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

September 2001
Division 1
Draft DG-1077

DRAFT REGULATORY GUIDE

Contact: C.E. Antonescu (301)415-6792

DRAFT REGULATORY GUIDE DG-1077

GUIDELINES FOR ENVIRONMENTAL QUALIFICATION OF MICROPROCESSOR-BASED EQUIPMENT IMPORTANT TO SAFETY IN NUCLEAR POWER PLANTS

A. INTRODUCTION

The NRC's regulations for design and qualification for commercial nuclear power plants are delineated in 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities." In particular, 10 CFR Part 50 requires that structures, systems, and components important to safety in a nuclear power plant be designed to accommodate the effects of environmental conditions (i.e., remain functional under postulated accident conditions) and that design control measures such as testing be used to check the adequacy of design. General requirements are contained in the following sections of 10 CFR Part 50.

Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criteria 1, 2, 4, 13, 21, 22, and 23;

Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants": Criterion III, *Design Control*; Criterion XI, *Test Control*; and Criterion XVII, *Quality Assurance Records*; and

10 CFR 50.55a, "Codes and Standards."

According to 10 CFR 50.55a(h)(2), protection systems must meet the requirements of the Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," or IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," contingent on the date of construction permit issuance. The design basis criteria identified in those standards, or by similar provisions in the licensing basis for such

facilities, include the range of transient and steady state environmental conditions during normal, abnormal, and accident circumstances throughout which the equipment must perform.

As reported in NUREG/CR-5904 (1994), "Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Reactors," microprocessor-based electric equipment important to safety can pose unique functional and qualification issues. These digital issues may not be fully addressed by traditional testing and evaluation approaches that have been developed primarily for analog equipment. The primary focus of IEEE Std 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," is the reliable operation of safety-related equipment under design basis accidents. With the inevitable use of microprocessor-based equipment for safety-related applications, the full scope of 10 CFR 50.55a(h) needs to be addressed.

This regulatory guide describes a method acceptable to the NRC staff for determining the environmental qualification procedures for microprocessor-based electric equipment important to safety for service in nuclear power plants. Adherence to these qualification practices contributes to the assurance that microprocessor-based equipment 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 Electrical Equipment Important to Safety for Nuclear Power Plants" (June 1984), which addresses compliance with 10 CFR 50.49 under design basis accidents and does not necessarily anticipate the unique issues associated with the application of microprocessor-based safety-related equipment.

In general, information provided by regulatory guides is reflected in the Standard Review Plan (NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants"). NRC's Office of Nuclear Reactor Regulation uses the Standard Review Plan to review applications to construct and operate nuclear power plants. This regulatory guide will conform to Revision 4 of Chapter 7, "Instrumentation and Controls," of the Standard Review Plan.

Regulatory guides are issued to describe to the public methods acceptable to the NRC staff for implementing specific parts of the NRC's regulations, to explain techniques used by the staff 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. Regulatory guides are issued in draft form for public comment to involve the public in developing the regulatory positions. Draft regulatory guides have not received complete staff review; they therefore do not represent official NRC staff positions.

The information collections contained in this draft regulatory guide are covered by the requirements of 10 CFR Part 50, which were approved by the Office of Management and Budget, approval number 3150-0011. If a means used to impose an information collection does not display a currently valid OMB control number, the NRC may not conduct or sponsor, and a person is not required to respond to, the information collection.

B. DISCUSSION

IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," was endorsed in Regulatory Guide 1.89, "Qualification of Class

1E equipment for Nuclear Power Plants" (November 1974), and in Revision 1 of Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants" (June 1984). IEEE Std 323-1974 was revised in 1983 and reaffirmed in 1991 and 1996. Thus, IEEE Std 323-1983 is supported by over 16 years of commercial experience.

Recognition that the use of computers in safety systems poses challenges different from those of analog systems prompted the development of IEEE Std 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." The standard recognizes that reliability and environmental compatibility need to be addressed in the application of computers in safety systems. In particular, it recommends that analyses must be performed 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 environmental qualification requirements for microprocessor-based systems important to safety is one method of ensuring that the probability of common cause failure caused by environmental stressors is reduced to an acceptable level.

In addition to IEEE Std 323-1983, qualification issues addressed by a European standard, International Electrotechnical Commission (IEC) 60780, "Nuclear Power Plants—Electrical Equipment of the Safety System—Qualification," have been included in the development of this regulatory guide. The IEC document was published in 1998 and reflects qualification concerns, from the European perspective, regarding the use of microprocessor-based safety systems in power plants.

For the purposes of this guide, "qualification" is a verification of design to demonstrate that the microprocessor-based equipment is capable of performing its safety function under the most limiting environmental stresses that can result from design basis accidents. The safety goal of qualification is to avoid a common cause failure of the safety system when it is needed for performing its safety function. According to 10 CFR 50.49(e)(5), equipment qualified by test must be preconditioned by natural or artificial (accelerated) aging to its end-of-installed-life condition. Further, 10 CFR 50.49(e)(5) specifies that consideration must be given to all significant types of degradation that can have an effect on the functional capability of the equipment. Humidity, corrosion, voltage transients caused by electromagnetic or radio-frequency interference, and accumulation of deposits are examples of such effects.

From a qualification standpoint, one significant difference between analog and advanced digital systems is the radiation tolerance of different integrated circuit (IC) technologies. Threshold radiation levels for metal oxide semiconductor (MOS) devices are generally lower than bipolar technologies. However, MOS is the preferred technology 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. Some MOS devices can fail at the relatively low dose of 1 krad (Silicon). In fact, commercial MOS devices are quite sensitive to ionizing doses, in contrast to their relative insensitivity to neutron fluence. Ionizing dose radiation hardness levels for MOS integrated circuit families range from about 1 krad (Si) for commercial off-the-shelf (COTS) circuits to about 10 Mrad (Si) for radiation-hardened circuits. In contrast, the threshold fluence hardness level for MOS devices is about 10^{14} neutrons/cm^2 (1 MeV equivalent).

Another significant difference between analog and advanced digital systems is the potential effect of the more rapid evolution of digital technology; in particular, the ever-increasing density and level of complexity of ICs at the wafer level makes previously

improbable failure mechanisms more significant. For example, at the level of complexity of current VLSI circuits, where metal interconnects and/or inter-level contacts are commonly designed to carry a current density exceeding 10^5 A/cm^2 (equivalent to an ordinary household electric wire carrying a current above 4000 Amps), electromigration becomes a significant problem. 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 may precipitate other failure mechanisms such as dielectric breakdown in semiconductor components.

These differences and analyses suggest a different approach to qualification for digital instrumentation and control (I&C) safety systems. First, qualification should begin at the IC manufacturing level. That is, quality of I&C systems must be "built in" as well as "tested for." From the IC manufacturer's perspective, built-in quality can be enhanced by ensuring, among other process control methodologies, a minimum of stress tests and a guarantee of correct operation in a specified environment. For example, IC components are typically rated for operation at temperature ranges that may exceed certain accident conditions. In particular:

Commercial grade components: Maximum temperature ratings for these are guaranteed to be in the range from 0°C to 70°C (32°F to 158°F).

Industrial grade components: Maximum temperature ratings for these are guaranteed to be in the range from 0°C to 85°C (32°F to 185°F).

Military grade components: Maximum temperature ratings for these are guaranteed to be in the range from -55°C to 130°C (-67°F to 266°F).

In order for the ICs to qualify for these ratings, the IC manufacturer typically establishes an extensive component stress testing and qualification methodology. These tests typically include the following.

Temperature/Humidity Bias Test
The main purpose of this environmental test is to measure the moisture resistance of plastic encapsulated circuits; it is typically performed at a temperature of 85°C (185°F) and a relative humidity (RH) of 85% for 1008 hours.

High-Temperature Operating Life Test
This type of stress testing is performed to accelerate failure mechanisms that are thermally activated through the application of extreme temperatures and the use of biased operating conditions. A typical stress temperature is 125°C (257°F) with the electrical bias applied exceeding the data sheet nominal value by some predetermined margin. Testing is normally performed either with dynamic signals applied to the device or in static bias configuration for a typical test duration of 1008 hours.

Temperature Cycle Test
The goal of this test is to accelerate the effects of thermal expansion mismatch among the different components within a specific die and packaging system. Typical minimum and maximum temperatures are −65°C (−85°F) and 150°C (302°F) respectively, with the test duration usually being 1000 cycles or more.

Autoclave Test

This is an environmental test designed to measure device resistance to moisture penetration and the resultant effects of galvanic corrosion with elevated temperature and humidity. Corrosion of the die is the expected failure mechanism. Typical test conditions are 121°C (250°F) at 100% RH and 0.205 MPa (15 psig) with a duration of 48 or 96 hours.

Low-Temperature Operating Life Test
This test is designed to accelerate hot carrier injection effects in MOS devices by applying biased operating conditions at room temperature. Failure indication includes parametric changes such as transconductance threshold shifts.

System Soft Error Test
This test is performed on memory devices only. "Soft error" refers to a random failure caused by ionization of silicon by impact of high-energy particles. The stress test is typically performed on a system-level basis and involves operating the system for millions of device hours to obtain an accurate measure of actual system soft error performance.

Despite these qualification stress tests at the IC component level, tests documented in NUREG/CR-6406 (1996), "Environmental Testing of an Experimental Digital Safety Channel,"[2] show that at high relative humidity, digital equipment can fail at temperatures considerably below manufacturer's maximum operating limit. Thus, manufacturer's ratings alone cannot be relied upon to guarantee reliable operation under abnormal and accident nuclear power plant environments.

From the licensee or applicant's perspective, built-in quality can be enhanced by a precise knowledge of the operating environment and the application of an appropriate margin of safety. To meet this objective, a more rigorous definition of the nuclear plant environment (i.e., other than "harsh" and "mild") is identified in this guide. Specifically, three location categories are identified as follows:

Category A Location:	All locations inside containment and other areas that exceed Category B conditions.
Category B Location:	Any location outside containment and for which the following service conditions apply:
	Radiation:	Normal total integrated gamma dose: $>4x10^2$ rad, but $<10^4$ rad, over 40 years.
	Temperature:	Normal service environment does not exceed 38°C (100°F), and accident service environment does not exceed 90% of the manufacturer's maximum rated operating temperature.
	Humidity:	Normal service environment does not exceed 80%, and abnormal and accident environment does not exceed 95%, noncondensing.
Category C Location:	Any location outside containment and for which the following service conditions apply:
	Radiation:	Normal total integrated gamma dose: $<4x10^2$ rad over 40 years.
	Temperature:	Both normal and accident service environment below 38°C (100°F).
	Humidity:	Normal service environment does not exceed 80%, and abnormal and accident environment does not exceed 95%, non-condensing.

A multi-tiered protection approach should be applied to the qualification of digital I&C systems. The objective is to minimize the potential impact of environmental stressors on the digital equipment throughout its service life.

A method acceptable to the NRC staff that incorporates these two approaches in the qualification of digital systems is specified in the Regulatory Position. The methodology has three elements: (1) an assurance of a minimum level of IC component qualification based on a knowledge of the type of IC making up the equipment as well as a knowledge of the operating environment under design basis events; (2) minimization, through design, of the potential effect of environmental stressors on the equipment throughout its service life; and (3) qualification at the equipment level using appropriate consensus standards.

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 [NUREG/CR-6476 (1996), "Circuit Bridging of Components by Smoke;" NUREG/CR-6406 (1996); NUREG/CR-6543 (1997), "Effects of Smoke on Functional Circuits;" NUREG/CR-6579 (1998), "Digital I&C Systems in Nuclear Power Plants: Risk-Screening of Environmental Stressors and a Comparison of Hardware Unavailability With an Existing Analog System;" and NUREG/CR-6597 (2001), "Results and Insights on the Impact of Smoke on Digital Instrumentation & Controls"], it is clear that smoke has the potential to be a significant environmental stressor that can result in adverse consequences. However, there is no practical, repeatable testing methodology so it is not feasible to assess smoke susceptibility as part of environmental qualification. As a result, the most reasonable approach to minimizing smoke susceptibility is to employ design, implementation, and procedural practices that can reduce the possibility of smoke exposure and enhance smoke tolerance. In particular, current fire protection methods are an appropriate preventive approach, employing isolation and detection practices. Additionally, post-event recovery procedures can mitigate the extent of smoke damage. Finally, there are design choices and implementation practices that can reduce equipment susceptibility to smoke exposure, such as chip packaging and conformal coatings. In the absence of consensus methods and practices for smoke-tolerant design and implementation, the most effective approach to addressing smoke susceptibility is to minimize the likelihood of smoke exposure by rigorously adhering to the fire protection guidance given in Appendix R to 10 CFR Part 50.

C. REGULATORY POSITION

The procedures, in their entirety, that are described by either IEEE Std 323-1983 (reaffirmed 1996), "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," or IEC 60780 (1998), "Nuclear Power Plants—Electrical Equipment of the Safety System—Qualification," are appropriate for satisfying the qualification of safety-related microprocessor-based equipment for service in nuclear power plants. The procedures from either standard may be applied in their entirety, without mixing and matching among standards, subject to the following enhancements and exceptions.

1. The dynamic response of a distributed system under environmental stress should be considered during qualification testing. Section 5, "Qualification Methods," of IEEE Std 323-1983 identifies type testing, operating experience, and analysis as methods for qualifying equipment for the nuclear power plant environment. Typically, these qualification approaches are applied to a single piece of equipment or module. Studies documented in NUREG/CR-

6406 show that communication interfaces are likely to be the most vulnerable elements for distributed systems. Thus, qualification testing should confirm the response of any digital interfaces to environmental stress in a distributed system. The NRC staff prefers type testing to achieve this. When it is not practical to type test an entire system as a unit, the confirmation of the dynamic response of the distributed system should be based on type testing of the individual modules and analysis of the entire system.

2. Electromagnetic/radio-frequency (EMI/RFI) susceptibility tests should be performed during qualification testing. Such tests are identified as part of the testing sequence in IEC 60780-1998. They should be performed at an equivalent stage of the test sequence under IEEE 323-1983, if that standard is being applied. Guidelines for addressing electromagnetic compatibility of safety-related I&C systems are provided in Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems."

3. IEEE Std 323-1983 requires a qualified life for microprocessor-based equipment in a Category A environment. Preconditioning (accelerated aging) should be applied in accordance with IEEE 323-1983 or IEC 60780-1998, depending on the standard being applied. In addition, the enumerated exceptions and clarifications in Regulatory Guide 1.89 apply.

Recommended documentation to provide evidence of qualification for a Category A environment is identical to the guidance for type test data in Section 8.3 of IEEE 323-1983 or Section 6.3 of IEC 60780-1998, depending on the standard being applied. Further guidance on documentation of equipment specification or service environment (Section 6.1 of IEEE 323-1983 or Section 5.2 or IEC 60780) is provided in Regulatory Guide 1.89.

4. For microprocessor-based equipment in a Category B environment, the need for preconditioning should be based on an assessment of environmental factors to identify any aging mechanisms that may have a significant effect on the expected life of the equipment. If no aging mechanisms that would lead to degraded performance over the expected installed life of the equipment are identified, preconditioning may be omitted from the test sequence.

Documentation recommended to provide evidence of qualification for a Category B environment is similar to the requirements for type test data in Section 8.3 of IEEE 323-1983. However, if no aging mechanisms are identified, in place of the age conditioning procedure [Section 6.3.1.1(5) as referenced in Section 8.3(6) of IEEE 323-1983], findings from the assessment of aging mechanisms should be documented. If IEC 60780-1998 is being applied, documentation should be provided in accordance with Section 6.3, and in lieu of an accelerated aging procedure documentation [Section 5.3.1.1 (d), as referenced in Section 6.3(c) of IEC 60780], findings from the assessment of aging mechanisms should be documented.

5. For microprocessor-based equipment in a Category C environment, preconditioning may be omitted from the test sequence. Documentation to provide evidence of qualification for a Category C environment is similar to the requirements for type test data in Section 8.3 of IEEE 323-1983 or in Section 6.3 of IEC 60780-1998, depending on the standard being applied. If IEEE 323-1983 is being applied, Section 6.3.1.1(5) [as referenced in Section 8.3(6)] should be omitted. The corresponding section to be omitted from the test plan documentation in IEC 60780-1998, if it is being applied, is Section 5.3.1.1(d) [as referenced in Section 6.3(c)].

6. Margin should be applied in accordance with either Section 6.3.1.5 of IEEE 323-1983 or Section 5.3.1.6 of IEC 60780-1998, depending on the standard being applied. If the latter is the standard being applied, a temperature margin of +15°F (8°C) should be applied when qualification testing is not being performed under saturated steam conditions.

7. Any life-limited component of the equipment should be identified and its shelf life should be documented.

8. The standards and testing practices used by the IC manufacturer for component stress testing and qualification should be identified and listed. The purpose is to provide evidence that quality processes were applied to the manufacturer's product line to confirm the IC's reliability. As a minimum, the tests covered by the standards should include, but are not limited to, the following tests.

- Temperature/Humidity Bias Test
- High Temperature Operating Life Test
- Temperature Cycle Test
- Autoclave Test
- Low Temperature Operating Life Test
- System Soft Error Test

9. A multi-tiered protection approach should be applied to digital I&C qualification. In particular, the system design of the microprocessor-based equipment should minimize the potential impact of environmental stressors on the equipment throughout its service life. The approaches employed to accomplish such protection should be identified and listed. Figure 1 illustrates the conceptual levels at which protection against environmental stressors is possible for the actual circuits or components performing a safety-related function. These levels can be characterized as follows.

9.1 Electronic Component Level

The first level of environmental protection for system components could occur at the IC level. Thermal management problems at the IC level become increasingly significant as clock frequencies increase and higher density circuitry is employed for microprocessors and other integrated circuits. Moreover, as the number of input/outputs to the chip increases, complex schemes become necessary to accommodate the connections between closely packed circuits. This leads to increasingly sophisticated packaging technologies and the potential for undesirable interface interactions. Thermal protection at the microcircuit level, however, is the responsibility of packaging engineers and not system design engineers. Thus the equipment qualifier only has to confirm that the ICs used for the design of safety-related equipment or systems have undergone adequate electronic stress screening tests. (Note that this evidence would be generated in the process of establishing compliance with Regulatory Position 8.)

9.2 Module or Circuit Board Level

Depending on the system design, the next level of protection may be modules, racks, or circuit boards inside the cabinet. Mounting circuit boards vertically may help to limit soot, dust, and water accumulation. Modules may be designed in a manner to reduce smoke and particulate deposits in case of fire. Certain packaging and coating techniques (e.g., use of solder mask, conformal coating) may provide significant defenses against short-term smoke exposure effects.

9.3 Cabinet Level

The next level of protection for the safety system electronics may be provided by the equipment cabinets. Various design features such as fans, filters, and EMI/RFI shielding could be considered in the cabinet design. The fans and fan filters may provide protection by drawing air away from sensitive components in case of smoke and by trapping smoke particulates. The bottom shelf of a cabinet may be raised off the floor to prevent submersion in standing water. Holes may also be provided on this shelf to drain standing water. Cable conduits connected to cabinets may help to prevent standing water if connections are made from the bottom of the cabinet.

9.4 Room Level

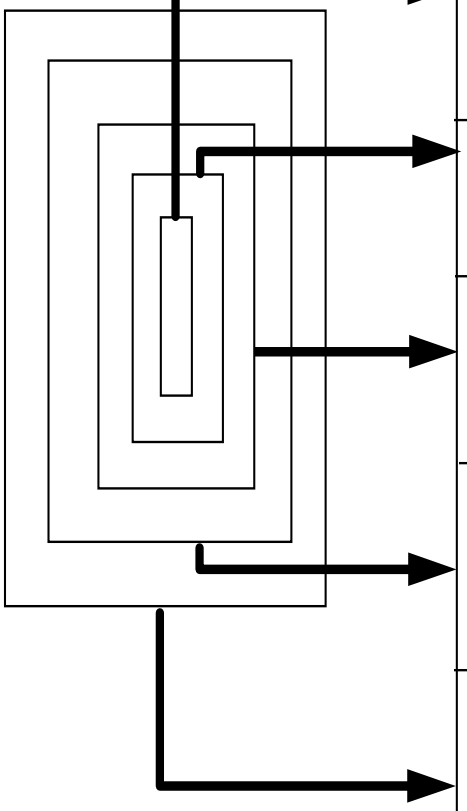
The final level of environmental protection may be provided by a heating, ventilation, and air-conditioning (HVAC) system in the room or enclosure where the safety-related equipment is installed. The HVAC system controls the environmental parameters such as humidity, temperature, and airborne particulates. The location of the room and its distance away from potential sources of smoke, fire, and radiation may serve as a shield for the equipment and contribute to protection against the spread of smoke and flames in case a fire occurs.

10. Random failures should be addressed using surveillance, on-line diagnostics, maintenance, and trending techniques at intervals based on the predicted failure rates. The possibility of multiple latent failures at the time the equipment is called upon to function should be made as low as possible. The use of microprocessors can enable advanced and on-line diagnostics to be performed, improving the ability to detect both random failures and degradation in hardware performance (e.g., reduced noise margin) beyond present capabilities. However, the diagnostic algorithms/procedures must not become so involved that their failure could cause more faults than they prevent.

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the NRC staff's plans for using this regulatory guide. No backfitting is intended or approved in connection with this guide.

This draft guide has been released to encourage public participation in its development. Except in those cases in which an applicant or licensee proposes an acceptable alternative method for complying with the specified portions of the NRC's regulations, the methods to be described in the active guide reflecting public comments will be used in the evaluation of submittals in connection with applications for construction permits, operating licenses, and combined licenses. The final guide will also be used to evaluate submittals from operating reactor licensees who propose system modifications, voluntarily initiated by the licensee, if there is a clear connection between the proposed modifications and this guidance.



	Stressors	Controls that Afford a Level of Protection Against the Stressors
Electronic component	• Radiation • Humidity (moisture) • Smoke, corrosive gases • Temperature • Vibration	• Technology (e.g., TTL, CMOS) • Packaging (plastic or hermetic-sealed, insertion mount, surface mount, chip-on-board, multi-chip module) • Circuit design (e.g., component ratings, soldering reliability)
Circuit Board	• Temperature • EMI/RFI effects • Smoke, corrosive gases	• Heat sinks • Shielding, grounding, board layout • Coating
Module/Rack	• Temperature • Smoke, corrosive gases • Humidity • Vibration • EMI/RFI effects	• Fans • Board enclosure design (e.g., inner foam cover) • vibration isolation (e.g.,elastic mounting) • Shielding, grounding
Cabinet	• Temperature • Smoke, corrosive gases • Vibration • EMI/RFI effects	• Fans, cabinet design (e.g., ventilation openings) • vibration isolation (e.g., elastic mounting) • Shielding, grounding
Room	• Temperature • Humidity • Smoke, corrosive gases • Radiation	• HVAC • Fire protection devices • Location (e.g., behind concrete wall to provide some level of gamma shielding)

Figure 1. Potential Levels of Protection Against Environmental Stressors for Safety-Related Electronic Hardware

REFERENCES

IEC 60780, "Nuclear Power Plants—Electrical Equipment of the Safety System—Qualification," International Electrotechnical Commission, 1998.[1]

IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1993.[2]

IEEE Std 279-1971,"Criteria for Protection Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1971.[2]

IEEE Std 323-1974, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers," 1974.[2]

IEEE Std 323-1983, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers," 1983.[2]

IEEE Std 603-1991,"Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.[2]

NUREG/CR-5904, "Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Reactors," USNRC, April 1994.[3]

NUREG/CR-6406, K. Korsah et al., "Environmental Testing of an Experimental Digital Safety Channel," USNRC, September 1996.[3]

NUREG/CR-6476, T.J. Tanaka, S.P. Nowlen, and D.J. Anderson, "Circuit Bridging of Components by Smoke," USNRC, October 1996.[3]

NUREG/CR-6543, T.J. Tanaka, "Effects of Smoke on Functional Circuits," USNRC, October 1997.[3]

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," USNRC, 1998.[3]

NUREG/CR-6597, "Results and Insights on the Impact of Smoke on Digital Instrumentation and Controls," USNRC, January 2001.[3]

[1] IEC publications may be purchased online at http://www.iec.ch.

[2] IEEE publications may be purchased from the IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855.

[3] Copies are available at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-1800); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161 (<http://www.ntis.gov/ordernow> or telephone (703)487-4650). Copies are available for inspection or copying for a fee from the NRC 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; email is PDR@NRC.GOV.

Regulatory Guide 1.89, "Environmental Qualification of Certain Electrical Equipment Important to Safety for Nuclear Power Plants," USNRC, November 1974.[4]

Regulatory Guide 1.89, "Environmental Qualification of Certain Electrical Equipment Important to Safety for Nuclear Power Plants," Revision 1, USNRC, June 1984.[4]

Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," USNRC, January 2000.[4]

"Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-0800, Chapter 7, "Instrumentation and Controls," Revision 4, USNRC, 1997.[2]

[4] Single copies of regulatory guides, both active and draft, may be obtained free of charge by writing the Distribution Services Section, OCIO, 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 <http://www.ntis.gov/ordernow>. Copies of certain guides and many other NRC documents are available electronically on the internet at NRC's home page at <WWW.NRC.GOV> in the Reference Library. Documents are also available through the Electronic Reading Room (NRC's ADAMS document system, or PARS) at the same web site.

REGULATORY ANALYSIS

1. PROBLEM

The NRC's regulations in 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," state that structures, systems, and components important to safety in a nuclear power plant must be designed to accommodate the effects of environmental conditions (i.e., remain functional under all postulated service conditions) and that design control measures such as testing must be used to check the adequacy of design. Further, 10 CFR 50.55a(h) requires that safety systems satisfy the criteria of the Institute of Electrical and Electronics Engineers (IEEE) Standard 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," or IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," contingent on the date the construction permit was issued. The design basis criteria identified in those standards, or by similar provisions in the licensing basis for such facilities, include the range of transient and steady state environmental conditions during normal, abnormal, and accident circumstances throughout which the equipment must perform. Criterion III, *Design Control*; Criterion XI, *Test Control*; and Criterion XVII, *Quality Assurance Records*, of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 establish practices to confirm that a design fulfills its technical requirements. Furthermore, 10 CFR 50.49 requires a qualification program to be established for all (safety-related) equipment that is relied upon to remain functional during and following design basis events. Design basis events, as defined in 10 CFR 50.49, include conditions of normal operation, including anticipated operational occurrences, design basis accidents, external events, and natural phenomena.

The use of commercial off-the-shelf (COTS) computers and microprocessor-based technology in safety systems poses potential environmental compatibility issues that are not necessarily addressed in current qualification guidelines. One issue is 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 electromagnetic interference/radio-frequency interference (EMI/RFI). Another issue is that the ever-increasing density and level of complexity at the wafer level makes previously improbable failure mechanisms more significant. In addition, some metal oxide semiconductor (MOS) devices can fail at the relatively low dose of about 1 krad (Si).

Recognition that the use of computers in safety systems poses challenges different from those of analog systems prompted the development of IEEE Std 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." The standard recognizes that reliability and environmental compatibility need to be addressed in the application of computers in safety systems. In particular, it recommends that analyses should be performed 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 environmental qualification requirements for microprocessor-based systems important to safety is one method of ensuring that the probability of common cause failure caused by environmental stressors is reduced to an acceptable level. Previous guidance on environmental qualification focused on aging effects and the reliable operation of safety-related equipment under design basis accidents. As a result, existing guidance does not specifically address the so-called "mild" environments to which microprocessor-based systems are likely to be subjected. Thus, with the inevitable use of microprocessor-based equipment for safety-related applications, the need has been recognized to address the full

scope of 10 CFR 50.49, i.e., an assurance of reliable operation under normal, abnormal, and accident environmental conditions throughout the life of the equipment.

2. ALTERNATIVE APPROACHES

Three approaches were considered for addressing the environmental qualification of digital and microprocessor-based systems:

1. Take no action.
2. Enhance current qualification approaches based on the unique features of microprocessor-based systems. (This might result in introducing a completely new standard.)
3. Tailor endorsement of existing qualification standards.

2.1 Take No Action

The first alternative, taking no action, would require no additional cost to the NRC staff, applicants, or licensees over current conditions since no change to the process would occur. However, this approach fails to address potential environmental compatibility issues posed by digital systems and would imply a lack of recognition that there is an absence in guidance that addresses the challenges presented by microprocessor-based safety-related systems.

2.2 Enhance Current Qualification Approaches

The second alternative, enhancing current qualification approaches based on the unique features of microprocessor-based systems, was also considered. One methodology proposed had three elements: (1) an assurance of a minimum level of integrated circuit (IC) component qualification based on a knowledge of the type of IC making up the equipment as well as a knowledge of the operating environment under design basis events; (2) minimization, through design, of the potential effect of environmental stressors on the equipment throughout its service life; and (3) qualification at the equipment level using appropriate consensus standards.

It was recognized that a more rigorous approach was needed for defining the operating environments of microprocessor-based systems in nuclear power plant environments (e.g., other than just categorizing the environment as “harsh” or “mild”). One proposal considered was three location categories for microprocessor-based equipment:

Category A Location: All locations inside containment and other areas that exceed Category B conditions.

Category B Location: Any location outside containment and for which the following service conditions apply:

Radiation: Normal total integrated gamma dose: $>4 \times 10^2$ rad, but $<10^4$ rad, over 40 years.

Temperature: Normal service environment does not exceed 38°C (100°F), and accident service environment does not exceed 90% of the manufacturer’s maximum rated operating temperature.

Humidity: Normal service environment does not exceed 80%, and abnormal and accident environment does not exceed 95% (non condensing).

Category C Location: Any location outside containment and for which the following service conditions apply:

Radiation: Normal total integrated gamma dose: $<4x10^2$ rad over 40 years.

Temperature: Both normal and accident service environment below 38°C (100°F).

Humidity: Normal service environment does not exceed 80%, and abnormal and accident environment does not exceed 95% (non condensing).

This categorization was based in part on studies that show that digital technologies proposed for advanced and digital safety-related I&C are less likely to be reliable in containment radiation levels where integral doses may exceed 10^4 over 40 years. In addition, IC components are typically rated for operation at temperature ranges that may exceed certain accident conditions. In particular:

Maximum temperature ratings for commercial grade components are guaranteed to be in the range from 0°C to 70°C (32°F to 158°F).

Maximum temperature ratings for industrial grade components are guaranteed to be in the range from 0°C to 85°C (32°F to 185°F).

Maximum temperature ratings for military grade components are guaranteed to be in the range from -55°C to 130°C (-67°F to 266°F).

In order to guarantee these ratings, integrated circuit components typically undergo extensive qualification stress tests. Despite these manufacturers' ratings, however, studies show that under conditions of high relative humidity, digital equipment can fail at temperatures considerably below the manufacturer's maximum operating limit. Thus, manufacturers' ratings alone cannot be relied upon to guarantee reliable operation under abnormal and accident nuclear power plant environments.

2.3 Tailor Endorsement

The third alternative, tailor endorsement of existing standards for environmental qualification, was considered. This option would allow the NRC staff, applicants, and licensees to benefit from existing consensus standards. European qualification standards were compared with their U.S. counterparts to determine how any new qualification issues have been identified in the latest updates. In particular, a comparative analysis was made with regard to IEEE 323-1983 (reaffirmed in 1996), "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and International Electrotechnical Commission (IEC) 60780, "Qualification of Electrical Items of the Safety System for Nuclear Power Generating Station." Since the IEC document was published in 1998, it reflects any new qualification concerns, from the European perspective, with regard to the use of microprocessor-based safety systems in nuclear power plants.

Significant findings resulted from the analysis of the two standards:

- The methods of qualification—type testing, operating experience, and analysis—are identical in both standards. However, digital I&C generally undergoes more rapid evolutions than their analog counterparts. Thus, it may be difficult to obtain sufficient documentation based on operating experience under identical environmental conditions for a particular piece of I&C equipment for qualification purposes. As stated in IEC 60780, type testing should be the preferred qualification method.

- The requirements for *on-going qualification* as stipulated in IEEE 323-1983 envelop those stipulated in IEC 60780 (1998). Furthermore, these procedures do not require modification for application to microprocessor-based and advanced digital systems.

- The IEC standard specifically requires electromagnetic (EMI/RFI) susceptibility tests to be performed. There is no specific mention of EMI/RFI tests in IEEE 323-1983. EMI/RFI susceptibility tests should be an explicit requirement for qualification of microprocessor-based safety systems. Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," addresses this issue.

- IEC 60780 offers more details on specific stress tests as well as references to other standards than IEEE 323-1983. In this respect, IEC 60780 provides better clarity as to how environmental qualification of safety-related equipment should be performed.

- The essential details of qualification by operating experience are the same in both standards.

- Procedures for qualification by analysis are essentially the same in both standards. They differ only with respect to the fact that IEEE 323-1983 allows qualification of *other* equipment *by similarity* if certain criteria are met, whereas IEC 60780 does not appear to explicitly allow this method of qualification.

3. VALUES AND IMPACTS

Values and impacts for each of the three identified approaches are analyzed below. In this analysis, the probability of an alternative approach having a positive effect on qualification and the probability of that effect on the achievement of overall safety goals are not known quantitatively. However, based on a qualitative assessment of existing literature and experience in the military, commercial industries, and the nuclear industry, microprocessor-based equipment has the potential to induce an undesirable safety consequence in certain nuclear environments and in a manner that is less predictable than the analog counterparts. Therefore, a positive correlation between addressing qualification of microprocessor-based systems for nuclear power plant environments and the achievement of safety goals is inferred from the negative effects of doing otherwise.

In the summary below, 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 since there are no "start-up" activities. It also provides flexibility, since each applicant or licensee would develop its own technical basis demonstrating that its new or modified I&C system complied with the NRC's regulations. However, the NRC staff would continue to receive applications or requests to review safety questions with no clear guidance on acceptable practices for qualification of microprocessor-based systems. The absence of an identified set of guidelines could have adverse effects on the level of staff effort required to conduct reviews or to ensure consistency among reviews for

each I&C system modification. Thus, NRC staff review would take longer and require greater effort. From the applicant's or licensee's perspective, this flexibility also would have potential costs because there are several unknowns associated with demonstrating compliance with regulations; in particular, there is no guidance on the level of evidence necessary during the commercial dedication process to establish environmental compatibility for digital COTS equipment. Thus, although the initial cost would apparently be low, taking no action could result in greater total costs, both to the NRC staff and the applicant or licensee, during the safety evaluation process.

Value – No value beyond the status quo
Impact – Schedule, budget, and staffing cost, to the staff and applicant or licensee, associated with regulatory uncertainty.

3.2 Alternative 2—Identify Enhancements to Current Qualification Approaches Based on the Unique Features of Microprocessor-Based Systems

The second alternative—identification of enhancements to current qualification approaches based on the unique features of microprocessor-based systems—would reduce costs to applicants and licensees by removing ambiguities with regard to appropriate operating environments for microprocessor-based I&C and by improving the availability of systems. The value in this alternative would be the common understanding between the NRC staff and applicants or licensees of approaches that have acceptance as good practice in the expert technical community. However, this approach by itself does not guarantee that the full scope of 10 CFR 50.55a(h) and 10 CFR 50.49 have been addressed. In addition, the current approach does not clearly address qualification of digital COTS equipment for non-harsh environments. Therefore, this alternative also has the potential for regulatory uncertainty that could result in greater costs, both to the NRC staff and the applicant or licensee, during the safety evaluation process.

Value – Probable improvement in the likelihood of achieving safety goals as a consequence of improvement in the application of qualification practices by the nuclear power industry.
Impact – Schedule, budget, and staffing cost, to the staff and applicant or licensee, associated with remaining regulatory uncertainty regarding determination of necessary and sufficient practices.

3.3 Alternative 3—Tailor Endorsement of Existing Qualification Standards

This alternative would enable the staff, applicants, and licensees to obtain the benefit of the effort of expert professional organizations to establish methods and practices to achieve a high level of environmental qualification. From a regulatory perspective, a clear determination of an acceptable level of qualification for microprocessor-based I&C would reduce the risks associated with regulatory uncertainty, which in turn would reduce the regulatory burden. Again, this alternative would have the value of promoting a predetermined common understanding between the staff and applicants or licensees of consensus methods that have acceptance as good practice in the technical community. The development of a more detailed understanding of environmental 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 environmental qualification for safety-related I&C systems in nuclear power plants.

Value – Probable improvement in the likelihood of achieving safety goals as a consequence of improvement in the application of environmental qualification practices by the nuclear power industry
– Consideration of consensus approaches to environmental qualification
– Common understanding of good design, testing, and implementation practices tailored to the nuclear power industry, based on established approaches to qualification for military and commercial industries.

Impact – Staff cost of evaluating qualification practices for specific relevance to the nuclear power industry
– Staff cost of endorsing the tailored set of practices from selected standards.

4. CONCLUSIONS

There is evidence that microprocessor-based I&C can be adversely affected in ways different from their analog counterparts. General Design Criteria 4 requires that systems, structures, and components important to safety be compatible with and accommodate the effects of environmental conditions associated with nuclear power plant service conditions. The primary focus of current environmental qualification standards is the reliable operation of safety-related equipment under design basis accidents. With the inevitable use of microprocessor-based equipment for safety-related applications, the need has been recognized to address the full scope and intent of Federal regulations, i.e., an assurance of reliable operation under *design basis events*, normal and abnormal as well as accident conditions, throughout the life of the equipment. Three approaches to providing environmental qualification guidance were examined.

Taking no action may result in accumulating regulatory expense as applicants or licensees submit proposed methods to assure the staff that safety-related equipment is compatible with the proposed environment for microprocessor-based I&C and, thus, meets the requirements of NRC's regulations.

The identification of enhancements to current qualification approaches based on the unique features of microprocessor-based systems, by itself, does not guarantee that the full scope and intent of 10 CFR 50.55a(h) and 10 CFR 50.49 have been addressed. Therefore, this alternative alone also leaves open the potential for regulatory uncertainty that could result in greater costs, to both the NRC staff and the applicant or licensee, during the safety evaluation process.

After a comparative analysis of both United States and European standards, it was concluded that the third alternative of tailored endorsement of current qualification standards would by itself not guarantee that the full scope and intent of 10 CFR 50.55a(h) and 10 CFR 50.49 have been addressed. Therefore, this alternative also leaves open the potential for regulatory uncertainty that could result in greater costs, both to the NRC staff and the applicant or licensee, during the safety evaluation process.

5. DECISION RATIONALE

Based on the highest value and reasonable impact for problem solution capability (especially regulatory burden), a combination of the second and third alternatives has been

chosen. The highest value will be achieved by identifying enhancements to current qualification approaches based on the unique features of microprocessor-based systems (Alternative 2), then using those enhancements identified to supplement mature consensus standards (Alternative 3, in this case IEEE 323-1983 and IEC 60780 (1998)).

REGULATORY ANALYSIS REFERENCES

IEC 60780, "Nuclear Power Plants—Electrical Equipment of the Safety System—Qualification," International Electrotechnical Commission, 1998.[1]

IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1993.[2]

IEEE Std 279-1971,"Criteria for Protection Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1971.[2]

IEEE Std 323-1974, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers," 1974.[2]

IEEE Std 323-1983, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers," 1983.[2]

IEEE Std 603-1991,"Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.[2]

Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," USNRC, January 2000.[3]

[1] IEC publications may be purchased online at http://www.iec.ch.

[2] IEEE publications may be purchased from the IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855.

[3] Single copies of regulatory guides may be obtained free of charge by writing the Distribution Services Section, OCIO, 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 <http://www.ntis.gov/ordernow>. Copies of active and draft guides are available for inspection or copying for a fee from the NRC 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; email <PDR@NRC.GOV>.