U.S. NUCLEAR REGULATORY COMMISSION

February 2010
Revision 1

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.47

(Draft was issued as DG-1205, dated October 2008)

BYPASSED AND INOPERABLE STATUS INDICATION FOR NUCLEAR POWER PLANT SAFETY SYSTEMS

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 a bypassed and inoperable status indication for nuclear power plant safety systems.

The regulatory framework that the NRC has established for nuclear power plants consists of a number of regulations and supporting guidelines applicable to a bypassed and inoperable status indication, including, but not limited to, General Design Criterion (GDC) 1, "Quality Standards and Records"; GDC 13, "Instrumentation and Control"; GDC 19, "Control Room"; GDC 21, "Protection System Reliability and Testability"; GDC 22, "Protection System Independence"; and GDC 24, "Separation of Protection and Control Systems," 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. 1). GDC 1 requires that structures, systems, and components important to safety be designed and installed to quality standards commensurate with the importance of the safety functions to be performed. GDC 13 requires 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 19 requires that a control room be provided from which actions can be taken to operate the

---

The NRC issues regulatory guides to describe and make available to the public methods that the NRC staff considers acceptable for use in implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in reviewing applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions that differ from those set forth in regulatory guides 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 Commission.

This guide was issued after consideration of comments received from the public.

Regulatory guides are issued in 10 broad divisions—1, Power Reactors; 2, Research and Test Reactors; 3, Fuels and Materials Facilities; 4, Environmental and Siting; 5, Materials and Plant Protection; 6, Products; 7, Transportation; 8, Occupational Health; 9, Antitrust and Financial Review; and 10, General.

Electronic copies of this guide and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC's Electronic Reading Room at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No.ML092330064.

nuclear power unit safely under normal operating conditions. GDC 21 requires that the protection system be designed for high functional reliability and inservice testability. GDC 22 requires that the protection system either be designed to ensure that the effects of normal operating, maintenance, and testing on redundant channels do not result in the loss of the protection function or be demonstrated to be acceptable on some other defined basis. GDC 24 requires that the interconnection of the protection and control systems be limited to ensure that safety is not significantly impaired.

In 10 CFR 50.55a(h), the NRC requires compliance with 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. 2). For nuclear power plants with construction permits issued before January 1, 1971, the applicant/licensee 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 applicant/licensee may elect to comply instead with the requirements in IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations" (Ref. 3). Both IEEE Std 603-1991 and IEEE Std 279-1971 list requirements with regard to a bypassed and inoperable status indication for safety systems. In addition, Criterion XIV, "Inspection, Test, and Operating Status," as given in Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50, requires that measures be established for indicating the operating status of structures, systems, and components of the nuclear power plant, such as by tagging valves and switches, to prevent inadvertent operation. The provisions of 10 CFR 50.34(f)(2)(v) also require an automatic indication of the bypassed and operable status of safety systems.

IEEE Std 603-1991 uses the term "safety systems" rather than "protection systems" to define its scope. The standard offers the following definition of a "safety system":

> …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." The standard also 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 4.13 of IEEE Std 279-1971 requires, in part, that, if the protective action of some part of the protection system has been bypassed or deliberately rendered inoperable for any purpose, this fact shall be continuously indicated in the control room. Section 5.8.3 of IEEE Std 603-1991 requires that, if the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room. Section 5.8.3 also states that (1) the bypass display instrumentation need not be part of the safety systems, (2) this indication shall be automatically actuated if the bypass or inoperative condition is (a) expected to occur more frequently than once a year and (b) expected to occur when the affected system is required to be operable, and (3) the capability shall exist in the control room to manually activate this display indication.

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

The Working Group Subcommittee 6.3 of the IEEE Nuclear Power Engineering Society developed 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 evolved from IEEE Std 279-1971 and, through interfaces with other referenced standards, reflects advances in digital technology. Nuclear power plants are replacing existing instrumentation and control (I&C) equipment with digital computer-based or advanced analog I&C systems. However, if designed, installed, operated, or maintained improperly, these technologies may pose new vulnerabilities for nuclear power plants, 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 a bypassed and inoperable status indication.

Section 5.8 of IEEE Std 603-1991 presents the requirements for safety system information displays. Section 5.8.2 of IEEE Std 603-1991 states, in part, that "display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status." Section 5.8.3 of the standard provides the specific guidance on the indication of bypasses, which may be provided by a nonsafety system. The section states, "If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room." IEEE Std 603-1991 defines a safety group as "a given set of interconnected components, modules, and equipment that can accomplish a safety function." Section 5.8.3.2 of IEEE Std 603-1991 specifically states that the indication of bypasses "shall be automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year and (b) is expected to occur when the affected system is required to be operable." Section 5.8.4 of the standard requires that the location of information displays be "accessible to the operator."

Current designs of safety systems and protective actions are such that certain safety functions of a nuclear power plant may be bypassed or made inoperable during the performance of periodic tests or maintenance. Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems"

(Ref. 4), endorses IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems" (Ref. 5), as an acceptable method for the periodic testing of electric power and protection systems. Generally, the plant's administrative procedures require that the operator give permission before the initiation of any activity that would or could affect a safety system. The decision to grant such permission should be based on knowledge of the operating status of the safety systems, the extent to which the activity will affect those systems, and whether that effect is permissible within the provisions of the license. Experience at operating plants, however, suggests that when the measures used to indicate inoperable status consist solely of administrative procedures, the operator is not always fully aware of the ramifications of each bypassed or inoperable component. An automatic indication display of any bypass or inoperability in a safety system supplements administrative procedures and aids the operator. Clause 5.16 of IEEE Std 338-1987 states that "indication should be provided in the control room if a portion of the safety system is inoperable or bypassed. Systems that are frequently placed in bypass or inoperative condition for the purposes of testing should have automatic indication."

Digital computer-based I&C systems make extensive use of self-testing. Digital computer-based I&C systems, if designed, installed, operated, or maintained improperly, are more prone to different kinds of failures than traditional analog systems. Self-testing and watchdog timers should reduce the time to detect and identify failures. Computer self-testing is most effective at detecting random hardware failures. A bypass and inoperable status indication system should include a capability of ensuring its operable status during normal plant operation to the extent that the indicating and annunciating function can be verified. However, the bypass and inoperable status indication system should be designed to avoid erroneous bypass indications. If the use of self-testing in digital computer-based I&C systems causes a protective action of some part of a safety system to be bypassed or deliberately rendered inoperative, then this fact should be automatically indicated in the control room.

With regard to surveillance testing, if the protective action of some part of a protection or safety system is bypassed or deliberately rendered inoperative for testing, that fact should be continuously indicated in the control room. Operations staff should also be able to confirm that a bypassed safety system has been properly returned to service. In a given plant design, it may be best to group the bypass indicators according to the dependence of the safety systems on a common electric power supply; for example, the bypass indicators for all engineered safety feature systems that are assigned to one standby power source could be located near the bypass indicator for that source. Other groupings could be acceptable. The arrangement of bypass indicators should enable the operator to determine the status of each safety system and whether continued reactor operation is permissible. When a protective function of a shared system can be bypassed, the control room of each affected unit should receive an indication of that bypass condition. In any design, it may be necessary to include an audible, as well as visual, alarm to attract the operator's attention when the status of the safety system changes.

Section 5.8.3.3 of IEEE Std 603-1991 requires that, for an indication of bypasses, "the capability shall exist in the control room to manually activate this display indication." The effectiveness of an automatic indicating system is enhanced by including a manual capability to activate the indicators. Manual capability is useful in displaying those inoperable or bypassed conditions, whether deliberately induced or not, that are not automatically indicated.

The bypass indication should aid the operator in recognizing the effects on plant safety of seemingly unrelated or insignificant events. Therefore, the indication of bypass conditions should be at the safety group level, whether or not it is also at the channel, component, or module level. Clause 5.8.3.1 of

IEEE Std 603-1991 states that "this display instrumentation need not be part of the safety systems." The indication system should be designed and installed in a manner that precludes the possibility of adverse effects on plant safety systems. The bypass and inoperable status indications may be provided using operator workstations or hardwired indicators and analog signal processing circuits.

Section 5.6.3.1(1) of IEEE Std 603-1991 specifies, in part, that interconnected "equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems." Equipment that is not classified as part of the safety systems must not be credited for performing safety functions. Unless the indication system is designed in conformance with criteria established for safety systems, it should not be used to perform functions that are essential to safety, and administrative procedures should not require immediate operator action based solely on bypass indications. If an operator action is based solely on the bypass indications, and this action is required to maintain the integrity of the safety systems, then the status indication should be classified as part of the safety systems, and the following paragraphs addressing single failure, independence, and qualification would apply.

If the bypass and inoperable status indication is part of the safety systems, then the single-failure criterion of IEEE Std 603-1991, Section 5.1, would apply to the indication system. Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Safety Systems" (Ref. 6), endorses IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Ref. 7), 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.

In addition to meeting the single-failure criterion, if the bypass and inoperable status indication is part of the safety systems, then 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. 8), provides guidance through the application of IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Ref. 9), 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 Digital Computers in Safety Systems of Nuclear Power Plants" (Ref. 10), endorses IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Ref. 11), as an acceptable method for addressing high functional reliability and design requirements for computers used in the safety systems of nuclear power plants, including safety-related digital communications, independence, and integrity.

If a bypass and inoperable status indication is part of the safety systems, the equipment qualification criterion of IEEE Std 603-1991, Section 5.4, would apply to the indication system. Section 5.4 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. 12), endorses IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" (Ref. 13), 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. 14), 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. 15), presents 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.

C. REGULATORY POSITION

The following regulatory positions provide the supplemental guidance for implementing IEEE Std 603-1991 to satisfy the NRC regulatory requirements with respect to the bypassed and inoperable status indication for nuclear power plant safety systems:

1. Administrative procedures should be supplemented by an indication system that automatically indicates, for each affected safety system or subsystem, the bypass or deliberately induced inoperability of a safety function and the systems actuated or controlled by the safety function. Provisions should also be made to allow the operations staff to confirm that a bypassed safety function has been properly returned to service.

2. The indicating system of Position 1 above should also be activated automatically by the bypassing or the deliberately induced inoperability of any auxiliary or supporting system that effectively bypasses or renders inoperable a safety function and the systems actuated or controlled by the safety function.

3. Annunciating functions for system failure and automatic actions based on the self-test or self-diagnostic capabilities of digital computer-based I&C safety systems should be consistent with Positions 1 and 2 above.

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

5. Bypass and inoperable status indicators should be arranged such that the operator can determine whether continued reactor operation is permissible. The control room of all affected units should receive an indication of the bypass of shared system safety functions.

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

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, design certifications, license amendment applications, and amendment requests.

REFERENCES[1]

1. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

2. 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.[2]

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

4. Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," U.S Nuclear Regulatory Commission, Washington, DC.

5. IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," Institute of Electrical and Electronics Engineers, Piscataway, NJ, 1987.

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

7. 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.

8. Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems," U.S. Nuclear Regulatory Commission, Washington, DC.

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

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

11. 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.

---

[1] Publicly available NRC published documents such as Regulations, Regulatory Guides, NUREGs, and Generic Letters listed herein are available electronically through the Electronic Reading Room on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. Copies are also available for inspection or copying for a fee from 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.

2 Copies of the non-NRC documents included in these references may be obtained directly from the publishing organization.

12. 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.

13. 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.

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

15. 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.