 1211 Geneva, Switzerland, Telephone +41 22 919 02 11.