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

October 2006
Division 1

DRAFT REGULATORY GUIDE

Contact: P. Kang
(301) 415-6800

DRAFT REGULATORY GUIDE DG-1142

(Previously Issued as Draft Regulatory Guide DG-1077, dated September 2001)

GUIDELINES FOR ENVIRONMENTAL QUALIFICATION OF SAFETY-RELATED COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR POWER PLANTS

A. INTRODUCTION

Title 10, Part 50, "Domestic Licensing of Production and Utilization Facilities," of the *Code of Federal Regulations* (10 CFR Part 50) delineates the design- and qualification-related regulations that the U.S. Nuclear Regulatory Commission (NRC) has established for commercial nuclear power plants. In particular, General Design Criterion 4 in Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50 requires that structures, systems, and components (SSCs) important to safety shall be designed to accommodate the effects of, and to be compatible with, the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (i.e., the equipment shall remain functional under postulated accident conditions). The following sections of 10 CFR Part 50 specify general requirements:

- 10 CFR 50.55a, "Codes and Standards"
- Appendix A, General Design Criteria 1, 2, 4, 13, 21, 22, and 23
- Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," specifically Criterion III, "Design Control," Criterion XI, "Test Control," and Criterion XVII, "Quality Assurance Records"

According to 10 CFR 50.55a(h)(2), protection systems shall meet the requirements set forth in the Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995, or IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," contingent on the date that the NRC issued the related construction permit. The design-basis criteria identified by those standards or by similar provisions in the licensing basis for such facilities include the range of transient and steady-state environmental conditions throughout which the equipment shall perform during normal, abnormal, and accident operational events.

As reported in NUREG/CR-5904, "Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Reactors," issued April 1994, safety-related microprocessor-based electric equipment can pose unique functional and qualification issues. Traditional testing and evaluation approaches developed primarily for analog equipment may not fully address these digital issues. The primary focus of IEEE Std. 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," is the reliable operation of safety-related equipment under normal, abnormal, design-basis accident, post-design-basis accident, and containment test conditions. At present, computer-based instrumentation and control (I&C) systems are primarily implemented in nuclear power plant locations that are characterized as mild environments that are not affected by design-basis accident conditions. Thus, the design-basis accident element of type testing for qualification does not apply to computer-based I&C systems in mild environments. In addition, because of ready accessibility for monitoring and maintenance in mild environments, the need to establish a qualified life does not apply. Nonetheless, the qualification criterion of 10 CFR 50.55a(h)(2) shall be addressed for safety-related computer-based I&C systems.

This regulatory guide 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. Adherence to these qualification practices contributes to ensuring that a computer-based I&C system can perform its safety-related function under all anticipated service conditions. This guide complements Revision 1 of Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," issued June 1984, which addresses compliance with 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," for harsh environments that are subject to design-basis accidents.

The NRC staff accepted the Electric Power Research Institute (EPRI) Topical Report (TR) 107330, "Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," in a safety evaluation report (SER) by letter dated July 30, 1998. The EPRI report includes guidance on an acceptable method for addressing mild-environment qualification of programmable logic controllers (PLCs). The mild-environment qualification practices endorsed in this regulatory guide are equivalent to, and consistent with, those described in the EPRI TR. The primary distinctions between the two methods are that the scope of this regulatory guide focuses exclusively on environmental qualification, while the EPRI report covers a more extensive scope (e.g., platform evaluation, selection, procurement, qualification, and quality assurance); this regulatory guide addresses all safety-related computer-based I&C systems, while the EPRI report focuses on PLC platforms; and this regulatory guide endorses the current national qualification standard, while the EPRI report provides guidance based on a previous version of the national qualification standard (i.e., IEEE Std. 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations").

The qualification practices endorsed in this regulatory guide are based on the current consensus national standard and employ sound engineering practices for ensuring environmental compatibility of a computer-based I&C system with the environment in which it operates. These practices apply to safety-related computer-based I&C systems intended for implementation in mild environments within a nuclear power plant. The NRC gives the technical basis for the selection of these particular practices in NUREG/CR-6479, "Technical Basis for Environmental Qualification of Microprocessor-Based Safety-Related Equipment in Nuclear Power Plants," issued January 1998.

The following related publications include supporting technical findings that were considered in determining the qualification needs for safety-related computer-based I&C systems:

- NUREG/CR-5904
- NUREG/CR-6406, "Environmental Testing of an Experimental Digital Safety Channel," issued September 1996
- NUREG/CR-6476, "Circuit Bridging of Components by Smoke," issued October 1996
- NUREG/CR-6543, "Effects of Smoke on Functional Circuits," issued October 1997
- NUREG/CR-6579, "Digital I&C Systems in Nuclear Power Plants: Risk-Screening of Environmental Stressors and a Comparison of Hardware Availability with an Existing Analog System," issued January 1998
- NUREG/CR-6597, "Results and Insights on the Impact of Smoke on Digital Instrumentation and Controls," issued January 2001
- NUREG/CR-6741, "Application of Microprocessor-Based Equipment in Nuclear Power Plants — Technical Basis for Qualification Methodology," issued January 2003

In general, the NRC's NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," issued 2003, reflects the information provided in regulatory guides. The NRC Office of Nuclear Reactor Regulation uses the Standard Review Plan as guidance in reviewing applications to construct and operate nuclear power plants. This regulatory guide will apply to the 1997 Revision 4 of Chapter 7, "Instrumentation and Controls," of the Standard Review Plan.

The NRC issues regulatory guides to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations, and compliance with regulatory guides is not required. The NRC issues regulatory guides in draft form to solicit public comment and involve the public in developing the agency's regulatory positions. Draft regulatory guides have not received complete staff review and, therefore, they do not represent official NRC staff positions.

This regulatory guide contains information collections that are covered by the requirements of 10 CFR Part 50 which 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

Both Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," issued November 1974, and Revision 1 of Regulatory Guide 1.89 (1984) endorse IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." Regulatory Guide 1.89 specifically limits its scope to compliance 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." Thus, Regulatory Guide 1.89 focuses on the environmental qualification of equipment intended for use in harsh environments that are subject to design-basis accidents.

The IEEE Std. 323 definition of qualification is "generation and maintenance of evidence to ensure that the equipment will operate on demand to meet system performance requirements." In effect, environmental qualification is verification and validation that a design adequately accommodates the effects of, and is compatible with, the environmental conditions associated with the normal, abnormal, and accident conditions that the equipment or system might encounter. The *Code of Federal Regulations* defines a mild environment as one "that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences." However, as a mild environment in a nuclear power plant can encompass environmental conditions that can affect the performance of sensitive equipment, qualification to demonstrate compatibility with those environmental conditions is necessary in those cases. Because Regulatory Guide 1.89 limits its scope to equipment intended for application in harsh environments, additional guidance is warranted to address qualification for mild environmental conditions, as needed for computer-based technologies.

IEEE revised the industry guidance for qualification, IEEE Std. 323, in 2003. A particular distinction between IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and IEEE Std. 323-1974 is that the current version does not require age conditioning to an end-of-installed-life condition for equipment in mild environments where significant aging mechanisms are not present. The practices in IEEE Std. 323-2003 are sufficiently comprehensive to address qualification for the less severe environmental conditions of typical plant locations where safety-related computer-based I&C systems are generally located. These plant areas are unaffected by design-basis accidents and the most severe conditions to which the equipment is subjected, which arise from the environmental extremes resulting from normal and abnormal operational occurrences.

Use of computers in safety systems poses challenges that differ from those associated with analog systems, prompting the development of IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," issued in 1993 and revised in 2003. This standard emphasizes that the application of computers in safety systems needs to address reliability and environmental compatibility. In particular, Annex F.2.3 to IEEE Std. 7-4.3.2 states that analyses must be performed to ensure both that the system has a high "correct response probability" and that the probability of common-cause failure is reduced to an acceptable level. Addressing qualification requirements for safety-related computer-based I&C systems is one method of ensuring that the probability of common-cause failure attributable to environmental stressors is reduced to an acceptable level. Specifically, Section 5.4.1 of IEEE Std. 7-4.3.2 provides criteria for the equipment qualification of computer-based safety systems, including performing testing under environment stress with the full range of safety-related software functioning.

Computer-based I&C systems present unique characteristics that must be considered in the qualification process. These characteristics include both functional and hardware considerations. One significant difference between analog and digital equipment is the higher functional density that is possible with computer-based I&C systems. Because of the expanding single-chip capabilities, many safety-related installations involve replacement of multiple functional modules with a multifunction microprocessor-based module. Another difference involves the sequential function execution that typifies computer-based I&C systems compared to the essentially parallel execution of analog modules. The effect of this behavior can be compounded for multiple systems that rely on either successful completion of digital data communication or error detection before continuation of discrete functional steps. The capability of digital system design accommodates the potentially cumulative effects of environmental stress and is an important consideration for qualification of computer-based I&C systems.

From a hardware standpoint, one significant difference between analog and advanced digital systems is the radiation tolerance of different integrated circuit (IC) technologies. The analog technology historically used in nuclear power plants includes discrete bipolar devices. Advanced digital systems tend to use metal oxide semiconductor (MOS) technology, particularly complementary MOS (CMOS) technology. The radiation threshold for MOS devices is generally lower than those for bipolar (analog) devices. However, MOS technology is preferred for ICs because of its technical superiority in other areas (such as higher input impedance, fewer manufacturing processing steps, better temperature stability, and lower noise). Commercial MOS devices are very sensitive to ionizing doses, in contrast to their relative insensitivity to neutron fluence. Ionizing dose radiation hardness levels for MOS IC families range from about 10 gray (Gy) or 1 kilorad (krad) for commercial off-the-shelf (COTS) circuits to about 10^5 Gy (10^4 krad) for radiation-hardened circuits. The threshold fluence hardness level for MOS devices is about 10^{14} neutrons per square centimeter (n/cm^2), 1 million electron volts (MeV) equivalent. In contrast, the ionizing radiation hardness level range for bipolar devices begins around 10^4 Gy (1000 krad). The threshold fluence hardness level for bipolar devices ranges on the order of 10^{14} to 10^{15} n/cm^2 (1 MeV equivalent).

Another significant difference between analog and advanced digital systems arises from the potential effect of the more rapid evolution of digital technology; in particular, the ever-increasing density and complexity of ICs at the wafer level make previously improbable failure mechanisms more significant. For example, at the level of complexity of current very-large-scale integrated (VLSI) circuits, electron migration can become a significant issue where metal interconnects and/or interlevel contacts are commonly designed to carry a current density exceeding 10^5 amps per cm^2 (A/cm^2), equivalent to an ordinary household electric wire carrying a current above 4000 A. Reliability tests by VLSI manufacturers typically address this problem by stressing devices at both high temperature and high current density. Synergistic effects of other parameters can precipitate other failure mechanisms, such as dielectric breakdown in semiconductor components.

One stressor not previously considered for analog safety system qualification is smoke exposure from an electrical fire. Based on the investigation of smoke susceptibility and the resulting understanding of key failure mechanisms (as discussed in NUREG/CR-6406, NUREG/CR-6476, NUREG/CR-6543, NUREG/CR-6579, and NUREG/CR-6597), smoke clearly has the potential to be a significant environmental stressor that can result in adverse consequences. However, as no practical, repeatable testing methodology is available, it is not feasible to assess smoke susceptibility as part of qualification.

As a result, the most reasonable approach to minimizing smoke susceptibility is to employ design, construction, installation, and procedural practices that can reduce the possibility of smoke exposure and enhance smoke tolerance. In particular, current fire protection methods focus on a preventive approach, employing isolation and detection practices. In addition, postevent recovery procedures can mitigate the extent of smoke damage. Moreover, certain design choices and construction practices, such as chip packaging and conformal coatings, can reduce equipment susceptibility to smoke exposure. In the absence of acceptable methods and practices for smoke-tolerant design and installation, the most effective approach for addressing smoke susceptibility is to minimize the likelihood of smoke exposure by rigorously adhering to the fire protection guidance in Appendix R, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979," to 10 CFR Part 50.

The safety goal of qualification is to avoid a common-cause failure of the safety-related system when it is needed to perform its safety function. The unique functional and hardware characteristics of computer-based I&C systems suggest that qualification guidance should explicitly state special considerations. These special considerations constitute good engineering practices that the industry generally follows. Nonetheless, the NRC staff developed this regulatory guide to promote clarity and avoid uncertainty, encourage the retention of the qualification records, and endorse the most appropriate standard. This guide does not intend to imply that a qualified life should be established for I&C systems in mild environments. Therefore, for the purposes of this guide, qualification is a validation of design to demonstrate that a safety-related computer-based I&C system is capable of performing its safety function under the specified environmental and operational stresses.

C. REGULATORY POSITION

The procedures described in IEEE Std. 323-2003 are appropriate for satisfying the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants. The standard can be applied subject to the following five enhancements and exceptions:

(1) For environmental qualification of safety-related computer-based I&C systems, type testing is the preferred method. Selective use of the service conditions mentioned in Section 6.1.5.1 of IEEE Std. 323-2003 should be based on the actual environmental conditions. The NRC does not consider the age conditioning in Section 6.2.1.2 to be applicable because of the absence of significant aging mechanisms on microprocessor-based modules.

(2) With appropriate justification, IEEE Std. 323-2003 allows the omission of elements of the test plan in Section 6.3.1.1 and the test sequence in Section 6.3.1.7 for mild environment qualification. The qualification testing should be performed with the I&C system functioning, with software and diagnostics that are representative of those used in actual operation, while the system is subjected to the specified environmental service conditions, including abnormal operational occurrences. Testing should exercise all portions of the safety-related computer-based I&C systems necessary to accomplish the safety-related function or those portions whose operation or failure could impair the safety-related function. Qualification testing should confirm the response of digital interfaces and verify that the design accommodates the potential impact of environmental effects on the overall response of the system. Although testing of a safety-related computer-based I&C system as a whole is preferred, type testing an entire system as a unit is not always practical. In those cases, confirmation of the dynamic response for a computer-based I&C system is based on type testing of the individual modules and analysis of the cumulative effects of environmental and operational stress on the entire system.

(3) Section 6.3.1.7(C) of IEEE Std. 323-2003 provides a note to the standards applicable to testing for electromagnetic interference/radio frequency interference (EMI/RFI) and surge as environmental conditions. Guidelines for conducting electromagnetic susceptibility testing of safety-related I&C systems appear in Revision 1 of Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," issued October 2003, and in Revision 1 of EPRI TR 102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," as endorsed in a related SER dated April 17, 1996.

(4) For safety-related computer-based I&C systems intended for implementation in a mild environment, the NRC staff takes exception to Section 7.1 of IEEE Std. 323-2003. The evidence of qualification in a mild environment should be consistent with the guidance given in Section 7.2 selectively based on actual environmental conditions and should be retained at the facility in an auditable form.

(5) Regulatory Guide 1.89 offers guidance for the environmental qualification of electrical equipment located in a harsh environment, as required by 10 CFR 50.49. For safety-related computer-based I&C systems installed in a harsh environment, the regulatory positions of this guide supplement the harsh environment qualification practices endorsed in Regulatory Guide 1.89.

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the NRC staff's plans for using this draft regulatory guide. This guide applies to new plants and its use is voluntary for modifications at plants that are operating in 2006. No backfitting is intended or approved in connection with its issuance.

The NRC has issued this draft guide to encourage public participation in its development. Except in those cases in which an applicant or licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the methods to be described in the active guide will reflect public comments and will be used in evaluating (1) submittals in connection with applications for construction permits, standard plant design certifications, operating licenses, early site permits, and combined licenses; and (2) submittals from operating reactor licensees who voluntarily propose to initiate system modifications if there is a clear nexus between the proposed modifications and the subject for which guidance is provided herein.

REGULATORY ANALYSIS

1. Statement of the Problem

Title 10, Part 50, of the *Code of Federal Regulations* (10 CFR Part 50) delineates the design and qualification-related regulations that the NRC has established for commercial nuclear power plants. In particular, 10 CFR Part 50 requires that SSCs important to safety in nuclear power plants shall be designed to accommodate the effects of environmental conditions (i.e., remain functional under postulated accident conditions) and design control measures (such as testing) shall be used to check the adequacy of design. Furthermore, 10 CFR 50.55a(h) requires that safety systems shall meet the requirements of IEEE Std. 603-1991 and the correction sheet dated January 30, 1995, or IEEE Std. 279-1971, contingent on the date that the NRC issued the related construction permit. The design-basis criteria identified by those standards or by similar provisions in the licensing basis for such facilities include the range of transient and steady-state environmental conditions throughout which the equipment shall perform during normal, abnormal, accident, and operational events. In addition, in Appendix B to 10 CFR Part 50, Criteria III, XI, and XVII establish practices to confirm that a design fulfills its technical requirements. Furthermore, 10 CFR 50.49 requires licensees to establish an environmental qualification program for all (safety-related) equipment that is relied on to remain functional during and following design-basis events.[1]

The use of COTS computers and microprocessor-based technology in safety systems poses potential environmental compatibility issues. These issues result from functional as well as hardware characteristics.

One unique characteristic of digital systems that should be considered in verifying design by qualification arises from the higher functional density that is possible with computer-based I&C systems. Because of expanding single-chip capabilities, many safety-related implementations involve replacing multiple functional modules with a multifunction microprocessor-based module. Therefore, failure of a single module for a computer-based I&C system can affect numerous functions.

Another characteristic that should be considered in verifying design by qualification involves the sequential function execution that typifies computer-based I&C systems in contrast to the essentially parallel function execution of analog modules. The effect of this behavior can be compounded for distributed implementations that rely on either successful completion of digital data communication or error detection before continuation of discrete functional steps.

The confirmation that digital system design accommodates the potentially synergistic effects of environmental stress is an important consideration for qualification of computer-based I&C systems. Hardware characteristics that warrant consideration result from the continuing trend toward higher clock frequencies, faster operating speeds, and lower logic-level voltages. The faster logic families have shown a greater susceptibility to upsets and malfunctions because of the effects of EMI/RFI. Another hardware characteristic is that the ever-increasing density and level of complexity at the wafer level make previously improbable failure mechanisms (e.g., electromigration) more significant. In addition, some MOS devices can fail at relatively low radiation doses on the order of 10 Gy (1 krad).

---

[1] As defined in 10 CFR 50.49, "design-basis events" include conditions of normal operation, including anticipated operational occurrences, design-basis accidents, external events, and natural phenomena.

Use of computers in safety systems poses challenges that differ from those associated with analog systems, prompting the development of IEEE Std. 7-4.3.2, issued in 1993 and revised in 2003. That standard emphasizes that the application of computers in safety systems needs to address reliability and environmental compatibility. In particular, Annex F.2.3 of IEEE Std. 7-4.3.2 requires the performance of analyses to ensure that the system has a high "correct response probability" and that the probability of common-cause failure is reduced to an acceptable level. Addressing qualification requirements for safety-related computer-based I&C systems is one method of ensuring that the probability of common-cause failure attributable to environmental stressors is reduced to an acceptable level. Specifically, Section 5.4.1 of IEEE Std. 7-4.3.2 provides criteria for the equipment qualification of computer-based safety systems, including performing testing with the full range of safety-related software functioning.

Revision 1 of Regulatory Guide 1.89 (1984) endorses IEEE Std. 323-1974. Regulatory Guide 1.89 specifically limits its scope to compliance 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." Thus, Regulatory Guide 1.89 focuses on the environmental qualification of equipment intended for use in harsh environments that are subject to the effects of design-basis accidents. Nonetheless, a mild environment in a nuclear power plant can encompass extreme environmental conditions that can affect the performance of sensitive equipment, so qualification to demonstrate compatibility with those environmental conditions is necessary in those cases. This requirement provides an assurance of reliable operation throughout the installed life of the equipment under all normal, abnormal, and anticipated operational occurrences as well as accident environmental conditions. Mild-environment qualification of most electrical equipment is accomplished through design analysis, predicting performance under environmental stress based on knowledge of material properties. However, because of the complexity of microprocessor design, such predictive analysis is not currently possible. Therefore, additional guidance is warranted to address qualification for all environmental conditions within a nuclear power plant.

The IEEE revised the consensus national standard for qualification, IEEE Std. 323, in 1983, reaffirmed it in 1991 and 1996, and revised it again in 2003. The 2003 version represents the current national consensus standard. The NRC staff does not currently endorse this version of the standard. The NRC continues to rely on the 1974 version of the standard, two generations old, for licensing actions. Therefore, it is desirable to endorse the 2003 version of the standard.

2. Alternative Approaches

The NRC staff considered the following alternative approaches to address the qualification of computer-based I&C systems:

(1) Take no action.

(2) Enhance current qualification approaches based on the unique features of computer-based I&C systems.

(3) Use tailored endorsement of existing environmental qualification standards.

2.1 Alternative 1: Take No Action

The first alternative, taking no action, would impose no additional costs on the NRC, applicants, or licensees compared to current conditions because no change to the process would occur. However, this approach fails to effectively address potential environmental compatibility issues posed by digital systems. Currently, guidance can be inferred from Chapter 7 of the Standard Review Plan, past regulatory practice, or recent SERs (in particular, the SER that the NRC issued by letter dated July 30, 1998, on EPRI 107330, which includes an acceptable mild-environment qualification approach for PLCs), but no comprehensive and explicit guidance for licensees addresses mild-environment qualification for all safety-related computer-based I&C systems. The absence of a well-defined roadmap for mild-environment qualification practices for computer-based technologies could result in inconsistency among the qualification process and its evidence for emerging technologies or commercially dedicated computers. Furthermore, if no action is taken, comprehensive guidance on the acceptable use of current versions of the national qualification standards will still be lacking.

2.2 Alternative 2: Enhance Current Qualification Approaches

The staff considered a second alternative, which would involve enhancing current qualification approaches on the basis of the unique features of computer-based I&C systems. This alternative consists of two elements, specifically (1) assurance of a minimum level of IC component qualification based on demonstrated capability of the subcomponents to meet the performance requirements and (2) minimization (through design) of the potential effect of environmental stressors on the equipment throughout its service life.

The first element involved identifying the tests that IC manufacturers employ to control quality and qualify their products for an extensive range of application environments. This approach emphasizes a "built in" philosophy as well as a "tested in" philosophy for quality and environmental compatibility. The second element of this approach used multitiered protection to establish environmental compatibility through implementations that minimize or counteract potential environmental stresses. This sound engineering practice minimizes environmental susceptibility. This approach is successful if the technology has matured for producing reliable components to meet the performance requirements.

2.3 Alternative 3: Use Tailored Endorsement of Existing Environmental Qualification Standards

As a third alternative, the NRC staff considered tailored endorsement of existing qualification standards. This option would enable the NRC staff, applicants, and licensees to benefit from the existing national consensus standard. Toward that end, the staff compared different versions of qualification standards to determine how the latest updates have identified new qualification issues. In particular, the staff conducted a comparative analysis of IEEE Std. 323-1974 and IEEE Std. 323-1983 (reaffirmed in 1991 and 1996). A subsequent review of IEEE Std. 323-2003 revealed consistency with previous findings. The following significant findings resulted from the analysis of the original and latest versions of this standard:

- The qualification methods (type testing, operating experience, and analysis) are identical in both versions. However, digital I&C generally undergoes more rapid evolutions than equivalent analog components. Thus, obtaining sufficient documentation on operating experience under identical environmental conditions for a particular I&C system for qualification purposes may be difficult. Therefore, type testing should be the preferred qualification method.

- IEEE Std. 323-2003 refers to standards for testing the EMI/RFI as an environmental condition, but the standard does not specifically prescribe the conduct of tests within the type-test sequence. Nonetheless, Revision 1 of Regulatory Guide 1.180 provides specific guidance on EMI/RFI susceptibility tests.
- Both versions provide the same essential details on qualification by operating experience.
- Both versions provide essentially the same procedures for qualification by analysis.

4. Values and Impacts

This section analyzes the values and impacts for each of the three identified approaches. In this analysis, the probability of an alternative approach having a positive effect on qualification is not known quantitatively, nor is the probability of achieving the overall safety goals. However, on the basis of a qualitative assessment of existing literature, experience with military applications of digital I&C, commercial industry experience, and experience in the nuclear industry, computer-based I&C systems have the potential to induce an undesirable safety consequence less predictably than similar analog systems. Therefore, the staff infers a positive correlation between addressing qualification of computer-based I&C systems for nuclear power plant environments and achieving safety goals, based on the negative effects of the alternate choice.

In the following summary, an impact is a cost in schedule, budget, or staffing or an undesired property or attribute that would accrue from taking the proposed approach. Both values and impacts may be functions of time.

3.1 Alternative 1: Take No Action

This alternative has a perceived cost-benefit advantage because it includes no startup activities. It also provides flexibility because each applicant or licensee would develop its own technical basis to demonstrate that its new or modified I&C system complies with NRC regulations. However, in the absence of explicit, definitive guidance on acceptable practices for qualification of all safety-related computer-based I&C systems, the NRC staff may receive applications or requests to review safety questions without adequate supporting evidence such as certificates of conformance and design specifications. As a result, the NRC may have to make time-consuming and costly requests for additional information. In addition, no established basis for endorsing the current national consensus standard for digital I&C qualification would be available. The absence of an identified set of guidelines could have adverse effects on the level of staff effort required to conduct reviews and to ensure consistency among reviewers for each I&C system modification. Thus, NRC staff reviews would take longer and require greater effort. From the applicant's or licensee's perspective, this flexibility would also entail potential costs because several unknowns are associated with demonstrating compliance with regulations. Thus, although the initial cost would apparently be low, taking no action could result in greater total costs for both the NRC staff and the applicant or licensee, as well as regulatory uncertainty during the safety evaluation process. The staff concludes that this alternative has the following value and impact:

- no value beyond the status quo
- schedule, budget, and staffing cost to the staff and applicant or licensee, associated with regulatory uncertainty

3.2 Alternative 2: Enhance Current Qualification Approaches

The second alternative, which involves identifying enhancements to current qualification approaches on the basis of unique computer-based I&C system features, could reduce costs to applicants and licensees by removing ambiguities regarding the appropriate set of qualification practices for the range of operating environments for computer-based I&C systems and by establishing the basis for receiving credit for sound engineering practices that minimize environmental susceptibilities. The value in this alternative would be the common understanding among the NRC staff and applicants or licensees of approaches that the expert technical community has accepted as good practices. However, by itself, this approach does not guarantee that the full scope of requirements in 10 CFR 50.55a(h) have been addressed. In addition, this approach does not clearly address the qualification of digital COTS equipment for mild environments. Moreover, this approach might introduce a new de facto standard that differs substantially from existing consensus standards. Therefore, this alternative also has the potential for regulatory uncertainty that could increase costs to both the NRC and the applicant or licensee during the safety evaluation. The staff concludes that this alternative has the following value and impact:

- probable improvement in the likelihood of achieving safety goals as a consequence of improved application of qualification practices by the nuclear power industry
- schedule, budget, and staffing costs to the staff and applicant or licensee, associated with remaining regulatory uncertainty regarding the determination of necessary and sufficient practices

3.3 Alternative 3: Use Tailored Endorsement of Existing Environmental Qualification Standards

This alternative would enable the staff, applicants, and licensees to obtain the benefit of the expert professional organizations that have established methods and practices to achieve a high level of qualification. From a regulatory perspective, a clear determination of an acceptable level of qualification for computer-based I&C would reduce the risks associated with regulatory uncertainty, which in turn would decrease the regulatory burden. Again, this alternative would have the value of promoting a predetermined common understanding of consensus methods among the staff and applicants or licensees regarding acceptable qualification activities. The development of a more detailed understanding of qualification would be a strength of this alternative. As a result, the staff, applicants, and licensees would gain a clearly defined technical basis for establishing and assessing qualification for safety-related I&C systems in nuclear power plants. The staff concludes that this alternative has the following values and impacts:

- *value*
  - probable improvement in the likelihood of achieving safety goals as a consequence of consistent qualification practices in the nuclear power industry
  - consideration of consensus approaches to qualification
  - common understanding of good design, testing, and implementation practices tailored to the nuclear power industry, on the basis of established qualification approaches by the military and by commercial industries
- *impact*
  - staff cost of evaluating qualification practices for specific relevance to the nuclear power industry
  - staff cost of endorsing tailored sets of practices from selected standards

4. Conclusions

Evidence is available that the plant environment can adversely affect computer-based I&C systems differently than their analog counterparts. General Design Criterion 4 requires that SSCs important to safety shall be compatible with and accommodate the effects of conditions associated with nuclear power plant service. The primary focus of the current qualification standard is the reliable operation of safety-related equipment if design-basis accidents occur. With the inevitable use of computer-based I&C systems for safety-related applications, it is essential to address the full scope and intent of Federal regulations (i.e., assurance of reliable operation in case of design-basis events, specifically normal and abnormal operational occurrences and anticipated operational accident conditions throughout the life of the system). Toward that end, the NRC staff considered three approaches to providing qualification guidance.

Taking no action might result in accumulating regulatory expenses, as applicants or licensees submit proposed methods to assure the staff that safety-related systems are compatible with the proposed environment for computer-based I&C systems and, thus, meet the requirements of NRC regulations.

By itself, the identification of enhancements to current qualification approaches on the basis of unique features of computer-based I&C systems does not guarantee that the full scope and intent of 10 CFR 50.55a(h) have been addressed. Therefore, this alternative alone also leaves the potential for regulatory uncertainty that could result in greater costs for both the NRC staff and the applicant or licensee during the safety evaluation process.

On the basis of the greatest value and most reasonable impacts of the problem solution (especially regulatory burden), the staff chose the third alternative. This alternative, tailored endorsement of the current qualification standard (i.e., IEEE Std 323-2003), would be sufficient when clarifications to address the unique characteristics of computer-based I&C systems are adequately addressed. This approach can contribute to establishing uniformity and consistency in environmental qualification practices for safety-related computer-based I&C systems in mild environments and can provide a roadmap to address the unique characteristics of microprocessor-based technology.

BACKFIT ANALYSIS

This regulatory guide does not require a backfit analysis, as described in 10 CFR 50.109, "Backfitting," because it is intended for new nuclear power plants. The use of this regulatory guide by current operating licensees is entirely voluntary.

REFERENCES

EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Electric Power Research Institute, September 1994.[2]

EPRI TR-107330, "Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," Electric Power Research Institute, December 1996.

IEEE Std. 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1993.[3]

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, 2003.

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

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

IEEE Std. 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1983.

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

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

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC, October 2003.[4]

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Chapter 7, "Instrumentation and Controls," Revision 4, U.S. Nuclear Regulatory Commission, Washington, DC, June 1997.

NUREG/CR-5904, K. Korsah, R.L. Clark, and R.T. Wood, "Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Reactors," U.S. Nuclear Regulatory Commission, Washington, DC, April 1994.

---

[2] EPRI publications may be purchased from the EPRI Distribution Center, 207 Coggins Drive, P.O. Box 23205, Pleasant Hill, CA 94523; telephone (510) 934-4212.

[3] IEEE publications may be purchased from the IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855; online at http://www.ieee.org; telephone (800) 678-4333.

[4] Copies are available at current rates from (1) the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328; telephone (202) 512-1800 or (2) the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161; online at http://www.ntis.gov; telephone (703) 487-4650. Copies are available for inspection or copying for a fee from the NRC's Public Document Room (PDR), 11555 Rockville Pike, Rockville, Maryland; the PDR's mailing address is USNRC PDR, Washington, DC 20555-0001. The PDR can also be reached by telephone at (301) 415-4737 or (800) 397-4205, by fax at (301) 415-3548, and by email to PDR@nrc.gov.

NUREG/CR-6406, K. Korsah et al., "Environmental Testing of an Experimental Digital Safety Channel," U.S. Nuclear Regulatory Commission, Washington, DC, September 1996.

NUREG/CR-6476, T.J. Tanaka, S.P. Nowlen, and D.J. Anderson, "Circuit Bridging of Components by Smoke," U.S. Nuclear Regulatory Commission, Washington, DC, October 1996.

NUREG/CR-6479, K. Korsah et al., "Technical Basis for Environmental Qualification of Microprocessor-Based Safety-Related Equipment in Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC, January 1998.

NUREG/CR-6543, T.J. Tanaka, "Effects of Smoke on Functional Circuits," U.S. Nuclear Regulatory Commission, Washington, DC, October 1997.

NUREG/CR-6579, M. Hassan and W.E. Vesely, "Digital I&C Systems in Nuclear Power Plants: Risk-Screening of Environmental Stressors and a Comparison of Hardware Availability with an Existing Analog System," U.S. Nuclear Regulatory Commission, Washington, DC, January 1998.

NUREG/CR-6597, T.J. Tanaka and S.P. Nowlen, "Results and Insights on the Impact of Smoke on Digital Instrumentation and Controls," U.S. Nuclear Regulatory Commission, Washington, DC, January 2001.

NUREG/CR-6741, K. Korsah and R.T. Wood, "Application of Microprocessor-Based Equipment in Nuclear Power Plants—Technical Basis for Qualification Methodology," U.S. Nuclear Regulatory Commission, Washington, DC, January 2003.

Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC, November 1974.[5]

Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," Revision 1, U.S. Nuclear Regulatory Commission, Washington, DC, June 1984.

Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 1, U.S. Nuclear Regulatory Commission, Washington, DC, October 2003.

[5] Single copies of regulatory guides, both active and draft, and draft NUREG documents may be obtained free of charge by writing the Reproduction and Distribution Services, USNRC, Washington, DC 20555-0001, or by fax to (301) 415-2289, or by email to DISTRIBUTION@nrc.gov. Active guides may also be purchased from the National Technical Information Service on a standing order basis. Details on this service may be obtained by writing NTIS, 5285 Port Royal Road, Springfield, VA 22161; telephone (703) 487-4650; online at http://www.ntis.gov. Copies of active and draft guides are available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, Maryland; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; email PDR@nrc.gov.

Safety Evaluation Report, issued by letter dated April 17, 1996, from Eric Lee, U.S. Nuclear Regulatory Commission, to Carl Yoder, Electric Power Research Institute, "Review of EPRI Utility Working Group Topical Report TR-102323, 'Guidelines for Electromagnetic Interference Testing in Power Plants.'"[6]

Safety Evaluation Report, issued by letter dated July 30, 1998, from Frank Miraglia, U.S. Nuclear Regulatory Commission, to Joseph Naser, Electric Power Research Institute, "Review of EPRI Utility Working Group Topical Report TR-107330, 'Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants'."

[6] Copies are available for inspection or copying for a fee from the NRC's Public Document Room, which is located at 11555 Rockville Pike, Rockville, Maryland; the PDR's mailing address is USNRC PDR, Washington, DC 20555-0001. The PDR can also be reached by telephone at (301) 415-4737 or (800) 397-4205, by fax at (301) 415-3548, and by email to PDR@nrc.gov.