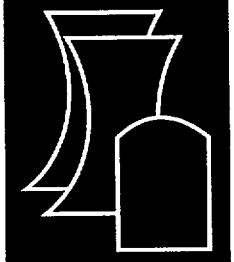
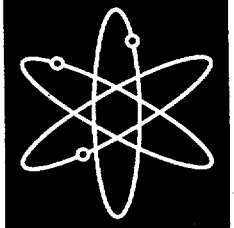
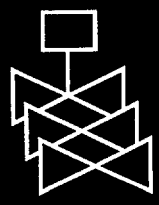
NUREG/CR-6741
ORNL/TM-2000/236







# Application of Microprocessor-Based Equipment in Nuclear Power Plants—Technical Basis for a Qualification Methodology

## Draft Report for Comment

Oak Ridge National Laboratory

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

## AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

### NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at www.nrc.gov/NRC/ADAMS/index.html.
Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address www.nrc.gov/NRC/NUREGS/indexnum.html are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

### Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

NUREG/CR-6741
ORNL/TM-2000/236

# Application of Microprocessor-Based Equipment in Nuclear Power Plants—Technical Basis for a Qualification Methodology

## Draft Report for Comment

Manuscript Completed: July 2001
Date Published: August 2001

Prepared by
K. Korsah, R.T. Wood, ORNL

Oak Ridge National Laboratory
Managed by UT-Battelle, LLC
Oak Ridge, TN 37831-6010

C.E. Antonescu, NRC Project Manager

**Prepared for**
**Division of Engineering Technology**
**Office of Nuclear Regulatory Research**
**U.S. Nuclear Regulatory Commission**
**Washington, DC 20555-0001**
**NRC Job Code L1798**

## COMMENTS ON DRAFT REPORT

Any interested party may submit comments on this report for consideration by the NRC staff. Comments may be accompanied by additional relevant information or supporting data. Please specify the report number NUREG/CR-6741 draft in your comments, and send them by the date published in the Federal Register Notice to:

Chief, Rules Review and Directives Branch
U.S. Nuclear Regulatory Commission
Mail Stop T6-D59
Washington, DC 20555-0001

You may also provide comments at the NRC Web site, http://www.nrc.gov. See the link under "Technical Reports in the NUREG Series" on the "Reference Library" page. Instructions for sending comments electronically are included with the document, NUREG/CR-6741 draft, at the web site.

For any questions about the material in this report, please contact:

Christina Antonescu
Mail Stop: T-10L1
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
Phone: 301-415-6792
E-mail: CEA1@nrc.gov.

## ABSTRACT

This document (1) summarizes the most significant findings of the "Qualification of Advanced Instrumentation and Control (I&C) Systems" program initiated by the Nuclear Regulatory Commission (NRC); (2) documents a comparative analysis of U.S. and European qualification standards; and (3) provides recommendations for enhancing regulatory guidance for environmental qualification of microprocessor-based safety-related systems.

Safety-related I&C system upgrades of present-day nuclear power plants, as well as I&C systems of Advanced Light-Water Reactors (ALWRs), are expected to make increasing use of microprocessor-based technology. The Nuclear Regulatory Commission (NRC) recognized that the use of such technology may pose environmental qualification challenges different from current, analog-based I&C systems. Hence, it initiated the "Qualification of Advanced Instrumentation and Control Systems" program. The objectives of this confirmatory research project are to (1) identify any unique environmental-stress-related failure modes posed by digital technologies and their potential impact on the safety systems and (2) develop the technical basis for regulatory guidance using these findings.

Previous findings from this study have been documented in several technical reports. This final report in the series documents a comparative analysis of two environmental qualification standards—Institute of Electrical and Electronics Engineers (IEEE) Std 323-1983 and International Electrotechnical Commission (IEC) 60780 (1998)—and provides recommendations for environmental qualification of microprocessor-based systems based on this analysis as well as on the findings documented in the previous reports. The two standards were chosen for this analysis because IEEE 323 is the standard used in the U.S. for the qualification of safety-related equipment in nuclear power plants, and IEC 60780 is its European counterpart. In addition, the IEC document was published in 1998, and should reflect any new qualification concerns, from the European perspective, with regard to the use of microprocessor-based safety systems in power plants. (IEEE 323-1983 was reaffirmed in 1990 and 1996.)

## CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

## ACKNOWLEDGMENTS

The authors would like to thank the NRC Program Manager, Christina Antonescu, of the U.S. NRC Office of Nuclear Regulatory Research (RES), for her help in initiating, planning, and implementing this study.

Two other U.S. Department of Energy (DOE) research laboratories—Sandia National Laboratories and Brookhaven National Laboratory—performed different aspects of the confirmatory research program to resolve environmental qualification issues posed by the use of microprocessor-based safety-related equipment. Findings from these studies [3,4,6,7] have been taken into account in proposing the qualification methodology documented in this report, and the contributions of the authors are gratefully acknowledged.

## ACRONYMS

| | |
|---|---|
| AWLR | Advanced Light Water Reactor |
| BNL | Brookhaven National Laboratory |
| CMOS | Complementary Metal Oxide Semiconductor |
| DBA | Design Basis Accident |
| DBE | Design Basis Event |
| DOE | Department of Energy |
| EDSC | Experimental Digital Safety Channel |
| EMI/RFI | Electromagnetic/Radio Frequency Interference |
| I&C | Instrumentation and Controls |
| IC | Integrated Circuit |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| LOCA | Loss of Coolant Accident |
| LSI | Large Scale Integrated circuit |
| MOS | Metal Oxide Semiconductor |
| NMOS | N-channel MOS |
| NRC | Nuclear Regulatory Commission |
| OBE | Operating Basis Earthquake |
| ORNL | Oak Ridge National Laboratory |
| RES | Office of Nuclear Regulatory Research |
| SSE | Safe Shutdown Earthquake |
| SNL | Sandia National Laboratory |
| STD | Standard |
| VLSI | Very Large Scale Integrated circuit |

## DEFINITION OF TERMS

This section includes a definition of terms as used in this document. Where applicable, the source of the definition is also included.

**Aging.**[a]
The effect of operational, and system conditions on equipment during a period of time up to but not including design basis events, or the process of simulating these events.

**Class 1E.**[b]
The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor cooling, and containment and reactor heat removal or that otherwise are essential in preventing significant release of radioactive material to the environment.

**Design Basis Accident (DBA).**[a]
The subset of a design basis event which requires safety function performance.

**Design Basis Event (DBE).**[b]
Postulated events, specified by the safety analysis of the station, used in the design to establish the acceptable performance requirements of the structures and systems. (Events include anticipated transients, design basis accidents, external events, and natural phenomena.)

**Harsh environment.**[a]
An environment expected as a result of the postulated service conditions appropriate for the design basis and post-design basis accidents of the station.

**Mild environment.**[a]
An environment expected as a result of normal service conditions and extremes (abnormal) in service conditions where seismic is the only design basis event of consequence.

**Installed life.**[a]
The interval from installation to removal during which the equipment or component thereof may be subject to design service conditions and system demands.

**Qualification.**[a]
The generation and maintenance of evidence to ensure that equipment will operate on demand to meet the system performance requirements.

**Qualified life.**[a]
The period of time, before the start of a design basis event, for which equipment was demonstrated to meet the design requirements for the specified service conditions.

**Service life.**[c]
Actual period from initial operation to retirement of structures, systems, or components.

---

[a]IEEE Std 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
[b]IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
[c]*Nuclear Power Plant Common Aging Terminology,* EPRI TR-100844, Electric Power Research Institute, Nov. 1992.

# 1 INTRODUCTION

This document (1) summarizes the most significant findings of the "Qualification of Advanced Instrumentation and Control (I&C) Systems" program initiated by the Nuclear Regulatory Commission (NRC); (2) documents a comparative analysis of U.S. and European qualification standards; and (3) provides recommendations for enhancing regulatory guidance for environmental qualification of microprocessor-based safety-related systems.

## 1.1 Background

Safety-related I&C system upgrades of present-day nuclear power plants, as well as I&C systems of Advanced Light-Water Reactors (ALWRs), are expected to make increasing use of microprocessor-based technology. The NRC recognized that the use of such technology may pose environmental qualification challenges different from current, analog-based I&C systems. Hence, it initiated the "Qualification of Advanced Instrumentation and Control Systems" program. The objectives of this confirmatory research project are to (1) identify any unique environmental-stress-related failure modes posed by digital technologies and their potential impact on the safety systems and (2) develop the technical basis for regulatory guidance using these findings.

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, although MOS is the preferred technology for ICs because of its technical superiority in other areas such as higher input impedance, fewer manufacturing processing steps (and consequent lower price), better temperature stability, and lower noise. In the MOS family, complementary metal-oxide semiconductor (CMOS) technology is the most common for large-scale and very-large-scale integrated circuits (LSI and VLSI). However, some MOS devices can fail at the relatively low dose of 1 krad (Si). In fact, commercial MOS devices are quite sensitive to ionizing dose, 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).[1]

Another significant difference is the ever increasing density and level of complexity at the wafer level, which 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 contact 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), electro migration 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.

Previous findings from the environmental qualification study have been documented in several technical reports.[2-8] This final report in the series documents a comparative analysis of two environmental qualification standards—IEEE 323-1983[a] and IEC 60780 (1998)[b]—and provides recommendations for

[a] IEEE publications may be purchased from the IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855-1331.

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

environmental qualification of microprocessor-based systems based on this analysis as well as on the findings documented in the previous reports. The two standards were chosen for this analysis because IEEE 323-1983 is the current U.S. standard for the qualification of safety-related equipment in nuclear power plants, and IEC 60780 is its European counterpart. In addition, the IEC document was published in 1998, and should reflect any new qualification concerns, from the European perspective, with regard to the use of microprocessor-based safety systems in power plants. (IEEE 323-1983 was reaffirmed in 1990 and 1996.)

## 1.2 Summary of Previous Research Findings

Three U.S. Department of Energy (DOE) research laboratories—Sandia National Laboratories (SNL), Oak Ridge National Laboratory (ORNL), and Brookhaven National Laboratory (BNL)—performed different aspects of the confirmatory research program to resolve environmental qualification issues posed by the use of microprocessor-based safety-related equipment. These studies have been documented in references 1 through 6. For convenience we have compiled the most significant findings from these studies, upon which we develop a basis for qualification of microprocessor-based safety-related equipment, below:

1. Communication interfaces were found to be the most vulnerable elements of an experimental digital safety channel (EDSC) designed and assembled at ORNL. Several environmental stress tests were performed on the EDSC, including smoke, temperature, humidity, and electromagnetic and radio-frequency interference (EMI/RFI). As was experienced with the EDSC, intermittent component upsets will typically impede communication, either at the board level (e.g., during bus transfers of data) or on the subsystem level (e.g., during serial or network data transfers). Thus, qualification testing should confirm the response of any interfaces to environmental stress.

2. During the EDSC tests, it was found that the combination of high temperature and high relative humidity resulted in failure of the system at temperatures considerably below the IC manufacturer's maximum temperature ratings.[c] This observation suggests that, despite qualification stress tests performed by IC manufacturers, the latter's temperature ratings alone cannot be relied upon to guarantee reliable operation under abnormal and accident conditions a nuclear power plant.

3. A stressor not previously considered for analog safety system qualification is smoke exposure (as opposed to direct fire exposure). Smoke may impair the operation of electrical circuits by shorting leads, corroding contacts, and inducing stray capacitance. Smoke tests on functional boards using different chip technologies suggest that conformal coatings and the characteristics of chip technologies should be considered when designing digital circuitry to be used in nuclear power plant safety systems. For example, (a) a polyurethane conformal coating brushed on a

[c]At the IC component level, semiconductor manufacturers identify three grades of components—commercial, industrial, and military. Maximum temperature ratings for commercial-grade components are guaranteed to be in the range 0°C to 70°C (32°F to 158°F). For industrial grade, this range is between 0°C to 85°C (32°F to 185°F), and the ratings for military grade components is -55°C to 130°C (-67°F to 266°F). The EDSC was assembled with commercial- and industrial grade components representing over 400 components from over 10 different manufacturers. During the tests, errors were recorded at temperatures at or above 49°C (85% RH).

number of the test boards in a test-set substantially reduced the damaging effects of smoke; (b) during tests on functional boards using different chip technologies, high voltage, low current (i.e., high-impedance) devices were found to be more susceptible to smoke than low voltage, high current (low impedance) devices; and (c) high impedance circuits tend to have a different failure mechanism (increase in leakage current) than low impedance circuits (corrosion).

4. Although smoke does adversely affect electronic equipment, current research and the state-of-the-art for testing do not support the explicit inclusion of smoke exposure as a stressor during type testing. In particular, there is no practical, repeatable testing methodology so it is not feasible to assess smoke susceptibility as part of environmental qualification. Based on existing research, present methodologies with regard to General Design Criteria (GDC) 39, IEEE 384, "Independence of Class 1E Equipment and Circuits," and Appendix R of 10 CFR 50, should continue to be applied for digital I&C safety systems.

5. A comparison of the hardware unavailability of an existing analog Safety Injection Actuation System to that of an assumed digital upgrade of the system indicated that with proper design and surveillance, advanced digital systems should be able to meet or improve on the hardware unavailability of current analog systems.

6. One study compared the unavailability of digital systems using equipment failure rates for nuclear power plant and off-shore platform applications. This study used estimates of failure probabilities in an assumed industrial environment and showed that system unavailability may be more sensitive to the architecture of the digital system than to the environmental and operational variations involved.

### 1.3 Basis for Environmental Qualification Standards

Part 50 of Title 10 of the Code of Federal Regulations (10 CFR 50), "Domestic Licensing of Production and Utilization Facilities," delineates the NRC's design and qualification regulations for commercial nuclear power plants. In particular, 10 CFR 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.

Section 50.55a(h) of 10 CFR Part 50 states that protection systems must meet the requirements of the IEEE standard (Std) 603-1991, "A Criteria for Safety Systems for Nuclear Power Generating Stations,"[a] or IEEE Std 279-1971, "A Criteria for Protection Systems for Nuclear Power Generating Stations,"[a] 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.

Section 5.4 of IEEE 603-1991, "Equipment Qualification," requires safety systems to be environmentally qualified in accordance to IEEE Std 323-1983. Section 50.49 of 10 CFR Part 50, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," identifies "equipment important to safety" as including (1) safety-related equipment required to remain functional during and following design basis events (DBEs) to ensure the performance of required safety functions,

(2) nonsafety-related equipment whose failure during postulated DBEs could prevent the accomplishment of safety functions, and (3) accident monitoring instruments providing information on certain key variables.

Regulatory Guide 1.89[d], "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," describes methods acceptable to the NRC staff for complying with 10 CFR 50.49. The regulatory Guide endorses IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." IEEE Standard 323-1974 was revised in 1983, reaffirmed in 1990, 1996, and is currently undergoing revision. In a comparative analysis of the IEEE 323-1974 and IEEE 323-1983 documented in NUREG/CR-6479,[5] the authors indicate that the 1983 version is adequate for applicability.

In 1998, the IEC published IEC 60780, "Nuclear Power Plants - Electrical Equipment of the Safety System - Qualification." This NUREG compares and contrasts IEEE 323-1983 and IEC 60780-1998, and provides recommendations for environmental qualification of microprocessor-based systems based on this analysis as well as on the findings resulting from the confirmatory research program and documented in the previous reports.

[d]Copies of issued guides may be purchased by contacting the U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, Attention: Publication Sales Manager.

# 2 COMPARISON OF IEEE 323-1983 AND IEC 60780 (1998)

## 2.1 Qualification Methods

Both IEEE 323-1983 (section 5) and IEC-60780 (section 4) allow **type testing, operating experience,** or **analysis** as alternative means of qualification. In addition, both standards allow any combination of the three basic methods to be used in some cases (e.g., where size, application, time or other limitations preclude the use of a type test on the complete equipment assembly). IEC 60780 (section 4.1) explicitly delineates type testing using simulated service conditions to be the preferred qualification method. There is no such explicit indication in IEEE 323-1983.

Comments:
The choice of methods of qualification–type testing, operating experience, and analysis–are the same in both standards. Type testing has traditionally been the most frequently used method of equipment qualification and involves subjecting the equipment to the environments and operating conditions for which it was designed. It also includes the concept of aging, in which the equipment is put in a condition that simulates its expected end of qualified life. However, depending on the intended application of a piece of equipment, the relative severity of its storage and use environment can vary greatly, and the particular goals of any aging during a type test program should reflect the intended application.

With microprocessor-based safety systems likely to see increased application in nuclear power plants, it is recommended that type testing continue to be the preferred test method for the following reasons:

(1) Digital I&C technology undergoes more rapid evolution compared to its analog counterpart. Since the non-nuclear industries are generally less regulated, they tend to upgrade their digital I&C more often. Thus it may be difficult to obtain sufficient documentation based on operating experience under identical environmental conditions for a particular I&C equipment for qualification purposes.

(2) No comprehensive database having sufficient detail to allow digital I&C system failures to be accurately related with causative mechanisms currently exits for either the nuclear or non-nuclear industries.

(3) It is usually difficult to construct a valid mathematical model of a microprocessor-based system for the purposes of qualification. Until such time as modeling improvements warrant, qualification by analysis for microprocessor-based equipment will therefore be limited.

## 2.2 On-Going Qualification

IEEE 323-1983
IEEE 323-1983 addresses on-going qualification under section 6.9, "Extension of Qualified Life." This section delineates several methods by which the qualified life of equipment can be extended, namely:

(1) Type testing of a piece of equipment of the same or similar design and construction which has been age-conditioned for a period equivalent to a longer time than the qualified life of the installed equipment. This process may be repeated as required to extend the qualified life to equal the anticipated installed life.

(2) Type testing of a piece of equipment of the same or similar design and construction that has been naturally aged in an environment equal to or more severe than the non-DBE service conditions for the intended application. The qualified life will be extended by the amount of time that the period of natural aging exceeds the initially established qualified life.

(3) Type testing of a piece of equipment of the same or similar design and construction which has undergone a combination of natural aging and age conditioning for a period equivalent to a longer time than the qualified life of the installed equipment.

(4) Use of periodic surveillance/maintenance, testing, and replacement/refurbishment programs based on manufacturers' recommendations and sound engineering practices.

(5) Qualified life may be extended if it can be shown that evaluation in the original qualified program was conservative with respect to the equipment's specified service conditions and performance specifications;

(6) Qualified life may be extended if it can be shown that an age-conditioning procedure, which limited the qualified life of the equipment, was overly conservative;

(7) Qualified life may be extended if it can be shown that the service or environmental conditions originally assumed were overly conservative with respect to those that apply at the equipment's locations, in its installed configuration.

IEC 60780

This standard also acknowledges (section 4.5) that there may be situations in which qualification may yield a qualified life of equipment that is less than the anticipated installed life of the equipment. In such a situation, the standard specifies three methods for implementing an on-going qualification program:

(a) replacement of the whole equipment or sensitive parts of it within a predetermined period of time as a preventive measure;

(b) execution of periodic pertinent testing on operating equipment (e.g., accuracy, insulation resistance, response time);

(c) additional items of equipment can be installed beside the required item, be removed before the end of the qualified life period and be tested to determine their additional qualified life.

Comments:

Item (b) in the IEC document is similar to item (4) in the IEEE 323-1983 document. Also, item (c) in IEC 60780 is similar to item (2) in the IEEE document. Although replacement of parts of an equipment [item (a) in IEC 60780], as a preventative measure, is not explicitly stated in IEEE 323-1983, a one-for-one replacement of a part can in principle be performed without violating any guidelines for safety-related systems (i.e., without generating an unreviewed safety question). Items (5) through (7) of IEEE 323-1983 do not have equivalents in the IEC document. In effect these items recognize the possibility that qualification methods used in the original procedures were overly conservative, and that new analysis may show that the qualified life is actually greater than what had originally been documented. It is not clear if this is allowed by the IEC standard.

It is our opinion that the requirements for on-going qualification given in IEEE 323-1983 envelop those in IEC 60780. Furthermore, the IEEE 323-1983 procedures do not require modification for application to microprocessor-based and advanced digital systems.

## 2.3 Aging

IEEE 323-1983
Aging is addressed in IEEE 323-1983 under section 6.3, "Type Testing." The standard requires an assessment of equipment aging effects to be performed to determine if aging has a significant effect on operability.

The standard acknowledges that natural aging is the most technically justified method to be used during qualification. It states that naturally-aged equipment may be used for type testing provided that:

(1) the equipment has been aged in an environment at least as severe as the normal one for the intended application;

(2) operating and maintenance/replacement records are available to verify the service conditions;

(3) the aged equipment was operated under load at least as severe as that specified for the equipment to be qualified.

If naturally-aged equipment is not available with proper documentation and significant aging mechanism(s) have been identified, the standard requires the equipment to be age-conditioned in the type test program unless the effects of the significant aging mechanism can be accounted for by in-service surveillance/maintenance.

The standard explicitly states that if type testing is the mode of qualification, then preconditioning prior to testing is not required if the equipment is determined not to have *significant aging mechanisms* (section 6.2.1, paragraph 4).

Paragraph 4 of section 4, "Introduction," states that "For equipment located in a mild environment and which has no significant aging mechanisms, a qualified life is not required." Paragraph 3 of section 6.2.1, "Aging Considerations," gives a definition of Significant Aging Mechanism as follows:

> "An aging mechanism is significant if in the normal and abnormal service environment, it causes degradation during the installed life of the equipment that progressively and appreciably renders the equipment vulnerable to failure to perform its safety function(s) under DBE conditions"

IEC 60780
The need for aging is addressed under section 5.3.3.1 of the standard. In particular, the section explicitly states that accelerated aging is not intended to be applied to all safety equipment in the safety system. "Safety equipment which is not supposed to be subjected to accident conditions is not intended to be pre-aged before being seismically tested."

Comments

While the need for aging is recognized by both standards, it appears that the criterion in IEC 60780 for determining whether or not an equipment should be aged has a slightly different focus than in IEEE 323-1983. That is, the IEC 60780 criterion depends on whether or not the equipment will be subjected to accident conditions (steam during a LOCA, flooding, etc.) and is independent of the environmental conditions during normal service. On the other hand, IEEE 323-1983 appears to indicate that the overriding concern should be the effect of the environment on the equipment's ability to perform its safety function *whenever it is called upon to do so* (i.e., "under DBE conditions" as stated in the definition of "significant aging mechanisms." Note that 10 CFR § 50.49 defines Design Basis Event as "conditions of **normal** operation, including anticipated operational occurrences, design basis accidents, external events, and natural phenomena").

## 2.4 Test Sequence

IEEE 323-1983

Significant elements of the type testing procedure in this standard (section 6.3.2) include the following:

1. Inspection of the sample to ensure that it has not been damaged due to handling since manufacture;

2. Functional tests under normal conditions to obtain baseline data;

3. Operation of the sample to the extremes of all performance and electrical characteristics given in the equipment specifications, excluding design basis event and post design basis event conditions, unless these data are available from other tests (e.g., design verification tests) on identical or similar equipment;

4. Placement of the sample, if required, in a condition that simulates its expected end-of-qualified-life (that is, the equipment is to be aged if necessary). Design basis event radiation may be included during this step. Appropriate measurements should be made following aging to determine the equipment's functionality. When it is practical and applicable, the functional capability should be demonstrated during the DBE radiation exposure;

5. Subjection of the sample to non-seismic mechanical vibration;

6. Subjection of the sample to a simulated operating basis earthquake (OBE), safe shutdown earthquake (SSE) and seismic vibration (IEEE 344 is referenced for this test);

7. For equipment located in harsh environment, the test sample is required to perform its required safety function(s) while exposed to the simulated design basis accident (DBA). The standard allows DBA radiation to be excluded in this test if incorporated in (4);

8. The test sample is required to perform its safety function(s) while exposed to the simulated post-DBA conditions as applicable.

IEC 60780

If type testing is to be used as a means of qualification, IEC 60780 (section 5.3.2) defines three main test groups as follows:

*1) Group 1: Testing to check the functional characteristics of equipment*

This includes:

a) Inspection to ensure that the equipment has not been damaged due to handling;
b) testing under normal conditions to provide baseline data (accuracy, drifts, dielectric insulation, etc.);
c) testing to the electrical and environmental extremes indicated in the equipment's performance specification. These are "preferably" to include the following conditions:
   (i) specified limits of normal supply voltage (or frequency);
   (ii) extreme limits of the temperature range;
   (iii) electromagnetic (conducted and/or radiated) susceptibility.

*2) Group 2: Testing to demonstrate seismic resistance of equipment*

The standard requires pre-aging to be performed before seismic testing only if significant aging factors exist for the equipment.

*3) Group 3: Testing to demonstrate resistance of equipment to accident and post-accident conditions*

a)Equipment Aging (assessment of behavior with time). The following aging factors have been called out to be considered during the aging program:
   - temperature (with or without cycling);
   - corrosion;
   - prolonged operation;
   - irradiation representative of cumulative dose to which the equipment would be subjected during its whole life;
   - mechanical vibration.

b) Accident and post-accident condition tests. The tests are intended to verify equipment behavior when subjected to accident conditions such as:
   - an earthquake (or other vibratory phenomena such as an aircraft crash);
   - accumulated irradiation dose likely to occur during a postulated initiating event (thermodynamic accident inside containment);
   - a sudden injection of saturated steam (rapid increase in temperature and pressure) to simulate an accident inside containment;
   - the pressure of saturated steam during the post-accident phase following an internal thermodynamic accident within the containment.

The standard mentions that the three test groups identified herein may be treated independently and may concern different samples of equipment. The standard does not give detailed guidance on functional testing methods because they are "considered as common industrial practices." However, it provides detailed guidance on aging tests (e.g., simultaneous and sequential tests, selection of tests and their sequencing, correlation with natural aging) because it is considered "more specific to nuclear power plants."

Comments

The two standards are nearly identical in their treatment of type testing methodology. For example, items 1 through 3 under IEEE 323-1983 are similar to the section entitled *Group 1: Testing to check the functional characteristics of equipment* under IEC 60780. Items 4 through 6 in IEEE-323 are similar to the section entitled *Testing to demonstrate seismic resistance of equipment* in IEC 60780. Finally, items 7 and 8 in IEEE 323 are similar to the section entitled *Testing to demonstrate resistance of equipment to accident and post-accident conditions* in IEC 60780.

It is the authors' opinion that the use of the phrase "...excluding design basis event... conditions," (item 3 in IEEE 323-1983) is ambiguous. It seems reasonable that the standard does not intend to exclude the environmental extremes associated with normal and abnormal operating conditions. These conditions are encompassed within the definition of "Design Basis Event" (DBE) given in 10 CFR § 50.49, which states that a DBE includes "conditions of ***normal operation***, including anticipated operational occurrences, design basis accidents, external events, and natural phenomena." In the authors' opinion, item 3 may simply be stated as follows:

> Operation of the sample to the extremes of all performance and electrical characteristics given in the equipment specifications, unless these data are available from other tests (e.g., design verification tests) on identical or similar equipment;

IEEE 323 requires non-seismic (mechanical vibration) testing to be performed where appropriate, and is required after (thermal) aging, (if needed) but before seismic testing is performed. Clarification of where non-seismic testing fits in the IEC test-sequence is provided under section 5.3.3.5 c —*mechanical vibration test.* Here, non-seismic testing is described as one of the standardized tests, and should be performed after any thermal and/or corrosion test. It may also be performed after irradiation aging testing (5.3.3.5 e). In this respect also, the two documents are essentially the same.

However, there are some differences in the two standards. For example, the IEC document specifically requires electromagnetic/radio-frequency interference[a] (EMI/RFI) susceptibility tests to be performed. There is no such specific mention of EMI/RFI tests in IEEE 323-1983.

## 2.5 Guidance on Specific Stressors and References to Other Standards

Both IEEE 323-1983 and IEC 60780 are system-level standards for the qualification of safety-related equipment. A system-level environmental qualification standard should, as a minimum, refer to specific standards for the detailed stress tests required. Both standards were therefore reviewed with regard to details they offer on specific stressors as well as references to other standards.

---

[a] It includes these tests under functional testing, instead of at the end of any aging. This may imply that there are no aging effects caused by EMI/RFI susceptibility (such as cycling of equipment due to disturbances over the service time of the equipment).

IEEE 323-1983

This standard offers little guidance on specific stressors and other standards that may be used to supplement guidelines offered within the document itself. For example, there is no guidance as to how or to what standards temperature, corrosion, or EMI/RFI tests are to be performed. The only stressor on which some detail is given is radiation (section 6.3.4). Significant details given on this stressor are the following:

a. The equipment shall be subjected to the significant type of radiation equivalent to or greater than that expected in service.

b. If more than one type of radiation is significant, each type can be applied separately.

c. If it can be shown that the combined normal and accident doses and dose rates do not affect the safety function(s) and there are no adverse effects if irradiation is done sequentially, either before or after thermal or wear cycling, then radiation testing may be excluded.

d. If it can be shown that the radiation effect is restricted to the heating effects of energy absorption, the effect may be taken into account during accelerated thermal aging.

e. A gamma radiation source may be used to simulate the expected effects of the radiation environment.

With regard to references to other standards for detailed stress testing, IEEE 323-1983 specifies ANSI/IEEE 344 as the standard to be used for seismic qualification testing. Although IEEE 323 also references other standards in section 2, "References," most of them do not contain details on any specific stress testing.

IEC 60780

The standard clearly states that standardized test specifications should be used wherever possible. Specifics given are based on the main tests that are likely to be incorporated into an aging sequence. They include the following:

a. *Thermal test and/or thermal tests with mechanical effects*

In this case, the only determining factor is temperature which may remain constant, vary slowly or show high temperature gradients. Whether the Arrhenius type law or some other method is used for thermal aging, the standard recommends the test procedures described in the following IEC publications to be used:

Dry heat (IEC 60068-2-2)
Cold (IEC 60068-2-1)
Rapid changes in ambient temperature (IEC 60068-2-14)

b. *Corrosion tests*

The standard recommends this type of test on equipment likely to be located in a damp or corrosive ambient atmosphere. The standard lists the following as the most common and easily implemented tests. The tests may be carried out in sequence and in supplement to thermal tests and/or thermal tests with mechanical effects:

Damp heat tests (IEC 60068-2-30 or IEC 60068-2-3)
Spraying or immersion test (IEC 600529 or IEC 60068-2-18)
Salt mist tests (IEC 60068-2-11 or IEC 60068-2-52)

c. *Mechanical vibration tests*

The standard recommends that equipment likely to be subjected to mechanical vibration during its use, whether self-induced (e.g., motors) or externally caused (e.g., movement of the mounting support, or pressure hammer blow in pipes), should be subjected to vibration tests reproducing the same effects. Recommended vibration and other mechanical test standards include the list following. The mechanical tests are generally carried out after the thermal and corrosion tests. They may also take place after the radiation aging test:

Sinusoidal vibration (IEC 60068-2-6). May be carried out on most electrical equipment.
Random vibration (IEC 60068-2-34)
Shock test (IEC 60068-2-27)
Hammer test (IEC 60068-2-75)
Drop and topple and free fall test (IEC 60068-2-31 and IEC 60068-2-32)
Bump test (IEC 60068-2-29)

d. *Prolonged operations test*

These tests are designed mainly for electro mechanical equipment—particularly those including moving parts—in order to simulate mechanical wear (lock-up, joint leaks, etc.), or electrical problems (contact pits, oxidation, etc.) that are likely to appear with time. Cyclic functional tests are generally performed consistent with the number of cycles during lifetime and at the specified limits of the normal range of use. No specific IEC standards are referred to for these tests.

e. *Radiation aging test*

Equipment necessary to achieve important functions to ensure reactor safety in the presence of radioactive stresses shall be subjected to a radiation test intended to check its correct behavior. The standard states that radiation aging procedures shall comply with those of IEC 60544-2.

Comments

IEC 60780 offers more details on specific stressors 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.

## 2.6 Margins

IEEE 323-1983

Section 6.3.1.5, "Margin," stipulates that "Margin shall be applied to the type test parameters for DBE testing." The suggested factors, for cases where no margins are given in specific equipment qualification standards, are as follows:

| | |
|---|---|
| Supply voltage | ±10% but not to exceed equipment design limits |
| Frequency | ±5% of rated value |
| Radiation (margin on accident dose) | +10% |
| Peak pressure | +10% of gage, but not more than 68.9 kPa (10 lbf/in$^2$) |

| | |
|---|---|
| Seismic vibration | +10% added to the acceleration requirements at the mounting point of the equipment |
| Peak temperature | +15°F (+8°C). When qualification testing is conducted under saturated steam conditions, the temperature margin shall be such that the test pressure will not exceed saturated steam pressure corresponding to peak service temperature by more than 10 $lbf/in^2$ (68.9kPa). |
| Equipment operating time | +10% of the period of time the equipment is required to be operational following the start of the DBE. |
| Environmental transients | Two methods are suggested:<br>(a). Temperature and pressure margins may be added;<br>(b). Peak transient without temperature and pressure margin may be applied twice. |

IEEE 323-1983 also states that "the margin factors...are not meant to be applied to aging....; age conditioning shall be performed on the basis of conservative estimates of service conditions and conservative accelerated aging techniques." The standard requires a 10% margin to be added to *equipment operating time*, i.e., the period of time the equipment is required to be operational following the start of the DBE.

IEC 60780

Section 5.3.1.6, "Qualification Margin," stipulates that "Qualification type testing shall include provisions to verify that an adequate qualification margin exists." Suggested margins to be applied "in the absence of detailed specifications" are as follows:

| | |
|---|---|
| For supply voltage | ±10% of nominal value, unless otherwise stated. |
| For frequency | ±5% of nominal value, unless otherwise stated. |
| Integrated aging and accident dose | +10% of theoretical calculated value. |

Characteristics of thermodynamic accident conditions:

- saturated steam temperature: the margin shall be chosen in such a manner that the pressure generated during tests does not exceed by more than 100 kPa the saturated steam pressure which corresponds to the maximum utilization temperature;

- pressure: + 10% of relative pressure of saturated steam with a maximum of 100 kPa;

- time: +10% of the period of time the equipment is required to be operational following the design basis event;

- transient: either one transient (pressure/temperature) with margin, or two transients without margins shall be carried out.

Comments:

The intent of the section on "Margin" is essentially the same in both standards, i.e., to account for normal variations in commercial production of equipment and reasonable errors in defining satisfactory performance. However two significant differences exist between the two standards:

(1) The IEC temperature margin under saturated steam conditions is more stringent. The IEC standard

requires the temperature margin to be such that the test pressure will not exceed saturated steam pressure corresponding to peak service temperature by more than about 14 lbf/in$^2$ (100 kPa), compared to the 10 lbf/in$^2$ (68.9 kPa) as stated in IEEE 323-1983.

(2) The IEC standard does not specify any temperature margin in the case where qualification testing is being performed under unsaturated steam conditions. The temperature margin in the IEEE standard in this case is +15°F (+8°C).

## 2.7 Guidance on Qualification By Operating Experience

A comparison of IEEE 323-1983 and IEC 60780 was made with regard to how operating experience is allowed to be used as a means of qualification:

IEEE 323-1983
Section 6.4, "Operating Experience," discusses how operating experience may be used to satisfy portions or all of an equipment qualification program. The essential details are the following:

- Equipment can be considered qualified if the same or similar equipment has functioned successfully under service conditions that are more severe than those postulated for the new application.

- Service conditions established from operating experience shall envelop the proposed service conditions plus appropriate DBE margin.

- If the equipment in service has not been subjected to the full range of postulated service conditions that are significant and not qualified by analysis, it shall be removed from service and tested so as to evaluate its capabilities under these conditions. Subsequently, it shall not be returned to safety service if it has been subjected to conditions that exceeded those due to normal or abnormal operating requirements (non-DBE conditions).

- The qualified life determined shall not exceed the amount of time the equipment operated under normal and abnormal service condition levels prior to the occurrence of an actual or simulated design basis event.

IEC 60780
Section 5.4, "Qualification by Operating Experience," discusses how operating experience may be used to satisfy an equipment qualification program. The essential details are the following:

- It shall be shown that ... the equipment whose operational history serves as a basis for qualification is typical of equipment bearing the same designation.

- The electrical equipment type shall be considered to be qualified by demonstrating that the recorded operating environment equals or exceeds the design environment in severity, and that the performance of the equipment in service equals or exceeds the specified user requirements.

- If the design environment includes seismic accelerations followed by a postulated initiating event that is more severe than the recorded operational environment, then the installed equipment shall, in general, be withdrawn from operation and subjected to a partial type test. This test shall subject the

equipment to the seismic and postulated initiating-event effects before the equipment can be considered fully qualified.

Comments
The essential details of qualification by operating experience is the same in both standards. The condition (third bullet under both standards) under which an equipment already in service can be removed for further testing in a qualification program, as stated in IEEE 323-1983, envelops that specified in IEC 60780. That is, "...full range of postulated service conditions which are significant..." as stated in IEEE 323-1983, encompasses a broader range of stressors than "...seismic accelerations followed by a postulated initiated event...," as stated in IEC 60780. This condition explicitly provides more flexibility in supplementing operating experience by partial testing.

## 2.8 Guidance on Qualification By Analysis

A comparison of IEEE 323-1983 and IEC 60780 was made with regard to how analysis is allowed to be used as a means of qualification:

IEEE 323-1983
Section 6.5, "Analysis," discusses how qualification by analysis may be used under this standard. The essential details are the following:

- Quantitative analysis may be used to qualify the equipment by construction of a valid mathematical model to demonstrate that the equipment can perform its safety function(s) under actual service conditions. This may be supplemented by test data or operating experience where the analytical techniques may be limited.

- Extrapolation and interpolation are analytical techniques which may be used to qualify equipment by extending the application of test data. Extrapolation or interpolation *to other equipment by similarity* can be used when the following criteria are met:
  1). Material of construction is either the same or equivalent;
  2). Size may vary if the basic configuration remains the same and dimensions are related by known scale factors;
  3). Shape may be the same or similar subject to restrictions of size and any differences shown shall not adversely affect the performance of the safety function(s).
  4). Operating and environmental stresses on the new equipment shall be equal to or less than those experienced on the qualified equipment under normal and abnormal conditions.

- The equipment shall be considered qualified through demonstration that its performance meets or exceeds that required under the specified service conditions during its qualified life or that the operation limitations of periodic inspection or surveillance have been identified.

IEC 60780
Section 5.5, "Qualification by Analysis," discusses how qualification by analysis may be used under this standard. The essential details are the following:

- The first step in a qualification by analysis is generally the application of a representative mathematical model to the equipment to be qualified. The mathematical model shall be based on established principles, verifiable test data, or operating data.

- Extrapolation is an analytical technique which may be used to supplement testing. However, in order to be considered valid, the modes of failure produced under intensified or accelerated environmental, or other influences, should be the same as those predicted under the required operational conditions.

- The equipment shall be considered to be qualified if it is demonstrated that the equipment performance will meet or exceed its specified values for the most severe environment or sequence of environments in the equipment specification throughout its qualified life.

Comments

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 (1-4 under the second bullet) are met, whereas IEC 60780 does not appear to explicitly allow this method of qualification.

The comparative analysis of IEEE 323-1983 and IEC 60780 is shown in tabular form in Table 1.

**Table 1 Comparison of IEEE 323-1983 and IEC 60780 (1998)**

| Header | IEEE 323-1983 | IEC 60780 | Comments |
|---|---|---|---|
| **2.1 Qualification Methods** | Type testing, operating experience, analysis, or any combination of the three is allowed. | Type testing, operating experience, analysis, or any combination of the three is allowed.<br><br>Type testing is explicitly stated as the preferred qualification method. | The methods of qualification are identical in both standards. Digital I&C generally undergoes more rapid evolutions than its analog counterpart. Thus, it may be difficult to obtain sufficient documentation based on operating experience under identical environmental conditions for a particular I&C equipment for qualification purposes.<br><br>As stated in IEC 60780, type testing should be the preferred qualification method. |

**Table 1 (continued)**

| | | | |
|---|---|---|---|
| **2.2 On-Going Qualification** | Qualified life may be extended under the following conditions:<br><br>1. Type testing of a piece of equipment of the same or similar design and construction which has been age-conditioned for a period equivalent to a longer time than the qualified life of the installed equipment.<br><br>2. Type testing of a piece of equipment of the same or similar design and construction which has been naturally aged in an environment equal to or more severe than the non-DBE service conditions for the intended application.<br><br>3. Type testing of a piece of equipment of the same or similar design and construction which has undergone a combination of natural aging and age conditioning for a period equivalent to a longer time than the qualified life of the installed equipment.<br><br>4. Use of periodic surveillance/maintenance, testing, and replacement/refurbishment programs based on manufacturers' recommendations and sound engineering practices.<br><br>5. If it can be shown that evaluation in the original qualified program was conservative with respect to the equipment's specified service conditions and performance specifications.<br><br>6. If it can be shown that an age-conditioning procedure, that limited the qualified life of an equipment, is in fact conservative.<br><br>7. If it can be shown that the service or environmental conditions originally assumed were overly conservative with respect to those that apply at the equipment's locations, in its installed configuration. | Methods by which qualified life can be extended are the following:<br><br>1. Replacement of the whole equipment or sensitive parts of it within a predetermined period of time as a preventive measure.<br><br>(b). Execution of periodic pertinent testing on operating equipment (e.g., accuracy, insulation resistance, response time).<br><br>(c). Additional items of equipment can be installed beside the required item, be removed before the end of the qualified life period and be tested to determine their additional qualified life. | The requirements as stipulated in IEEE 323-1983 envelop those stipulated in IEC 60780. Furthermore, it is our opinion that the IEEE 323 procedures do not require modification for application to microprocessor-based and advanced digital systems. |

**Table 1 (continued)**

| Header | IEEE 323-1983 | IEC 60780 | Comments |
|---|---|---|---|
| **2.3 Aging** | If type testing is the mode of qualification, then preconditioning prior to testing is not required if the equipment is determined not to have significant aging mechanisms. | Accelerated aging is not intended to be applied to all safety equipment in the safety system. Safety equipment which is not supposed to be subjected to accident conditions is not intended to be pre-aged before being seismically tested. | While the need for aging is recognized by both standards, it appears that the criterion in IEC 60780 for determining whether or not an equipment should be aged has a slightly different focus than in IEEE 323-1983. That is, the IEC 60780 criterion depends on whether or not the equipment will be subjected to accident conditions (steam during a LOCA, flooding, etc.) and is independent of the environmental conditions during normal service. On the other hand, IEEE 323-1983 appears to indicate that the overriding concern should be the effect of the environment on the equipment's ability to perform its safety function *whenever it is called upon to do so* (i.e., "under DBE conditions" as stated in the definition of "significant aging mechanisms." Note that 10 CFR § 50.49 defines Design Basis Event as "conditions of normal operation, including anticipated operational occurrences, design basis accidents, external events, and natural phenomena"). |

**Table 1 (continued)**

| Header | IEEE 323-1983 | IEC 60780 | Comments |
|---|---|---|---|
| **2.4 Test Sequence** | Significant elements of the type testing sequence include the following:<br><br>1. Inspection of the sample to ensure that it has not been damaged due to handling since manufacture.<br><br>2. functional tests under normal conditions to obtain baseline data.<br><br>3. operation of the sample to the extremes of all performance and electrical characteristics given in the equipment specifications, excluding design basis event and post design basis event conditions.<br><br>4. Aging of the equipment if necessary). Design basis event radiation may be included during this step.<br><br>5. Subjection of the sample to non-seismic mechanical vibration;<br><br>6. Subjection of the sample to simulated operating basis earthquake and safe shutdown earthquake seismic vibration.<br><br>7. For equipment located in harsh environment, the test sample is required to perform its required safety function(s) while exposed to the simulated DBA. The standard allows DBA radiation to be excluded in this test if incorporated in (4).<br><br>8. The test sample is required to perform its safety function(s) while exposed to the simulated post-DBA conditions as applicable. | Significant elements of the type testing sequence include the following:<br><br>1. *Functional Testing*<br>a). Inspection.<br>b). Testing under normal conditions to provide baseline data.<br>c). Testing to the electrical and environmental extremes indicated in its performance specification (this includes electromagnetic susceptibility testing).<br><br>2. *Testing to demonstrate seismic resistance of equipment*<br>Pre-aging is to be performed before seismic testing only if significant aging factors exist for the equipment.<br><br>3. *Testing to demonstrate resistance of equipment to accident and post-accident conditions*<br>a). Equipment aging (assessment of behavior with time).<br>b). Accident and post-accident condition tests. | The IEC document specifically requires electromagnetic (EMI/RFI) susceptibility tests to be performed. There is no specific mention of EMI/RFI tests in IEEE 323.<br><br>The use of the phrase "...excluding design basis event... conditions," (item 3 in IEEE 323-1983) is ambiguous. It seems reasonable that the standard does not intend to exclude the environmental extremes associated with normal and abnormal operating conditions. These conditions are encompassed within the definition of "Design Basis Event" (DBE) given in 10 CFR § 50.49, which states that a DBE includes "conditions of ***normal operation***, including anticipated operational occurrences, design basis accidents, external events, and natural phenomena." |

**Table 1 (continued)**

| Topic | IEEE 323-1983 | IEC 60780 | Comments |
|---|---|---|---|
| **2.5 Guidance on specific stressors and reference to other standards** | Standard offers little guidance on specific stressors and other standards that may be used to supplement guidelines offered in the document itself. For example, there is no guidance as to how temperature, corrosion, or EMI/RFI tests are to be performed. Some detail is given on radiation. | Standard clearly states that *standardized* test specifications should be used wherever possible. Specifics given are based on the main tests that are likely to be incorporated into an aging sequence. They include the following:<br><br>a. *Thermal test and/or thermal tests with mechanical effects.* Referenced standards are:<br><br>Dry heat (IEC 60068-2-2)<br>Cold (IEC 60068-2-1)<br>Rapid changes in ambient temperature (IEC 60068-2-14)<br><br>b. *Corrosion tests*<br>Referenced standards are:<br>Damp heat tests (IEC 60068-2-30 or IEC 60068-2-3)<br>Spraying or immersion test (IEC 600529 or IEC 60068-2-18)<br>Salt mist tests (IEC 60068-2-11 or IEC 60068-2-52)<br><br>c. *Mechanical vibration tests*<br>Recommended vibration and other mechanical test standards are the following:<br><br>Sinusoidal vibration (IEC 60068-2-6).<br>Random vibration (IEC 60068-2-34)<br>Shock test (IEC 60068-2-27)<br>Hammer test (IEC 60068-2-75)<br>Drop and topple and free fall test (IEC 60068-2-31 and IEC 60068-2-32)<br>Bump test (IEC 60068-2-29)<br><br>d. *Prolonged operating test*<br>No specific IEC standards are referred to for these tests.<br><br>e. *Irradiation aging test*<br>The standard states that irradiation aging procedures shall comply with those of IEC 60544-2. | IEC 60780 offers more details on specific stress tests as well as references to other standards than IEEE 323. In this respect, IEC 60780 provides better clarity as to how environmental qualification of safety-related equipment should be performed. |

**Table 1 (continued)**

| Topic | IEEE 323-1983 | IEC 60780 | Comments |
|---|---|---|---|
| **2.6 Margins** | The suggested factors are as follows:<br>Supply voltage.....±10% but not to exceed equipment design limits<br>Frequency.....±5% of rated value<br>Radiation (margin on accident dose) .....+10%<br>Peak pressure.....+10% of gage, but not more than 68.9 kPa (10 lbf/in$^2$)<br>Seismic vibration..... +10% added to the acceleration requirements at the mounting point of the equipment<br>Peak temperature.....+15$^o$F.<br>When qualification testing is conducted under saturated steam conditions, the temperature margin shall be such that the test pressure will not exceed saturated steam pressure corresponding to peak service temperature by more than 10 lbf/in$^2$<br>Equipment operating time....+10% of the period of time the equipment is required to be operational following the start of the DBE.<br>Environmental transients.....Two methods are suggested:<br>(a). Temperature and pressure margins may be added;<br>(b). Peak transient without temperature and pressure margin may be applied twice. | Suggested margins to be applied "in the absence of detailed specifications" are as follows:<br><br>For supply voltage.....±10% of nominal value, unless otherwise stated.<br>For frequency.....±5% of nominal value, unless otherwise stated.<br>Integrated aging and accident dose .....+10% of theoretical calculated value.<br>Characteristics of thermodynamic accident conditions:<br>- saturated steam temperature;<br>- pressure: + 10% of relative pressure of saturated steam with a maximum of 100 kPa;<br>- time: +10% of the period of time the equipment is required to be operational following the design basis event;<br>- transient: either one transient (pressure/temperature) with margin, or two transients without margins shall be carried out. | The intent of the section on "Margin" is essentially the same in both standards, i.e., to account for normal variations in commercial production of equipment and reasonable errors in defining satisfactory performance. However two significant differences exist between the two standards:<br><br>(1) The IEC temperature margin under saturated steam conditions is more stringent. The IEC standard requires the temperature margin to be such that the test pressure will not exceed saturated steam pressure corresponding to peak service temperature by more than about 14 lbf/in$^2$ (96.5 kPa), compared to the 10 lbf/in$^2$ (68.9 kPa) as stated in IEEE 323-1983.<br><br>(2) The IEC standard does not specify any temperature margin in the case where qualification testing is being performed under non-saturated steam conditions. The temperature margin in the IEEE standard in this case is +15$^o$F (+8$^o$C). |

**Table 1 (continued)**

| Topic | IEEE 323-1983 | IEC 60780 | Comments |
|---|---|---|---|
| **2.7 Guidance on Qualification By Operating Experience** | The essential details are the following:<br><br>• Equipment can be considered qualified if the same or similar equipment has functioned successfully under service conditions that are more severe than those postulated for the new application.<br><br>• Service conditions established from operating experience shall envelop the proposed service conditions plus appropriate DBE margin.<br><br>• If the equipment in service has not been subjected to the full range of postulated service conditions that are significant and not qualified by analysis, it shall be removed from service and tested so as to evaluate its capabilities under these conditions. Subsequently, it shall not be returned to safety service if it as been subjected to conditions which exceeded those due to normal or abnormal operating requirements (non-DBE conditions).<br><br>• The qualified life determined shall not exceed the amount of time the equipment operated under normal and abnormal service condition levels prior to the occurrence of an actual or simulated design basis event. | The essential details are the following:<br><br>• It shall be shown that ... the equipment whose operational history serves as a basis for qualification is typical of equipment bearing the same designation.<br><br>• The electrical equipment type shall be considered to be qualified by demonstrating that the recorded operating environment equals or exceeds the design environment in severity, and that the performance of the equipment in service equals or exceeds the specified user requirements.<br><br>• If the design environment includes seismic accelerations followed by a postulated initiating event that is more severe than the recorded operational environment, then the installed equipment shall, in general, be withdrawn from operation and subjected to a partial type test. This type shall subject the equipment to the seismic and postulated initiating-event effects before the equipment can be considered fully qualified. | The essential details of qualification by operating experience is the same in both standards. The condition under which an equipment already in service can be removed for further testing in a qualification program, as stated in IEEE 323, envelops that specified in IEC 60780. |

**Table 1 (continued)**

| Topic | IEEE 323-1983 | IEC 60780 | Comments |
|---|---|---|---|
| **2.8 Guidance on Qualification by Analysis** | The essential details are the following:<br>• Quantitative analysis may be used to qualify the equipment by construction of a valid mathematical model to demonstrate that the equipment can perform its safety function(s) under actual service conditions.<br>• Extrapolation and interpolation may be used to qualify equipment by extending the application of test data. Extrapolation or interpolation *to other equipment by similarity* can also be used.<br>• The equipment shall be considered qualified through demonstration that its performance meets or exceeds that required under the specified service conditions during its qualified life or that the operation limitations of periodic inspection or surveillance have been identified. | The essential details are the following:<br>• Application of a representative mathematical model to the equipment to be qualified.<br>• Extrapolation may be used to supplement testing.<br>• The equipment shall be considered to be qualified if it is demonstrated that the equipment performance will meet or exceed its specified values for the most severe environment or sequence of environments in the equipment specification throughout its qualified life. | 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. |

## 2.9 Conclusions

Topical comparisons have been performed between IEEE 323-1983 and IEC 60780 (1998) in this document. Conclusions from these comparisons are as follows:

1. 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 its analog counterpart. 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. This is because equipment may be replaced with newer systems before sufficient operating experience has been accumulated. As stated in IEC 60780, **type testing** should be the preferred qualification method.

2. The requirements for on-going qualification as stipulated in IEEE 323-1983 envelop those stipulated in IEC 60780. Furthermore, it is our opinion that the IEEE 323 procedures do not require modification for application to microprocessor-based and advanced digital systems.

3. The reasons and concepts for aging are essentially the same in both versions.

4. 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. It is our opinion that EMI/RFI susceptibility tests should be an explicit requirement for qualification of microprocessor-based safety systems.

5. IEC 60780 (1998) offers more details on specific stress tests as well as references to other standards than IEEE 323-1983. In this respect, IEC 60780 (1998) provides better clarity as to how environmental qualification of safety-related equipment should be performed.

6. The intent of the section on "Margin" is essentially the same in both standards, i.e., to account for normal variations in commercial production of equipment and reasonable errors in defining satisfactory performance. Except for temperature, the margin values for all other parameters are essentially the same in both standards.

7. The essential details of qualification by operating experience is the same in both standards. The condition under which an equipment already in service can be removed for further testing in a qualification program, as stated in IEEE 323-1983, envelops that specified in IEC 60780 (1998).

8. 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 (1998) does not explicitly allow this method of qualification.

# 3 RECOMMENDATIONS FOR ENVIRONMENTAL QUALIFICATION OF MICROPROCESSOR-BASED EQUIPMENT IMPORTANT TO SAFETY IN NUCLEAR POWER PLANTS

Based on results of comparisons of the two qualification documents as well as the results of previous research, we suggest here a framework for qualifying microprocessor-based equipment for safety system applications. This methodology is based on (a) an assurance of a minimum level of integrated-circuit-component (IC) 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; (b) minimization, through design, of the potential effect of environmental stressors on the equipment throughout its service life; and (c) qualification at the equipment level using appropriate consensus standards. In particular:

It is our opinion that qualification methods and procedures described by either IEEE Std 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," or IEC 60780, "Nuclear Power Plants - Electrical Equipment of the Safety System - Qualification,"are appropriate, in its entirety, for satisfying the qualification of safety-related microprocessor-based equipment for service in nuclear power plants 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 equipment or module. Studies documented in NUREG/CR-6406[3] show that for distributed systems communication interfaces are likely to be the most vulnerable elements. Thus qualification testing should confirm the response of any digital interfaces to environmental stress in a distributed system. Type testing should be the preferred method to achieve this. In cases where 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. We suggest a more rigorous definition of the nuclear plant environment (i.e., other than "harsh" and "mild") based on three location categories as follows:

| | | |
|---|---|---|
| Category A Location: | | All locations inside containment and those 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 (4Gy), but $<10^4$ rad (100Gy), over 40 years. |

| | | |
|---|---|---|
| | *Temperature:* | Normal service environment shall not exceed 38°C (100°F), and accident service environment shall not exceed 90% of the manufacturer's maximum rated operating temperature. |
| | *Humidity:* | Normal service environment shall not exceed 80%, and abnormal and accident environment shall 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 shall be below 38°C (100°F). |
| | *Humidity:* | Normal service environment shall not exceed 80%, and abnormal and accident environment shall not exceed 95% non-condensing. |

For microprocessor-based equipment in a Category A environment, a qualified life is required. 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 established in Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," apply.

Recommended documentation to provide evidence of qualification for a Category A environment is identical to the requirements for type test data in IEEE 323-1983. Further guidance on documentation of equipment specification/service environment (IEEE 323-1983, section 6.1, or IEC 60780, section 5.2), is provided in Regulatory Guide 1.89.

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 lead to degraded performance over the expected installed life of the equipment are identified, then preconditioning may be omitted from the test sequence.

Recommended documentation to provide evidence of qualification for a Category B environment is similar to the requirements for type test data in IEEE 323-1983, section 8.3. However, if no aging mechanisms are identified, then, in place of age conditioning procedure [6.3.1.1(5) referenced in section 8.3(6)], 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) referenced in section 6.3(c)], findings from the assessment of aging mechanisms should be documented.

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

4. 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 then, in addition, a temperature margin of +15°F (8°C) should be applied in the case where qualification testing is not being performed under saturated steam conditions.

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

6. Qualification should begin at the integrated-circuit-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 assuring, among other process control methodologies, a minimum level of stress tests and a guarantee of correct operation in a specified environment. For example, integrated circuit components are typically rated for operation at temperature ranges that may exceed certain accident conditions. In particular:

   Commercial grade components: Guaranteed operating temperature range is between 0°C and 70°C (32°F and 158°F).

   Industrial grade components: Guaranteed operating temperature range is between 0°C and 85°C (32°F and 185°F).

   Military grade components: Guaranteed operating temperature range is between -55°C and 130°C (-67°F and 266°F).

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

   **Temperature/Humidity Bias Test**
   This is an environmental test whose main purpose is to measure the moisture resistance of plastic encapsulated circuits, and 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 which 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 205 kPa (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 metal oxide semiconductor (MOS) devices by applying operating conditions at room temperature. Hot carrier injection-induced transistor degradation is thought to be due to interface damage and charge disposition in the gate oxide, giving rise to parasitic substrate and gate currents. The overall consequence is a shift in drain current, transconductance and/or threshold voltage.

**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 integrated-circuit-component-level, however, tests documented in NUREG/CR-6406[3] 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 environments in nuclear power plants.

We recommend that the standards and testing practices used by the integrated circuit (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 characteristics. As a minimum, the tests covered by the standards should include, but are not limited to, the following:

a. Temperature/Humidity Bias Test
b. High Temperature Operating Life Test
c. Temperature Cycle Test
d. Autoclave Test
e. Low Temperature Operating Life Test
f. System Soft Error Test

7. 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. 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 value of this recommendation is that it encourages the applicant to consider and document the protection against environmental stress afforded to safety-related I&C equipment.

A description should be provided of the approaches employed to accomplish such protection. Figure 1 illustrates the conceptual levels at which protection against environmental stressors is possible for the actual circuits/components performing a safety-related function. These levels can be characterized as follows:

**Electronic Component Level**

The first level of environmental protection for system components should occur at the IC level.

The tolerance to radiation of the particular circuit technology [e.g., Transistor-Transistor Logic (TTL) or CMOS] used should be considered, if the radiation environment is significant. Some MOS devices can fail at the relatively low dose of 1 krad (Si). In fact, commercial MOS devices are quite sensitive to ionizing dose, 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).

Thermal management problems at the IC level become increasingly significant as clock frequencies increase, and higher density circuitry are employed for microprocessors and other integrated circuits. Moreover, as the number of input/outputs to the chip increase, 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 has to only 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 exception 6).

**Module or Circuit Board Level**

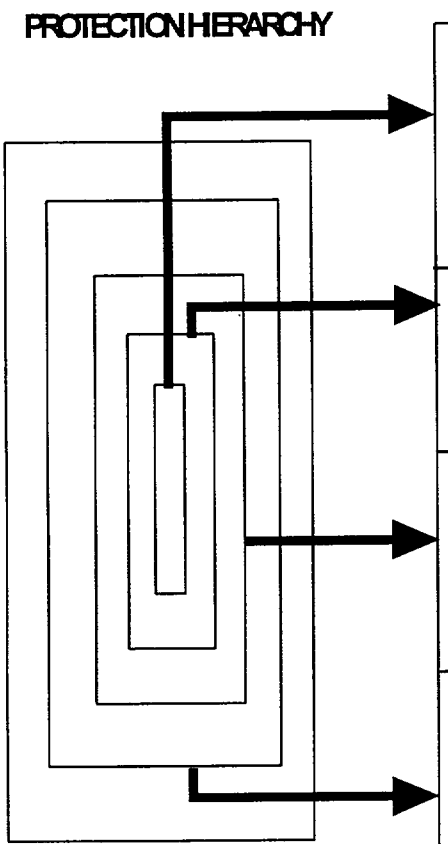
Depending on the system design, the next level of protection may be modules, racks, or circuit boards inside the cabinet. Mounting circuit boards vertically may help to limit soot, dust, and water accumulation. Modules may be designed in such a manner as to reduce smoke and particulate deposits in case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

**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. With regard to this, cable conduits connected to cabinets may help to prevent standing water if connections are made from the bottom of the cabinet.

**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 in which the equipment is installed, considering its distance away from potential sources of smoke, fire, and radiation, may serve as a shield for the equipment and contribute on this level to protection against the spread of smoke and flames in case a fire occurs.




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

**Figure 1 Illustrating Potential Levels of Protection Against Environmental Stressors for Safety-Related Electronic Hardware.** (NOTE: The sequential order of the stressors is approximately related to the sequential order of the controls and should not be interpreted as indicating order of importance.)

8. Random failures should be addressed using surveillance, on-line diagnostics, maintenance, and/or trending techniques at intervals based on the predicted failure rates. The possibility of multiple latent failures existing at the time that 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, such approaches should be chosen so that unreasonable complication is not added to the quality assurance process for the software development.

## REFERENCES


1. G. C. Messenger and M. S. Ash, "The Effects of Radiation on Electronic Systems," Second Edition, Van Nostrom Reinhold, 1992 (ISBN 0-442-23952-1).

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

3. K. Korsah, T. J. Tanaka, T. L. Wilson, Jr., and R. T. Wood, *Environmental Testing of an Experimental Digital Safety Channel*, NUREG/CR-6406, U.S. Nuclear Regulatory Commission, September 1996.

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

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

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

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

8. Tina J. Tanaka and Steven P. Nowlen, *Results and Insights on the Impact of Smoke on Digital Instrumentation & Controls*, NUREG/CR-6597, U.S. Nuclear Regulatory Commission, January 2001.

9. *Criteria 3—Fire Protection,* Appendix A to part 50 of Title 10 of the Code of Federal Regulations.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

# BIBLIOGRAPHIC DATA SHEET

*(See instructions on the reverse)*

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-6741
ORNL/TM-2000/236

2. TITLE AND SUBTITLE

Application of Microprocessor-Based Equipment in Nuclear Power Plants --Technical Basis for a Qualification Methodology

Draft Report for Comment

3. DATE REPORT PUBLISHED

| MONTH | YEAR |
|---|---|
| August | 2001 |

4. FIN OR GRANT NUMBER

L1798

5. AUTHOR(S)

K. Korsah, R.T. Wood, ORNL
C.E. Antonescu, NRC

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

8. PERFORMING ORGANIZATION - NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Oak Ridge National Laboratory
Managed by UT-Battelle, LLC
Oak Ridge, TN 37831-6010

9. SPONSORING ORGANIZATION - NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Division of Engineering Technology
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

C.E. Antonescu, NRC Project Manager

11. ABSTRACT *(200 words or less)*

This document (1) summarizes the most significant findings of the "Qualification of Advanced Instrumentation and Control (I&C) Systems" program initiated by the Nuclear Regulatory Commission (NRC); (2) documents a comparative analysis of U.S. and European qualification standards; and (3) provides recommendations for enhancing regulatory guidance for environmental qualification of microprocessor-based safety-related systems. The comparative analysis of two environmental qualification standards involves Institute of Electrical and Electronics Engineers (IEEE) Std 323-1983 (reaffirmed in 1996) and International Electrotechnical Commission (IEC) 60780 (1998). The two standards were chosen for this analysis because IEEE 323 is the current U.S. standard addressing the qualification of safety-related equipment in nuclear power plants, and IEC 60780 as its European counterpart. In addition, the IEC document was published in 1998, and should reflect any new qualification concerns, from the European perspective, with regard to the use of microprocessor-based safety systems in power plants. The findings of the program, as summarized in this document, provide the technical basis for recommendations on the endorsement of the current qualification standards, with clarifications and exceptions that address unique characteristics of microprocessor-based systems.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

aging
digital
EMI/RFI
environmental capability
environmental stressors
instrumentation and controls (I&C)
microprocessor
nuclear power plant
qualification
radiation
reactor protection system
smoke
temperature
vibration

13. AVAILABILITY STATEMENT

unlimited

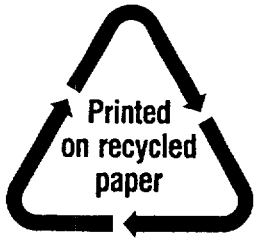
14. SECURITY CLASSIFICATION

*(This Page)* unclassified

*(This Report)* unclassified

15. NUMBER OF PAGES

16. PRICE




Federal Recycling Program