U.S. NUCLEAR REGULATORY COMMISSION

June 2010
Revision 1

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.62

(Draft was issued as DG-1190, dated December 2008)

MANUAL INITIATION OF PROTECTIVE ACTIONS

A. INTRODUCTION

This guide describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for use in complying with the NRC's regulations with respect to the means for manual initiation of protective actions provided (1) by otherwise automatically initiated safety systems or (2) as a method diverse from automatic initiation. The means for manual initiation of protective actions provided by otherwise automatically initiated safety systems serves a safety-related function to complete all credited protective actions for the safety system as required by Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet, dated January 30, 1995 (Ref. 1). The diverse means for manual initiation should satisfy Point 4 of Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," issued March 2007 (Ref. 2).

The regulatory framework that the NRC has established for nuclear power plants consists of a number of regulations and supporting guidelines applicable to manual initiation of protective actions, including, but not limited to, General Design Criterion (GDC) 1, "Quality Standards and Records"; GDC 13, "Instrumentation and Control"; GDC 21, "Protection System Reliability and Testability"; and GDC 22, "Protection System Independence," as set forth in Appendix A, "General Design Criteria for

---

Nuclear Power Plants," to Title 10, of the *Code of Federal Regulations*, Part 50, "Domestic Licensing of Production and Utilization Facilities," (10 CFR Part 50) (Ref. 3). GDC 13 requires, in part, that appropriate controls be provided to maintain variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems within prescribed operating ranges. GDC 21 requires, in part, that the protection system be designed for high functional reliability. GDC 22 requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation, be used to the extent practical to prevent loss of the protection function.

In 10 CFR 50.55a(h), the NRC requires compliance with IEEE Std 603-1991. For nuclear power plants with construction permits issued before January 1, 1971, the applicants or licensees may elect to comply instead with its plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971, and May 13, 1999, the applicants or licensees may elect to comply instead with the requirements stated in IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations" (Ref. 4).

Working Group Subcommittee 6.3 of the IEEE Nuclear Power Engineering Committee prepared IEEE Std 603-1991, and the IEEE Standards Board approved it on June 27, 1991. The standard provides guidance on the minimum functional design criteria for the electrical power, instrumentation, and control portions of nuclear power plant safety systems. This standard developed from IEEE Std 279-1971 and, through interfaces with other referenced standards, reflects advances in digital technology.

IEEE Std 603-1991 uses the term "safety systems" rather than "protection systems" to define its scope. This standard defines a "safety system" 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 offsite exposures comparable to the 10 CFR Part 100 guidelines." In addition, IEEE Std 603-1991 defines a "safety function" 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." Finally, the standard defines a "division" as "the designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components."

IEEE Std 279-1971 states that a "protection system" 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 a reactor trip and that, in the event of a serious reactor accident, actuate engineered safety features such as containment isolation, core spray, safety injection, pressure reduction, and air cleaning. This standard defines "protective function" 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."

Section 4.17 of IEEE Std 279-1971 requires, in part, that protection systems include the means for manual initiation of each protective action at the system level and that the single-failure criterion, as set forth in Section 4.2 of IEEE Std 279-1971, be met. Section 6.2 of IEEE Std 603-1991 requires, in part, that means be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions and those protective actions identified by Section 4.5 that have not been selected for automatic control. Section 6.2 of IEEE Std 603-1991 further requires, in part, that means be provided in the control room to implement the manual actions necessary to maintain safe control after the protective actions are completed.

In SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993 (Ref. 5), the staff made an initial statement of a four-point diversity and defense-in-depth (D3) position. In a staff requirements memorandum regarding SECY-93-087, dated July 21, 1993 (Ref. 6), the Commission approved a modified version of the four-point position. This guidance was incorporated into BTP 7-19. The fourth point of BTP 7-19 states, in part, that independent and diverse displays and manual controls should be available in the main control room so that operators can initiate a system-level actuation of critical safety functions.

This regulatory guide contains information collection requirements covered by 10 CFR Part 50 and 52 that the Office of Management and Budget (OMB) approved under OMB control numbers 3150-0011 and 3150-0151. 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

Existing instrumentation and control (I&C) equipment in nuclear power plants is currently being replaced with computer-based digital I&C systems or advanced analog systems. However, if designed, installed, operated, or maintained improperly, these technologies may pose new vulnerabilities for the nuclear power plant, compared to existing I&C systems. This regulatory guide provides an acceptable method for establishing the design criteria for existing I&C systems and for establishing the design criteria for digital and advanced analog systems for the manual initiation of protective actions. To meet these objectives, (1) manual initiation of protective actions provided by otherwise automatically initiated safety systems must meet the requirements in IEEE Std 603-1991 in regard to manual initiation as incorporated in 10 CFR 50.55a(h), and (2) manual initiation of protective actions provided as a diverse method for automatic initiation should meet the guidance specified in Point 4 of BTP 7-19.

1. Meeting IEEE Std 603-1991 requirements:

IEEE Std 603-1991 defines a "protective action" as "the initiation of a signal within the sense and command features or the operation of equipment within the execute features of the safety system for the purpose of accomplishing a safety function." Sections 6.2 and 7.2 of IEEE Std 603-1991 provide the general functional, design, and executive requirements for manual control. Section 6.2 specifically states that means shall be provided to (1) implement manual initiation at the division level of all automatically initiated protective actions, while maintaining independence between redundant portions of the safety system, (2) implement manual system initiation and control of the protective actions not selected for automatic controls, based on the analysis conducted in Section 4.5 of IEEE Std 603-1991, and (3) maintain the plant in a safe condition after the protective actions are completed, using manual controls. The number of discrete operator manipulations to implement manual initiation of protective actions shall be minimized and shall depend on the operation of a minimum amount of equipment. Section 5.8.4 requires, in part, that indications required for manually controlled protective actions shall be accessible to the operator and visible from the location of the controls used to effect the actions. Another acceptable method is the system-level manual initiation of protective actions that results in the actuation of all divisions at once if it meets the independence, single failure, and minimum equipment requirements of IEEE Std 603-1991. Section 7.2 requires, in part, that additional design features in the execute features necessary to accomplish manual control of the actuated component shall not defeat the requirements of the single-failure criterion.

Design analyses determine the appropriate safety functions and corresponding protective actions for each plant design. The protective actions can be initiated automatically, or, in certain cases, can be accomplished solely by manual controls. Protective actions initiated solely by manual controls are subject to consideration of (1) the time necessary for the operator to analyze and manually respond to an adverse condition, (2) the time available for actions to be taken to mitigate adverse plant conditions, (3) the plant conditions expected at the time operation of manual controls is credited, (4) the range of conditions over which manual controls are expected to be in effect, and (5) the display variables necessary to provide for effective manual control.

Once initiated, the intended sequence of protective actions should continue until completion, whether the initiation occurred through automatic controls or through manual controls, as outlined in Section 5.2 of IEEE Std 603-1991. However, it is acceptable for protective equipment interlocks to interrupt a sequence of protective actions. In addition, when directed by procedure, it is acceptable for an operator to deliberately intervene in the intended sequence of protective actions, such as in the case of a verified spurious actuation of a protective action.

Section 5.6.3.1 of IEEE Std 603-1991 specifies that interconnected “equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems.” Therefore, equipment that is not classified as part of a safety system must not be credited for performing safety functions. Nevertheless, nonsafety multidivisional control and display stations may be used to perform functions that support plant safety. The control and monitoring of functions credited with the protection of the plant in the plant safety analyses must be capable of being performed using only safety-related resources. Nonsafety multidivisional control and display stations may supplement the safety-related control and display equipment that is credited in the plant’s safety analyses.

Display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems, in accordance with IEEE Std 603-1991, Section 5.8.1. This section states, in part, that indications for manually controlled actions shall have the possibility for ambiguity minimized to limit the potential to confuse an operator. Indications should also (1) be readily present during the time that manual actuation is necessary, (2) be visible from the location of the manual controls, and (3) provide unambiguous indications that will not confuse the operator. Regulatory Guide 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants” (Ref. 7), endorses IEEE Std 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations” (Ref. 8), as an acceptable method for providing instrumentation to monitor variables for accident conditions.

The single-failure criterion in IEEE Std 603-1991, Section 5.1, applies to safety systems, whether control is by automatic or manual means. Regulatory Guide 1.53, “Application of the Single-Failure

Criterion to Safety Systems" (Ref. 9), endorses IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Ref. 10), as an acceptable method to meet the regulations concerning the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems. Digital system common-cause failures are not treated as a single failure with respect to the single-failure criterion.

Maintaining independence between redundant portions of the safety system is essential to the effective use of the single-failure criterion. Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems" (Ref. 11), provides guidance through the application of IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Ref. 12), to meet the regulations with respect to the physical independence requirements of the circuits and electric equipment that comprise or are associated with safety systems. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. 13), endorses IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Ref. 14), as an acceptable method for addressing high functional reliability and design requirements for computers used in safety systems of nuclear power plants, including communication independence.

Section 5.4 of IEEE Std 603-1991 requires that safety system equipment be environmentally qualified. Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Controls Systems in Nuclear Power Plants" (Ref. 15), endorses IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" (Ref. 16), as acceptable guidance for the environmental qualification of safety-related, computer-based I&C systems for service in mild environments. Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants" (Ref. 17), provides guidance for the environmental qualification of equipment intended for use in harsh environments. Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems" (Ref. 18), provides guidance for complying with the NRC's regulations on design, installation, and testing practices for addressing the effects of electromagnetic and radiofrequency interference and power surges on safety-related I&C systems. Clause 5.4 of IEEE Std 7-4.3.2-2003 provides requirements for the equipment qualification of digital computers used in safety systems.

2. Meeting BTP 7-19 guidance:

The potential for common-cause failure has become increasingly important as the complexity of digital and advanced analog protection systems has increased. Credible common-cause failures should be addressed by D3 in the system design. Approaches to address D3 considerations for automatically initiated protective actions may include the use of diverse nonsafety manual controls. IEEE Std 7-4.3.2-2003 provides guidance on using diversity to address common-cause failures in computer-based safety systems. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994 (Ref. 19), describes a method for analyzing computer-based nuclear reactor protection systems to identify design vulnerabilities to common-cause failure. The fourth point of the Commission's diversity position listed in BTP 7-19 states, in part, that independent and diverse displays and manual controls should be available in the main control room so that operators can initiate a system-level actuation of critical safety functions. These displays and controls may be safety or nonsafety. Guidance provided to the NRC staff in BTP 7-19 asserts that manual controls provided for compliance with Point 4 of the NRC position on D3 should be connected downstream of the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. The manual controls may be connected either to discrete hardwired components or to simple, dedicated, and diverse software-based digital equipment that performs the coordinated actuation logic. Nevertheless, for digital system modifications to operating plants, retention of existing displays and controls in the main control room may satisfy this fourth point.

3. Meeting both IEEE Std 603-1991 requirements and BTP 7-19 guidance:

As an alternative to the two different manual controls discussed above, applicants or licensees may propose, as an optional acceptable method, a single safety-related means of manual initiation of protective actions that satisfies the criteria of both IEEE Std 603-1991 and Point 4 of the NRC position on D3.

C. REGULATORY POSITION

Regulatory Positions 1, 2, 3, 4, 5, and 6 below provide an acceptable method for complying with IEEE Std 603-1991 in regard to the manual initiation of protective actions. The manual initiation of protective actions noted below are at the divisional-level basis. However another acceptable method is the system-level manual initiation of protective actions that results in the actuation of all divisions at once. The system-level method is acceptable as long as the requirements for independence, single failure criteria, and minimum equipment in the IEEE Std 603-1991 are met. Position 7 is an acceptable method for diverse manual initiations of protective actions that satisfies Point 4 of BTP 7-19. Position 8 is an optional acceptable method for satisfying both IEEE Std 603-1991 requirements and Point 4 of BTP 7-19 guidance.

1. Means should be provided for the manual initiation of each protective action (e.g., reactor trip, containment isolation) on a division-level basis, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve).

2. Manual initiation of a protective action on a division-level basis should perform all actions performed by automatic initiation, such as starting auxiliary or supporting systems, sending signals to appropriate valve-actuating mechanisms to ensure correct valve position, and providing the credited action-sequencing functions and interlocks.

3. The control interfaces for manual initiation of protective actions on a division-level basis should be located in the control room. They should be easily accessible to the operator so that action can be taken in an expeditious manner at the point in time or under the plant conditions for which the protective actions of the safety system shall be initiated, as required in Section 4.10.1 of IEEE Std 603-1991. Information displays associated with manual controls should (i) be readily present during the time that manual actuation is necessary, (ii) be visible from the location of the manual controls, and (iii) provide unambiguous indications that will not confuse the operator.

4. No single failure within the manual, automatic, or common portions of the protection system should prevent initiation of a protective action by manual or automatic means.

5. Manual initiation of protective actions should depend on the operation of a minimum amount of equipment, consistent with Positions 1, 2, 3, and 4 above.

6. Manual initiation of a protective action on a division-level basis should be designed so that, once initiated, the action will go to completion, as required in Section 5.2 of IEEE Std 603-1991.

7. In providing diverse manual initiation of protective actions, a set of independent and diverse displays and manual controls should be provided in the main control room. These displays and controls may be safety or nonsafety. The point at which the manual controls are connected to safety equipment should be downstream of the digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment.

8. An optional acceptable method that satisfies both requirements of IEEE Std 603-1991 and guidance on Point 4 of the NRC position on D3, would be a single safety related manual initiation of protective actions that satisfies Positions 1, 2, 3, 4, 5, 6, and 7 above.

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the NRC's plans for using this regulatory guide. The NRC does not intend or approve any imposition or backfit in connection with its issuance.

In some cases, applicants or licensees may propose or use a previously established acceptable alternative method for complying with specified portions of the NRC's regulations. Otherwise, the methods described in this guide will be used in evaluating compliance with the applicable regulations for license applications, license amendment applications, and amendment requests.

REFERENCES

1. IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Piscataway, NJ, 1991, and the correction sheet, dated January 30, 1995.[1]

2. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)," Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Washington, DC, March 2007.[2]

3. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.[3]

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

5. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," U.S. Nuclear Regulatory Commission, Washington, DC, April 2, 1993.[4]

6. Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," U.S. Nuclear Regulatory Commission, Washington, DC, July 21, 1993.

7. Regulatory Guide 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC.[5]

---

[1] Copies of Institute of Electrical and Electronics Engineers (IEEE) standards may be purchased from the IEEE Standards Association, 445 Hoes Lane, Piscataway, NJ 08855-1331; telephone (800) 678 4333. Purchase information is available through the IEEE Standards Association Web site at http://www.ieee.org.

[2] All NUREG-series reports listed herein were published by the U.S. Nuclear Regulatory Commission. Copies are available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; e-mail pdr.resource@nrc.gov.

[3] All NRC regulations listed herein are available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/cfr/part050. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; e-mail pdr.resource@nrc.gov.

[4] Commission Papers (SECY) listed herein are available electronically through the Public Electronic Reading Room on the NRC's public Web, site at http://www.nrc.gov/reading-rm/doc-collections/commission/secys/
Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; e-mail pdr.resource@nrc.gov.

[5] All regulatory guides listed herein were published by the U.S. Nuclear Regulatory Commission. Where an ADAMS accession number is identified, the specified regulatory guide is available electronically through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html. All other regulatory guides are available electronically through the Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/.

8. IEEE Std 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2002.

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

10. IEEE Std 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2000.

11. Regulatory Guide 1.75, “Criteria for Independence of Electrical Safety Systems,” U.S. Nuclear Regulatory Commission, Washington, DC.

12. IEEE Std 384-1992, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 1992.

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

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

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

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

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

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

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