Qualification of Microprocessor-Based Equipment for Nuclear Power Plant Environments

Christina Antonescu
U.S. NRC Office of Nuclear Regulatory Research
Tel: 011-1-301-415-6792, Fax: 011-1-865-301-415-5160, E-mail: cea1@nrc.gov

Kofi Korsah[1]
Richard T. Wood[2]
Oak Ridge National Laboratory
[1]Tel: 011-1-865-576-6064, Fax: 011-1-865-576-8380, E-mail: korsahk@ornl.gov
[2]Tel: 011-1-865-574-5578, Fax: 011-1-865-576-8380, E-mail: woodrt@ornl.gov

`Abstract

In the past several years, studies have been performed by Oak Ridge National Laboratory, Sandia National Laboratory, and Brookhaven National Laboratory in a confirmatory research program initiated by the U.S. NRC with the objective of identifying methodologies for enhancing current qualification guidelines for the application of microprocessor-based I&C in safety-related systems in nuclear power plants. The results of these studies have been published in several journals and NUREG/CR reports.

This paper summarizes the results of these studies, and employs those findings as the technical basis to establish an enhanced qualification process for microprocessor-based systems.

1. Introduction

Most nuclear power plants in the United States were built decades ago and typically employ analog components in their safety systems. As microprocessor-based components increase in application for newer designs as well as system upgrades, current qualification methodologies may need to be enhanced to maintain a high level of confidence in the safe, reliable operation of such safety-related systems. In the past several years, studies have been performed by Oak Ridge National Laboratory, Sandia National Laboratory, and Brookhaven National Laboratory in a confirmatory research program initiated by the U.S. NRC with the objective of identifying methodologies for enhancing present-day qualification guidelines. The results of these studies have been published in several journals and NUREG/CR reports [1-7].

We summarize the results of these studies in this paper. Based on the technical basis provided by these findings, we suggest a method for using the most recent consensus practices, with some enhancements, for the qualification of microprocessor-based safety-related systems in nuclear power plants.

2. Summary of Previous Work on I&C Qualification Studies

The most significant findings from the studied reported in references 1-7 are the following:

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 integrated circuit (IC) manufacturer's maximum temperature ratings. 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 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) 3 in Appendix A of Title 10, Part 50 of the Code of Federal Regulations (10 CFR 50); 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. 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.

3. Comparison of Current Qualification Standards

Current U.S. and European qualification standards have been compared in two NUREG/CR reports: NUREG/CR-6479 compares IEEE 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and IEEE 323-1983, while NUREG/CR-6741 compares IEC 60780-1998, "Nuclear Power Plants – Electrical Equipment of the Safety Systems - Qualification," and IEEE 323-1983. The results of these comparisons are summarized below:

3.1. Inter-comparison of IEEE 323-1974, IEEE 323-1983, and IEC 60780-1998

Qualification methods

Type testing, operating experience, analysis, or a combination of all three, are allowed in all the three standards. Type testing is explicitly stated as the preferred method in IEEE 323-1974. It is also explicitly stated as the preferred method in IEC 60780.

On-Going Qualification

Procedures and conditions for on-going qualification in both IEEE standards are similar. IEEE 323-1983 includes extension of qualified life if it can be proven, with suitable documentation and auditable records, that the original qualification program was conservative. Procedures and conditions for on-going qualification in IEEE 323-1983 envelop those stipulated in IEC 60780.

Aging

All three standards imply that there may be situations where aging may not be required. IEEE-1983 introduced the concept of "significant aging mechanism" as a way for the user to determine whether or not aging should be considered during type testing. IEC 60780 refers to the existence of "significant aging factors" in the application of accelerated aging. IEC 60780 embodies detailed guidance on accelerated aging.

Temperature, radiation, wear (prolonged operation in IEC 60780), and vibration are indicated age conditioning factors in both versions while IEC 60780 explicitly includes corrosion.

Test Sequence

Basic sequence for qualification programs in all three standards is the same: testing under normal conditions and anticipated extremes, thermal aging, irradiation to aging plus accident dose, vibration and seismic testing, design basis accident (DBA) testing, and post-DBA testing, to be performed as applicable. Electromagnetic (EMI/RFI) susceptibility tests are explicitly required in IEC 60780. Aging prior to seismic testing is not required under IEC 60780 if equipment will not be subject to accident conditions.

IEC 60780 defines three test groupings that may be treated independently and may be conducted on different samples: (a) Functional (normal conditions and extremes); (b) Seismic (preconditioning not required if equipment not intended to be subject to accident conditions); (c) Accident and post-accident (including aging as initial step). IEC 60780 also gives more detailed guidance on preferential stresses and standardized tests.

Margins

Suggested factors to be applied to service conditions for type testing are essentially the same in both IEEE standards. However, the 1983 version adds that "Margin shall be applied to the type test parameters for DBE testing" and that the suggested margin factors "are not meant to be applied to aging" [given the conservatism already employed in age conditioning]. IEC 60780 identifies the suggested margins as applying to "operational conditions for type testing."

For the suggested margin factors in the IEEE standards, the 1983 version offers clarification regarding environmental transients (also shown in the simulated service condition test profile). Temperature and pressure margin may be added to transient conditions. Peak transient, without temperature and pressure margin, may be applied twice.

IEC 60780 gives a more stringent temperature margin for saturated steam conditions [96.5 kPa (14 psi) versus 68.9 kPa (10 psi)]. IEC 60780 does not specify any temperature margin for conditions other than saturated steam conditions while IEEE 323-1983 specifies 15ºF (8ºC).

4. Enhanced Qualification Process

Based on the previous research summarized in this paper, as well as the analysis of current environmental qualification standards, it is our opinion that methods and procedures described by either IEEE Std 323-1983, or IEC 60780, are suitable, in their entirety, for satisfying the qualification of safety-related microprocessor-based equipment for service in nuclear power plants. However, to enhance the process to account for unique characteristics of digital technology, selected conditions and clarifications are suggested, as stated below.

1. Distributed Systems

The dynamic response of a distributed system under environmental stress should be considered during qualification testing: This enhancement contributes to the assurance that qualification testing addresses system response to environmental stress of any digital interfaces.

2. EMI/RFI Testing

Electromagnetic compatibility testing (i.e., EMI/RFI susceptibility and surge withstand testing) should be included as part of qualification testing: This enhancement is similar to testing requirements for qualifying programmable logic controllers (PLCs) (EPRI TR-107330). The EMI/RFI testing should be performed as part of the test sequence per IEC 60780, or at an equivalent stage of the test sequence under IEEE 323-1983, if that standard is being applied.

3. Location Categories for Aging Determinations

In order to clarify when accelerated aging is needed in a qualification program, we suggest the three location categories—A, B, and C as discussed below—for a nuclear environment. The suggested environmental thresholds are based on a conservative assumption on the survivability of commercial grade integrated circuits, current literature on radiation tolerance of different chip technologies, and an examination of normal and accident environmental conditions documented in Safety Analysis Reports (SARs). For example, Table 1 shows typical normal and accident conditions in nuclear power plants estimated from SAR reports.

Category A locations include all locations inside containment, and all areas subject to DBA conditions.

Category B locations include all areas not within Category A which exceed Category C conditions. Representative environmental conditions (i.e., radiation, temperature, and humidity) for this

Table 1. Typical normal and accident conditions in nuclear power plants estimated from SAR reports

Typical Physical Location in Plant	Normal/Accident Operating Temperature (Deg. F)[a]	Normal/Accident Humidity (%)[a]	Normal/Accident Dose (rad)[c]
Reactor Building			
• Operating floor	50-120/250-385[b]	50-100/100	$3.5 \times 10^3/8 \times 10^6$
• Steam generator loop compartment	50-120/250-385[b]	50-100/100	$6 \times 10^6/8 \times 10^6$
• Outside steam generator loop compartment	50-120/250-385[b]	50-100/100	$3.5 \times 10^3/8 \times 10^6$
Auxiliary Building	50-120/100-325	5-70/70-100	10^2 - 10^6
Control building	60-104/84-120	10-70/70-95	<200
Turbine Building	60-110	5-95	<200
Diesel Generator Building	60-122/122	5-95/95	<200/<500

category are as follows (Note that all temperatures indicated are ambient; thus, temperatures inside cabinets may be higher):

Radiation: > 800 rad, but < 10,000 rad
Temperature: normal, ≤ 50°C (122°F);
accident, ≤165°C (329°F)
Humidity: normal, ≤ 99% non-condensing
accident, 100%

Category C locations include any location in which the following representative environmental conditions are met:

Radiation: > 800 rad, but < 10,000 rad
Temperature: normal, ≤ 40°C (104°F);
abnormal, ≤ 50°C (122°F)
Humidity: normal, ≤ 95% non-condensing
abnormal, ≤ 99% non condensing

Characterization of a specific plant location according to these three suggested categories should be based on comparison of the actual environmental conditions with each representative stressor condition. Thus, if a location exceeds the identified range for an individual stressor, then it should be designated according to the next highest category that encompasses its particular environmental conditions. However, it should be noted that these location categories are not intended to be rigorously applied. For example, if the temperature and humidity conditions for a specific location clearly meet Category C conditions, but the integrated dose over 40 years is estimated to be 810 rad instead of 800 rad, the location would correctly be interpreted as Category C.

For microprocessor-based equipment in a Category A environment, establishment of qualified life is needed. Preconditioning (accelerated aging) should be applied in accordance with IEEE 323-1983 or IEC 60780-1998, depending on the standard being

[a] For both normal and accident parameters, the table gives a range (minimum and maximum) values.

[b] Following a postulated main steam line break, containment temperature may exceed 380 for a brief period of time but settle down considerably below this value. Thus, the values given should be considered conservative.

[c] Normal dose values are derived by integrating dose rates over 40 years. However, accident values are derived by integrating dose rates over 6 months following the accident.

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," should be applied. Recommended documentation to provide evidence of qualification for a Category A environment is identical to the guidance for type test data in IEEE 323-1983, section 8.3, or IEC 60780-1998, section, section 6.3, depending on the standard being applied. 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 a 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, there are clearly no significant aging mechanisms resulting from the customary factors (e.g., temperature, radiation, wear, vibration) so 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

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 to the suggested margin factors, a temperature margin comparable to the guidance in IEEE 323-1983 should be applied for qualification testing under high temperature environments not characterized by saturated steam conditions.

5. Life-Limited Components and Surveillance

Any life-limited component of the microprocessor-based system being qualified should be identified and its operational-life should be documented along with a surveillance, testing, and maintenance program sufficient to detect potential degradation.

5. The Enhanced Process is Consistent with Current Qualification Guidance

In this section we discuss how the enhanced qualification process relates to current environmental qualification guidance and the existing regulatory approach.

First, RG 1.89 guidance for harsh environments is incorporated by reference in the conditions for qualification for a Category A locations (which is equivalent to a "harsh" environment covered by 10 CFR 50.49).

Second, the inclusion of EMI/RFI testing in the qualification process is consistent, although perhaps less conservative, with EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants." Section 6.3.1 of the EPRI document requires EMI/RFI testing to be performed after "other environmental tests" (i.e., to account for potential aging).

Third, the suggested Location Categories and associated qualification activities are comparable with the Equipment Category requirement as identified in NUREG-0588, "Interim Staff Position on Environmental Qualification of Safety-Related Electrical Equipment," Revision 1.

Figure 1 shows how the equipment categories identified in Appendix E of NUREG-0588 map into the environmental categories suggested in this paper.

It can be seen that, in general, the suggested Category A location covers NUREG-0588 category 2a and 2b equipment; suggested category B location, in general, encompasses all NUREG-0588 Category 2c Equipment; and suggested category C location encompasses all NUREG-0588 category 2d equipment.

6. References

1. 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.

2. 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.

3. 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.

4. 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.

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

6. 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.

7. 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.

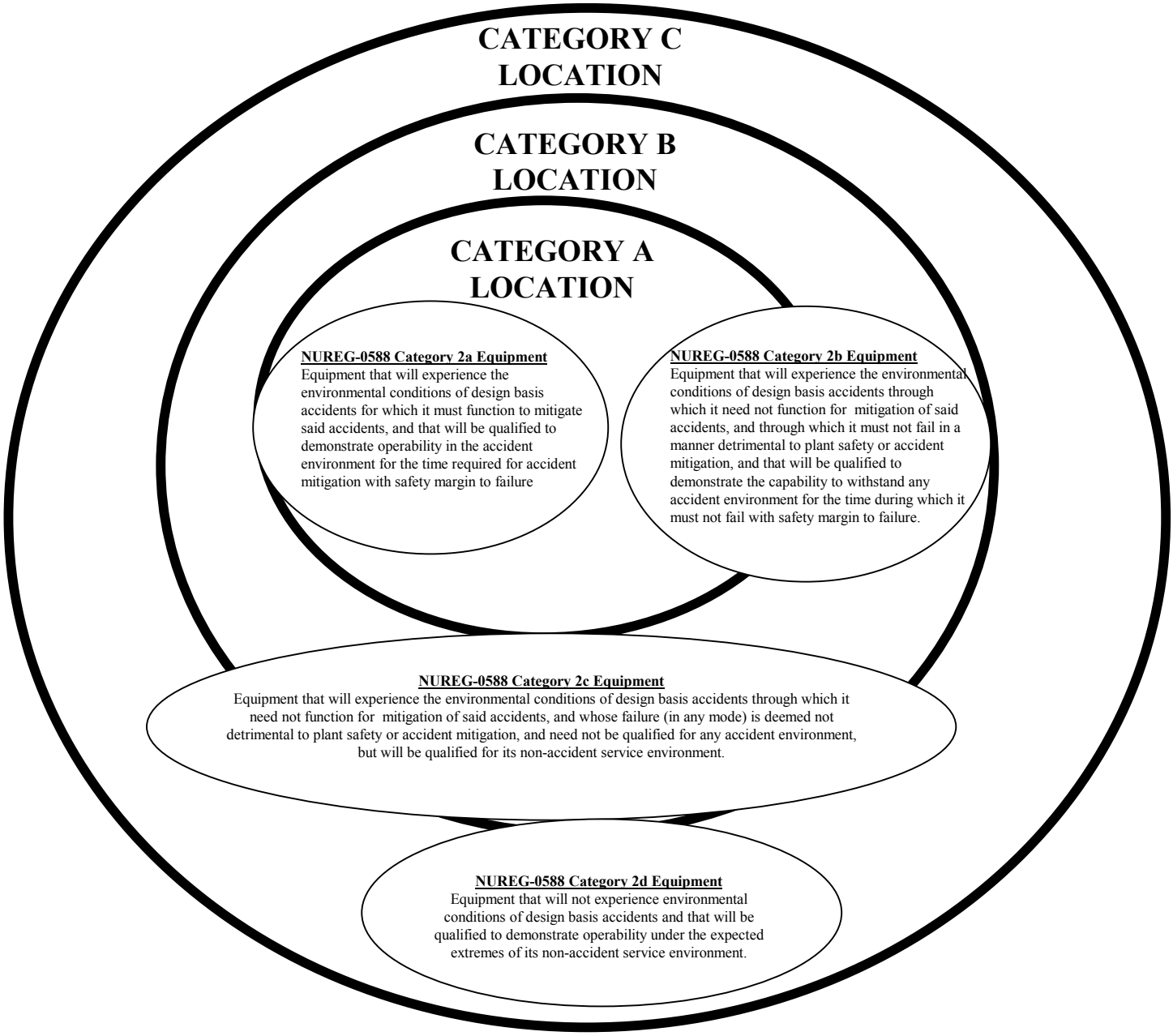

Figure 1. Pictorial mapping of the equipment categories identified in Appendix E of NUREG-0588 into the proposed location categories