NUREG/CR-6479
ORNL/TM-13264

Technical Basis for Environmental Qualification of Microprocessor-Based Safety-Related Equipment in Nuclear Power Plants

Manuscript Completed: December 1997
Date Published: January 1998

Prepared by
K. Korsah, ORNL
M. Hassan, BNL
T. J. Tanaka, SNL
R. T. Wood, ORNL

Oak Ridge National Laboratory
Managed by Lockheed Martin Energy Research Corp.

Brookhaven National Laboratory
Department of Energy

Sandia National Laboratories
Managed by Sandia Corporation

Oak Ridge National Laboratory
Oak Ridge, TN 37831-6010

Brookhaven National Laboratory
Upton, NY 11973

Sandia National Laboratories
Albuquerque, NM 87185-0747

C. E. Antonescu, NRC Project Manager

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

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ABSTRACT

This document presents the results of studies sponsored by the Nuclear Regulatory Commission to provide the technical basis for environmental qualification of computer-based safety equipment in nuclear power plants. The studies were conducted by Oak Ridge National Laboratory, Sandia National Laboratories, and Brookhaven National Laboratory.

The studies address the following: (1) adequacy of present test methods for qualification of digital instrumentation and control (I&C) systems; (2) preferred (i.e., Regulatory Guide–endorsed) standards; (3) recommended stressors to be included in the qualification process during type testing; (4) resolution of need for accelerated aging for equipment to be located in a benign environment; and (5) determination of an appropriate approach for addressing the impact of smoke in digital equipment qualification programs.

Significant conclusions from the studies are the following:

(1) **Type testing** should continue to be the preferred test method for safety-related I&C systems.

(2) The state of the art does not warrant any changes to be made with regard to **aging methodologies** for digital systems in nuclear power plants.

(3) A stressor not previously considered for analog safety system qualification is **smoke exposure**. Research documented in this report confirms that smoke is a stressor that can adversely impact digital safety equipment. However, 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. Additional research into the susceptibility of digital components and modules to smoke-induced effects is ongoing and should be continued. Based on existing research, present methodologies with regard to fire and its effects (i.e., smoke, heat, ignition, explosions, and toxic gases), which are addressed via General Design Criteria (GDC) 3, Institute of Electrical and Electronics Engineers (IEEE) 384, and Appendix R of Title 10 of the *Code of Federal Regulations* (10 CFR 50), should continue to be applied for digital I&C safety systems.

(4) The synergistic effect of high temperature in combination with high relative humidity is potentially risk-significant to digital I&C. Therefore, although high relative humidity is not as likely in the controlled environments where digital I&C is typically located (e.g., control rooms), the synergistic effect of these two stressors needs to be considered on a case-by-case basis, especially for postaccident monitoring equipment.

(5) Based on a comparative analysis of IEEE 323-1974 and IEEE 323-1983, we recommend that IEEE 323-1983 be endorsed, with appropriate exceptions as specified in this report.

(6) The dynamic response of a *distributed* system under environmental stress should be considered during type testing. System response time is usually considered during design, but the sequential nature of digital processes (as opposed to the essentially instantaneous nature of analog processes) increases the significance of the potential of environmental stressors to cause intermittent upsets in subsystems, leading to degraded performance in the *total* system. Dynamic performance under environmental

stress is especially important in postaccident monitoring systems, which typically are required to function following a reactor trip or engineered safety feature actuation.

(7) There is a need for electromagnetic compatibility standard(s) for the nuclear power plant environment. The information provided in the following reports can be used as the basis for electromagnetic compatibility of I&C systems in nuclear power plants:

NUREG/CR-6431, *Recommended Electromagnetic Operating Envelopes for Safety-Related I&C Systems in Nuclear Power Plants*

NUREG/CR-5941, *Technical Basis for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems*

NUREG/CR-6436, Survey of Ambient Electromagnetic and Radio-Frequency Interference Levels in Nuclear Power Plants.

(8) The nuclear industry should adopt a new philosophy of qualification, in which the assurance that safety-related equipment will perform properly is "built-in" as well as being "tested-in." In this approach, assurance of an equipment's quality starts at the ***semiconductor component*** level. As a minimum, it might be required as part of the environmental qualification process that the manufacturer of the safety-related I&C equipment document the qualification standards used by the semiconductor manufacturer for stress testing. Integrated circuits are susceptible to long-term failure mechanisms under various environmental stressors so the use of components from high quality manufacturing process, as demonstrated through manufacturer stress testing, can minimize that susceptibility.

CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The authors wish to thank the NRC Program Manager, Christina Antonescu, for her help in planning and implementing this study.

Several people from three national laboratories contributed to the success of the studies documented in this report. In particular, we would like to thank D. Michael Ramirez, Edward Baynes, John Garcia, Robert Nichols, Lizdabel Morales, Andrea Hirst, and Karla Waters, all of Sandia National Laboratories, for their assistance in performing the smoke tests and analyzing data in the SNL study. The technical contributions of Dr. S. Wong, Dr. W. E. Vesely, S. Kasturi, and M. Villaran to the BNL study are also acknowledged. We wish to thank Gary Turner, Jim Mullens, David McMillan, Mike Moore, Brian Swail, Paul Ewing, Boyd Beets, Ed Reed, and Dr. Jose March-Leuba for their contributions during the ORNL study.

Finally, the authors wish to thank Dr. Robert Kryter and Ron Battle for reviewing the manuscript and providing many helpful suggestions for its improvement, as well as Linda Sparks for her help in the final editing of the manuscript.

ACRONYMS

A/D	Analog to digital
AIEG	Automotive Industrial Electronics Group
ALWR	Advanced light-water reactor
ARW	Airborne rotary-winged
BNL	Brookhaven National Laboratory
CDF	Core damage frequency
CDIP	Ceramic dual-in-line package
CFP	Ceramic flat package
CFR	*Code of Federal Regulations*
CMOS	Complementary MOS
D/A	Digital-to-analog
DBE	Design basis event
DIP	Dual-in-line package
DOE	U.S. Department of Energy
DTC	Digital trip computer
EDSC	Experimental digital safety channel
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
EPRI	Electric Power Research Institute
ESF/MUX	Engineered safety feature multiplexing unit
EUT	Equipment under test
FDDI	Fiber-distributed data interchange
FOM	Fiber-optic module
GDC	General Design Criteria
GF	Ground fixed
GM	Ground mobile
HOSTP	Host processor
HVAC	Heating, ventilation, and air conditioning
I&C	Instrumentation and control
IC	Integrated circuit
IEEE	Institute of Electrical and Electronics Engineers
IPC	Interconnecting and packaging electronic circuit
IRRAS	Integrated Risk and Reliability Analysis System
ISO	International Organization for Standardization
JEDEC	Joint Electron Device Engineering Council
LER	Licensee event report
LLCC	Ceramic leadless chip carrier
LOCA	Loss-of-coolant accident
LOOP	Loss of offsite power
MOS	Metal-oxide semiconductor
MSLB	Main steam-line break
MTBF	Mean time between failures
NMOS	N-channel MOS

NPP	Nuclear power plant
NQML	Nuclear Qualified Manufacturers List
NRC	U.S. Nuclear Regulatory Commission
NSSS	Nuclear steam supply system
OEM	Original equipment manufacturer
ORNL	Oak Ridge National Laboratory
PAM	Postaccident monitoring
PCB	Printed circuit board (used interchangeably with PWB)
PDIP	Plastic dual-in-line package
PEM	Plastic encapsulated microcircuit
PLCC	Plastic leaded chip carrier
PMOS	P-channel MOS
PRA	Probabilistic risk assessment
PRS/MUX	Process multiplexing unit
PVC	Polyvinyl chloride
PWB	Printed wire board (used interchangeably with PCB)
PWR	Pressurized-water reactor
QM	Quality management
QML	Qualified manufacturers list
RH	Relative humidity
RFI	Radio-frequency interference
RHA	Radiation hardness assurance
SAR	Safety analysis report
SEU	Single event upset
SNL	Sandia National Laboratories
SOIC	Small outline integrated circuit
SPC	Statistical process control
SSC	Structures, systems, and components
STI	Surveillance test interval
TOC	Transistor outline can
TTL	Transistor-transistor logic
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 definitions is also included.

Aging.[a] The effect of operational, environmental, 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.

Benign.[b] An environment in which a seismic event is the only design basis event that can be expected to have catastrophic effects on all redundant safety equipment and in which the expected normal and abnormal service conditions with regard to other environmental stressors do not exceed the following:

Radiation: total dose less than 4×10^2 rad over 40 years.
Temperature: normal, 60 to 80°F; abnormal and accident, > 80°F (120°F maximum).
Humidity: normal, 30 to 50%; abnormal and accident, < 95%.

Class 1E.[c] 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 events (DBE).[c] 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.)

Design basis accident. The subset of a design basis event, which requires safety function performance.

Design life.[c] The time during which satisfactory performance can be expected for a specific set of service conditions.

End-of-qualified-life condition.[d] The worst state of deterioration permissible in equipment before the occurrence of a design basis event. Equipment qualification is demonstrated if the worst state of deterioration is created *and then* equipment operability is verified during the design basis event.

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.

Platform.[e] Any vehicle, surface, or medium, that carries equipment. For example, land is the platform for a ground radar set, and a person is the platform for a hand-carried radio.

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.[f] Actual period from initial operation to retirement of structures, systems, or components.

***Significant* aging mechanism.**[a] 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 design basis event conditions.

Synergistic effect.[e] Portion of changes in characteristics of structures, systems, or components produced solely by the interaction of stressors acting simultaneously, as distinguished from changes produced by superposition from each stressor acting independently.

[a] IEEE Standard 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
[b] As defined by this document.
[c] IEEE Standard 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.
[d] Hall, Robert A., and James F. Gleason, "Environmental Qualification of Nuclear Power Plant Control Equipment," *Instrumentation in the Power Industry*, Vol. 23, Instrument Society of America, January 1978.
[e] MIL-STD-810E, "Environmental Test Methods and Engineering Guidelines, July 1989.
[f] *Nuclear Power Plant Common Aging Terminology*, EPRI TR-100844, Electric Power Research Institute, November 1992.

1 INTRODUCTION

Because of the increasing unavailability of analog replacements for instrumentation and control (I&C) systems and the potential benefits of microprocessor-based systems, considerable use of computers and digital technology in safety-related systems of nuclear power plants is likely. In fact, fully digital safety and control systems are envisioned[1] for advanced light-water reactors (ALWRs) such as the Westinghouse AP-600 or GE Advanced Boiling Water Reactor.

Although digital technology has several advantages over comparable analog equipment and, in fact, has been in widespread use in nonnuclear industries for several years, a concern over its use in safety-related systems in nuclear power plants is the limited experience with microprocessor-based equipment in these environments. For example, issues that need to be resolved are adequacy of present qualification standards and guides to address unique performance characteristics and potential vulnerabilities for microprocessor-based systems, preferred test methods for qualification of digital I&C systems, recommended environmental stressors to be included in the qualification process during type testing, and determination of an appropriate approach to assess smoke as a stressor in a qualification program.

Accordingly, the U.S. Nuclear Regulatory Commission (NRC) initiated confirmatory research to address the environmental compatibility issues posed by the introduction of digital technologies (specifically, microprocessor-based equipment) into safety-related I&C systems in nuclear power plants. This document reviews the technical basis provided by the findings of confirmatory research performed by three U.S. Department of Energy (DOE) research laboratories—Brookhaven National Laboratory (BNL), Oak Ridge National Laboratory (ORNL), and Sandia National Laboratories (SNL)—and provides recommendations for the enhancement of guidance on environmental qualification of safety-related, microprocessor-based I&C equipment in nuclear power plants.

1.1 Background

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 (SSCs) 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. These general requirements are contained in the following sections of 10 CFR 50:

> Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criteria (GDC) 1, 2, 4, 13 and 23.
>
> Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," Criterion III, *Design Control*, Criterion XI, *Test Control*, and Criterion XVII, *Quality Assurance Records*.

Section 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," contains specific requirements pertaining to qualification of certain electric equipment important to safety. It requires that three categories of electric equipment important to safety be qualified for their application in the nuclear power plant environment, namely, (1) safety-related electric equipment (Class 1E), (2) nonsafety-related electric equipment (non-Class 1E) the failure of which under postulated environmental conditions could prevent satisfactory accomplishment of safety functions by safety-related equipment, and (3) certain postaccident monitoring (PAM) equipment.

Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants,"[2] identifies the qualification standard IEEE 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,"[3] as providing an acceptable method for complying with the requirements of 10 CFR 50.49. The qualification approach established in IEEE 323-1974 is well suited to analog/electromechanical equipment that has traditionally been used in the nuclear power plant environment. However, issues of obsolescence and lack of infrastructural support in analog spare parts, coupled with the potential benefits of digital systems, are driving the nuclear industry to retrofit analog I&C systems with advanced digital systems. Research[4] and military experience[5] have identified functional and environmental qualification issues related to microprocessor-based I&C equipment that can be addressed through enhanced guidance on the systems aspects of environmental compatibility for digital I&C technology.

Recognition that the use of computers in safety systems poses challenges different from that of analog systems prompted the development of IEEE 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."[6] The standard recognizes that reliability and environmental compatibility issues need to be addressed in the application of computers in safety systems. In particular, it recommends that an analysis be performed to ensure that the system has a high "correct response probability" and that the probability of common-cause failure is reduced to an acceptable level.[6] Addressing environmental qualification requirements for microprocessor-based safety-related I&C systems is one method of ensuring that the probability of common-cause failure caused by environmental hazards is reduced to an acceptable level. The overall approach is illustrated in Figure 1.1.

Section 50.49 of the *Code of Federal Regulations* does not address requirements for seismic and dynamic qualification, protection of electric equipment against other natural phenomena and external events, and equipment located in a mild environment. Thus, although GDC 4 requires that SSCs be "designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents," the environmental qualification requirements of 10 CFR 50.49 do not address the environmental hazards in nuclear power plant locations where microprocessor-based safety-related I&C systems either are or are likely to be located in nuclear power plants (i.e., "mild" environments). Although IEEE 7-4.3.2-1993 presents high-level guidance on the need for environmental compatibility for computers in safety systems and IEEE 323-1974 provides guidance on qualification methods that can be applied to evaluate the environmental susceptibility of Class 1E equipment in harsh (e.g., containment) environments, enhanced guidance that specifically addresses the qualification of microprocessor-based I&C systems can help provide greater assurance of the environmental compatibility of the safety-related systems and components in nuclear power plants.

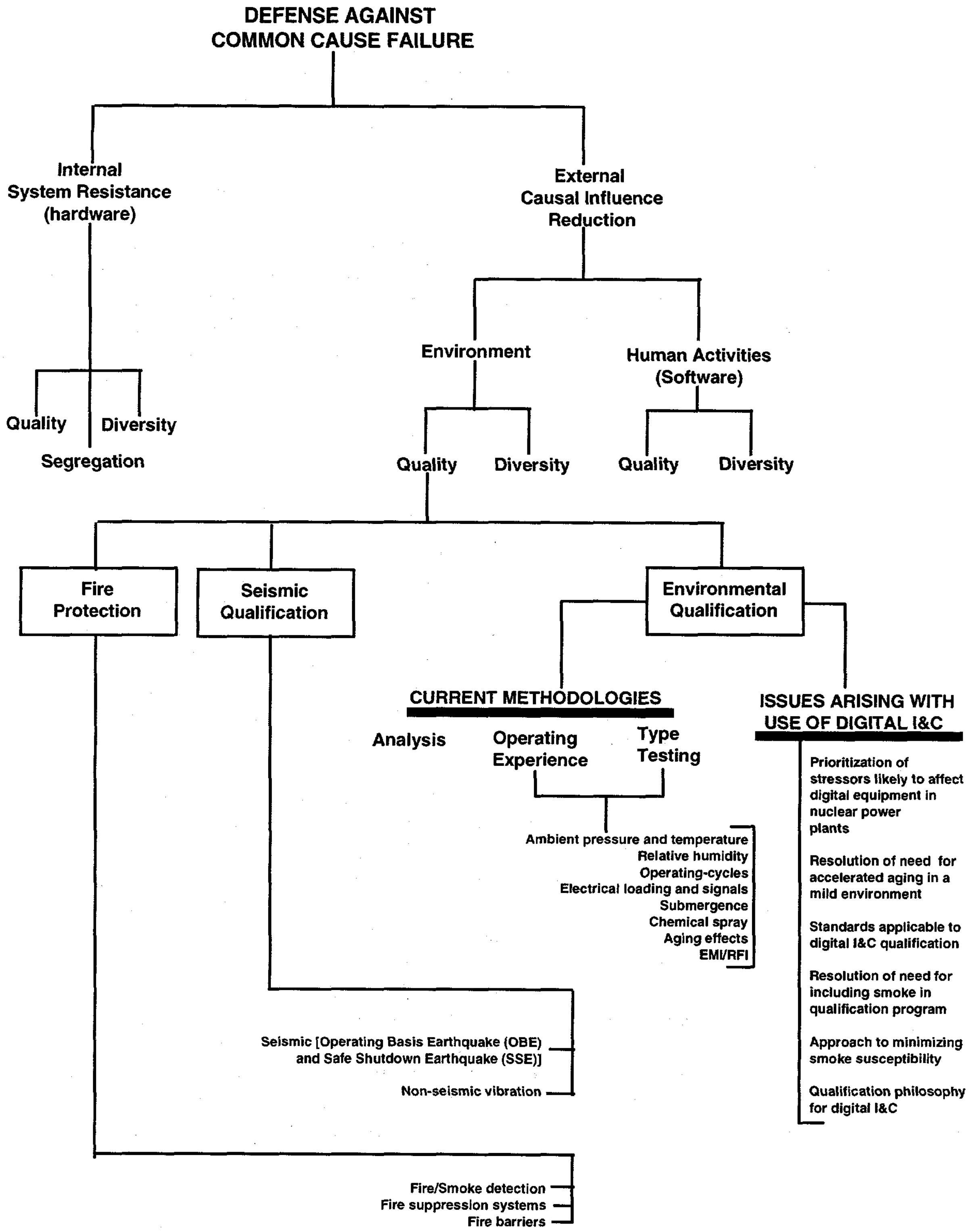


Figure 1.1 Role of environmental qualification in defense against common-cause failures (drawn from references 4 and 7)

1.2 Objective and Scope

The objective of this document is to provide recommendations for guidance on environmental qualification of microprocessor-based equipment important to safety in nuclear power plants. Findings from studies performed by BNL, ORNL, and SNL have been used in developing the technical basis for these recommendations.

To provide the technical basis, the following research was performed:

a. Review of the technical literature to identify the significant long-term failure mechanisms associated with microelectronic circuits and the component qualification methodologies used by manufacturers in an attempt to reduce failure rates in the field.

b. Review of present-day nuclear power plant environmental qualification standards, with a view to identifying new issues relevant to the application of computers in safety systems, as well as standards that should be endorsed to enhance the qualification of digital I&C systems.

c. Review of the U. S. military's overall approach to qualification, with a view to identifying new qualification methodologies that may be relevant to the nuclear environment.

d. A study of the relative risk significance of environmental stressors on digital equipment in the nuclear power plant environment to identify stressors that should be included in a nuclear plant qualification program.

e. A study of environmental-stress-related vulnerabilities and system-level failure modes that can be anticipated with digital safety systems to identify/suggest modifications to present-day qualification testing that will help maintain adequate safety margins.

f. A study of the effect of smoke exposure on integrated circuits (ICs), with a view to identifying qualification implementation issues relevant to smoke susceptibility.

1.3 Research Approaches by National Laboratories

The confirmatory research presented in this document was conducted to investigate and resolve the environmental qualification issues associated with the introduction of digital technology into nuclear power plants. The overall approach employed in this research program involves assessing the significance of various environmental stressors that are or could be addressed in the qualification process, determining any unique vulnerabilities of digital I&C technologies to the effects of environmental stress, and evaluating whether enhanced guidance is needed for the environmental qualification of digital I&C systems for safety-related applications. In conducting this research program, the NRC made use of the expertise available at DOE research laboratories by sponsoring complementary projects at BNL, ORNL, and SNL. A brief discussion of the research responsibilities at each laboratory follows.

BNL

The BNL study investigated the relative risk effects of environmental stressors by quantifying the plant's risk-sensitivities to them. The risk-sensitivities are changes in plant risk caused by application of the stressors and are quantified by estimating their effects on I&C failure occurrences and the consequent increase in risk in terms of core damage frequency (CDF). Available military data and nuclear power plant (NPP) operating experience on the effects of environmental stressors on the reliability of digital I&C

equipment were used during the study. The methods developed were used to determine and compare risk-sensitivities to temperature, humidity, vibration, electromagnetic interference from lightning, and smoke as stressors in an example plant using a probabilistic risk assessment (PRA).

ORNL

The ORNL study involved an overall assessment of the current qualification process, an investigation of vulnerabilities of digital technologies to environmental hazards, identification of functional and environmental qualification issues for microprocessor-based systems, and development of recommendations for environmental qualification guidance. A significant element of that effort was an experimental study of the characteristic environmental stressor effects on an experimental digital safety channel that includes components representative of advanced safety systems or some retrofits. The tests investigated the stress levels at which temporary failures (upsets) began, the nature of the upsets, and the severity of consequences of the upsets. Stressors employed were electromagnetic interference/radio-frequency interference (EMI/RFI), temperature, humidity, and smoke. The system designed for the purpose consisted of advanced digital components, including fiber-optic network interface systems, serial communication links (optical fiber and copper transmission), analog-to-digital (A/D) converters, multiplexers, and computers.

SNL

The SNL study investigated the consequences of smoke exposure for digital technology. SNL performed smoke exposure tests on digital components and circuit boards, with a focus on short-term effects such as circuit bridging in typical components and the factors that can influence how much the smoke will affect them. These factors include the component technology and packaging, physical board protection, and environmental conditions such as the amount of smoke, temperature of burn, and humidity level. The likelihood of circuit bridging was tested by measuring leakage currents and converting those currents to resistance in ohms. The SNL study also included background studies on the smoke scenarios that can be expected in nuclear power plants as well as smoke damage to electrical equipment.

The findings from the studies conducted at the three DOE laboratories contribute to the development of the technical basis for environmental qualification of digital I&C systems by meeting the research goals described previously. Specifically, the BNL study addressed item (d) as outlined in section 1.2; while the ORNL and SNL studies addressed items (e) and (f), respectively. In addition, ORNL also performed tasks (a), (b), and (c). This document integrates the research findings from each project to support recommendations on environmental qualification guidance for microprocessor-based safety-related I&C systems.

2 FAILURE MECHANISMS AND STRESS TESTING METHODOLOGIES FOR INTEGRATED CIRCUIT COMPONENTS

2.1 Introduction

Equipment qualification is "a verification of design limited to demonstrating that the electric equipment is capable of performing its safety function under significant environmental stresses resulting from design basis accidents in order to avoid common-cause failures."[2] Paragraph 50.49(e)(5) of 10 CFR calls for equipment qualified by test to be preconditioned by natural or artificial (accelerated) aging to its end-of-installed-life condition and further specifies that consideration must be given to all significant types of degradation that can have an effect on the functional capability of the equipment. Humidity, corrosion, voltage transients caused by EMI/RFI, and accumulation of soot deposits, are examples of such effects.

This chapter summarizes the most significant failure mechanisms in ICs, and identifies methodologies used by component manufacturers during reliability stress tests in an attempt to reduce failure rates. The objective is to develop a qualitative assessment of the qualification needs for microprocessor-based equipment in nuclear power plants.

2.2 Basic IC Types

ICs can be classified into two groups based on the type of transistors that they employ. One type is the bipolar IC, in which the principal element is the bipolar junction transistor. The other type is the metal oxide semiconductor (MOS) IC, in which the principal element is the MOS transistor. The MOS type is more suitable for very large-scale integrated circuit (VLSI) design than bipolar circuits because MOS transistors are self-isolating and smaller (average size is less than 10^{-5} mm^2).

Various MOS device fabrication technologies are currently in use:[8]

(1) Metal-gate or silicon-gate p-channel MOS (PMOS). Metal-gate PMOS devices use aluminum for electrodes and interconnections. Silicon-gate PMOS devices employ polycrystaline silicon for gate electrodes.

(2) N-channel MOS (NMOS). These are typically silicon-gate devices.

(3) Complementary MOS (CMOS). These devices employ both PMOS and NMOS transistors to form the logic elements of the IC.

IC fabrication begins with a thin, polished slice of high-purity, single-crystal silicon and employs a combination of chemical and physical processes to build successive layers of insulating, conducting, and semiconducting material. Precision lithographic processes are used throughout the fabrication sequence to define the geometric features required. The resulting die is packaged using ceramic or plastic molding technology.[8,9] Figure 2.1 shows a silicon die (chip) and bond wires that connect the chip to the leadframes. For plastic packaged ICs as shown in the figure, the technology uses thermosetting epoxy resins molded around the leadframe-chip subassembly after the chip is wire-bonded to the leadframe. The external leads are solder-plated or solder-dipped after package molding.

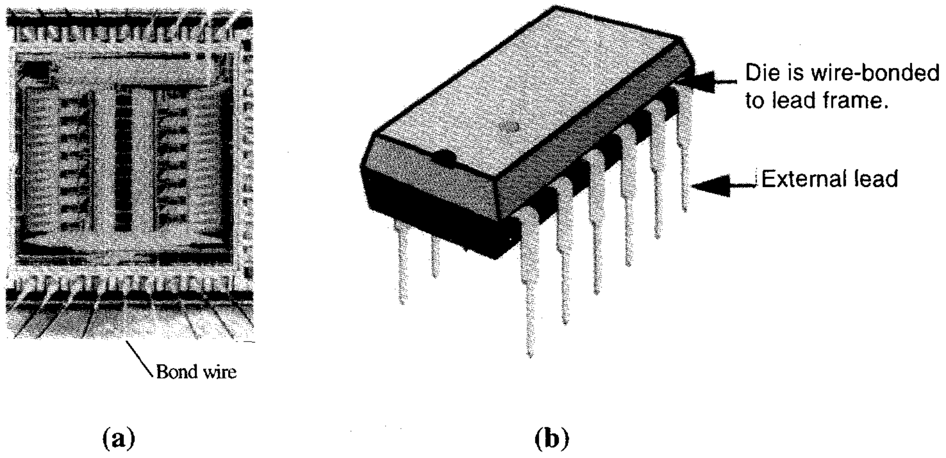


Figure 2.1 Major components of an integrated circuit (a) Die and bond wires connecting die to external leads (b) Plastic-molded dual-in-line package

A number of factors influence the reliability of ICs, and to reduce failure rates, the failure mechanisms of the fabricated devices must be understood. Extensive work has been done in this area and the failure modes and mechanisms of ICs are well documented in the literature.[10-19] Some of the most significant of these failure mechanisms are discussed subsequently.

2.3 Electromigration

Electromigration is the transport of mass under the influence of an electric current. Under normal conditions, the effect of this phenomenon is negligible because the current density required to produce a significant effect is very high. (For example, current densities would need to be greater than 10^5 A/cm^2.[20] To put this number in perspective, this current is equivalent to an ordinary household electric wire carrying a current above 4000 Amps.) However, at the level of complexity of current VLSI circuits, metal interconnects and/or inter-level contacts are commonly designed to carry a current density exceeding this value. This makes the problem of electromigration of considerable significance in VLSI technology. In devices using aluminum metallization, discontinuities in the conductor caused by electromigration is the most important mode of failure.[21] The addition of copper to aluminum or Al-Si alloys considerably increases the device's resistance to electromigration.[20]

Since current density as well as temperature becomes a significant accelerating factor, accelerated life tests performed to study electromigration-related failures are typically done under accelerated current density and temperature conditions [at temperatures greater than 150°C (302°F) and current density greater than 10^6 A/cm^2]. The electrical resistance of the device is continually monitored during application of the stress. The device lifetime is determined when the interconnect lines and/or interlevel contacts become open or their resistances change more than a pre-specified percentage.[22]

2.4 Dielectric Breakdown

Dielectric breakdown is one of the primary failure mechanisms for MOS ICs.[21] High-quality, relatively defect-free dielectrics under typical bias conditions of 2 to 3 MV/cm have lifetimes that far exceed the expected circuit lifetime. However, when defects and/or other anomalous conditions are present in the dielectric or electrodes, component lifetime is reduced, resulting in premature failure. Assessment of dielectric quality therefore becomes primarily a matter of assessing the extent and severity of defects.

Common test methods to predict failure rates at nominal operating conditions employ elevated temperature stressing of semiconductor packages at or near the maximum operating voltage for periods of several weeks.[21]

2.5 Corrosion of Metallization Interconnects

ICs are encapsulated by a process that sandwiches the die and its leadframe between two layers of mold compound. Conductive films (metallization) are required to provide interconnection between the several thousands of semiconductor devices on the wafer and between devices and the outside world. A potential route for moisture and contaminant ingression to the die surface is along the interface between these layers of mold compound.[23,24] Some plastics, like the currently used epoxies (e.g., Novolac) are thought to be in compression around the metal leads, thus forming good seals.[25] Others (e.g., phenolics) do not form equivalent seals and create microgaps along the metal to plastic interface that provide substantial moisture paths for devices with large numbers of leads. Another route for moisture ingression is through the bulk of the plastic (polymer). A third (although remote) possibility is for moisture to be adsorbed by the glassivation because of improper manufacturing procedures and thus become encapsulated in the package.[25]

The basic ingredients needed for corrosion are moisture and ions for the formation of an electrolyte, metal for electrodes, and an electric field. Corrosion will not occur if any of these components is missing. The metallization interconnect of the die forms the metal electrodes needed for corrosion to occur. Corrosion in a plastic IC may deteriorate the leads outside the package, or the metallization interconnect of the die inside the package.

Because of improvements in passivation technology, interconnect corrosion has largely been eliminated as a reliability problem. However, bonding pad corrosion remains an issue.[24] Pressure/temperature/humidity bias stress tests are typically employed by semiconductor manufacturers to study the contribution of environmental conditions on corrosion.

2.6 Other Factors Affecting IC Failures

Table 2.1 summarizes the time-dependent failure mechanisms that are commonly identified as degrading IC reliability. This does not include infant mortality type failures, which are typically caused by manufacturing defects such as photoresist or etching defects resulting in near-opens or shorts, contamination on the chip or in the package, weak chip or wire bonds, and partially cracked chips or packages.[9] Typically in mature products, much of the infant mortality type failures will have been eliminated (once identified by burn-in tests), either through modifications in the manufacturing processes or in the design.

Table 2.1 Time-failure mechanisms in silicon semiconductor devices (adapted from reference 9)

Device association	Failure mechanism	Relevant factors	Accelerating factors	E_a= apparent activation energy for temperature (eV)
Silicon oxide and silicon-silicon oxide interface	Surface charge accumulation	Mobile ions, voltage, temperature	Temperature	1.0 to 1.05 (depends upon ion density)
	Dielectric breakdown	Electric field, temperature	Electric field, temperature	0.2 to 1.0
	Charge injection	Electric field, temperature	Electric field, temperature	1.3
Metallization	Electromigration	Temperature, current density, area, gradients of temperature and current density, grain size	Temperature, current density	0.5 to 1.2
	Corrosion (chemical, galvanic, electrolytic)	Contamination, humidity, voltage, temperature	Humidity, voltage, temperature	~ 0.3 to 1.1 (for electrolysis)
	Contact degradation	Temperature, metals, impurities	Varied	
Bonds and other mechanical interfaces	Intermetallic growth	Temperature, impurities, bond strength	Temperature	Al-Au: 1.0 to 1.05
	Fatigue	Bond strength, temperature cycling	Temperature extremes in cycling	
Hermeticity	Seal leaks	Pressure differential, atmosphere	Pressure	

Two other failure mechanisms that are not eliminated by burn-in, but that are not listed in Table 2.1 are electrostatic discharge and alpha-particle-induced soft errors. ("Soft error" refers to a random failure not related to a physically defective device.)

Electrostatic discharge damage is caused by excessive voltage applied to the gate oxide of an IC. In a VLSI circuit, the gate oxide is typically less than 2.5 μm thick. The dielectric breakdown strength of SiO_2 is approximately 8×10^6 V/cm. Thus, the gate oxide will not sustain voltages of more than 20 V. However, much higher voltages (>1500 V) can be generated simply by a person walking across a room, or even by removing an IC from its packaging material. (Voltages generated in this manner are caused by triboelectricity, that is, electricity produced by rubbing two materials together.)

Alpha-particle-induced soft errors are caused by radioactive naturally occurring impurities (e.g., uranium or thorium) in IC packaging materials.[9,26] When an alpha particle penetrates into the silicon, electron-holes pairs are generated along the path of the alpha particle. Depending on the incident energy of the alpha particle, the resulting charge may be large enough to cause loss of information if the IC is a logic element. For example, a 4-MeV alpha particle can generate 10^6 electron-hole pairs, resulting in a charge greater than that stored in a dynamic memory cell.[27]

2.7 Overview of Accelerated Testing for IC Components

The objective of aging in a qualification program in the nuclear power plant environment is to "put the equipment in a state corresponding to the condition of its greatest vulnerability to an accident during the period it is expected to perform a safety-related function."[28] That is, the equipment must be shown to remain functional following an accident, assuming the accident occurred at the end of the equipment's qualified life. Before testing the equipment under accident conditions, *accelerated aging* is typically used to put the equipment into a state exhibiting the same properties, relative to its safety function, as it would if it had been operating under normal service conditions for a relatively long time.

Although similar to accelerated aging, semiconductor manufacturers use *accelerated testing* at the IC component level for a slightly different purpose. Here, the objective is to identify the dominant failure modes in the IC so that improvements can be made, either in the design or manufacturing processes, to improve reliability.

Five types of stresses are typically used to accelerate IC failure mechanisms: temperature, voltage, current, humidity, and temperature cycling.

Temperature acceleration is based on the fact that many of the mechanisms that cause failure are chemical or physical processes that can be accelerated by temperature. Let us assume that some parameter of the IC changes with time, and that the IC fails when this parameter exceeds some arbitrary value. We further assume that when the temperature of the device is T_1 the parameter increases such that failure occurs at time t_1, and when the temperature is T_2 the parameter increases at a different rate such that failure occurs at time t_2. In general, $T_2 > T_1$ and $t_2 < t_1$. Assuming that the parameter causing the reaction to change is governed by the Arrhenius equation, the relationship among t_1, t_2, T_1, and T_2 is given by[9]

$$\frac{t_1}{t_2} = e^{(\frac{\phi}{\kappa})(\frac{1}{T_1} - \frac{1}{T_2})} \qquad \textbf{(2.1)}$$

where

ϕ = activation energy (eV/molecule),
κ = Boltzmann's constant (8.617×10^{-5} eV/K-molecule), and
the ratio t_1/t_2 is the acceleration factor.

The equation assumes that failure is caused by the single parameter (chemical reaction) and that this single parameter occurs under both actual and accelerated conditions. In general, activation energy varies with the chemical concentrations and the failure mechanism. Table 2.1 lists activation energies associated with some of the more significant failure mechanisms.

The Eyring type of model can be used to account for environmental stresses other than temperature. For example, if corrosion is under consideration and the median life (t_{50}) is considered as a measure of the corrosion rate, then the process may be described by an Erying type relationship of the form[23]

$$t_{50}=Ae^{\frac{\phi}{KT}}F_{RH}F_{\upsilon}\cdots \tag{2.2}$$

where

A = constant,
ϕ = activation energy ,
T = temperature in °K,
F_{RH} = humidity stress factor, and
F_{υ} = voltage stress factor.

For failure accelerated by voltage (dielectric breakdown) and current (electromigration), a generalized Erying model may be used.[9] In particular, if R is the reaction rate of the failure mechanism and S is the applied stress, then

$$R=C\sinh[\frac{a(T)S}{\kappa T}]e(\frac{-Q}{\kappa T}) \tag{2.3}$$

where

C is a constant,
$a(T) = \kappa T\gamma(T)$, and the parameter $\gamma(T)$ varies between 1 to 4.5, and
$Q = \phi_o + a(T)S_B$ (S_B is the breakdown stress, the value of applied stress where failure of the device occurs essentially instantaneously).

2.8 Comparison of Packaging Technologies

The main package fabrication technologies are based on refractory ceramic technology or molded plastics. These fabrication methods are covered in detail in several books[9] and articles.[29] Basically, a plastic-encapsulated microcircuit consists of an IC chip physically attached to a leadframe, electrically interconnected to input/output leads, and molded in plastic that directly contacts the chip, leadframe, and interconnects. Hermetically sealed microcircuits (generally called hermetic packages), on the other hand, consist of an IC chip mounted in a metal or ceramic cavity, interconnected to leads and hermetically sealed.

Historically, state-of-the-art ICs have been packaged in hermetic packages, allowing evaluation and initial reliability studies to be carried out under optimum conditions. As the devices mature, the advantage of lower costs results in the use of plastic packages. Over the years, advances in the quality of molding compounds combined with better passivation technology and better in-process control have dramatically improved the reliability of plastic packages. For example, Figure 2.2 shows the observed comparative failure rate data for plastic-encapsulated microcircuits (PEMs) and hermetically packaged devices from 1978 to 1988.[29,30] The failure rates are for the same part (or part function) over time. It can be seen that both packaged devices improved by a factor of 10 in early life failure rate during this period. More recent data show that for PEMs, the early 1990s failure rate was 0.3 to 3.0 failures per 10^6 device hours, with less variability between encapsulant materials and vendors. This very closely correlates with figures for hermetic parts.[29,31]

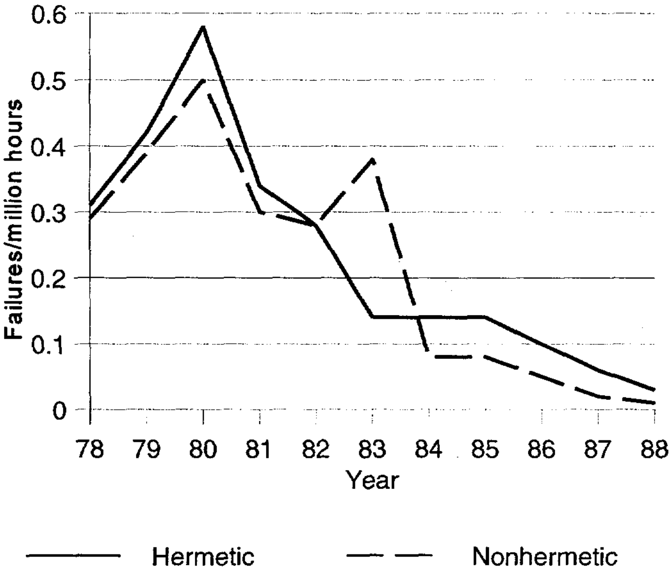


Figure 2.2 Integrated circuit failure rate as a function of year (adapted from reference 29)

Condra *et. al.*[32] compared the functional reliability of mature custom bipolar ICs in plastic and hermetic ceramic dual-in-line packages (DIPs) on 12-circuit card assemblies. The parts were subjected to 1000 temperature cycles from −55°C to +85°C. No differences were observed in any of the 26 measured parametric values. These parts were then added to untested groups of 50 of the same devices in another set of circuit-card assemblies, with an older discrete version of the card as a control. The new assemblies were subjected to 1000 hours of 85°C/85%RH, with 28 Vdc of intermittent bias (30 min off, 30 min on). Among previously untested parts, neither plastic nor ceramic failures occurred. However, previously thermally-cycled parts (both plastic and ceramic) could only be tested up to 650 hours before failures occurred elsewhere on the cards. Conservative time-to-first failure estimates for both plastic and ceramic types in avionic applications were well over 13 years, even under combined testing.

Autoclave storage tests run at 15 psig, 121°C, for 24 hours and temperature humidity-bias tests run at 85°C/85%RH for 1000 hours under bias have shown that PEMs are acceptable for many harsh environments.[33] Such harsh environments include automobiles, where some stress levels (e.g., temperature) exceed that found in several locations in nuclear power plants. Component qualification testing for the automotive industry represents some of the most stringent tests used by semiconductor manufacturers. For example, qualification tests used by Motorola's Automotive Industrial Electronics Group (AIEG) include temperature cycling for 1000 cycles, thermal shock for 500 cycles, 55°C/85%RH testing for 1000 hours, life testing for 1000 hours, high-temperature reverse bias for 1000 hours, intermittent operational life testing for 20,000 cycles, and autoclave (live steam) testing for 96 hours. The number of rejects for all these tests is zero.[29] During tests performed by AIEG on non-Motorola components that have been qualified to AIEG internal qualification procedures, most vendors were found to easily pass these tests, indicating an industry-wide capability to meet or exceed the harsh automotive standards.[34]

2.9 Concluding Remarks

ICs are susceptible to long-term failure mechanisms under various environmental stressors. Examples of these failure mechanisms are electromigration and corrosion of metal interconnects. However, environmental testing and stress screening methodologies exist to enable the severity of these potential failures in a particular technology to be identified during manufacture.

It is proposed that the nuclear industry put mechanisms in place to ensure that digital equipment for the nuclear environment use components from semiconductor manufacturers that employ adequate testing methodologies to reduce potential failures. Several semiconductor manufacturers, in fact, already have quality assurance procedures in place and are likely to meet the demands of a harsh environment such as a nuclear power plant, as is exemplified by the capability to meet or exceed harsh automotive standards. This proposal is therefore not likely to put further strain on the nuclear industry, and at the same time it will ensure that the highest quality is maintained for safety equipment. An overall methodology for qualification of digital I&C equipment of nuclear power plants is suggested the Appendix.

3 REVIEW AND INTERCOMPARISON OF CURRENT ENVIRONMENTAL QUALIFICATION STANDARDS

3.1 Comparison of IEEE 323-1974 and IEEE 323-1983

The basis for the qualification of equipment important to safety comes from the *Code of Federal Regulations*. According to 10 CFR 50.49, equipment important to safety includes (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 the failure of which 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[2] describes methods acceptable to the NRC staff for complying with 10 CFR 50.49. IEEE Standard 323 establishes the basic requirements and methods for qualification. Regulatory Guide 1.89 endorses IEEE 323-1974[3] but does not endorse IEEE 323-1983.[35] (This 1983 revision of IEEE 323 was reaffirmed in 1990 and 1996.) In this section we compare and contrast IEEE 323-1974 and IEEE 323-1983 to provide the rationale for our subsequent recommendations.

3.1.1 Qualification Methods

Section 5 of both versions of IEEE 323 stipulate **type testing**, **operating experience**, and **analysis** as the primary means of qualification. In addition, both versions allow a 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). IEEE 323-1974 explicitly delineates type testing using simulated service conditions as the preferred qualification method. The 1983 version contains no such explicit indication.

Comments:
The methods of qualification—type testing, operating experience, and analysis—are identical in both versions. 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 evolutions compared with its analog counterparts. Because the non-nuclear industry is generally less regulated, it tends to upgrade its digital I&C equipment more often. Thus it may be difficult to obtain sufficient documentation based on operating experience under identical environmental conditions for particular I&C equipment for qualification purposes.

(2) A comprehensive database does not exist that has sufficient detail to allow digital I&C system failures to be accurately related with causative mechanisms 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 should therefore be limited to non-microprocessor-based equipment.

3.1.2 Ongoing Qualification

IEEE 323-1974

IEEE 323-1974 (Section 5.5) acknowledges 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. For such situations the 1974 version permits an on going qualification program to be implemented using any of the following methods:

(1) Aging and testing of identical equipment or components during the qualified period of the installed equipment.

(2) Installation of additional equipment beside the required equipment. This additional equipment is then removed before the end of the qualified life period and is then type tested to determine its additional qualified life.

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 that 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 that 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.

In addition to the preceding, the 1983 standard permits qualified life to be extended if it can be demonstrated with suitable documentation and auditable records that:

(a) evaluation in the original qualified program was conservative with respect to the equipment's specified service conditions and performance specifications;

(b) an age-conditioning procedure, which limited the qualified life of equipment, is in fact conservative; and

(c) 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.

Comments:
Although the 1974 version states that methods other than the two explicitly stated could be used, with proper justification, it is our opinion that procedures and conditions for on-going qualification are more succinctly stipulated in the 1983 version. These procedures do not appear to require modification for application to microprocessor-based and advanced digital systems.

3.1.3 Aging

IEEE 323-1974
Aging is addressed in IEEE 323-1974 under Section 6.3, "Type Test Procedures." According to Section 6.3.3, "the objective of aging is to put samples in a condition equivalent to the end-of-life condition." The standard permits data from previous aging of various devices to be used provided these data are applicable and justifiable in regard to the service conditions that are required by the performance specifications of the device to be tested.

In the Supplement to the Foreword (published in 1975), the standard provides this clarification:

> "It was not the intent that aging must be applied to all Class 1E equipment, but rather that aging must be considered in the same manner as environmental parameters. The need for aging for particular equipment should be determined based on an evaluation of the specific design and application If aging is needed, a further determination must be made as to whether accelerated aging techniques can be applied to the equipment and yield valid results, that may be correlated to real time, on-going qualification."

The standard also allows, in section 6.3.2(4), the exclusion of radiation during aging "if the required radiation level (necessary to simulate the equipment's expected end-of-qualified-life condition) can be shown to produce less effect than that which would cause loss of the equipment's Class 1E function."

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, and

(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 before 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."

Comments:
While the reasons and concepts for aging are essentially the same in both versions, two issues need to be resolved with the anticipated increased use of microprocessor-based technologies in safety systems:

(1) Are present aging methodologies adequate for microprocessor-based systems?
(2) How do we apply the concept of "significant aging mechanisms" as delineated in IEEE-323-1983?

Adequacy of Aging Methodologies for Microprocessor-Based Systems

Wel- established models relating aging to stress are the Arrhenius, Eyring, and Inverse Power formulations.[28] The Arrhenius model is an accepted methodology for simulating accelerated aging (time-temperature effects)[9,28] and is endorsed by Regulatory Guide 1.89. The Arrhenius equation is the most frequently used equation for equipment qualification. However, the equation assumes that degradation is caused by a single chemical reaction and that this single chemical reaction occurs under both actual and accelerated conditions. In general activation energy varies with the chemical concentrations and the degradation mechanism. For example, as discussed in Section 2 of this report, several types of degradation mechanisms are associated with ICs. These include electromigration (~0.5 eV), aluminum-silicon contact degradation (0.8 eV), surface degradation (1.0 eV), and aluminum-gold bond degradation (1.0 eV).[9] Recent studies give a more accurate methodology to estimate activation energy values.[36] In addition, a typical subsystem or assembly consists of several parts that have different characteristics and that age at different rates. Reference 28 provides methods for aging assemblies.

Although actual studies comparing Arrhenius predictions to naturally aged materials in the nuclear environment are limited,[37-39] industry opinion appears to be that present aging methodologies used in qualification testing (for cables) are conservative. However, it could be argued that this may not necessarily be the case for advanced digital technologies (e.g., VLSI circuits). Although many of the mechanisms that cause failure are chemical or physical processes that can be accelerated by temperature, other parameters such as voltage and current may be more effective accelerating stressors for other failure mechanisms observed in ICs. For example, device operation at increased current levels is used primarily as a method of accelerating failures caused by electromigration in the metallic conductors.[20] Studies have shown that for failure accelerated by voltage (dielectric breakdown) and current (electromigration), the activation energy depends on the applied stress.[9] In such cases the Eyring model[9,28] may be more appropriate. The Arrhenius model assumes that the energy required for the reaction involved in the failure mechanism to take place is supplied by the thermal energy of the reactants. On the other hand, the Eyring model assumes that the energy required for the reaction to take place is affected by the applied stress—generally current and voltage in the case of VLSI circuits. Semiconductor manufacturers typically employ temperature stressing of IC components under bias (i.e., with voltage/current applied) during qualification testing.

Aging procedures and models for synergism caused by different stresses (e.g., radiation and vibration) are less well understood. However, digital retrofits and those proposed for ALWRs are likely to be in "mild" environments, where the synergistic effects from other stresses may be negligible.

Altogether, it is our opinion that the state of the art does not warrant any changes to be made with regard to aging methodologies for digital **equipment** in nuclear power plants, especially since **IC component** stress testing addresses many of the issues that could be raised in favor of using other testing methodologies.

Concept of "Significant Aging Mechanisms"

IEEE 323-1983 appears to have introduced the concept of "Significant Aging Mechanisms" so that the user of the standard can determine whether aging should be considered during type testing. Paragraph 3 of Section 6.2.1, "Aging Considerations," defines 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." The problem with this definition is in how "progressively" and "appreciably" may be quantified. It is important to note however that the 1974 version does allow, in Section 6.3.2(4), the exclusion of radiation during aging "if the required radiation level (necessary to simulate the equipment's expected end-of-qualified-life condition) can be shown to produce less effect than that which would cause loss of the equipment's Class 1E function." Thus, as in the 1983 version, the 1974 version allows an environmental stressor to be excluded in the aging program if its effect is "not significant."

It is our opinion that the fuzziness associated with definitions that include words like "appreciable" and "significant" may be eliminated if we can find a crisper definition for a "mild" environment, and then show that equipment proposed for use *is* in such an environment and therefore does not require aging.
IEEE 323-1983 defines a mild environment as "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." By this definition, the control room is ostensibly a mild environment because it is not subject to high radiation or other adverse environmental effects such as steam-line breaks inside or outside containment. In such an environment, the only DBE "of consequence" is a seismic event.

A study by Gleason and Hall[40] appears to support the conclusion that aging is not significant in a mild environment. The study analyzed a group of safety-related components for age sensitivity to the aging mechanisms of time-temperature effects, operational cycling and radiation degradation. One group of electrical and electronic components were aged and compared with a similar group that had not been aged by subjecting both groups to seismic testing after the aging. Components tested included resistors, diodes, ICs, transistors, capacitors, terminal blocks, optical couplers, and printed circuit boards (PCBs). During the thermal aging, the PCBs containing the ICs and optical couplers were energized. The ICs and optical couplers were operated throughout the thermal aging., as well as the resistors and transistors used in the circuitry. Since the items were varied, the equivalent lives were also varied and ranged from 10 to 225 years.

The conclusion from the study was that aging has no effect on seismic performance and that aging before seismic testing does not have to be performed for resistors (carbon-composition, wire wound and metal film), diodes, ICs, transistors, optical couplers, capacitors (tantalum and ceramic), terminal blocks, PCBs, IC sockets, transistor sockets, and soldered connections. The study also implies that aging is insignificant for the service environments for which the components were tested.

I&C systems of ALWRs and some retrofits are likely to include technologies (e.g., surface-mounted devices) that were not included in the Gleason study. Thus, no firm conclusions can be drawn with regard to such devices based on this study. However, the review of failure mechanisms in VLSI circuits presented in Section 2 showed that elevated temperature/temperature cycling, voltage, current density, and humidity can all accelerate failures in semiconductor devices. Manufacturers typically employ such stresses to induce any potential failures so that corrective action can be taken before components get to the market place. For example, a common test method to predict failure rates at nominal operating conditions employs elevated temperature stressing of semiconductor packages at or near the maximum operating voltage for periods of several weeks.

The preceding discussions suggest that, depending on the actual location and service conditions, modern microcircuits can be expected to operate reliably for long periods of time and that simulated aging may not be needed during qualification testing for safety equipment designed with such components. (This assertion is further strengthened by the discussion in Section 3.1.4.) Since the need for simulated aging for digital safety equipment depends on environmental conditions, we propose a methodology for I&C equipment qualification based on the *Location Category* and the expected normal and abnormal environmental conditions during the service life of the equipment. (An example of how this methodology can be applied is given in the Appendix.)

Proposed Location Categories for Nuclear Power Plant I&C Qualification

Figure 3.1a shows a typical arrangement for a nuclear power plant. The nuclear steam supply system is housed inside the containment structure. The containment is generally the harshest environment, especially under accident conditions. However, there are also several locations outside containment (e.g., the transmitter rack area, steam-line tunnel area, and some non-ventilated areas in the auxiliary and turbine building) where environmental conditions can also be harsh under normal and/or accident conditions. Finally, there are certain areas that have, and are likely to maintain, relatively low radiation, temperature, and humidity levels even under accident conditions. Based on these facts, we propose a classification of the nuclear plant environment into three general location categories. We examined various safety analysis reports (SARs) and equipment qualification data packages[41-44] to determine general normal and abnormal environmental conditions expected in these areas.

A location category defines temperature, humidity, and radiation boundaries that equipment in that location is likely to experience under normal and accident conditions. Three location categories are defined. At one extreme is the category A location, which represents the most environmentally severe conditions in a nuclear power plant. That is, a category A location has environmental conditions that promote aging. Accelerated aging must be considered in the qualification program for such equipment. At the other extreme is the category C location. A category C location is typically environmentally controlled. The normal and abnormal conditions in such a location are such that aging is highly unlikely. Thus, accelerated aging is unnecessary for equipment in a category C location.

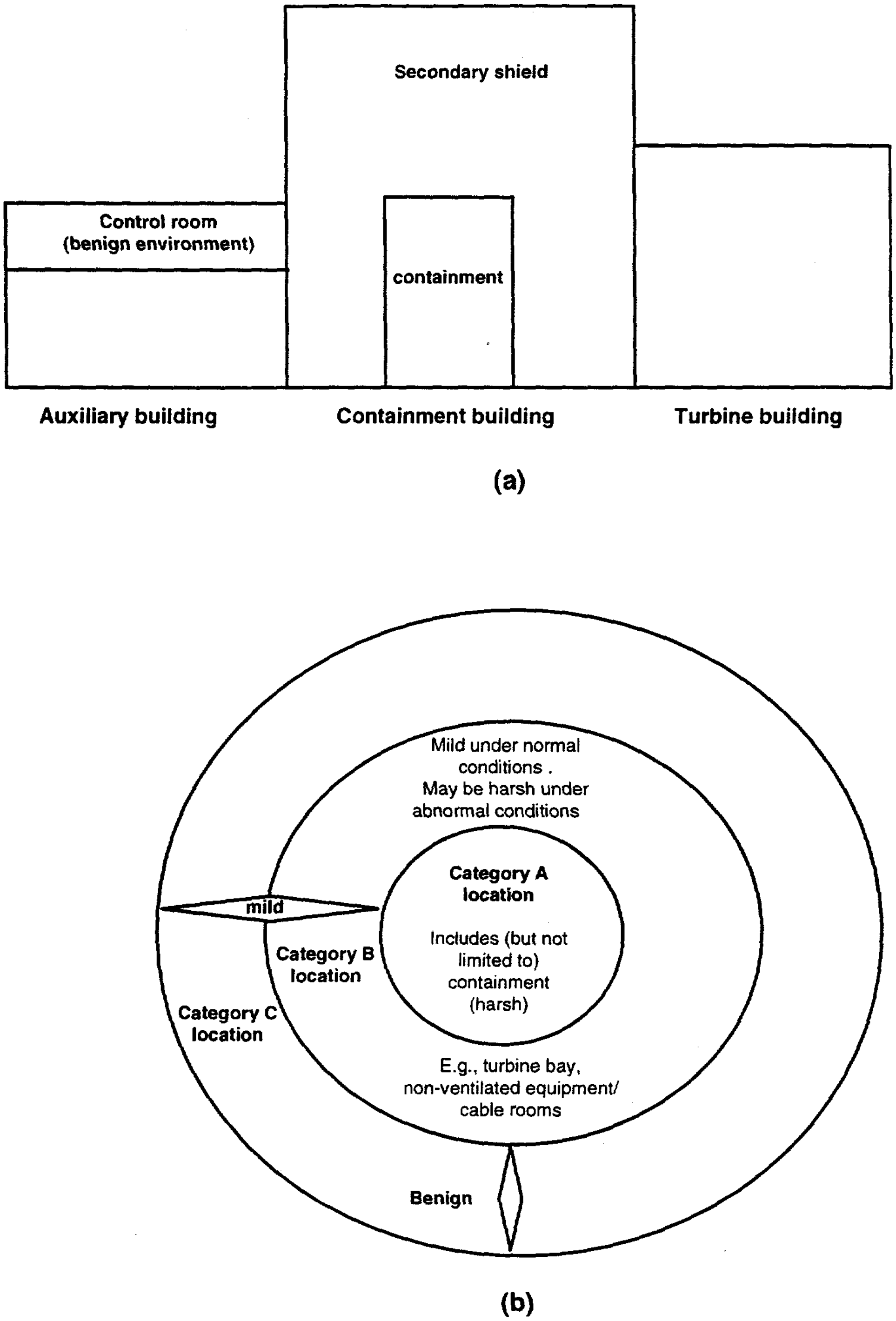


Figure 3.1 Illustration of (a) the general nuclear plant layout and (b) proposed environmental categories

A category B location has environmental conditions that bridge those of the two location category extremes, A and C. Under this proposal, a category A location is any area inside containment, a category B location is an area outside containment, and a category C location is an area outside containment where conditions are such that it may be described as benign under expected service conditions. The following sections define the radiation, temperature, and humidity values that bound these categories.

Location category A

Location category A is any location where the expected normal and abnormal service conditions with regard to environmental stressors are likely to be equal to, or exceed, the following:

Radiation	Normal gamma dose: >10^4 over 40 years.
Temperature	Normal: 32 to 49°C (90 to 120°F); abnormal and accident: >49°C (120°F).
Humidity	Normal: 20 to 90%; abnormal and accident: >95%.

Notes:

(1) There are areas inside containment where the integrated 40-year gamma dose is likely to exceed 10^4 rad. Examples include locations next to the reactor vessel, where the total dose may exceed 1.8×10^{10} rad in pressurized-water reactors (PWRs).[44] However, such locations are not likely to house microprocessor-based I&C equipment.[4] The dose value used here represents the expected dose in the general area outside the reactor loop compartment wall.

(2) The temperature and humidity figures are average values estimated from the SAR and equipment data packages examined.

(3) Environmental qualification of equipment located in this area has typically included simulated aging.

Location category B

Location category B is any location where the expected normal and abnormal service conditions with regard to environmental stressors are likely to correspond to the following:

Radiation	Normal total gamma dose: >4×10^2 rad, but <10^4 rad, over 40 years.
Temperature	Normal: 27 to 41°C (80 to 105°F); Abnormal and accident: >41°C (105°F).
Humidity	Normal: 20 to 70%; Abnormal and accident: >95%.

Notes:

(1) Category B locations may be ventilated or nonventilated. Examples of such locations include pipe and electrical penetration rooms and parts of the auxiliary building containing equipment having safety-related functions.

(2) A category B location may be mild under normal conditions but under accident conditions may experience high temperature, humidity, and/or radiation conditions comparable to containment in the event of a loss-of-coolant accident (LOCA) or high-energy line break.

(3) Environmental qualification of equipment located in this area has typically included simulated aging.

Location category C

Location category C is any location where the expected normal and abnormal service conditions with regard to environmental stressors are likely to correspond to the following:

Radiation	Normal total gamma dose: <4x10^2 rad over 40 years.
Temperature	Normal: 16 to 27°C (60 to 80°F); Abnormal and accident: >27°C (80°F) [49°C (120°F) maximum]
Humidity	Normal: 30 to 50%; Abnormal and accident: <95%.

Notes:

(1) Category C locations are typically air conditioned or ventilated. The control room is an example of a category C location.

(2) We define a *benign* environment to be identical to a category C location. In such a service environment, a seismic event is the only design basis event that can be expected to have catastrophic effect on all redundant safety equipment. Note that benign (category C) environments constitute a subset of category B locations.

(3) Environmental qualification of equipment located in this area has typically *not* included simulated aging. A total 40-year dose of less than 400 rad is quoted by reference[44] for reactor protection system equipment located in the control room.

3.1.4 Justification for Recommended Stressors in a Category C (Benign) Environment

The aging mechanisms of electrical and electronic circuits in a nuclear power plant environment are a combination of the classical effects of radiation on organic materials and inorganic metallics[45] and the sum of all other operating effects on the circuit. The other operating effects include any degradation caused by operations and maintenance as well as the operating environmental effects of moisture, temperature, and contamination. The degradation can appear as deterioration of insulation, changes to dielectric materials, increased resistance to conducting paths, formation of shunt conducting paths, and changes in operating characteristics of electronic devices. Physically, the degradation can take the form of softening or embrittlement of materials, changes in mechanical/metallurgical properties, color, corrosion, cracking of materials, or changes in weight of materials.[20] In this section we identify the basis for the stressor specifications proposed in the previous section for a category C (benign) environment.

Radiation

A study by Gleason[46]of radiation susceptibility of several electronic components indicates that, if the specified total integrated radiation dose (normal plus accident) is less than 100 rads gamma, radiation testing will not be required. On radiation testing, reference 46 recommends the following:

> "If the specified dose is greater than 100 rad gamma, a review should be conducted of the equipment material list to identify radiation damage threshold levels for radiation-sensitive materials. 'Damage threshold' is defined as that level above which there is a measurable change in any property of the material. If the lowest damage threshold is significantly greater than the specified dose, the equipment can be exempted from radiation testing."

Regulatory Guide 1.89 acknowledges that numerous studies have compiled radiation effects data on all classes of organic compounds. In particular, the guide states that:

> ". . . radiation effects data on . . . organic compounds show that compounds with the least radiation resistance have damage thresholds greater than 10^4 rads and remain functional with exposures somewhat above the threshold value . . . However, for electronic components, studies have shown failures in metal oxide semiconductor devices at somewhat lower doses. Therefore, radiation qualification for electronic components may have a lower exposure threshold."

Radiation susceptibility of ICs has improved considerably over the years, and available data strongly suggest that radiation dose levels in benign environments may be well below threshold levels. A very brief discussion of semiconductor device susceptibility to ionizing radiation is presented here. The reader interested in a more detailed discussion is referred to reference 47.

The primary means by which ionizing radiation can cause degradation of electrical devices and systems are through total-dose ionizing radiation damage, soft errors, and displacement damage.[47] Displacement damage is caused primarily by neutrons; ionizing radiation damage is caused primarily by gamma and x rays. Because neutrons are relatively heavy (1840 times heavier than electrons) uncharged particles, they collide with the lattice atoms of the semiconductor—instead of merely ionizing atoms or molecules—dislodging or displacing them from their lattice sites to cause them to take up interstitial positions within the crystal.[48] A soft error refers to a random failure not related to a physically defective device. *Alpha-particle-induced* soft errors are caused by radioactive naturally occurring impurities (e.g., uranium or thorium) in IC packaging materials.[9,47,48]

One way of measuring the radiation threshold of various semiconductor families is to determine the upset level. The term *upset* has the general meaning of the action of exceeding a tolerance level. For example, the radiation upset threshold of a logic gate corresponds to that dose rate for which the output exceeds the noise margin. Table 3.1 shows transient upset radiation levels for various digital logic families. It is seen from the table that the threshold radiation levels for these logic families are much higher than what a mild environment in a nuclear power plant is likely to experience.

Table 3.1 Radiation upset levels of various logic families of integrated circuits[49]

Logic family	Threshold range [rad (Si)/s]
Emitter coupled logic	4×10^7 to 2×10^8
Resistor transistor logic	5×10^7 to 1×10^9
Diode transistor logic	5×10^7 to 5×10^8
Transistor-transistor logic (TTL)	1×10^8 to 3×10^8
Low-power TTL	5×10^6 to 4×10^7
Dielectrically isolated TTL	6×10^8 to 5×10^9
Schottky clamped TTL	10^8 to 10^9
Metal-oxide semiconductor (MOS)	see text

Threshold radiation levels for MOS devices are generally lower than bipolar technologies, although the MOS is the preferred technology for ICs because of its several advantages. These include high-input impedance, fewer processing steps, better temperature stability, and less noise. In the MOS family, NMOS is the most commonly used technology for large scale integrated circuits and VLSIs. However, many NMOS devices fail at ionizing doses of 1 krad (Si), and the range of 1 to 3 krad (Si) appears to be the safe upper limit for commercial (not radiation-hardened) NMOS devices.[49]

Single-event upsets (SEU) are mainly upsets that occur in high density ICs.[50] A cell that has suffered such a logic upset will typically exhibit no degradation in any of its characteristics when tested. Such transitory errors are called single-event upsets (resulting from the transit of a single ionizing particle through the chip) because the corresponding hardware is not damaged or permanently altered. The main source of single-event upsets in nuclear power plant environments is the ionization of the device from alpha particles that are the decay products of naturally occurring radioactive actinides (e.g., uranium, thorium, and their daughter nuclei). The heavy actinides are part of the earth's crust and thus are found in trace amounts within the very material used to fabricate the chip as well as its package. Hence, SEUs cannot be eliminated through qualification testing simply by stipulating a radiation threshold that is higher than that suggested in this section. One partial remedy for the SEU problem is to use error detection and correction or redundancy methods, especially if the packing density is to be maintained or increased.

Temperature/Humidity

The effect of temperature and humidity on ICs is a function of packaging material and technology. There are currently a variety of package types both for through-hole mounting and surface mounting to PCBs. Figure 3.2 illustrates some of the different package types. Chip and package are commonly connected by wire bonding or tape-automated bonding, depending on the number and spacing of input/output pads on the chip and substrate as well as the permissible cost. The main package fabrication technologies are based on refractory ceramic technology or molded plastics. These fabrication methods are covered in detail in several books[9] and articles.[49, 51, 52] Basically, a plastic-encapsulated microcircuit consists of an IC chip physically attached to a leadframe, electrically interconnected to input/output leads, and molded in plastic that directly contacts the chip, leadframe, and interconnects. Hermetically sealed microcircuits (generally called hermetic packages), on the other hand, consist of an IC chip mounted in a metal or ceramic cavity interconnected to leads and hermetically sealed.

The lifetime of an IC has a strong dependence on temperature.[52] In general, optimal cooling through engineering design is the basis for high reliability of computer-based systems. In particular, Wessely *et. al.*[52] estimate that high computer reliability requires chip temperatures that do not exceed about 50°C (122°F) under normal conditions. Semiconductor manufacturers' quality assurance activities generally ensure that maximum temperature ratings of industrial-grade semiconductors exceed 80°C (176°F).[a] Reliability stress tests routinely employed by semiconductor manufacturers to ensure component quality typically use temperature and humidity levels that equal or exceed the maximum values used in the ORNL study. These tests typically include the following: autoclave test (measures device resistance to moisture penetration and the resultant effect of galvanic corrosion), high-temperature high-humidity bias test (measures moisture resistance of plastic-encapsulated devices), high-temperature gate bias test (designed to

[a] At the 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 from 0 to 70°C (32 to 158°F). For industrial-grade component,s this range is between 0 to 85°C (32 to 185°F), and the ratings for military-grade components is -55 to 130°C (-67 to 266°F).

electrically stress the gate oxide under a bias condition at high temperature), and high-temperature storage-life test (performed to accelerate failure mechanisms that are thermally activated through the application of extreme temperatures). Temperatures in control room environments under *abnormal* conditions (e.g., loss of heating, ventilation, and air conditioning) are not likely to exceed 49°C (120°F).[44] (Normal temperature range in the control room is 16 to 27°C (60 to 80°F). Protection systems, which are typically located in the control room, are required to function for at least 12 hours under abnormal conditions.) Under these conditions, semiconductors are not likely to exhibit significant failure mechanisms because of temperature. High humidity (~85%) is unlikely to be a problem unless it is accompanied by high temperature.[53] In the environments proposed for digital safety system equipment, such high humidity is likely only under accident conditions. Tests have shown that, even under such conditions, modern digital components can be expected to survive long enough to effect a safe shutdown.[53]

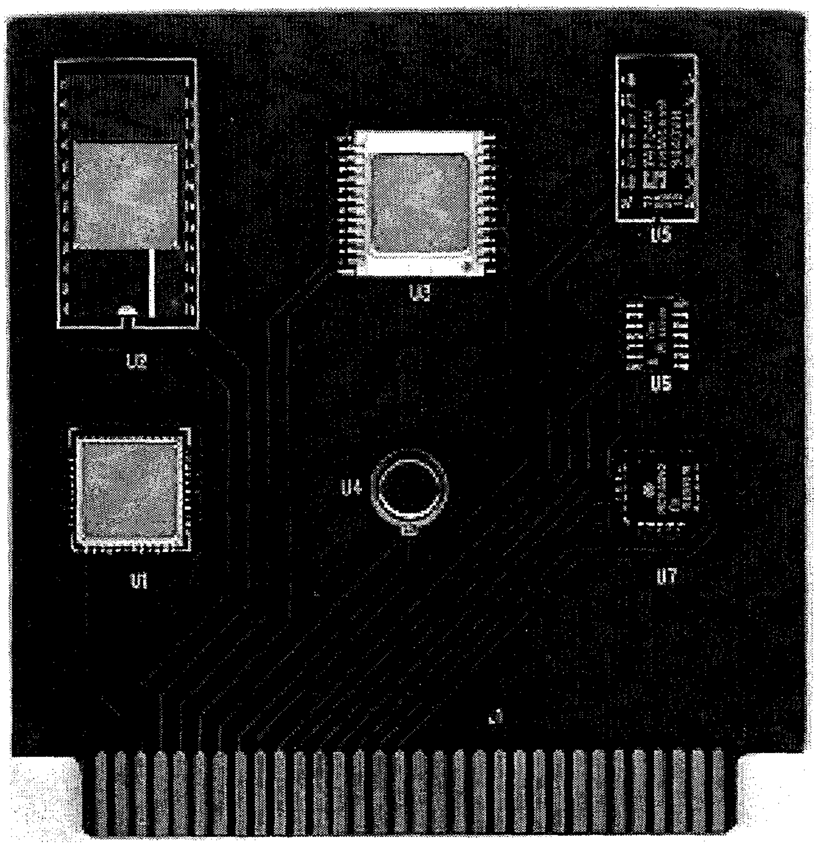


Figure 3.2 Examples of chip packages

U1—Ceramic leadless chip carrier (LLCC). U2—Ceramic dual-in-line package (CDIP). U3—Ceramic flat package (CFP). U4—Transistor outline can (TOC). U5—Plastic dual-in-line package (PDIP). U6—Small-outline integrated circuit (SOIC). U7—Plastic leaded chip carrier (PLCC). The CDIP, PDIP, and TOC are through-hole-mounted packages, while the LLCC, CFP, SOIC, and PLCC are surface-mounted packages.

Thus, we propose that for digital systems located in a category C environment, type testing (without aging) should be sufficient to qualify safety system equipment for use in a nuclear power plant environment.

3.1.5 Stressors

IEEE 323-1974:
Environmental and operational stressors are primarily responsible for equipment aging. Section 6.3.3, "Aging," and Section 6.3.5, "Vibration," of IEEE 323-1974, imply that temperature, radiation, mechanical wear, and vibration are the primary environmental stressors contributing to aging. However, this implication is buried in the text; there is no explicit statement as such.

During preconditioning the standard requires thermal aging to be performed first to simulate service life. The equipment is then subjected to the *significant* type of radiation equivalent to that expected in service. If more than one type of radiation is significant, the standard permits each type to be applied separately. If the required radiation level can be shown to produce less effect than that which would cause loss of the equipment's Class 1E function, radiation need not be included as part of aging (see item 4 of Section 6.3.2, "Test Sequence"). The aged equipment is then subjected to such mechanical vibration as will be seen in service, including simulated seismic vibration (IEEE 344)[54] and self-induced vibration (IEEE 334).[55]

IEEE 323-1983:
The stressors identified as contributing to equipment aging in IEEE 323-1974 are also more explicitly reiterated in Section 6.3.3, "Aging," of IEEE 323-1983. The first paragraph of Section 6.3.3 states that "the types of aging include thermal, radiation, wear, and vibration." With regard to radiation, the standard requires the equipment to be qualified to be subjected to "the significant type of radiation equivalent to or greater than that expected in service. However, if more than one type of radiation is significant, each type can be applied separately." The standard also requires the equipment to be qualified for expected seismic events (in accordance with IEEE 344) following any required aging. Equipment subject to non-seismic vibration that produces significant effects (fatigue and wear) during normal and abnormal use are also required to be subjected to vibration testing *before the seismic tests.* Vibration to be simulated includes self-induced vibration, vibration from piping, or hydrodynamic loading.

Comments:
The types of stressors and the sequential method of their application during preconditioning are more clearly stated in IEEE 323-1983. However, both standards are silent on how to address situations where synergistic effects may exist. Synergistic effects are those that result from two or more stresses acting together, rather than separately. Depending on their aging characteristics, synergistic stressors may produce more degradation than similar application of non-synergistic stressors. Regulatory Guide 1.89 addresses this issue by requiring any known synergistic effects to be accounted for in the qualification program. Two commonly known sources of synergistic effects on certain materials are dose-rate effects and aging sequence effects during accelerated aging simulations.[2]

In conformity with current applicable standards, the basic sequence followed in most programs is thermal aging, irradiation to aging-plus-accident dose, seismic testing and main steam-line break (MSLB)/LOCA testing. However, this sequence is not necessarily the most conservative for microprocessor-based equipment and/or some packaging technologies. Since microprocessor-based safety systems are inherently more complex than their analog counterparts, it is important that aging methodologies increase, as much as possible, the assurance of their long-term performance. It is suggested however, that present methodologies continue to be applied until more is known about the aging sequence and synergistic effects on advanced digital technologies. It is worth noting here that not all qualified equipment has followed the traditional methods. For example, on some cable specimens, Anaconda, Samuel Moore, and Raychem have qualified them using pre-aging with irradiation, followed by thermal aging. Also, ITT Suprenant, BIW, and Raychem have qualified some of their cables using simultaneous thermal and irradiation conditions during pre-aging.[45]

For safety equipment located in a control room environment, the potential initiating events for equipment stress originate from events other than DBEs or anticipated abnormal occurrences. For increasing temperature, the primary initiating event is a loss of heating, ventilation, and air conditioning (HVAC) systems in the equipment room. For humidity, the initiator could be a water spill or use of water for fire suppression. EMI/RFI sources include walkie-talkies, welding equipment, contact arcing, switching on heavy inductive loads, or spurious emissions from other electronic equipment. An electric equipment fire is the primary initiator for smoke.

A stressor not previously considered for analog safety system qualification is smoke from an electrical fire. With increased use of microprocessor-based systems, concern has arisen[56] as to whether smoke should be included in a qualification program. A number of studies by ORNL,[53] SNL,[56] and BNL,[57] have aimed at resolving this issue. These studies are summarized in Section 5 of this report.

3.1.6 Margins

IEEE 323-1974

Section 6.3.1.5, "Margin," defines margin as "the difference between the most severe specified service conditions of the plant and the conditions used in type testing to account for normal variations in commercial production of equipment and reasonable errors in defining satisfactory performance." The standard requires qualification type testing to include adequate margins. Suggested factors to be applied to service conditions for type test testing are as follows:

Pressure, radiation, time, and vibration....................	+10%.
Supply voltage..	±10%.
Temperature...	+8 °C (15 °F).
Frequency..	±5%.
Radiation (margin on accident dose)	+10%.
Environmental transients...	The initial transient and the dwell at peak temperature shall be applied at least twice.

With regard to aging, Section 6.3.3, "Aging," of IEEE 323-1974 stipulates that "Margins over that expected in the qualified life shall be provided in the application of each influence." This requirement, taken together with the definition of margin previously quoted, suggests that the margins are to be applied to the type test parameters for DBE testing, since DBE environmental conditions represent ". . . the most severe specified service conditions . . ." However, the interpretation of this requirement is not necessarily straightforward. For example, some interpretations of the standard could lead to applying a temperature margin of 8 °C (15 °F) to the aging test temperature.

In addition to applying margin to each of the preceding stressors, some manufacturers have also applied margin to the aging time. For example, if equipment to be thermally aged requires an aging time of 10 days at 93 °C (200 °F) to simulate a 40-year qualified life, then the equipment is subjected to the specified temperature for *11 days*.

IEEE 323-1983

Section 6.3.1.5, "Margin," stipulates that "Margin shall be applied to the type test parameters for DBE testing." This statement, in our opinion, reduces the possibility of misinterpretation as previously discussed because it specifically states how the margins are to be applied. The suggested factors are as follows:

Pressure, radiation, time, and vibration	+10%.
Supply voltage	±10%
Temperature	+8 °C (15 °F).
Frequency	±5%.
Radiation (margin on accident dose)	+10%.
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: (a) Temperature and pressure margins may be added and (b) peak transient without temperature and pressure margin may be applied twice.

The last paragraph of Section 6.3.1.5 states that ". . . age conditioning shall be performed on the basis of conservative estimates of service conditions and conservative accelerated aging techniques." This phrase essentially carries the same idea contained in Section 6.3.3 of IEEE 323-1974. However, as the in the earlier version, the 1983 version lacks specificity by not pointing to a specific standard or NUREG document that can be used as a guideline in applying these "conservative techniques."

Comments:

The intent of the section on "Margin" is essentially the same in both versions of the IEEE standard, that is, to account for normal variations in commercial production of equipment and reasonable errors in defining satisfactory performance. However, the 1983 version provides further clarification on how the margins are to be applied by stipulating that margins are to be applied to the **type test parameters for DBE testing**. We are also of the opinion that conservative qualification testing of I&C equipment requires that margin be applied to *both* the aging time, as has been done by some manufacturers in the past, as well as to type test parameters during DBE testing, as is required in IEEE 323-1983. The two margins address two separate issues. Margin on aging time seeks to compensate for uncertainties in the assumptions made in the use of the Arrhenius equation. On the other hand, margin on test parameters during DBE testing seeks to compensate for variations in commercial production of equipment and their ability to satisfy a minimum operational time requirement during a DBE.

3.1.7 Qualification Documentation

Documentation provides the means for verifying that equipment is qualified for its application and meets its specified performance requirements. The documentation required per IEEE 323-1974 and IEEE 323-1983 are summarized subsequently.

IEEE 323-1974

The standard requires the user to maintain a qualification file containing information appropriate to the qualification method used.

i. Documentation for Type Test Data (1974 Version)

Documentation for type test data is required to include the following:

(1) The equipment performance specifications
(2) Identification of the specific features to be demonstrated by the test
(3) Test plan
(4) Report of test results.

ii. Documentation for Operating Experience Data (1974 Version)

Documentation for operating experience data is required to include the following:

(1) The equipment performance specifications
(2) The interface or boundary conditions of the equipment
(3) The specifications of equipment for which operating experience is available
(4) Identification of the specific features to be demonstrated by operating experience
(5) Comparison of past application and specifications with the new equipment specifications for each feature identified above
(6) Summary and source of operating experience applicable to equipment qualification
(7) The basis on which the data has been determined to be suitable and the equipment qualified.

iii. Documentation for Analysis Data (1974 Version)

Documentation for analysis data is required to include the following:

(1) The equipment performance specifications
(2) The interface or boundary conditions of the equipment
(3) The specific features, postulated failure modes, or the failure effects to be analyzed
(4) The assumptions, empirically-derived values, and mathematical models used together with appropriate justification for their use
(5) Descriptions of analytical models or computer programs used
(6) A summary of analytically-established performance characteristics and their acceptability

IEEE 323-1983
As in the 1974 version, the 1983 version requires the user to maintain a qualification file containing information appropriate to the qualification method used.

i. Documentation for Type Test Data (1983 Version)

Documentation for type test data is required to include the following:

(1) Identification of the equipment qualified
(2) Equipment specification
(3) Qualification program
(4) Identification of any scheduled surveillance/maintenance, periodic testing, and any parts replacement required to maintain qualification

(5) Identification of safety functions to be demonstrated by test data
(6) Test plan
(7) Report of test results
(8) Summary and conclusions, including limitations and qualified life or periodic surveillance/maintenance interval determination.

ii. Documentation for Operating Experience Data (1983 Version)

Documentation for operating experience data is required to include the following:

(1) Identification of the equipment qualified
(2) Equipment specification
(3) Qualification program
(4) Identification of any scheduled surveillance/maintenance, periodic testing, and any parts replacement required to maintain qualification
(5) Identification of safety functions to be demonstrated by operating experience
(6) Specification of the equipment for which operating experience is available
(7) Comparison of specifications and functions of equipment with operating experience and new equipment to be qualified
(8) Summary of operating experience data, including service conditions, maintenance records, operating history, etc.
(9) Conclusions, including limitations and qualified life or periodic surveillance/maintenance interval determination.

iii. Documentation for Analysis Data (1983 Version)

Documentation for analysis data is required to include the following:

(1) Identification of the equipment qualified
(2) Equipment specification
(3) Qualification program
(4) Identification of any scheduled surveillance/maintenance, periodic testing, and any parts replacement required to maintain qualification
(5) The specific safety function(s), postulated failure modes, or the failure effects or the failure effects to be demonstrated by analysis
(6) Descriptions of analytical methods, computer program or mathematical model used, and the method of verification
(7) The assumptions and empirically derived values used, with appropriate justification
(8) Summary of analytically-established performance characteristics and their acceptability
(9) Conclusions, including limitations and qualified life or periodic surveillance/maintenance interval determination.

In addition to the three broad qualification documentation categories, IEEE 323-1983 also includes a separate section detailing documentation procedures for "equipment located in a mild environment."

iv. **Documentation for Equipment Located in a Mild Environment (1983 Version)**

Documentation for equipment located in a mild environment is required to include the following:

(1) Identification of the equipment qualified
(2) Equipment specification
(3) Identification of any scheduled surveillance/maintenance, periodic testing, and any parts replacement required to maintain qualification
(4) Identification of the equipment's safety function(s)
(5) Certificate of compliance that the equipment supplied meets the requirements of the equipment specification

Comments:
A comparison of the two versions show that the documentation procedures stipulated in IEEE 323-1983 are more detailed and leave less room for differing interpretations with regard to the *contents* of the documentation. However, a significant difference between the two versions is that the 1983 version implies that neither a **qualification program**, nor a **test plan**, is required for equipment located in a mild environment (compare the documentation requirements for type test data and for equipment located in a mild environment). This implies that

(1) No qualification, either by testing, operating experience, or analysis is required to be performed for equipment located in a mild environment, whether or not "significant aging mechanisms" exist.

(2) Factory acceptance testing by the equipment supplier is sufficient to meet the "certificate of compliance" requirement [see item iv(5) under **Documentation for Equipment Located in a Mild Environment (1983 Version)**]

First, we feel that if significant aging mechanisms have been determined to exist for equipment located in a mild environment, then a qualification program, as well as a test plan, should be provided as part of the documentation. This also implies that preconditioning should be performed prior to type testing.

We propose therefore the following documentation methodology for equipment located in a mild environment:

(1) Identification of the equipment qualified
(2) Equipment specification
(3) Qualification program for equipment for which significant aging mechanisms have been identified
(4) Identification of any scheduled surveillance/maintenance, periodic testing, and any parts replacement required to maintain qualification
(5) For equipment for which significant aging mechanisms have been identified—
    (a) Identification of safety function(s) to be demonstrated by test data
    (b) A test plan
    (c) Report of test results
    (d) Summary and conclusions, including limitations and qualified life or periodic surveillance/maintenance interval determination

(6) For equipment for which *no* significant aging mechanisms have been identified—
   (a) Identification of the equipment's safety function(s)
   (b) Certificate of compliance that the equipment supplied meets the requirements of the equipment specification

The comparative analysis of the two versions of IEEE 323 are summarized in Table 3.2.

3.2 Conclusions

Topical comparisons have been performed between the 1974 and 1983 versions of IEEE 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." Conclusions from these comparisons are as follows:

(1) The methods of qualification—type testing, operating experience, and analysis—are identical in both versions. 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. 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.

(2) The reasons and concepts for aging are essentially the same in both versions. It is our opinion that the state of the art does not warrant any changes to be made with regard to aging methodologies for *digital* systems in nuclear power plants.

(3) IEEE 323-1983 appears to have introduced the concept of "Significant Aging Mechanisms" so that the user of the standard can determine whether aging should be considered during type testing. Although this concept is not explicitly stated in the 1974 version, it is important to note that the 1974 version does allow the exclusion of radiation during aging "if the required radiation level (necessary to simulate the equipment's expected end-of-qualified-life condition) can be shown to produce less effect than that which would cause loss of the equipment's Class 1E function." Thus, as in the 1983 version, the 1974 version allows an environmental stressor to be excluded in the aging program if its effect is "not significant."

    We believe that the approach to qualification that we propose in the Appendix constitutes an improvement on both the 1974 and 1983 standards. The methodology is based on the approach used by the military (introduced in the next section), analysis of the effect of the stressors on the equipment, and the expected normal and accident conditions in the location in which the equipment will be placed.

(4) The types of stressors and the sequential method of their application during preconditioning are more clearly stated in IEEE 323-1983. However, both standards are silent on how to address situations where synergistic effects may exist. In conformity with current applicable standards, the basic sequence followed in most programs is thermal aging, irradiation to aging-plus-accident dose, seismic testing and MSLB/LOCA testing. However, this sequence is not necessarily the most conservative for microprocessor-based equipment and/or some packaging technologies. Because microprocessor-based safety systems are inherently more complex than their analog counterparts, it is important that aging methodologies increase, as much as possible, the assurance of their long term performance. It is suggested, however, that present methodologies continue to be applied until more is known about the aging sequence and synergistic effects on advanced digital technologies. It is worth noting here

Table 3.2 Comparison of IEEE 323-1974 and 323-1983

Topic	IEEE 323-1974	IEEE 323-1983	Comments
Qualification methods	Type testing, operating experience, analysis, or any combination of the three is allowed. Type testing using simulated service conditions is explicitly stated as the preferred qualification method.	Type testing, operating experience, analysis, or any combination of the three is allowed.	Digital I&C generally undergoes more rapid evolutions than their analog counterparts. Thus, it may be difficult to obtain sufficient documentation based on operating experience under identical environmental conditions for a particular I&C equipment for qualification purposes. Type testing alone may be used if adequate stress testing **at the component level** to identify failure mechanisms can be assured.
Ongoing Qualification	Methods by which qualified life can be extended include: (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 that 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.	Same as in IEEE 323-1974. In addition, IEEE 323-1983 allows qualified life to be extended if it can be demonstrated with suitable documentation and auditable records that (a) evaluation in the original qualified program was conservative with respect to the equipment's specified service conditions and performance specifications; (b) an age-conditioning procedure, which limited the qualified life of equipment, is in fact conservative; and (c) 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.	The procedures and conditions for on-going qualification are more succinctly stipulated in the 1983 version. These procedures do not appear to require modification for application to microprocessor-based and advanced digital systems.

Table 3.2 (continued)

Topic	IEEE 323-1974	IEEE 323-1983	Comments
Ongoing qualification (continued)	(4) Use of periodic surveillance/maintenance, testing, and replacement/refurbishment programs based on manufacturers' recommendations and sound engineering practices.		
Aging	The need for aging should be determined based on an evaluation of the specific design and application. If aging is needed, a further determination must be made as to whether accelerated aging techniques can be applied to the equipment and yield valid results that may be correlated to real time, ongoing qualification.	If type testing is the mode of qualification, then preconditioning before testing is not required if the equipment is determined not to have significant aging mechanisms.	Both standards imply that there may be situations under which aging may not be required. This document suggests one method by which such a determination can be made.
Stressors	Temperature, radiation, mechanical wear, and vibration are indicated to be the primary environmental stressors contributing to aging. If more than one type of radiation (e.g., gammas and/or neutrons) is significant, the standard permits each type to be applied separately. With regard to radiation aging, if the required radiation level can be shown to produce less effect than that which would cause loss of the equipment's class 1E function, radiation need not be included as part of aging. Radiation aging, if necessary, is applied before equipment is subjected to such mechanical vibration as will be seen in service.	Temperature, radiation, mechanical wear, and vibration are indicated to contribute to aging. If more than one type of radiation (e.g., gammas and/or neutrons) is significant, the standard permits each type to be applied separately.	The basic sequence followed in most qualification programs is thermal aging, irradiation to aging-plus-accident dose, seismic testing and MSB/LOCA testing. Although this sequence is not necessarily the most conservative for microprocessor-based equipment, it is suggested that present methodologies continue to be applied until more is known about the aging sequence and the synergistic effects on advanced digital technologies. A stressor not previously considered for analog safety system qualification is smoke from an electrical fire. The issue as to whether smoke should be included in a qualification program has been studied and is documented in this report. Conclusions are that 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. Present methodologies with regard to fire and its effects (smoke, heat, ignition, explosions, and toxic gases), which are addressed via GDC3, IEEE 384, and Appendix R of 10 CFR 50, should continue to be applied to digital I&C safety systems.

Table 3.2 (continued)

Topic	IEEE 323-1974	IEEE 323-1983	Comments
Margins	Suggested factors to be applied to service conditions for type testing are as follows: Pressure, radiation, time, and vibration .... +10% Applied voltage ..... 10% Temperature .... +8°C Frequency .... ±5% Radiation (margin on accident dose .... +10% Environmental transients: The initial transient and the dwell at peak temperature shall be applied at least twice.	Suggested factors to be applied to service conditions for type testing are as follows: Pressure, radiation, time, and vibration .... +10% Applied voltage ..... ±10% Temperature .... +8°C Frequency .... ±5% Radiation (margin on accident dose .... +10% Equipment operating time: +10% of the period of time the equipment is required to be operational following the start of the DBE. Environmental transients: The initial transient and the dwell at peak temperature shall be applied at least twice.	Although the intent of the section on "Margin" is essentially the same in both versions of the IEEE standard, the 1983 version provides clarification on how the margins are to be applied by stating that "Margins are to be applied to the **type test parameters for DBE testing**." We are also of the opinion that conservative qualification testing of I&C equipment requires that margin be applied to *both* the aging time, as has been done by some manufacturers in the past, as well as to type test parameters during DBE testing, as is required in IEEE 323-1983. The two margins address two separate issues. Margin on aging time seeks to compensate for uncertainties in the assumptions made in the use of the Arrhenius equation. On the other hand, margin on type test parameters during DBE testing seeks to compensate for variations in commercial production of equipment and their ability to satisfy a minimum operational time requirement during a DBE.
Qualification Documentation	The standard requires the user to maintain a qualification file containing information appropriate to the qualification method used.	The standard requires the user to maintain a qualification file containing information appropriate to the qualification method used.	The 1983 version appears to imply that neither a **qualification program**, nor a **test plan**, is required for equipment located in a mild environment. To clarify this we have proposed a documentation methodology in the text for equipment located in a mild environment.

that not all equipment has been qualified according to traditional methods. For example, on some cable specimens, Anaconda, Samuel Moore, and Raychem have qualified them using pre-aging with irradiation, followed by thermal aging. Also, ITT Suprenant, BIW, and Raychem have qualified some of their cables using simultaneous thermal and irradiation conditions during pre-aging.

A stressor not previously considered for analog safety system qualification is smoke from an electrical fire. With increased use of microprocessor-based systems, concern has arisen[56] as to whether smoke should be included in a qualification program. Studies performed by ORNL,[53] SNL,[56] and BNL[57] that attempt to resolve this issue are summarized in Section 5 of this report.

(5) Although the intent of the section on "Margin" is essentially the same in both versions of the IEEE standard, the 1983 version provides clarification on how the margins are to be applied by stating that "margins are to be applied to the type test parameters for DBE testing." However, we are of the

opinion that conservative qualification testing of I&C equipment requires that margin be applied to *both* the aging time, as has been done by some manufacturers in the past, as well as to type test parameters during DBE testing, as is required in IEEE 323-1983. The two margins address two separate issues. Margin on aging time seeks to compensate for uncertainties in the assumptions made in the use of the Arrhenius equation. On the other hand, margin on type test parameters during DBE testing seeks to compensate for variations in commercial production of equipment and their ability to satisfy a minimum operational time requirement during a DBE.

(6) Comparison of the two versions shows that the documentation procedures stipulated in IEEE 323-1983 are more detailed and leave less room for differing interpretations with regard to the *contents* of the documentation. However, a significant difference between the two versions is that the 1983 version implies that neither a **qualification program**, nor a **test plan**, is required for equipment located in a mild environment. This implies that no qualification, either by testing, operating experience, or analysis needs to be performed for equipment located in a mild environment, whether or not "significant aging mechanisms" exist. If significant aging mechanisms have been determined to exist for equipment located in a mild environment (the 1983 version requires that this assessment be performed), then a qualification program, as well as a test plan, should be provided as part of the documentation. Based on this analysis, we have proposed modification of the section on documentation for equipment located in a mild (as defined in IEEE 323-1983) environment.

3.3 Recommendations

Based on the comparative analysis of IEEE 323-1974 and IEEE 323-1983 performed in this section, we recommend that IEEE 323-1983 be endorsed with the following exceptions:

(1) Locations in which preconditioning is not required be more crisply defined. One way of achieving this has been proposed in this document (see the Appendix).

(2) Methodologies for documenting qualification procedures be augmented with the procedures proposed in this document.

4 A REVIEW OF THE U.S. MILITARY'S APPROACH TO ENVIRONMENTAL QUALIFICATION

4.1 Introduction

The primary reason for environmental qualification in the NPP environment is to ensure correct performance of safety-related I&C in the case of a DBE, even after the safety system has been operating in a harsh environment for some time. The high reliability required of nuclear safety I&C components to meet such demands is also true of military, where high temperature, humidity, EMI/RFI, and vibration are typical. At the system or equipment level, MIL-STD-810E, "Environmental Test Methods and Engineering Guidelines,"[58] is a military standard that performs a similar function to IEEE Standard 323. In this section, we first briefly review MIL-STD-810E to identify practices that could be used to enhance I&C qualification in the NPP environment. We then examine the overall approach used by the military to ensure high-reliability equipment.

4.2 MIL-STD-810E: Qualification Testing Standard for Military Applications

MIL STD 810E, "Environmental Test Methods and Engineering Guidelines," provides:

a. Guidelines for conducting environmental engineering tasks to tailor environmental tests to end-item equipment applications.

b. Test methods for determining the effects of natural and induced environments on equipment used in military applications.

The bulk of the standard is devoted to test methods, and includes methodologies designed to encourage accurate determination of the environmental stresses that equipment will encounter during its service life. Guidelines for accelerated testing during the design process are also included in some cases.

The document contains six sections. Sections 1 through 3 contain general information. Section 4 contains both tailoring guides and general test information that relates to the test methods of Section 5. Section 5 contains climatic and dynamic test methods, and Section 6 has references to contractual requirements.

4.2.1 Tailoring

The objective of tailoring, as applied to MIL-STD-810E, is to ensure that military equipment is designed and tested for resistance to the environmental stresses it will encounter during its life cycle. The tailoring process is described in Section 4.2 and consists of (1) identification of the natural environment characteristics for regions in which the item is to be deployed, (2) identification of characteristics of platforms on which the item is to be carried or operated, (3) tailoring of design requirements to platform environment characteristics that will affect the item and its effectiveness and integrity, and (4) tailoring of test methods and procedures to platform environments and design requirements.

4.2.2 Stressors

The following is a list of the environmental stressors addressed in MIL-STD-810E:

1. Low pressure (altitude): Test Method 500.3
   This test is performed to determine if the equipment can withstand and operate in a low-pressure environment and withstand rapid pressure changes.

2. High temperature: Test Method 501.3
   This test is performed to determine if the equipment can be stored and operated under hot climatic conditions without experiencing physical damage or deterioration in performance.

3. Low temperature: Test Method 502.3
   This test is performed to determine if the equipment can be stored, manipulated, and operated under pertinent low-temperature conditions without experiencing physical damage or deterioration in performance.

4. Temperature shock: Test Method 503.3
   This test is performed to determine if the equipment can withstand sudden changes in temperature of the surrounding atmosphere without experiencing physical damage or deterioration in performance.

5. Solar radiation (sunshine): Test Method 505.3
   This test is performed to determine the effect of solar radiation on equipment that may be exposed to sunshine during operation or unsheltered storage on the earth's surface or in the lower atmosphere.

6. Rain: Test Method 506.3
   This test is conducted to determine the following:
   a. The effectiveness of protective covers or cases in preventing the penetration of rain.
   b. The capability of the test item to satisfy its performance requirements during and after exposure to rain.
   c. The physical deterioration of the test item caused by the rain.

7. Humidity: Test Method 507.3
   This test is performed to determine the resistance of the test item to the effects of a warm, humid atmosphere.

8. Fungus: Test Method 508.4
   The fungus chamber test is performed to assess the extent to which the test item will support fungal growth or how the fungal growth may affect performance or use of the test item.

9. Salt fog: Test Method 509.3
   This test is performed to determine the resistance of equipment to the effects of an aqueous salt atmosphere.

10. Sand and dust: Test Method 510.3
    This test method is divided into two procedures. The small-particle procedure (dust and fine sand) is performed to ascertain the ability of equipment to resist the effects of dust particles that may penetrate cracks, crevices, bearings, and joints. The blowing sand test is performed to determine whether the

test item can be stored and operated under blowing sand (149 to 850 μm particle size) conditions without experiencing degradation of its performance, effectiveness, reliability, and maintainability because of the abrasion (erosion) or clogging effect of large, sharp-edged particles.

11. Explosive atmosphere: Test Method 511.3
    This test is performed to demonstrate the ability of equipment to operate in flammable atmospheres without causing an explosion, or to prove that a flame reaction occurring within encased equipment will be contained and will not propagate outside the test item.

12. Leakage (immersion): Test Method 512.3
    These tests are performed to determine whether the test item is constructed so that it can be immersed in water without the water leaking into the enclosure.

13. Acceleration: Test Method 513.4
    This test is performed to ensure that equipment can structurally withstand the gravitational forces that are expected to be induced by acceleration in the service environment, and function without degradation during and following exposure to these forces.

14. Vibration: Test Method 514.4
    Vibration testing is performed to determine the resistance of equipment to vibrational stresses expected in its shipment and application environments.

15. Acoustic noise: Test Method 515.4
    This test is conducted to measure how well a piece of equipment will withstand or operate in intense acoustic noise fields.

16. Shock: Test Method 516.4
    Shock tests are performed to ensure that equipment can withstand the relatively infrequent, non-repetitive shocks or transient vibrations encountered in handling, transportation, and service environments. Shock tests are also used to measure an item's fragility, so that packaging may be designed to protect it, if necessary, and to test the strength of devices that attach equipment to platforms that can crash.

17. Gunfire vibration: Test Method 519.4
    The gunfire vibration test is performed to ensure that equipment mounted in an aircraft with onboard guns can withstand the vibration levels caused by the overpressure pulses emitting from the gun muzzle.

18. Temperature, humidity, vibration, altitude: Test Method 520.1
    The purpose of this test is to identify failures that temperature, humidity, vibration, and altitude can induce in aircraft electronic equipment either individually or in any combination, during ground and flight operations.

19. Icing/freezing rain: Test Method 521.1
    This test is conducted to evaluate the effect of icing produced by a freezing rain, mist, or sea spray on the operational capability of equipment. This method also provides tests for evaluating the effectiveness of deicing equipment and techniques, including field expedients.

20. Vibro-acoustic, temperature: Test Method 523.1
    This method seeks to produce the combined temperature, vibration, and other operating stresses as needed, that an externally-carried aircraft store will experience during in-service flights.

4.2.3 General Test/Qualification Philosophy

The general test/qualification approach used in MIL-STD-810E is to use the tailoring process described previously to determine the appropriate tests and test variables. Because the objective of Test Method 520.1, "Temperature, Humidity, Vibration, Altitude," is to identify failures in aircraft electronic equipment, and because this objective is similar to that of nuclear I&C qualification, we briefly discuss this test method in the following:

MIL-STD-810E identifies three areas in which Test Method 520.1 can be applied: (1) engineering development, (2) flight or operation support, and (3) qualification testing.

I—Engineering Development Tests
This test is used to find defects in a new design while it is still in the development stage. The test is failure oriented, meaning that the tester should hope to uncover as many defects as possible. First, procedures (based on mission profiles) outlined in MIL-STD-810E are used to determine realistic environment stress levels, durations, and rates of change. The amplitude of environmental stresses can be increased to accelerate the occurrence of failures. Depending on available facilities, environmental stresses may be tested in combination or singly.

II—Flight or Operational Support Test
This test is performed in preparation for, or during, flight or operational testing. Its purpose is to minimize delays in the flight testing program due to environmental factors. It is not directly applicable to the NPP environment, and therefore will not be considered further in this document.

III—Qualification Testing
The intent of qualification testing in MIL-STD-810E is to demonstrate compliance with contract requirements. Generally, qualification testing is an accelerated test that emphasizes the most significant environment stress conditions. MIL-STD-810E requires qualification testing to include the maximum amplitude of each stress and any unique combinations of stress types that were found to be important in the engineering development testing stage. Qualification can be accomplished either with a single test that combines all the appropriate environmental stresses or with a series of separate tests. The standard does *not* recommend running all environmental stresses in separate tests. When the use of separate environmental tests is selected, the standard recommends using certain single and combined environment stress tests. For example, the vibration test may be performed as a separate test, but temperature testing should be combined with altitude and humidity testing.

4.3 Qualified Manufacturers List: An Approach to Qualification Philosophy

4.3.1 Scope

The military's approach to ensuring high quality and reliability in equipment starts at the ***component*** level, where the manufacturer of the safety equipment is required to purchase ICs for manufacturing the equipment from a qualified manufacturers list (QML). The details of this methodology are defined in military specification MIL-PRF-38535C.[59] In this approach, a production line is certified on a one-time basis, and all products from that line are subsequently qualified per the requirements of MIL-PRF-38535C. Thus, the quality of a product from a QML line is defined by its conformance to MIL-PRF-38535C. In other words, a manufacturer wishing to be included on a QML has to conform to this standard. After the listing of a technology flow on a QML, the manufacturer must continually meet or improve the established baseline of certified and qualified procedures, the quality management (QM) program, the manufacturer's review system, the status reporting and quality and reliability assurance requirements for all QML products.

4.3.2 QML Implementation Phases

There are three phases to QML implementation: certification, qualification, and quality assurance. These phases use statistical process control (SPC) of technology parameters relevant to radiation hardness, test structure to IC correlation, and extrapolation from laboratory to threat scenarios, to control factors affecting not only manufacturing yield but also reliability and radiation hardness.

Certification Requirements

The manufacture is required to meet the following minimum procedures for QML certification:

QM Program Documentation
The manufacturer is required to establish a dedicated system of review, referred to as the Technical Review Board, to be responsible for implementation of the QM program. Guidelines are provided in Appendix G of the standard.

Process Capability Demonstration
The manufacturer is required to build devices, perform tests, and run software benchmarks necessary to demonstrate that the manufacturer has a comprehension of the capability of the manufacturing process as related to quality, reliability, and producibility. Process capability demonstration includes circuit and package design, wafer fabrication, SPC and in-process monitoring programs, wafer acceptance plans, assembly and packaging, and radiation hardness assurance (RHA). Guidelines are provided in Appendix H of the standard. In addition, Appendix C provides guidelines for RHA.

Demonstration of Manufacturer's Control of any Off-Shore Operations
Appendix E of the standard provides guidelines to be used when a manufacturer having QML status decides to perform selected operations at an off-shore site.

All Procedures Used to Manufacture Masks for Monolithic Fabrication
Guidelines are provided in Appendix H of the standard.

Qualification Requirements

QML certification requires a manufacturer to put in place a process monitoring system to control key processing steps to ensure product yield and reliability. The monitoring system can use various test chips, methods, and measurement techniques. The resulting data should be analyzed by appropriate methods to determine control effectiveness. The following should be addressed as a minimum by the manufacturer:

(1) Incoming assembly process materials,
(2) Incoming package acceptance,
(3) Equipment used for assembly,
(4) Wafer acceptance criteria,
(5) Die attach,
(6) Chip-to-package interconnect,
(7) Package seal,
(8) Marking,
(9) Rework,
(10) Lead trim, form, and final finish,
(11) Atmosphere and cleanliness control,
(12) Chip encapsulation/molding,
(13) Encapsulant purity, and
(14) Internal water vapor.

The manufacturer is required to present a qualification test plan as part of the certification information which details the test flow; test limits; test data to be measured, recorded, and analyzed; test sampling techniques; and traceability records. The test plan should detail materials, manufacturing construction techniques (including design CAD tools), testing and reporting techniques and should be made available at the time of certification. The test plan should include traceability documentation, and all test limits should be in accordance with the requirements of the qualification test plan. The various test methods to be used are provided in Appendix H of MIL-STD-38535. These test methods are from MIL-STD-883, "Test Methods and Procedures for Microelectronics."[60] As an example, Tables 4.1 and 4.2 (adapted from Appendix H of MIL-STD-38535) provide recommended test methods for assembly process qualification testing for hermetic and plastic packages, respectively.

If any particular test results are not successful, the manufacturer is required to perform failure analysis and take necessary corrective action. The manufacturer is also to notify the QML qualifying activity of any decision not to pursue qualification of any material or manufacturing construction technique previously certified. After corrective actions have been implemented, qualification testing can restart.

4.3.3 Comments

The military's "tailoring" approach to qualification—where the characteristics of the environment in which the equipment is going to be deployed is taken into account—is similar to our proposal that the location of a safety I&C equipment in the NPP be taken into account during qualification (see Section 3.1.3 and the Appendix).

In the military's approach to qualification, the assurance that an equipment will perform properly is "built-in" as well as "tested-in." That is, the assurance of an equipment's quality starts at the component level. We suggest that this approach be adopted in the nuclear industry. As a minimum, it might be required that the manufacturer of the safety I&C equipment document the qualification standards used by the semiconductor manufacturer for stress testing. Note that unlike the military's QML certification process, this proposed approach does not involve certification of I&C vendors, nor does it require that military-grade components be used in the design of nuclear safety equipment. Rather, the intent is to encourage the adoption of the International Organization for Standardization (ISO) 9000[61] approach of ensuring a quality process. Also, the approach does not contradict the recommendations proposed in previous sections with regard to qualification standards such as IEEE 323. The documentation of component qualification standards may be used to ensure quality at the IC (component) level; while IEEE 323-1983 may be used, with appropriate exceptions, at the equipment or system level.

Table 4.1 Assembly process qualification testing for hermetic packages

Process	Test	MIL-STD-883 test method (TM) or JEDEC* TM
Die-attach and interconnect	Thermal shock (100 cycles)	TM 1011, condition C per device specification
	X-ray or ultrasonic inspection	TM 2012 or TM 2030
	Visual inspection	TM2010 (die-mount and wire bond) plus die cracks
	Bond strength	TM 2011
	Die shear or stud pull	TM 2019 or TM 2027
Die-attach, interconnect, and seal	Mechanical shock	TM 2002, condition B
	Variable frequency vibration	TM 2007, condition A
	Constant acceleration	TM 2001
	Fine and gross leak	TM 1014
	Visual inspection	TM 1010 criteria, 20 × magnification per device specification
Lid seal	Internal water vapor content (5000 ppm maximum at 100°C)	TM 1018
Lid seal	Lid torque	TM 2024 (glass seal)
Code marking	Resistance to solvents	TM 2015
Final package testing	High-temperature storage	TM 1008, 1000 hours at 150°C.
Post burn-in lead finish	Solderability	TM 2003 (245°C ±5°C)

*Joint Electron Device Engineering Council

Table 4.2 Assembly process qualification testing for plastic packages

Process	Test	MIL-STD-883 test method (TM) or JEDEC* TM
Die-attach and interconnect	In-line visual inspection	TM 2010 (die mount and wire bond)
	In-line bond strength	TM 2011
	In-line ball bond shear	ASTM F 1269
	In-line die shear or stud pull	TM 2019 or TM 2027
	Post molding X-ray.	TM 2012
Die-attach, interconnect, and molding	X-ray, ultrasonic inspection, etc.	TM 2012 (die mount and wire bond), TM 2030
Die attach, interconnect, and molding	Temperature cycling (1000 cycles)	TM 1010, condition C or JESD 22-A104
Die attach, interconnect, and molding	Thermal shock (100 cycles)	TM 1011 condition C or JESD 22-A106 condition C
Marking	Resistance to solvents	TM 2015
Storage conditions	High-temperature storage	TM 1008, 1000 hours at 150°C.
Post burn-in lead finish	Solderability	TM 2003

*Joint Electron Device Engineering Council

5 TECHNICAL BASIS FOR ENVIRONMENTAL STRESSORS TO BE CONSIDERED DURING QUALIFICATION TESTING FOR DIGITAL I&C EQUIPMENT

5.1 Introduction

A number of tasks were performed to identify approaches that could be used in enhancing digital I&C qualification for the NPP environment. In particular, we sought to identify (1) environmentally-related I&C system failure rate information in both the nuclear and non-nuclear industries; (2) literature on survivability of digital I&C equipment to smoke exposure in NPP environments; (3) literature and standards on qualification methodologies for digital I&C in NPPs; and (4) foreign nuclear plant experience with digital I&C. The following conclusions were drawn from these studies:

(a) The efficacy of digital I&C qualification methodologies could not be accurately determined because no database currently exists in either the nuclear or non-nuclear environment to enable one to accurately relate digital I&C system failures with causative mechanisms.

(b) While some earlier work had indicated[62] that through-hole PCBs can be reconditioned, with good results, after deposition of up to 100 µg chloride/cm^2, very few tests have been performed to determine the reliability of microprocessor-based electronic equipment in a smoke atmosphere.

(c) A stressor not previously considered for analog safety system qualification is smoke from an electrical fire. It was evident from the available data that further studies had to be performedto resolve the need for inclusion of smoke in a qualification program.

In order to address these issues, three separate studies were performed at BNL, SNL, and ORNL. This section summarizes the approach and results of these studies.

5.2 BNL Study: Risk-Screening of Environmental Stressors[†]

This study, conducted by BNL, was performed to identify environmental stressors for digital I&C systems in an NPP that could be potentially risk significant. The screening of environmental stressors was based on their risk-sensitivities, which are changes in plant risk caused by the stressors and are quantified by estimating their effects on the occurrences of I&C failure and the consequent increase in risk in terms of CDF.

5.2.1 Scope of Study

The study included reviewing and collecting available military data and NPP operating experience on the effects of environmental stressors on digital I&C failures, developing approaches for estimating risk-sensitivities based on available data, and then applying these data and methods to screen stressors in an example plant (a NUREG-1150 PWR), using its specific PRA model.

[†] Research performed for theNRC Office of Nuclear Regulatory Research by BNL.[57]

The stressors evaluated for risk effects are temperature, humidity, vibration, radiation, EMI from lightning, and smoke. EMI from other sources could not be evaluated because of a lack of data. The stressor effects were considered in plant areas where digital I&C equipment may be located during normal, abnormal, and accident conditions.

5.2.2 Approach

Evaluating Risk-Sensitivity of Environmental Stressors

Plant risk-sensitivity to an environmental stressor is defined in this study to be the change in risk contributions from plant equipment that can occur from the detrimental effect of the stressor. The higher the change in risk contributions from a stressor, the higher the risk-sensitivity of the specific equipment, and consequently the plant, to the stressor. Risk-sensitivity results are obtained by accounting for the effects of the stressor on the equipment's failure occurrences and then by determining the increase in risk caused by those failures.

The increase in risk to a plant from the effect of a stressor depends on four factors:

(1) The likelihood of the stressor,

(2) The components affected by the stressor,

(3) The increase in failure rates of the affected components, and

(4) The risk contribution from the affected components.

The risk-sensitivity of a stressor can be obtained by quantifying or estimating ranges for these factors. For stressors that can affect safety systems the function of which is to prevent core damage, the risk-sensitivity is related to the expected increase in CDF. A PRA model of a plant may be used to estimate changes in risk caused by a stressor.

For the case of I&C equipment in NPPs, if we let

C' = CDF contributions from cutsets containing I&C basic events with stressor effects,
L = likelihood of the stressor,
C = CDF contributions without stressor effects from cutsets containing I&C basic events,
F = factor increase in the I&C failure rate caused by the stressor, and
N = number of I&C components in the cutset affected by the stressor,

then

$$C' = LF^{N}C \qquad \textbf{(5.1)}$$

In words, this relationship can be expressed as

$$\begin{matrix}\text{Plant Risk Including}\\ \text{Stressor Effects}\end{matrix} = \left\{\begin{matrix}\text{Stressor}\\ \text{Likelihood}\end{matrix}\right\} \text{x} \left\{\begin{matrix}\text{I and C Failure}\\ \text{Rate Increase}\end{matrix}\right\}^{N} \text{x} \left\{\begin{matrix}\text{I and C Risk}\\ \text{Contribution}\end{matrix}\right\} \qquad \textbf{(5.2)}$$

The increase in CDF contributions caused by a stressor can then be obtained by quantifying or estimating ranges for L and F. The equation applies for stressors that systematically degrade equipment and cause its failure rate to increase. When the stressor is assumed to occur, i.e. L=1, Equation 5.1 reduces to

$$C' = F^{N} C \tag{5.3}$$

For the purposes of the study, it was assumed that the stressor has the same effect on failure rates of all relevant components. However, if these effects differ, then the term F^N in Equation 5.1 is substituted by ΠF_i, where

ΠF_i = the product of factor increase, F_i, in failure rates of individual I&C basic events, i, affected by the stressor. **(5.4)**

For stressors that occur infrequently but that have immediate or near-immediate effects on common failures of components, and for which it is difficult to estimate the factor increase in component failure rates, C′ can be estimated based on the occurrence frequencies of these stressors and the probability of equipment failure when the stressor event occurs. If we let

f	=	occurrence frequency of the stressor event,
p	=	conditional probability of equipment failure given the event occurs,
Ti	=	detection interval for equipment failure from the event, and
u_i	=	unavailability of the ith I&C basic event in the cutset without the stressor,

then

$$C' = (\,fpTi/2\,)C/\Pi u_i \tag{5.5}$$

where the term in parentheses is the unavailability of the I&C basic events in the cutset affected by the stressor and where Πu_i is the product of the unavailabilities of the affected I&C basic events in the cutset.

In general, Equations 5.1, 5.3, and 5.5 apply where there is one dominant combination of equipment failure (i.e. one dominant minimal cutset) that contributes to the CDF. If there are several dominant combinations, then C′ is determined from each combination, that is, each minimal cutset, using the preceding formula and then summed over the contributions.

The risk-sensitivity of the stressor, S, is then the conditional increase in CDF (from some reference value, such as CDF without the stressor effects), which occurs given the stressor. In this study, S is expressed as the increase in I&C relative CDF contribution caused by the stressors to the plant baseline CDF calculated by the PRA; that is,

$$S = (\,C' - C\,)/C_{TOTAL} \tag{5.6}$$

where C_{TOTAL} is the plant baseline CDF calculated by the PRA.

The risk-significance of a set of potential stressors can thus be judged according to their risk-sensitivities, S. If the risk-sensitivity of a stressor is large, then even a small change in likelihood of occurrence can significantly change the plant risk. Conversely, if the risk-sensitivity is small, then the likelihood will need to have a large change to significantly impact plant risk.

The risk-sensitivities for a set of stressors can be presented by determining S for each stressor using the estimated values for L, C, F, and N. The relative risk-sensitivities for different stressors can then be compared, or the results can be used to identify risk-significant stressors.

Assembling Data for Evaluating Risk-Sensitivity of Stressors

Temperature

Temperature was cited in Ref. 63 as an important stressor that accelerates the degradation and failure of digital equipment. The associated component failure mechanisms are electrical shorts and open circuits. However, these failures result from sustained operation in high temperatures and not from a transient change in operational temperatures. No discussions on the short-term effects of temperature on digital equipment were identified in the literature, possibly because environmental qualifications require that equipment temperatures under normal and postulated abnormal or accident conditions do not exceed specified maximums. Ref. 63 gives a table on temperature-based conversion factors for equipment mean-time-between-failures (MTBF); however, these factors are estimated for a collection of discrete semiconductor devices and ICs and not separately for digital equipment. This table, reproduced as Table 5.1, shows the temperature dependence of MTBF. A range for maximum expected temperatures considering normal, abnormal, and accident conditions in the control building in a PWR plant is between 24 and 40°C (lower number for control room, higher number for cable spreading room or switchgear room). Assuming temperature conversion factors in Table 5.1 are bounding values for changes in MTBF of all equipment including digital microcircuits, the maximum change in MTBF over this range is approximately 1.1 or about 10%. Assuming a negligible time to repair the equipment (valid for most failures) compared to mean-time-to-failure, this translates into a change in the equipment's failure rate by a factor of approximately 1.1, where the failure rate is inverse of MTBF (assuming negligible mean time to repair equipment compared to the mean time to failure).

Table 5.1 Temperature conversion factors (by which to multiply MTBF)

From Temperature (°C)	To Temperature (°C)			
	20	30	40	50
20	-	0.9	0.9	0.7
30	1.1	-	1.0	0.8
40	1.2	1.0	-	0.8
50	1.4	1.2	1.2	-

Review of data[53] from environmental tests of digital I&C systems conducted at ORNL for temperatures of up to 71°C (160°F) gave no conclusive evidence of the dependence of short-term performance on temperature. There were some communications errors reported in these tests that, in one case, tended to increase statistically with temperature. However, the same pattern was not observed in similar tests. Consequently, no data could be extracted from the ORNL tests for risk-sensitivity analysis.

Humidity

Humidity, as an agent in the corrosion process, was cited in Ref. 64 as the largest single risk factor in the reliability of microcircuit devices. Corrosion can degrade equipments' reliability by attacking the connector pins, exposed contact surfaces, and unprotected metallization runs that serve as conductive interconnects of metal film between elements of the IC and as bonding pads for external connections. Although corrosion is an important concern for all microcircuits, it is more so for today's high-density microprocessors and other digital circuits because of their closer interconnect spacings and thinner metallic sections used to achieve the needed compactness. The failure mechanism associated with corrosion is an open circuit. Although commercial plastic-encapsulated devices are more vulnerable to moisture ingression and subsequent corrosion, this process also was reported for more robust hermetically sealed microcircuits. In the presence of appropriate contaminants, humidity can significantly reduce the service life of microcircuits. Corrosion also depends on environmental temperature which affects moisture condensation, the first step in the process. Temperature can also affect moisture permeation within the device and chemical reaction rates.

Corrosion models are given in Ref. 64 to calculate a component's time to failure. These models separate the time to failure into two time elements, the time necessary for the moisture content within the package to reach a threshold level to support corrosion, and the time needed for the corrosion process to terminate in component failure. Time needed for moisture ingress to reach threshold level is generally far smaller than time for corrosion processes to cause failure. Consequently, corrosion time to failure can be approximated by the latter. The corrosion process depends on the type of circuit package, material, and environmental conditions. Correlations were developed,[64] as shown subsequently in Equation 5.7, based on analysis of test data, which provide acceleration factors for microcircuit failure times through corrosion in terms of temperature-humidity environment. Details on the corrosion model are presented in Ref. 65. The correlation is as follows:

$$k = \frac{7.6 \times 10^{6}}{(RH)^{-3}\exp(10444/(T+273))} \tag{5.7}$$

where

k = temperature-humidity environmental acceleration factor,
RH = relative humidity in percent, and
T = temperature in °C.

Component time to failure is inversely proportional to k. Using this correlation for the temperature range and humidity levels for NPP locations of interest, Table 5.2 was generated for k. The correlation factors are normalized to control room environment (24°C and 60% relative humidity) to illustrate the effects of temperature and humidity on time to failure through corrosion. For example, if the operating temperature increases from 24 to 30°C at 60% RH, the component's time to failure is shortened by a factor of 2.01. Similarly, if the humidity level changes from 60 to 100% RH at 24°C, the time to failure is decreased by a factor of 4.63. These factors are used to modify I&C failure rates in the PRA.

Table 5.2 Factor reduction in digital microcircuit device time to failure caused by corrosion (normalized to 24°C and 60% RH)

Temperature (°C)	Relative Humidity (%)					
	50	60	70	80	90	100
24	0.58	1.00	1.59	2.37	3.38	4.63
30	1.16	2.01	3.19	4.76	6.77	9.29
40	3.49	6.03	9.58	14.31	20.37	27.94
50	9.81	16.96	26.93	40.19	57.23	78.5

Vibration and Shock

Microprocessors and other digital microcircuit devices are structurally quite rigid and hence, not very prone to vibration-induced damage at the device level. Ref. 64 cited literature to indicate that vibration forces encountered in the field are rarely severe enough to cause fatigue and damage in individual devices. Large components in assembled systems are likely to fail much earlier.

At the device level, one concern with vibration is possible bond damage. However, Ref. 64 indicates that for military ground and airborne applications, excitation frequencies encountered in the field (from ~5 to ~2000 Hz) are much lower than that necessary to excite wire bonds in these devices. Environments for microprocessor-based I&C systems in NPPs are not expected to include vibrations that are either higher in frequencies or in amplitudes than that encountered in various military applications, particularly since the latter include driven equipment often with components with reciprocating motion. Seismic frequencies that are of importance also lie in the low end of this frequency range. Control building locations in NPPs generally do not contain any significant sources of vibration. However, in some locations in the auxiliary building, there can be sources of vibration from mechanical equipment.

Information reviewed in this study did not yield any data directly relating vibration to the failure of digital equipment. However, the environmental factors reported in Ref. 63 for various categories of military applications include the effects of vibration, particularly in some airborne applications and for equipment mounted on projectiles. These environments can be taken into account in making assumptions about the possible range of vibrational effects on digital equipment in NPPs.

From a review of military application categories, the BNL study assumed that vibration for digital equipment in NPPs probably will not be worse than that for equipment installed in rotary-winged equipment [military category: airborne, rotary winged (ARW)], such as on helicopters. A low end for vibration/shock effect can be assumed as that experienced by equipment installed in vehicles on the ground [military category: ground mobile (GM)]. It also was assumed that the differences in equipment failure rates among ground-fixed (GF), GM , and ARW applications can be attributed primarily to the differences in vibration/shock in these environments. A check from Ref. 63 on the failure rates of several categories of digital equipment in GM and ARW environments, presented in Table 5.3, shows that these rates vary by a factor from less than 2 (for GM) to a factor of approximately 4 (for ARW) compared to failure rates in a GF environment (assumed no vibration/shock). Therefore, a possible range of up to a factor of 4 change in

Table 5.3 Failure rates of selected digital equipment (failures per million hours)

Equipment type		Environment		
		GF	GM	ARW
Gate/Logic Arrays:				
	Bipolar, <100 gates	.012	.024	.047
	MOS, 10000-60000 gates	.31	.53	.9
Microprocessors:				
	Bipolar, 32 bit	.23	.36	.65
	MOS, 32 bit	.34	.49	.82
Memories:				
	SRAM <16k	.022	.038	.073
	SRAM >256k, <1MB	.092	.14	.26
	DRAM <16k	.014	.027	.055
	DRAM >256k, <1MB	.032	.057	.11

Note: GF=ground fixed, GM=ground mobile, ARW= airborne, rotary winged

failure rates over the base rate is assumed for equipment in NPP locations of interest that may be caused by vibration.

Radiation

Radiation can have several effects on digital I&C equipment: degradation due to accumulated dose, upsets of memory bits or flip-flops due to an ionizing radiation, and latchup of susceptible components induced by an ionizing radiation. The effects of accumulated radiation are determined by the total dose exposure that is incurred by the equipment during an accident, or during its normal operational life. If this exposure is above the limit established for the equipment, then it can fail or perform abnormally. For I&C equipment located in control building areas, no significant dose exposure during normal operation is expected to occur. Also, since the control room is isolated and well controlled, PRAs do not identify any accidents that cause exposure in the control room. Accumulated dose tolerances for digital equipment, expressed by dose hardness levels (see Appendix A, Ref. 66), are significantly higher than that expected in control building environments (10^3 rad for a plant lifetime of 40 years). For single-event-latchup events, data presented in Ref. 67 on some CMOS devices in low-orbit space applications indicate that the device reliability may still be acceptable (device failure probability from latchup events approximately within 10% of random failure rates). Such an environment is characterized by highly ionizing cosmic rays, proton fluxes produced by solar flares, and trapped charged particles in radiation belts by the earth's magnetic field. Because digital I&C upgrade equipment are expected to be located in plant areas where there are no significant ionization sources, radiation does not appear to be a likely stressor through latchup events for these systems.

EMI

EMI events in digital I&C systems in NPPs have been documented in licensee event reports (LERs). In a study reported in Ref. 68, in which LERs for 1990 to 1993 were studied, EMI was identified as the root cause contributing to a significant number (~19%) of system malfunctions or failures. EMI was the only stressor specifically identified.

Of the EMI sources identified, a significant amount of information only for lightning-related events. Lightning is also a significant source of plant trips and engineered safety feature (ESF) actuations compared to all other sources of EMI events in NPPs.[4] Consequently, efforts were made to develop estimates of the frequency of lightning-related EMI events in NPPs to evaluate its risk-sensitivity.

In a study on surge-protecting devices in U.S. NPPs from 1980 to 1994,[69] 199 lightning-related events were reported, including loss of offsite power (LOOP), partial LOOP, and ESF actuations or equipment failures. Twenty-nine of these events could be attributed to perturbations or failures of I&C systems resulting from electrical spike or noise generated through electromagnetic couplings, and involved both digital and analog systems. The number of reactor years of operation during 1980 to 1994 for all operating U.S. nuclear plants was estimated at 1409.4 years.[69]

Because digital equipment operates at lower voltages than analog equipment (e.g., for actuating equipment), it is more vulnerable to electrical disturbances and overstress. Assuming that electrical perturbations that affect analog equipment would also affect digital equipment under similar circumstances, the frequency of lightning-related EMI events (f_{emi}) averaged over all U.S. plants can be estimated as follows.

$$f_{emi} = \frac{N_{emi}}{N_{RY}} \tag{5.8}$$

where

N_{emi} = number of lightning-related EMI events in the given period, and
N_{RY} = number of reactor years of operation during the period.

Then,

$$f_{emi} = \frac{29}{1409.4} = 2.1E\text{-}02/plant\text{-}yr \tag{5.9}$$

A conditional probability, p, of I&C equipment failure of 1.0 is assumed for these events. Such failures may be detected immediately or within a short span of time following failures, or may remain undetected for some time period. A recent study[70] based on three system-years of operational data on failures in the Eagle 21 system indicate that over 70% of these failures were detected during maintenance while the rest were detected during normal operation. For estimating risk-sensitivities, we consider two possibilities in this regard: (1) early detection, that is, failures are detected during shift checks (12 hourly), and (2) late detection, that is, failures are detected during scheduled surveillance tests [surveillance test interval (STI) = 31 days, typical for safety systems, such as the engineered safety feature actuation system (ESFAS)].[71]

The equipment unavailability, q, caused by lightning-related EMI events can then be obtained as

$$q = f_{emi} p \frac{Ti}{2} \qquad \textbf{(5.10)}$$

where

f_{emi} = definition in Equation 5.8,
p = conditional probability of equipment failure given the event, and
Ti = failure detection interval.

Then the unavailabilities are

$$q_{12hours} = 2.1E{-}02 * 1 * \frac{12}{2x24x365} = 1.4E{-}05$$

and **(5.11)**

$$q_{31days} = 2.1E{-}02 * 1 * \frac{31}{2x365} = 8.8E{-}04$$

The unavailability values estimated are the probabilities that the affected equipment will be unavailable and unable to function. The unavailabilities calculated are averages over all U.S. plants. The number of events occurring in a particular plant and, consequently, the unavailabilities, will depend on the thunderstorm activities in the region where the plant is located. To provide a perspective, in the United States, the average number of thunderstorms varies from a low of 10 per year in the northwest to as high as 100 per year in some parts of the south,[68] or a factor of 10 difference in frequency between the high and the low.

Assuming a factor of 10 difference also between high and low values of equipment unavailabilities (since f_{emi} is directly proportional to the number of lightning-related EMI events) and using $q_{12\,hours}$ and $q_{31\,days}$

calculated above as the mid-value between the high and the low, the following range is obtained for equipment unavailabilities:

$$
\begin{array}{lll}
Ti\ = 12 \text{ hours} & q_{high} = 4.4\times10^{-5}, & q_{low} = 4.4\times10^{-6} \\
Ti\ = 31 \text{ days} & q_{high} = 2.8\times10^{-3}, & q_{low} = 2.8\times10^{-4}
\end{array}
\qquad \textbf{(5.12)}
$$

This range can now be used to determine the risk-sensitivity of lightning-related EMI events.

Smoke

The environmental testing of an experimental digital safety channel by the Oak Ridge National Laboratory also included exposing the system to different densities of smoke in a chamber. The tests were conducted at the Sandia National Laboratories. Ref. 53 documents details of the tests. The system's performance was monitored during smoke exposure and for a period after smoke was vented out of the chamber. Different ambient temperature and humidity conditions were maintained in the chamber during the tests. The equipment's susceptibility was tested at three different levels of smoke densities corresponding to

- control room effects of a large cabinet fire,
- room effects of a general area fire, and
- a small in-cabinet fire.

The results from these tests were used to make assumptions about smoke-density thresholds for equipment malfunction and damage. The data from eight tests showed that the severity of the errors generally increased as the density of the smoke increased. The system experienced communication errors at all levels of smoke density, ranging from network retransmissions at low-smoke densities to serial link timeout errors at higher smoke densities. Although some of these errors possibly can be avoided in a real system through design, for risk-sensitivity evaluations, the BNL study assumed that the digital system would be vulnerable to all three levels of smoke.

The fire frequencies were used as surrogates for frequencies of smoke occurrences in relevant areas of the plant in the absence of any available estimates on the latter. Table 5.4 shows the fire frequencies in control room area developed for SURRY,[72] and used in calculating smoke risk-sensitivity in this study.

Table 5.4 SURRY fire-initiating event frequencies in control room

Estimate	Frequency (/yr)
Mean	1.8E-3
Low (5th percentile)	1.2E-6
High (95th percentile)	7.4E-3

Again, as in the case of EMI events, assuming a conditional probability, *p*, of I&C equipment failure of 1.0 from smoke events, estimates of equipment unavailability, *q*, due to smoke events can be obtained as follows

$$q = f_{smoke} \times p \times \frac{Ti}{2} \tag{5.13}$$

where

f_{smoke} = frequency of smoke events,
p = conditional probability of equipment failure given the event, and
Ti = failure detection interval.

Using the fire event frequencies given in Table 5.4 and applying Equation 5.13, Table 5.5 gives our estimates of unavailabilities of I&C equipment due to smoke in control room area for two different failure detection intervals, 12 hours (shift check) and 31 days (STI). These values are the probability that affected equipment will be unavailable and unable to perform its intended function.

Table 5.5 Estimated I&C unavailabilities from smoke events in control room

Estimate	Unavailability	
	Ti = 12 hours	*Ti* = 31 days
Mean	1.2E-06	7.6E-05
Low (5th percentile)	8.2E-10	5.1E-08
High (95th percentile)	5.1E-06	3.1E-04

Assumptions on Locations and Environments of I&C Equipment in NPPs

Environmental conditions in a NPP can be categorized broadly as those inside the containment and those in other plant areas, such as the control building and the auxiliary building. Environmental conditions in the containment areas can be very harsh with high levels of temperature and radiation. However, digital I&C equipment is generally located in the other areas where the environmental conditions are not so severe. For example, for SURRY I&C equipment that is modeled in the PRA and documented in Ref. 73, only the process sensors are located within the containment; other I&C equipment are located in the control room, relay room, and the auxiliary building. All safety-related control cabinets are located in the control building. Equipment in the control room is expected to receive negligible radiation exposure. Table 5.6, edited from Ref. 74, shows environmental conditions under normal and other situations in control building areas where the I&C cabinets may be located. The abnormal condition refers to LOOP. The accident condition is a LOCA coupled with a LOOP.

Table 5.6 Environmental conditions in selected areas of the example PWR

Area	Condition[‡]	Temperature (°F)		Humidity (%)		Radiation (rad*)
		Max.	Min.	Max.	Min.	
Main Control Room	Normal 1	75	70	60	30	1×10^3
	Abnormal 3	75	-	-	-	1×10^3
	Accident 1	75	-	60	-	1×10^3
Cable Spreading Room	Normal 1	104	55	60	3	1×10^3
	Abnormal 3	95	-	-	-	1×10^3
	Accident l	95	-	60	-	1×10^3
Switchgear Room	Normal 1	104	55	60	3	1×10^3
	Abnormal 3	104	-	-	-	1×10^3
	Accident l	104	-	60	-	1×10^3

*cumulative dose over 40 years

[‡] Normal 1: full power operating conditions

Abnormal 3: loss-of-offsite-power (LOOP) at full power operating conditions

Accident 1: loss-of-coolant-accident (LOCA) coupled with a LOOP event

Example Case

The SURRY Unit 1 Integrated Risk and Reliability Analysis System (IRRAS) PRA Data Base[75] is used in the following way in the evaluations:

- The PRA is used to generate a list of minimal cutsets.
- The minimal cutsets containing I&C basic events are then identified .
- Where environmental stressors and their levels are known for possible plant locations of digital I&C equipment, the likelihood of these stressors is taken to be 1 in calculating their effects on the increase in I&C contributions to the CDF.
- Where there is information on the effects of stressors on I&C failure rates in the form of environmental factors, the basic event probabilities are accordingly modified, and used to recalculate increases in I&C contributions to CDF.
- Where environmental stressors possibly could cause multiple I&C equipment failures, the probabilities of such failures are used to estimate unavailabilities for relevant I&C basic events, and the corresponding CDF contributions are calculated.

- The CDF contributions from each of the minimal cutsets containing I&C basic events are summed to obtain the total contribution from the affected equipment.

- The sum of the I&C contributions to CDF is divided by the plant's baseline CDF to obtain the relative changes in risk from I&C due to stressors.

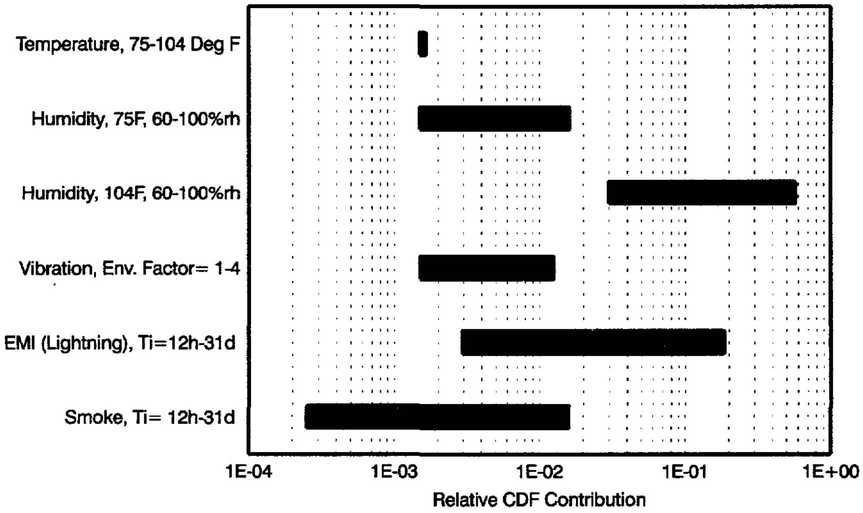
- These relative changes form the basis for screening the environmental stressors for risk-significance.

In the SURRY PRA model, the detail available for the I&C equipment is at the actuation train level. Relevant I&C components are combined together and modeled as a single basic event (actuation train); the assigned probability of failure then is the combined unavailability of the entire train.

5.2.3 Results of Risk-Based Stressor Prioritization Studies

Risk-Screening of Environmental Stressors

Figure 5.1 shows the example plant's risk-sensitivities to different environmental stressors. Details of all the assumptions made are given in Ref. 66. The figure represents relative and not absolute contributions to CDF from I&C. The risk-sensitivities of environmental stressors shown in Figure 5.1 are plotted on a scale (relative CDF contribution) where risk effects from I&C failures equal the baseline total plant CDF when the x-axis value reaches 1.0. Relative CDF contributions from stressors are shown as ranges represented by a bar. These ranges for temperature, humidity, and vibration represent variations in potential risk effects from the stressors for parametric variations in stressor levels. The ranges for lightning-related EMI and smoke represent variations in potential risk effects for average estimated occurrence-frequencies and assumed periods of detection of failed I&C equipment.



Relative CDF Contribution = CDF Contribution from I&C Cutsets /Baseline Plant CDF

Figure 5.1 Risk-sensitivities of environmental stressors in example plant

The risk-sensitivities to temperature are shown for normal control-room operation [24°C (75°F) maximum, no stressor effect], the cable-spreading room, and switchgear room [40°C (104°F) maximum, see Table 5.6]. Risk-sensitivities to humidity through corrosion are given for two different temperatures, normal temperatures in control room [24°C (75°F) maximum] and in the cable-spreading room/switchgear room [40°C (104°F) maximum], for humidity levels from 60% (maximum under controlled conditions) to a maximum of 100% under uncontrolled environmental conditions. This range in relative humidity represents situations in which air-conditioning is lost in environmentally controlled areas, such as the control room, and climatic conditions where the plant is located. Risk-sensitivities from humidity are significantly higher at the higher temperature. The results for vibration show the risk-sensitivities from a baseline, where there are no vibrations (Environmental Factor = 1), to fairly high vibrations (Environmental Factor = 4), such as would be experienced by equipment mounted on a helicopter.

The risk-sensitivities for lightning-related EMI events are shown for two different periods of detection of equipment failure from these events; shift checks and STIs, 12 hours and 31 days, respectively. Risk-sensitivities to smoke are also shown for the same two periods. In each case, the results show the plant risk-sensitivities for estimated average frequency of occurrences of these events.

The environmental stressors were screened for their potential for risk-significance from the results presented in Figure 5.1. The assessment was based on comparing the risk-sensitivities from environmental stressor-induced I&C failures. The base-case I&C relative CDF contributions, the current contributions to CDF from I&C cutsets, was the reference value used. A factor of 10, or one order of magnitude change in I&C risk contributions, was considered as constituting a significant risk-sensitivity. Use of this factor allowed an error factor of approximately 3 in the estimates of the environmental effects, with the highest order of I&C basic-event combinations in the involved cutsets being 2. Other factors may also be used to define the risk-significance of stressors.

The base-case relative CDF contribution from I&C cutsets for the example plant is 1.5 x 10^{-3} or 0.15% of the CDF. A factor of 10 over this value implies that the relative CDF contribution is at least 1.5 x 10^{-2} or 1.5% for the stressor to be considered as risk-significant. Hence, from the results in Figure 5.1, environmental stressors are categorized as risk-significant or risk-insignificant in Table 5.7.

From these results, it appears that temperature acting alone, and vibration are unlikely to be risk-significant stressors for digital I&C in a PWR. Corrosion from humidity potentially is risk-significant, more likely at higher temperatures, such as in the cable-spreading room and the switchgear room even at 60% RH, but possibly only at very high RH levels for temperature in the control room. For EMI from lightning and smoke events, using their average occurrence rates, risk-significance depends on the interval before the equipment's failure is detected, and is significant for *Ti* = 31 days but insignificant if they are detected within *Ti* = 12 hours. This conclusion still holds for bounding estimates from EMI events from lightning, which account for uncertainties in its occurrence rates. For smoke events in the control room, the conclusion holds for *Ti* = 12 hours, that is, the stressor is not risk-significant even when bounding estimates account for uncertainties in occurrence rates.

Sensitivity of the Stressor Risk-Screening Results to Specific Assumptions

The risk-sensitivity results presented in the previous section include two implicit assumptions:

(a) equipment failures are all critical to system functions, that is, prevent the system from performing its functions, and

Table 5.7 Risk-screening of environmental stressors in example plant

Stressor and Level	Risk from Stressor	
	Insignificant	Significant*
Temperature, 75–104°F	✓	
Humidity, 60–100% @ 75^{0}F		✓
Humidity, 60–100% @ 104°F		✓
Vibration, Env. Factor 1–4	✓	
EMI from Lightning, avg. occ. rate	for *Ti* = 12 hours	for *Ti* = 31 days
Smoke, Control Room, avg. occ. rate	for *Ti* = 12 hours	for *Ti* = 31 days

*At least a factor of 10 increase in relative CDF contribution from I&C over the base-case value
Ti = interval for detecting equipment failures from lightning and smoke

(b) equipment failures are not detected until the next scheduled test, that is, the self-diagnostic capabilities of the digital systems are ignored.

The assumptions give conservative results. The sensitivity of the estimated stressor risk-effects to these two assumptions were analyzed in the BNL study; specifically, to the fraction of failure events that may be critical for the system's function and to the probability of detecting such failures by the system's self-diagnostic features. From the risk-screening results, the following conclusions were made about the stressor's risk effects involving digital I&C:

(1) Temperature at the I&C cabinet locations in the example plant does not appear to be a risk-significant stressor.

(2) Vibration at the levels noted also appears to have no significant risk-effects.

(3) Humidity could be a significant stressor at cable-spreading room and switchgear-room temperatures; however, at control-room temperatures, humidity does not appear to be potentially risk-significant except at very high levels.

(4) EMI from lightning can be potentially a risk-significant stressor for digital I&C systems; however, the risk-significance clearly depends on the interval before equipment failure is detected.

(5) Under the assumptions made in the study, smoke also appears to have the potential to significantly increase relative risk contributions from digital I&C systems; again, such risk depends on the interval before failure is detected.

We reiterate that bounding assumptions in the BNL study were made in the risk-sensitivity evaluations involving lightning-induced EMI and smoke as stressors. Consequently, the risk-screening results should be seen only as potential effects.

5.2.4 Findings and Conclusions From the BNL Study

A review of military data in the BNL study showed that limited information is available on the effects of stressors on digital equipment at the component level. The stressors identified in the military data were temperature, humidity, shock/vibration, and radiation. In reporting the failure rates of equipment in different environments, operation under sustained levels of stressors is assumed. The environmental effects reported are generally synergistic. Since application environments for the military differ from environments within NPPs, such information and data must be adapted for the risk-screening of stressors in NPPs.

The review of NPP operating experience identified EMI/RFI as a stressor. The principal sources of the EMI/RFI were lightning, welding near I&C equipment, sources internal to the equipment, and poor grounding as a causal factor. Furthermore, the failure rates of digital equipment in NPPs appear to be higher than those reported by the military. However, the differences could not be attributed to any specific factor since the quality requirements for military hardware are generally higher than those for commercial-grade equipment used in NPPs. For electronic equipment in general, the military reported a factor of 5 difference in MTBF between military quality equipment and commercial equipment,[63] with the latter having the shorter MTBF; this translates roughly into a factor of 5 higher expectation in failure rates of commercial equipment compared to military quality equipment. An overall estimate of failure rate of all digital equipment in NPP environments from Nuclear Plant Reliability Data System (NPRDS) data shows that this estimate is comparable to the Asea Brown Boveri Combustion Engineering (ABB-CE) experience,[†, 76] with a factor of approximately 3 lower for processors and memory and a factor of approximately 7 higher for input/output units.

In reviewing the failure modes of digital I&C systems, the study identified several incidents of spurious operation of such systems in NPPs. However, these events generally led to more conservative plant configurations through inadvertent and unneeded operations of safety systems. None of these events resulted in failure of the system to perform its essential safety functions. In only one event identified in Ref. 76, a software deficiency in a digital I&C-based protection system caused the system to fail to set a trip output. Nevertheless, the trip was accomplished through a redundant trip output. In some instances of stressor effects, multiple redundant equipment were affected. Such failures are an important concern for plant risk considerations because of the possibility of loss of redundancy in safety systems.

The risk-screening results for the stressors in the example plant, subject to the bounding assumptions, indicate that humidity, EMI from lightning, and smoke can be potentially risk-significant. The risk-significance of EMI from lightning and smoke are sensitive to the periods before equipment failure is detected. If failures are detected only during the surveillance tests (*Ti* = 31 days), these stressors can be risk-significant even when only critical failures are considered and credit is given for detecting some failures through system self-diagnostics. For shorter detection periods, however, these two stressors may not be risk-significant. The results also show that the risk effects of some stressors, such as humidity, can be sensitive to the location of the equipment. For the levels of stressors analyzed, risk effects from

[†] Since 1980, Combustion Engineering plants have been using digital computer-based systems along with analog systems for reactor protection functions. The system was initially based on 16-bit computers but a more recent version uses 32-bit hardware. Reference 74 shows the performance statistics of digital elements of the system based on 67 reactor years of operating experience.

temperature in digital I&C equipment locations, and that from assumed levels of vibration, appear to be insignificant.

Evaluations of stressor risk-sensitivities used existing I&C models in the PRA, and only one plant was used in the screening analysis. Nevertheless, the risk-screening application demonstrates the usefulness of the BNL approach in identifying environmental stressors that have the potential to be risk-significant. In practice, plant-specific variations are expected in implementing digital I&C systems. Variations in the choice of equipment, its complexity, layout of the system, plant-specific locations, and levels of stressors in those locations may influence the overall risk impacts of the stressors, as well as their relative impacts on plant risk. Such information must be incorporated in risk evaluations to address specific concerns with implementing digital I&C systems.

5.3 ORNL Study: Environmental Effects Testing of an Experimental Digital Safety Channel[†]

This study, performed by ORNL, investigated failure modes and vulnerabilities of microprocessor-based technologies when subjected to the environmental stressors of EMI/RFI, temperature, humidity, and smoke exposure. The effect of smoke exposure on digital equipment was of particular interest because this stressor had not previously been considered in analog safety system qualification testing.

5.3.1 Scope of Study

An objective of the study was to identify failure modes and vulnerabilities that are associated with advanced digital systems. The study sought to determine experimentally the characteristic effects caused by environmental stressors using a system that is *representative* of advanced trip system designs. The tests examined stress levels at which failures began and attempted to quantify the severity of consequences for advanced trip systems.

Ranges of stress were selected at a sufficiently high level to induce errors so that failure modes characteristic of the technologies employed could be identified. Subsystems of the Experimental Digital Safety Channel (EDSC) assembled for the tests included computers, electrical and optical serial communication links, fiber-optic network links, analog-to-digital and digital-to-analog converters and multiplexers. In addition, the trip system design was typical of ALWR and/or some retrofits in the areas of chip fabrication and packaging technology used, temperature ratings and reliability stress tests used during component quality assurance procedures, subsystem functions and communication protocols, and expected memory/board density.

5.3.2 Approach

Test System Description

A block diagram of the EDSC is presented in Figure 5.2. It consists of two major functional subsystems: the test system (i.e., the equipment under test) and the control system. The test system represents a single channel of an advanced reactor protection system, based on ALWR designs, and consists of the process

[†] Research performed for the NRC Office of Nuclear Regulatory Research by ORNL.[53]

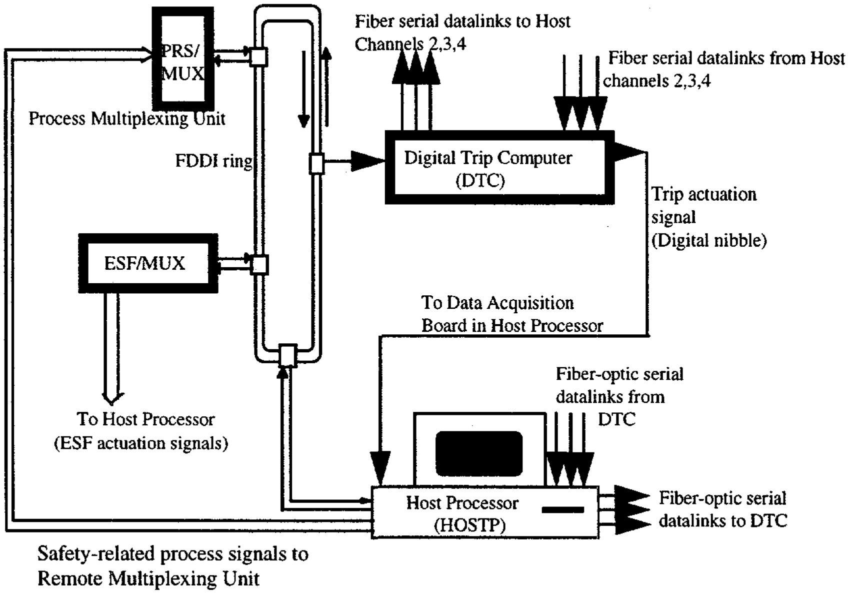

Fiber serial datalinks to Host Channels 2,3,4
Fiber serial datalinks from Host channels 2,3,4
PRS/ MUX
Process Multiplexing Unit
FDDI ring
Digital Trip Computer (DTC)
Trip actuation signal (Digital nibble)
ESF/MUX
To Data Acquisition Board in Host Processor
Fiber-optic serial datalinks from DTC
To Host Processor (ESF actuation signals)
Host Processor (HOSTP)
Fiber-optic serial datalinks to DTC
Safety-related process signals to Remote Multiplexing Unit

Figure 5.2 Block diagram of the experimental digital safety channel

multiplexing unit (PRS/MUX), a digital trip computer (DTC), and an engineered safety feature multiplexing unit (ESF/MUX). The test control system stimulates the test scenarios (i.e., generates analog signals corresponding to various postulated reactor conditions), simulates the other three channels of a reactor protection system (some advanced designs include isolated interchannel communication for trip voting), and monitors and logs the performance of the test system during environmental testing. The host processor (HOSTP) performs the test control functions.

The function of the PRS/MUX is to acquire process analog signals, digitize these data, and format them into frames suitable for transmission over a fiber distributed data interchange (FDDI) network. In the EDSC implementation, these process analog signals are generated by a 16-channel digital-to-analog (D/A) plug-in card inside the HOSTP, rather than by actual field instrumentation such as transmitters.

The DTC polls the network to acquire the digital values of the process signals from the PRS/MUX. It then compares individual process values with trip set point values and sends a trip/no trip indication for each variable over three independent fiber-optic serial datalinks (i.e., fiber-optic modules) to the HOSTP. At the same time, the Host Processor sends trip/no trip information for each variable to the DTC via three independent serial datalinks. The DTC performs 2-out-of-4 voting (local coincidence) on each set of process trip/no trip information received (note that for each process parameter, the DTC votes on four trip/no-trip data sets—one calculated from the PRS/MUX process data received via the FDDI network and three received from the HOSTP via the serial datalinks).

The ESF/MUX demultiplexes the digital information sent by the HOSTP via the FDDI network into the appropriate analog signals. In this way, it simulates engineered safety system actuation signals.

The HOSTP acts as a test monitoring and error logging system, but also simulates the data communication and interface functions typically performed by the other three divisions of a reactor protection system.

Implementing the system in this way enables one complete channel, its interfaces, and its interactive behavior with other channels, to be tested while at the same time considerably reducing the cost of the experimental system.

System Behavior and Failure Identification Methodology

Most failures of electronics components and systems fall into one of the following categories:[68] (a) hard failures, (b) upsets,[77] and (c) latent failures.[78] Of particular interest in the study were temporary or intermittent upsets caused by environmental stressors and how these upsets were likely to affect a digital trip system's performance. At the component level, some of the failure mechanisms associated with ICs include cracked substrate, loss of hermetic seal, short circuits, and changes in leakage current and offset voltages (see also Table 2.1). At the board or system level however, the effect of component upsets and failures include data errors caused by bit changes in memory cells, communication failures, processor lock-up, and interface failures (e.g., timeouts on serial interfaces). To relate the system upsets and failures observed in the tests to generic potential *consequences* in a digital trip system, the study classified all errors into five consequence categories: (A) critical failures, (B) potentially unsafe failures, (C) conditionally safe failures, (D) latent failures, and (E) fail-safe failures. For the short-term effects considered, failure category A was considered to be the most serious, while failure category E was the least serious. As explained below, failure category A will almost certainly result in loss of functionality of the associated safety channel; failure category B has a high probability of resulting in loss of functionality; failure categories C and D may not necessarily cause loss of functionality, and failure category E *will not* result in loss of functionality. In this regard, it is important to realize that, in a redundant system such as a reactor protection system, an error that leads to any of these failure categories will not necessarily prevent the entire safety system from performing its function, unless there is a common-mode failure in two or more redundant channels of the system.

A: Critical Failure

This is an upset in a component or module that will almost certainly prevent a safety-related channel from performing its function if and when required to do so. That is, the upset can cause the channel to fail in an unsafe manner. For example, during the tests, EMI-induced upsets (from sparkers used to ignite fuel to generate the smoke) were suspected to have caused the digital actuation nibble (4-bit) output from the DTC to give erroneous results.

B: Potentially Unsafe Failure

This is an upset in a component or module that is likely to prevent a channel from performing its intended function. However, the adverse effect of such an upset can usually be offset in a typical power plant safety system by engineering design. For example, during the stressor tests, a number of serial and network communication timeouts occurred due to parity and overrun errors. In an actual safety system, the effect of such timeouts would be offset by automatically placing the channel in a tripped state.

C: Conditionally Safe Failure

This is an upset in a component or module that has the *potential* to prevent a channel from performing its function. However, the affected component or module recovers in time for the required function to be performed without exceeding the channel response time requirements. For example, during the stressor tests, the DTC had to retransmit data on the network on several occasions due to lack of acknowledgment by the receiveing unit for messages sent. A conditionally safe failure, if it persists, will lead to a potentially unsafe failure.

D: Latent Failure

This is an upset in a component or module that will typically not prevent a channel from performing its function in the presence of the stressor causing the upset. However, failure may occur at a future date long after the stressor has been removed. Examples are changes in leakage current, pulse rise and fall times, and other component parameters that nevertheless remain sufficiently within tolerance for the affected channel to perform normally for some time. It was impractical in the study to thoroughly investigate latent failure effects. Therefore, no errors were attributed to this category during the course of this investigation, which included a two-month monitoring period after the conclusion of the environmental tests.

E: Fail-Safe Failure

This is an upset in a component or module that places the channel in a tripped or safe state. A possible example is the digital output nibble being stuck in a tripped state.

Table 5.8 illustrates generic environmental stressor-induced upsets in digital systems and their potential consequences in terms of the classification scheme used in this report. The table also lists some specific examples of the generic stressor-induced upsets that were observed with the EDSC.

Test Procedures

EMI/RFI Tests

Electromagnetic interference/radio-frequency interference tests were performed on the EDSC according to applicable test criteria and methods stipulated in Military Standard (MIL-STD) 461C[79] and MIL-STD 462[80] respectively. MIL-STD 461C establishes the military's emission and susceptibility requirements for electronic, electrical, and electromechanical equipment and subsystems. It also provides a basis for evaluating the electromagnetic characteristics of equipment and subsystems by setting operational acceptance criteria. The test methods corresponding to the MIL-STD 461C requirements are described in MIL-STD 462.

The objective of the EMI/RFI tests was to identify/confirm EMI/RFI-induced upsets and failure modes in a microprocessor-based safety system, and also to have a basis for comparing the likely effects of EMI/RFI-related upsets to other environmental effects such as smoke exposure. The tests were *not* intended to ascertain whether the EDSC met emissions criteria. Thus, only applicable susceptibility criteria were used in the tests. The tests performed are the following:

CS01 - Conducted Susceptibility, Low Frequency (evaluates response of equipment to EMI/RFI present on the power leads in the frequency range 30 Hz to 50 kHz).
CS02 - Conducted Susceptibility, High Frequency (similar to CS01 except that it covers the higher frequency range from 50 kHz to 400 MHz).
CS06 - Conducted Susceptibility, Spikes (evaluates response of equipment to spikes on the power leads).
RS01 - Radiated Susceptibility, Magnetic Fields; (evaluates response of equipment to radiated magnetic fields in the frequency range 30 Hz to 50 kHz).
RS02 - Radiated Susceptibility, Spikes (evaluates the response of the equipment to radiated magnetic and electric fields generated by spikes and power line frequency current).
RS03 - Radiated Susceptibility, Electric Fields (evaluates the response of the equipment to radiated fields in the frequency range from 14 kHz to 1 GHz).

Table 5.8 Generic environmental stressor-induced upsets in digital systems and their potential consequences for safety systems

GENERIC STRESSOR-INDUCED ERRORS IN DIGITAL SYSTEMS	SOME PLAUSIBLE OR ACTUAL EXAMPLES OBSERVED WITH EDSC	CONSEQUENCE CLASSIFICATION
Permanent component/board failures and upsets that lead to unintended and unsafe digital actuation errors.	EMI-induced upsets were suspected to have caused the DTC digital actuation nibble to give erroneous result.	Critical Failure
Component/module upsets that are likely to prevent a channel from performing its function, but whose adverse effect in an actual plant safety system can typically be offset by engineering design.	Serial and network communication timeouts occurred due to parity and overrun errors.	Potentially Unsafe Failure
Component/module upsets that have the *potential* to prevent a channel from performing its function. However, the affected component or module recovers in time for the required function to be performed without exceeding the channel response time requirements.	The DTC had to retransmit data on the network on several occasions due to lack of acknowledgment of messages sent.	Conditionally Safe Failure
Component/module upsets that will typically not prevent a channel from performing its function in the presence of the stressor causing the upset. However, failure may occur at a future date long after the stressor has been removed.	Changes in leakage currents, noise margins, rise and fall times, and other component parameters that nevertheless remain within tolerance for the affected channel to perform normally. (NOTE: the tests were not designed to thoroughly investigate latent failures.)	Latent Failure
Component/module upsets that places the safety channel in a tripped state.	Digital nibble output stuck in a "tripped state". (NOTE: While this is a plausible example that could have occurred in the EDSC, the phenomenon was not actually observed.)	Fail-Safe Failure

Temperature/Humidity Tests

A total of 16 elevated temperature/humidity tests were performed; eight of these were performed with the PRS/MUX as the Equipment Under Test (EUT) and eight with the DTC as the EUT. With the process multiplexing unit as the EUT, temperature tests at 30% RH were performed at 38°C (100°F), 49°C (120°F), 60°C (140°F), and 71°C (160°F). The tests were then repeated at the same temperature values, but at a relative humidity of 85%. Both test sequences were then repeated using the digital trip computer as the EUT.

The maximum test temperature of 71°C (160°F) was used for three reasons. First, this value is at a sufficiently high level (taking into account the operating limits of the systems comprising the EDSC) to induce errors so that failure modes, which are characteristic of the technologies employed, could be identified. Second, it is well beyond what the channel is likely to experience in a normal NPP (control room) environment. Third, it is comparable tó the temperature limits used by some manufacturers in qualifying safety equipment for control room environments. [In a typical control room environment, one manufacturer postulates that the loss of heating ventilation, and cooling will increase the temperature in the control room to about 40°C (104°F). Qualification testing is performed to about 50°C (122°F), while the actual environmental temperature ratings of the system and/or components are typically about 75°C (167°F). This qualification methodology is typical of reactor manufacturers and suppliers.]

The general procedure followed was to obtain data for about 18 hours at the baseline temperature and humidity, then increase only the temperature to the next test value. The EUT was then monitored at this new steady-state test value for a period of 4 hours. The temperature was then reduced to the baseline value and monitoring was continued for an additional 18 hours, after which the temperature was raised to the next test value. The purpose of running a baseline test before each elevated temperature test was to account for any short-term synergistic effects due to the previous elevated temperature tests.

Smoke Exposure Tests

Based on credible smoke exposure scenarios evaluated by Nowlen,[81] three different smoke loads corresponding to three different fire threat scenarios were used for these tests. The smoke loads used are defined as follows:

Small In-Cabinet Fire: In this scenario, only a small fire (confined to 5-15% of the available fuel within the panel) is postulated. In this case, the other non-involved components may not be damaged by the effects of heat and flames but would be exposed to the smoke generated during the fire. The smoke loads for this scenario are most severe because of the relatively small enclosed volume and high fuel loadings found to be typical of nuclear plant control panels. A smoke load of 26-560 g/m^3 was identified for this scenario. For the ORNL tests, a moderate smoke load of 160 g/m^3 was used. Earlier work has shown that through-hole electronics can be reconditioned, with good results, after deposition of up to 100 µg chloride/cm^2 in the surrounding area.[62] The lower limit for when cleaning is needed is often specified to be 10 µg chloride/cm^2. For comparison, analysis of our smoke load of 160 g/m^3 showed the chloride deposition to be 742 µg chloride/cm^2. [The chloride content of smoke from burned cable is significant because when combined with water (from a humid environment), the chloride will form hydrochloric acid, which may dissolve minute, but significant, conducting substrate material.]

Large Control Room Panel Fire: The smallest smoke load postulated by Nowlen is associated with the effects of a large cabinet fire on the general environment within a control room. In this scenario, it is assumed that the fire source is a fully involved electrical panel, and hence it is assumed that all of the components within the burning cabinet would be destroyed by direct thermal effects. This scenario was considered by Nowlen to represent the most severe fire that might be experienced in the main control room. Nonetheless, the relative density of the smoke exposure for this scenario is significantly lower than that of the small in-cabinet fire because it is assumed that the smoke would be distributed throughout the much larger volume of the control room. Based on a consideration of both typical control panel fuel loads and typical control room air volumes, Nowlen estimated the smoke load for this scenario to be from 2.8-11.2 g/m^3. For the ORNL tests, a smoke load of approximately 3 g/m^3 was used to simulate this scenario. Analysis of the smoke deposition showed the circuit board chloride surface contamination to be about 29 µg chloride/cm^2.

Significant Fires in General Plant Areas: This scenario is intended to be representative of the types of fires that might take place in general plant areas where advanced digital systems might be housed. This would include areas such as relay rooms, cable penetration rooms, cable vault and tunnel areas, etc. It was *not* intended to represent very large plant areas such as the turbine hall. The smoke load for this scenario falls between the two previous scenarios and was estimated by Nowlen to be 14-56 g/m^3. For the ORNL tests, a smoke load of 20 g/m^3 was used to simulate this scenario. Analysis of this smoke load showed the chloride deposition on the boards to be about 57 µg chloride/cm^2.

A total of ten tests were performed on the PRS/MUX subsystem, the DTC subsystem, and the Fiber-Optic Modules (FOMs). These included three tests designed to simulate and study the short term effects of fire suppression—the increase in humidity (in the presence of smoke) and the presence of carbon dioxide from a fire extinguisher. The general procedure adopted for the tests is as follows:

1. The EUT was placed in the exposure chamber and baseline data was obtained over a period of about 3 hours. The environmental chamber was maintained at 24°C (75°F) and 30% RH during this time.

2. A predetermined mixture of different types of cables was burned to produce a desired smoke density in the exposure chamber. (NOTE: Experience showed that the cables completely burned in about 5 min.)

3. In the case where the test called for smoke and humidity, a predetermined amount of water was boiled off inside the exposure chamber, 15 min. into the test, to provide 85% RH.

4. The EUT was exposed to the smoke for a total of 1 hour. The smoke was then vented from the exposure chamber.

5. The EUT was left in the exposure chamber and monitoring continued for approximately 20 hours. Chamber temperature was maintained at approximately 24°C (75°F) and 30% RH.

6. The EUT was examined for damages/malfunctions and thoroughly cleaned. Cleanup consisted of first removing the electronic boards and blowing the deposited, non-sticky soot off with compressed air. The boards were then sprayed with Tech Spray no. 1677-125 Universal Cleaner Degreaser or Chemtronics Electronics Cleaner/Degreaser 2000. The exposure chamber was also thoroughly cleaned and made ready for the next test.

5.3.3 Results of Environmental Stressor Effects Testing

Summary of EMI/RFI Test Results

Of the six different EMI/RFI susceptibility tests performed, the EDSC and its interfaces were found to be least susceptible (no errors) to radiated magnetic fields in the range 30 Hz to 30 kHz (RS01 tests). Most of the errors were found to occur with the conducted spike tests (CS06) and the radiated electric field tests (RS03).

Results of electric field tests (RS03) of the EDSC showed that the equipment was not susceptible to EMI/RFI effects at frequencies below 10 MHz. At frequencies between 10 and 200 MHz, the errors observed occurred at field strengths that are higher (above 20 V/m) than what is typical of NPP environments.

High-voltage spikes on power leads were found to cause a greater number of upsets and within a relatively short time (i.e., seconds) as compared to low-voltage, sinusoidal root-mean-square (rms) noise on the same power leads. In the latter case, errors did not occur until several minutes into the application of the noise voltage. These results are consistent with expectations, since EMI/RFI-related upsets/failures are typically caused by the EMI/RFI inducing a high enough voltage to cause malfunctions such as false triggering of digital devices, inadvertent bit changes in memory devices, or breakdown of on-chip protection. If an EMI/RFI burst is going to have an effect via these mechanisms, it is reasonable to expect it to do so in a relatively short time within the application of the EMI/RFI burst.

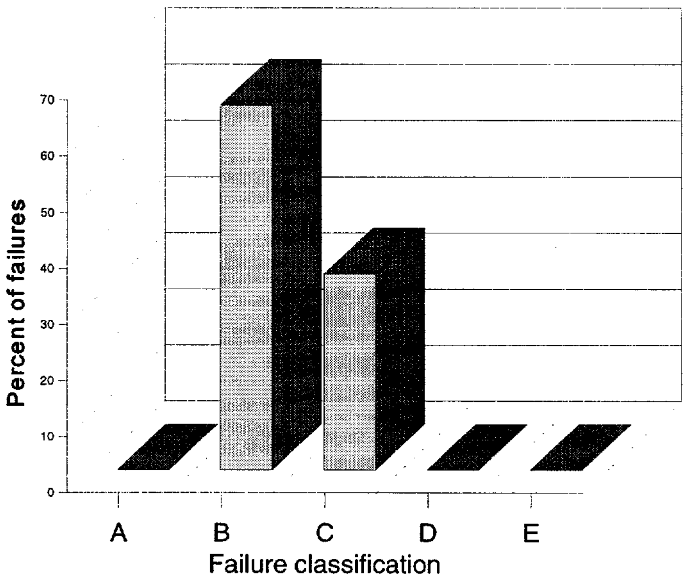
Although the EDSC test demonstrated system-level effects for both conducted and radiated EMI, the commercial components used exhibited greater susceptibility to conducted EMI. This observation is consistent with general industrial experience by European EMI experts. It should be noted that the relative susceptibility of particular systems can be mitigated by grounding, shielding, isolation, and surge withstand practices.[82]

Failures encountered during the EMI/RFI tests are shown in Figure 5.3, as a function of the failure classifications used in this paper. Most of the upsets resulted in categories B or C failures. Indeed, the EMI/RFI tests produced the only permanent failure of the EDSC. (A multiplexer power supply failed at 72 V/m, 20 MHz. This failure occurred at a level much higher than what is typical of NPP environments. The power supply was replaced and the tests continued.) In all other cases, the EDSC was able to recover after the source of the malfunction was removed and/or the system was rebooted and, thus, acquisition of baseline data taken before the application of each each subsequent stress level showed no degradation or residual effect. Therefore, no errors were attributed to undetected permanently degraded components (failure category D).

Since it is possible to prevent both failure categories B and C by engineering design, we conclude that given adequate quality assurance, qualification and/or commercial item dedication, as well as surveillance and testing schedules, present-day microprocessor-based equipment are likely to perform their safety functions satisfactorily in the EMI/RFI environments typically found in NPP environments.

Summary of Temperature/Humidity Test Results

The major subsystems of the EDSC—the industrial computers, the fiber-optic line drivers, and the A/D modules of the PRS/MUX unit—all had different environmental temperature specifications. This afforded the opportunity to investigate the effect of temperature/humidity stressors on various I&C subsystems as they approached and exceeded their rated temperature specifications. For example, the FOMs failed to perform their communication functions when the test temperature was about 8°C (15°F) below their maximum rated operating temperature of 55°C (115°F). At the higher relative humidity (85%), some of the A/D modules in the PRS/MUX failed temporarily when test temperatures reached 59°C (120°F), which is 11°C (20°F) below their maximum rated operating value [60°C (150°F) at 95% RH]. The computer systems did not fail, and it is interesting to note that the maximum temperature achieved [71°C (160°F)] during the tests was 21°C (38°F) *above* the manufacturer's maximum rating of 50°C (122°F) at 95% RH, noncondensing. These observations underscore the need to qualify commercial-grade components regardless of the manufacturer's advertised equipment ratings. Note that the temperature specifications indicated here are ambient temperatures for the *equipment* involved, not the components in the equipment. During equipment design, the maximum temperature rating of the individual components are taken into account. This maximum temperature rating would have been already determined by the semiconductor manufacturer. By ensuring that the operating point (voltage, current) is well below that which will give rise to a temperature exceeding the maximum junction temperature of each component, the *equipment* manufacturer will have reasonable assurance that the equipment as a whole will perform its function as long as the ambient temperature is below some specified value. In other words, if equipment is stated to function at some ambient temperature, the claim implies that the operating conditions—component voltage, current, and maximum allowable junction temperature, etc.—should already have been taken into account during design and verified through functional testing. The point of this discussion is to emphasize the value of the concept that is the basis for environmental qualification, which is that equipment compatibility with its intended environment should be verified through testing or other means.



(a)

Failure classifications used in (a)

FAILURE CATEGORY	DESCRIPTION	NUMBER OF ERRORS IN FAILURE CATEGORY	PERCENT OF ERRORS IN FAILURE CATEGORY
A	Critical failure	0	0
B	Potentially unsafe failure	55	65
C	Conditionally safe failure	30	35
D	Latent failure	0	0
E	Fail-safe failure	0	0

(b)

Figure 5.3 Summary of EMI/RFI test results as a function of failure classification

Elevated temperature at low relative humidity did not cause failures in the EDSC. Because of the EDSC's similarity to advanced safety systems with regard to chip fabrication and semiconductor manufacturer stress screening tests, we judge that elevated temperature (e.g., due to loss of heating, ventilation, and air conditioning (HVAC)] at low relative humidity is unlikely to cause catastrophic failures in a microprocessor-based safety I&C system located in a mild environment, provided that the equipment's performance can be demonstrated through functional testing.

Due in part to experience gained from stress tests routinely performed by semiconductor manufacturers, the reliability of current digital *components* appears to be such that system vulnerability to degraded performance, rather than catastrophic failures, is the likely result of temperature/humidity stresses on microprocessor-based systems in controlled environments. Consideration of these effects during design can address the consequences of these upsets so that fail-safe conditions will result.

With regard to temperature and humidity, the study found that the combination of high temperature at high relative humidity was the condition to affect the EDSC, rather than temperature acting alone. High relative humidity is not likely in a controlled environment such as a control room, but still needs to be considered in qualification, especially for postaccident equipment.

Failures encountered during the temperature/humidity tests, as a function of the failure classifications used in the document, are shown in Figure 5.4. All the upsets resulted in categories B or C failures. No permanent failures occurred. Also, as in the case of the EMI/RFI tests, there were no processor lock-ups, and the EDSC was able to recover each time after the source of the malfunction was removed. Thus, no errors were attributed to permanently degraded components (failure category D).

Since it is possible to prevent both failure categories B and C by engineering design, we conclude that given adequate quality assurance, qualification and/or commercial item dedication, as well as surveillance and testing schedules, present-day microprocessor-based equipment are likely to perform their safety functions satisfactorily under normal and abnormal ambient conditions in the locations in which microprocessor-based safety systems are likely to be placed (e.g., control room).

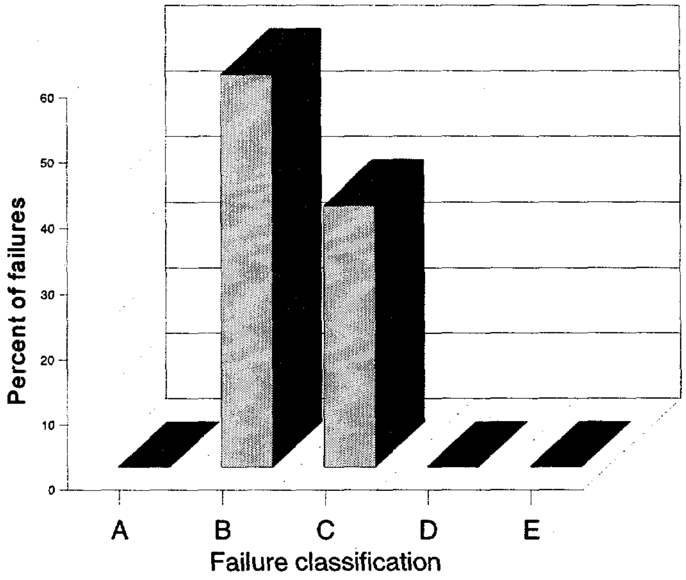
Summary of Smoke Exposure Tests

Several conclusions are suggested by the smoke test results:

(1) Smoke can cause circuit bridging and thereby affect the operation of digital equipment. Because the circuit board edge connections and interfaces are typically uncoated, the most likely effect of the smoke is to impede communication and data transfer between subsystems. These effects are likely to be temporary, however, and with appropriate software could be compensated by repeated attempts to transfer data or by tripping the affected channel in the case of a safety system.

(2) The solder mask on commercial electronic boards appears to be an effective mechanism in preventing catastrophic and/or permanent failure of the board, even when exposed to a high level of smoke. Since none of the boards used in these tests had conformal coating, no conclusions can be drawn as to any possible increase in protection with the use of conformal coating .

(3) During the exposure tests for various smoke densities, upsets for the EDSC typically were not encountered until about an hour into the exposure interval. Of particular note, the EDSC did not lose functionality when exposed to smoke equivalent to a large control room panel fire (smoke



(a)

Failure classifications used in (a)

FAILURE CATEGORY	DESCRIPTION	NUMBER OF ERRORS IN FAILURE CATEGORY	PERCENT OF ERRORS IN FAILURE CATEGORY
A	Critical failure	0	0
B	Potentially unsafe failure	3	60
C	Conditionally safe failure	2	40
D	Latent failure	0	0
E	Fail-safe failure	0	0

(b)

Figure 5.4 Summary of temperature/humidity test results as a function of failure classification
(NOTE: All failures occurred at 85% RH)

density of about 3 g/m^3). A large control room panel fire has been postulated by Nowlen[81] as the most likely severe fire that might be experienced in the main control room. (In this scenario, a whole panel burns, all equipment within the panel is destroyed, and the smoke from this fire is dispersed throughout the control room. Because the smoke under this scenario was postulated to be uniformly distributed throughout the entire main control room, this represents the smallest smoke density of the three fire scenarios postulated in the Sandia study. Larger smoke densities were postulated for scenarios involving small panel fires with the smoke contained within the panel and for equivalent fires in small volume spaces.) Because of similarities between the EDSC and digital safety systems with regard to circuit board and chip fabrication and packaging, it is reasonable to postulate that commercial digital equipment will likely maintain functionality during its initial period of exposure to smoke equivalent to a large control room panel fire unless any of the equipment is contained in the burning panel or in close proximity to the fire source. Given early detection of a fire and subsequent application of fire suppression measures, digital systems should maintain functionality (to allow safe shutdown) for as much as an hour or more following exposure, provided that the equipment is not directly exposed to the fire.

(4) Humidity may be an important factor in creating temporary short circuits. The adverse effect of the humidity is likely to increase at higher smoke density levels, but this hypothesis was not tested experimentally.

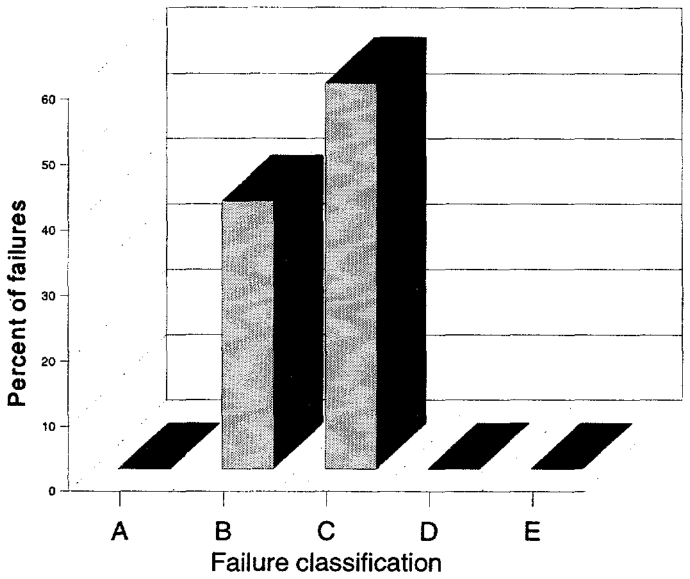
(5) The smoke exposure tests have shown that the important failure mechanisms are not only long-term effects such as corrosion, but also short-term and perhaps intermittent effects such as erratic operation due to circuit bridging.

The failures as a function of the failure classifications used in the study are shown graphically in Figure 5.5. Here again, as in the previous stress tests, the worst case vulnerabilities encountered resulted in potentially unsafe failures. Ongoing research indicates that implementation options such as chip packaging and circuit board coating can reduce the susceptibility of microprocessor-based equipment to smoke-induced failures.[56] This suggests that, using industrial-grade components and engineering design methodologies (e.g., packaging techniques to reduce ingress of smoke particulates, etc.), it is possible to design robust digital safety equipment for the most severe smoke exposure anticipated in the control room under accident conditions.

5.3.4 Conclusions from the ORNL Study

Overall findings from the environmental tests are the following:

(1) Interfaces were found to be the most vulnerable elements of the EDSC. The majority of effects resulting from the application of the stressors were communication errors, particularly for serial communication links. Many of these errors were intermittent timeout errors or corrupted transmissions, indicating failure of a microprocessor to receive data from an associated multiplexer, optical serial link, or network node. Because of similarities in fabrication and packaging technologies, other digital safety systems are likely to be vulnerable to similar upsets. As was experienced with the EDSC, intermittent component upsets will typically impede communication, either on 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 digital interfaces to environmental stress.



(a)

Failure classifications used in (a)

FAILURE CATEGORY	DESCRIPTION	NUMBER OF ERRORS IN FAILURE CATEGORY	PERCENT OF ERRORS IN FAILURE CATEGORY
A	Critical failure	0	0
B	Potentially unsafe failure	7	41
C	Conditionally safe failure	10	59
D	Latent failure	0	0
E	Fail-safe failure	0	0

(b)

Figure 5.5 Summary of smoke exposure test results as a function of failure classification

(2) Based on incidence of functional errors observed during testing, EMI/RFI, smoke exposure, and high temperature coupled with high relative humidity, in that order, were found to be the most significant of the stressors investigated. The most prevalent stressor-induced upsets, as well as the most severe, were found to occur during the EMI/RFI tests. For example, these tests produced the only permanent failure of the EDSC (i.e., power supply).

(3) Although the EDSC test demonstrated system-level effects for both conducted and radiated EMI, the commercial components used exhibited greater susceptibility to conducted EMI. This observation is consistent with general industrial experience voiced by European EMI experts. It should be noted that the relative susceptibility of particular systems can be mitigated by grounding, shielding, isolation, and surge withstand practices.[82]

(4) With regard to temperature and humidity, the study found that the combination of high temperature at high relative humidity was the condition most likely to affect the EDSC, rather than temperature acting alone. High relative humidity is not as likely in a controlled environment such as a control room, but still needs to be considered in qualification, especially for postaccident monitoring equipment.

(5) For smoke exposure, important failure mechanisms are not only long-term effects such as corrosion, but also short-term and perhaps intermittent effects such as current leakage. Smoke can cause circuit bridging and, thus, affect the operation of digital equipment. Because the edge connections and interfaces are typically uncoated, the most likely effect of the smoke is to impede communication and data transfer between subsystems.

(6) During the smoke tests, upsets typically were not encountered until about an hour into the exposure tests. The EDSC did not lose functionality when exposed to smoke equivalent to a large control room panel fire conditions (smoke density of about 3 g/m^3). A large control room panel fire has been postulated by Nowlen[81] as the most likely severe fire that might be experienced in the main control room. In this scenario, a whole panel burns, all equipment within the panel is destroyed, and the smoke from this fire is dispersed throughout the control room. Because of similarities between the EDSC and digital safety systems with regard to circuit board and chip fabrication and packaging, it is reasonable to postulate that commercial digital equipment will likely maintain functionality during its initial period of exposure to smoke equivalent to a large control room panel fire unless any of the equipment is contained in the burning panel or in close proximity to the fire source. Given early detection of a fire and subsequent application of fire suppression measures, digital systems can therefore be expected to maintain functionality (to allow safe shutdown) for as much as an hour or more following exposure, provided that the equipment is not directly exposed to the fire.

(7) The solder mask on commercial electronic boards appear to be effective in preventing catastrophic and/or permanent failure of the board even when they are exposed to a reasonably high level of smoke. The lower limit that necessitates cleaning of circuit boards, due to chloride deposits from smoke, is often specified[62] to be 10 μg chloride/cm^2. For comparison, analysis of the largest smoke load used (160 g/m^3) showed the chloride deposition to be 742 μg chloride/cm^2. (Tests with uncoated boards using comparable smoke loads showed a marked decrease in resistance.[56])

5.4 SNL Study: Impact of Smoke on Digital Components[†]

5.4.1 Scope of Study

This study, performed by Sandia National Laboratories, consisted of smoke exposure tests on digital components and circuit boards, with a focus on short-term effects such as circuit bridging in typical components and the factors that can influence how much the smoke will affect them. These factors include the component technology and packaging, physical board protection, and environmental conditions such as the amount of smoke, temperature of burn, and humidity level. The likelihood of circuit bridging was tested by measuring leakage currents and converting those currents to resistance in ohms. The lower the resistance, the higher the likelihood of shorts.

5.4.2 Approach

Since circuit bridging by smoke was isolated as one of the early failure mechanisms, the researchers studied factors in smoke generation that affect circuit bridging. Experience with shorts in the SNL preliminary tests indicated that intermittent pathways between contacts develop as a result of smoke. Thus the objective of the component-level tests was to determine the smoke-related factors that are important in causing failures from shorts. Components were exposed to smoke and loss of function or changes in resistance between contacts were measured. To measure the resistance, a bias voltage was applied between the contacts and the resulting leakage current was monitored. Ohms Law ($R = V/I$) was then used to calculate the resistance. The components tested consisted of seven chip packages, four comb patterns at different voltages, an operating optical isolator chip, and two 16-K memory chips. The chip packages included a ceramic leadless chip carrier (LLCC), a ceramic dual-in-line package (CDIP), a ceramic flat package (CFP), a transistor outline can (TOC), a plastic dual-in-line package (PDIP), a small-outline integrated circuit (SOIC), and a plastic leaded chip carrier (PLCC). The ceramic packages and the TOC were empty packages, while the PDIP and SOIC both contained four hex inverter circuits. These components were chosen because they typify modern microprocessor electronics. They represent both surface and plated-through-hole mounting schemes. The comb patterns represent standard patterns used to measure circuit board process quality and surface insulation resistance. To determine whether coatings or housings had any effect on the chips or comb patterns, some of these test components were coated with an acrylic spray or housed in a computer case. The factors that were tested included the amount of fuel, the presence of polyvinyl chloride (PVC), the burning temperature, the humidity, introduction of CO_2 and the presence of galvanic material.

A drop in resistance indicates current leakage. It is known from surface insulation resistance tests that current leakage increases almost immediately upon introduction of high temperature and humidity.[83] Typical pretest resistance measurements are $>10^{12}$ ohms, which drop to approximately 10^8 ohms some time after introduction of environmental conditions. In the tests the leakage currents were expressed in terms of resistance for the seven chip packages. Loss of function for the optical isolator chip was determined by changes in the amplitude, delay, and rise time of an output pulse. The functionality of memory chips was measured before and after the smoke exposures.

[†] Research performed for the NRC Office of Nuclear Regulatory Research by SNL.[56]

Test Procedures

General:
The components to be exposed were placed in a Lexan exposure chamber that was connected by stainless steel chimneys to the combustion chamber underneath the exposure chamber as shown in Figure 5.6. Fuel (pieces of cable) was placed in the center of the chamber inside aluminum foil-lined stainless steel trays and burned by lamps immediately above the quartz chamber. Smoke was produced by heating the fuel with radiant heat lamps. The smoke was produced over a period of 15 minutes or less and the components were exposed to the smoke for approximately 1 hour. Then the smoke was vented and the exposure chamber was opened, exposing the components to the controlled temperature and humidity of the environmental chamber. They remained in the controlled environment for 24 hours from the beginning of the smoke exposure. The components were monitored before each smoke exposure and at least every 5 minutes throughout the test for 24 hours from the beginning of the exposure.

Components Tested:

Chip Packages

The objective of the chip package experiments was to measure how smoke changes the resistance between contacts in components. A chip mounting board was designed that allowed the leakage current between adjacent conductors to be measured while 5 Vdc was supplied to the contacts. There were between 7 and 44 contacts for the seven chips. Since any pair of these contacts may be bridged, as many contacts as possible were monitored.

When plastic chip packages are made, the chip and pins are manufactured first, and then the plastic package is molded around the electronics. For metal or ceramic packages, the package is fabricated first, and then the chip is mounted within the package. The easiest packages to monitor were the four empty chip packages; every other conductor was connected by paths on the printed circuit board. The three plastic packages contained integrated chips, therefore only adjacent conductors that were independent of one another were monitored. The PLCC was especially complicated, because it contained an 8-bit A/D converter with serial interface with 1370 field effect transistors.

Both through-hole and surface-mounted components are represented in this list of chip packages. The LLCC, CFP, SOIC, and PLCC are surface-mounted packages and the CDIP, PDIP, and TOC are through-hole-mounted packages.

For the empty packages, all of the even-numbered pins were connected to a 5-Vdc supply and all of the odd-numbered pins were connected to ground. For the hex inverters, the power and ground pins were allowed to float, the inputs to the inverters were connected to 5 V, and the outputs were connected to ground. Leakage current measurements were made between the input (5V) and ground (0V). The PLCC chip had 11 analog input pins; alternate input pins were connected to 5V and ground while the chip was powered with 5 V. Leakage current measurements were made between the set of inputs connected to 5V and the set of inputs connected to ground. The chip-mounting boards were connected by ribbon cables and card edge connectors to the instrument measuring current leakage, which was located outside of the environmental chamber.

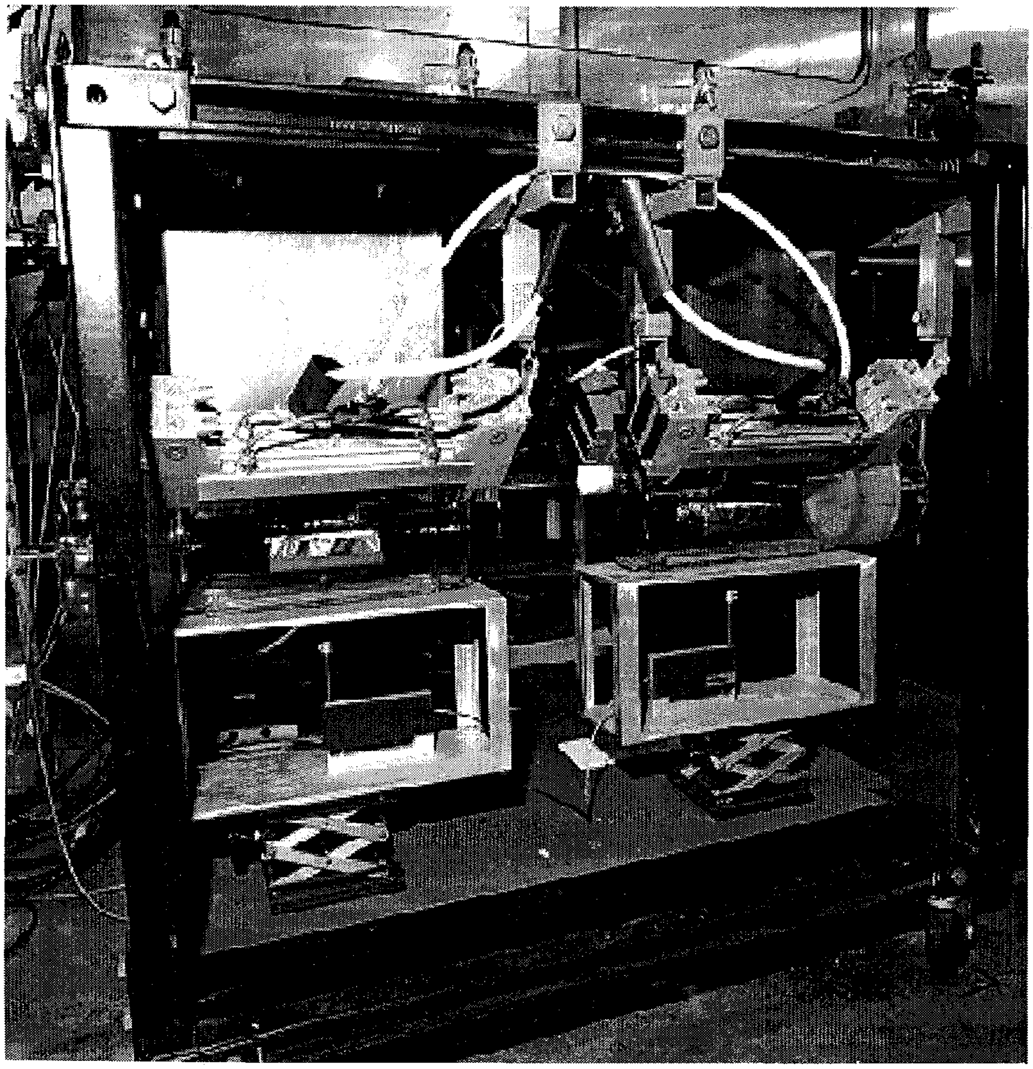
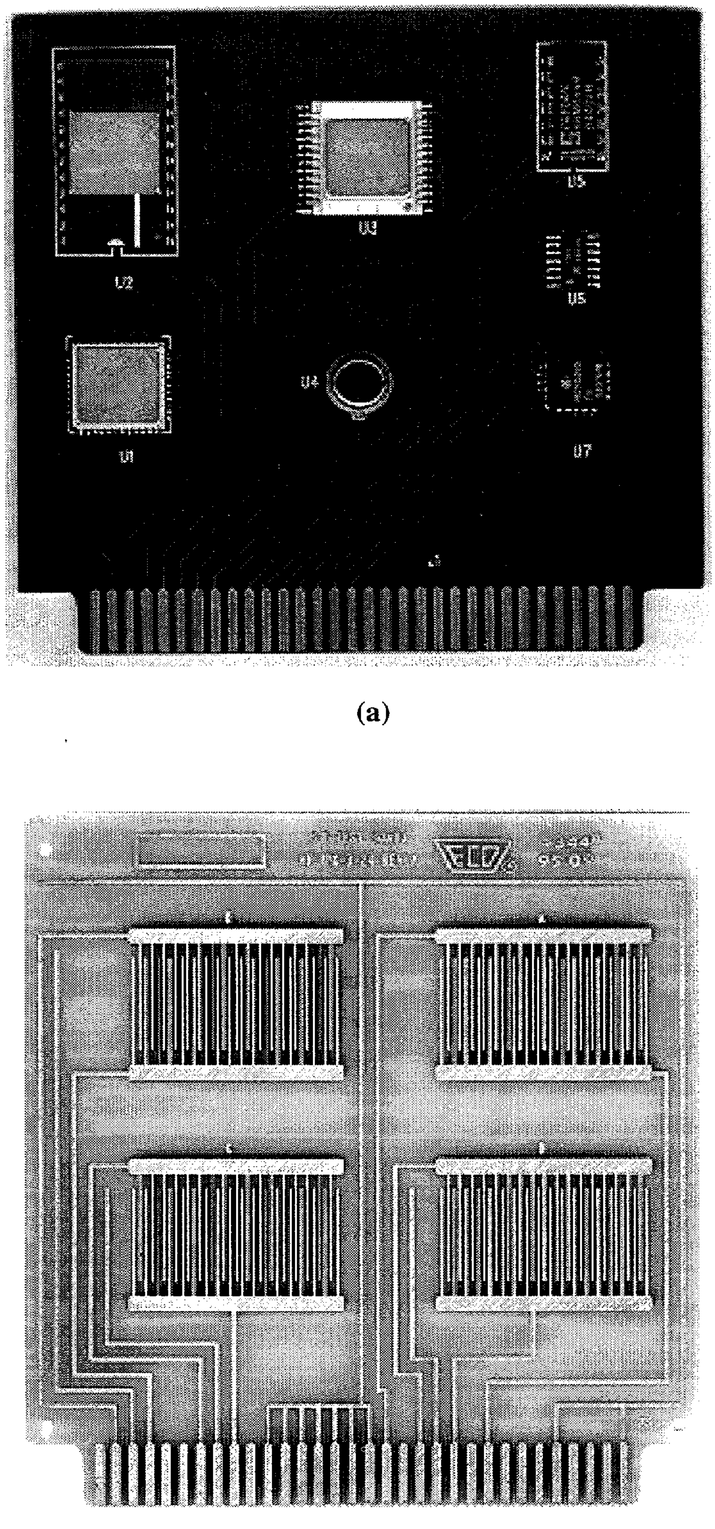


Figure 5.6 Smoke chamber [The combustion chambers (quartz cylinders) are shown underneath the exposure chamber]

For each smoke exposure, four chip-mounting boards (see Figure 5.7a) in different configurations were tested. Three boards were mounted inside the smoke exposure chamber; these boards were either bare, coated with an acrylic spray, or housed in a personal computer (PC) chassis equipped with an operating fan (i.e., a typical chassis "muffin" fan). A bare board (used as an experimental control) was located inside the environmental chamber, but outside the smoke exposure chamber. The boards were placed in position approximately 1 hour before the test in most cases. The card edge connectors were wrapped in black electrical tape to prevent smoke from corroding the connectors.

The resistances were measured with a Keithley 617 multimeter and two Hewlett-Packard (HP) switcher/controllers. The multimeter, used as an ammeter, was switched between the chip packages and comb patterns. The switching was controlled so that the chip packages always had 5 V between the pins. The ammeter was switched into a circuit for 3 seconds before each measurement to allow it to settle to a stable condition. To ensure that the power supplies were not overdrawn by chip package shorts, series



(a)

(b)

Figure 5.7 (a) Chip mounting board and (b) Comb pattern board

resistors were included in the circuit to limit the current drawn. Measurements were repeated at approximately 5 minute intervals.

Comb Patterns:

Surface insulation resistance was measured on comb patterns on Institute for Interconnecting and Packaging Electronic Circuits (IPC) B-24 printed circuit boards. The IPC-B-24 boards (Figure 5.7b) contain four identical comb patterns. The comb teeth were 0.4 mm wide with 0.5-mm spaces between opposing teeth. The resistances of the comb patterns were measured similarly to those of the chip packages except that the voltages were different. One comb pattern was biased with 160 Vdc, one with 50 Vdc, one with 5 Vdc, and one was grounded except during measurements, when it was biased with 5 V dc. (As with the chip boards, measurements with the comb patterns were repeated at approximately 5 minute intervals.) The different voltages allowed evaluation of the effect of electric field strength on circuit bridging during and after smoke exposure. As with the chip boards, four boards were included for each test: a bare board, an acrylic-coated board, a board housed in the PC chassis, and an unexposed control board. The boards were connected to the power and measurement circuit in the same manner as the chip boards and were measured by the same ammeter.

Optical Isolators:

A functioning 6N138 optical isolator, which provides a coupling for electrical circuits with a direct electrical connection, was included in all of the smoke exposures. This device operates by using a light-emitting diode and a photodetector that are built into a plastic DIP body. The 6N138 is a low-input current, high-gain optocoupler built for TTL applications. The test circuit consisted of a square wave input pulse, and the resistors and capacitors necessary to provide a switching test circuit as shown in Figure 5.8.

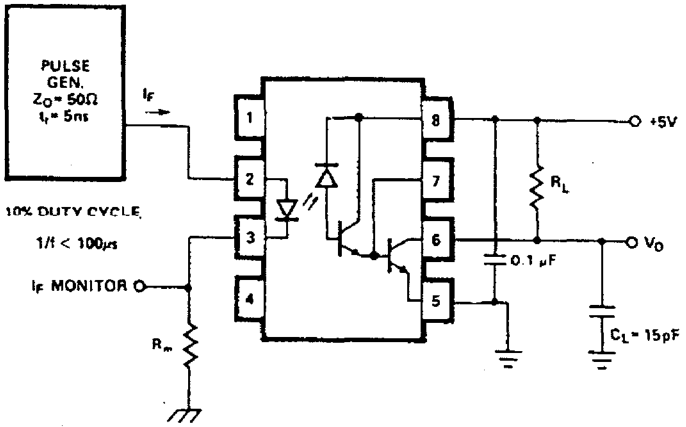


Figure 5.8 Switching test circuit (adapted from HP Optoelectronics Designer's catalog)

For each exposure, a new optical isolator chip was placed in a socket containing the supporting circuit. The input and output wave form parameters of pulse rise time, amplitude, and delay from the input pulse were measured on a digital oscilloscope. A starting wave form was recorded, and if the values of rise time, delay, or amplitude varied by more than 5% from the starting values, a new wave form was recorded.

Memory Chips:

Two package types for 16-K memory chips were exposed for each test: a plastic-packaged commercial chip and a ceramic-packaged chip developed at SNL. The two chips had identical circuitry. They were powered with 5 V, but were not operated during the exposure. Standard functional tests were performed on the chips before and after the tests.

Scenarios Tested

The factors varied for the smoke exposures were fuel amount, presence of PVC as part of the fuel, burn temperature, humidity, introduction of CO_2, and presence of galvanic material. Some of the factors that were varied directly affected the smoke production; however humidity, CO_2, and galvanic metal were included because they were likely to interact with the smoke and affect electronic components. High humidity is known to affect electronics and is commonplace after a fire if sprinklers or water-based fire extinguishers were used. CO_2 is another common fire suppressant. It has been proposed that CO_2 may affect electronics by suddenly cooling the electronics and cracking the bonds. It has been included in some of the smoke exposures to determine of it would cause problems for the electronics. Zinc in galvanized metals has been known to combine with chlorides that are frequent components of smoke. $ZnCl_2$ is hygroscopic and will absorb water from the air. The $ZnCl_2$-water mixture forms a syrup, which can drip onto components under the right conditions.

Fuel load, burn temperature, and humidity factors were either at a high or low level. The levels were chosen to span a range for a credible fire. For CO_2 and galvanic metal, the material was either present or absent. Because of the high number of parameters, every possible permutation was not performed; instead, only conditions that corresponded to likely scenarios in plants were produced.

A fire condition matrix was generated according to likely smoke scenarios, and tests 1 to 15 followed this procedure until CO_2 and galvanic metal were determined not to be detrimental to the components. The experimental design matrix was then modified so that PVC could be included as a parameter and other combinations of factors could be tested, such as the combination of high burn temperature and high fuel load. In all, 27 tests were performed.

Fuel Level

Two standard amounts of cable were used as fuel in these tests as the high and low levels: 3 g and 100 g of plastic insulation and jacket material. The fuel consisted of a mixture of cables that are typical of nuclear power plants. The exact amount of plastic that was available for burning is not known because the plastic was not stripped from the cable conductors and measured directly; however, the mass loss of the fuel was measured for each test. The proportion of each type of cable was determined by the number of plants that use the cable as reported by EPRI.[84] Table 5.9 shows the total mass of the fuel samples used to produce smoke for the tests.

Burn Temperature

The cable material was burned at either high (50 kW/m^2) or low heat fluxes (25 kW/m^2). For the low heat flux burns the cables just smoldered, but for high heat flux tests the cables were ignited if possible with a butane pilot light. For all high-heat flux burns at least part of the burn took place with a flaming fire; however, the flame did not last the full time that the radiant lamps were on, presumably because the amount of oxygen available in the combustion cell had dropped.

Table 5.9 Cable fuel weights [total mass (g)]

Cable name	Insulation	Jacket	Low fuel no PVC	High fuel with PVC	High fuel no PVC
Rockbestos Firewall III	FRXLPE	CSPE	1.8	38.6	57
Anaconda Flameguard 1kv	EPR	CSPE	1	17.3	30.4
Brand Rex XLPE	XLPE	CSPE		20	
Okonite Okolon	EPR	CSPE		16.3	
Kerite HTK			0.8	16.7	23.3
Rockbestos Coax (le)			0.5	13.8	15.6
Raycheon XLPE	XLPE		0.4	9.9	10.2
Dekoran Dekorad	EPDM	CSPE	0.7	11.7	23.3
BIW	EPR	CSPE		8.11	
Kerite FR				7	
PVC	PVC	PVC		4.4	

Humidity

High (75% RH) and low (<20% RH) humidity levels were controlled by an environmental chamber that housed the smoke exposure chamber. The humidity was always set before the test, but the humidity within the smoke exposure chamber was not controlled during the smoke exposure since the chamber was entirely enclosed to control the corrosive smoke. After the smoke was vented, the exposure chamber was opened and the environmental chamber controlled the humidity and temperature. The humidity level before the test can affect the resistance of the circuit bridging measurements before the smoke is introduced.

Suppression (CO_2) and Galvanic

Additional effects were added by flooding the exposure chamber with CO_2 from a fire extinguisher and adding a piece of corrugated galvanic roofing material above the test articles. When the CO_2 was added, 60% of the volume of the smoke exposure chamber was filled with CO_2, a standard percentage of the volume that automatic fire suppression systems will flood a room with in case of a fire. This corresponds to 2.5 lb of CO_2 in the smoke exposure chamber.

The galvanized roofing material was included in some of the tests to simulate industrial environments and provide a source of zinc. In past fires,[85] the presence of galvanic metal has increased damage to electronics because droplets of $ZnCl_2$ and water have deposited on the electronics.

The roofing material was cut so that it was above all of the test samples, but did not cover the chimney areas of the chamber. This metal piece was suspended approximately 1 foot above the test samples and covered almost the entire smoke exposure chamber.

Other measurements

Temperature, humidity, smoke deposition, smoke optical density (turbidity), and fuel mass loss were measured, and soot samples were chemically analyzed. Descriptions of the methods used for these measurements can be found in reference 56.

Text Matrix

The test matrix for all exposures performed is presented in Table 5.10. A value of 1 indicates a high level for fuel, burn, or humidity. A value of 1 for PVC, suppression, or galvanic indicates the presence of these conditions. Results of the tests were evaluated in terms of these bipolar indicators rather than individual values. Test numbers were assigned in order of the test performance.

Table 5.10 Test matrix

Test no.	Fuel	PVC	Burn	Suppression	Galvanic	Humidity
1	0	0	1	0	0	1
2	0	0	0	0	0	1
3	0	0	0	0	0	1
4	1	1	0	1	0	1
5	1	1	0	0	0	1
6	0	0	1	0	1	1
7	1	1	0	0	1	1
8	0	0	1	1	0	1
9	0	0	0	0	1	1
10	0	0	0	1	0	1
11	0	0	1	1	1	1
12	1	1	0	0	0	0
13	1	1	0	0	1	0
14	1	1	0	1	0	0
15	0	0	1	0	0	1
16	1	1	0	0	0	1
17	1	1	1	0	0	1
18	1	0	1	0	0	1
19	0	0	1	0	0	0
20	0	0	0	0	0	0
21	1	0	0	0	0	1
22	0	0	0	0	0	0
23	0	0	1	0	0	0
24	1	1	0	0	0	0
25	1	0	1	0	0	1
26	1	1	1	0	0	1
27	1	0	0	0	0	1

(A 1 represents a high level or presence of a condition, 0 represents a low level or absence of a condition.)

5.4.3 Results of Smoke Exposure Studies on Digital Components/Comb Patterns

Resistance Measurements

Smoke exposure caused changes in resistance in all components and comb patterns. Figure 5.9 shows exposed chip-mounting boards from several different tests. The upper left board is a control board (unexposed to smoke) from test 25, the upper right board is the coated board from test 16, the lower left board was in the PC chassis during test 25, and the lower right board was in the PC chassis during test 17. During test 25 the soot from the fan tended to form clumps, fly off the fan, and deposit on the boards housed inside the chassis. The lower right hand board from test 17 experienced very nearly the same environment as the lower left hand board from test 25, differing only in that the fuel mixture for test 17 contained PVC while that for test 25 did not.

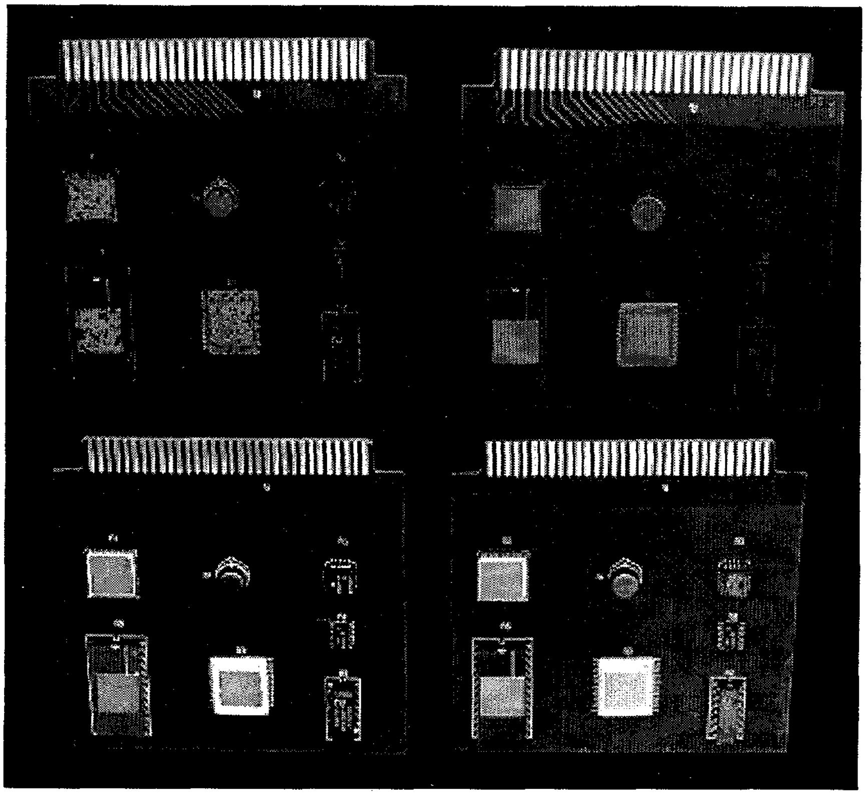


Figure 5.9 Exposed chip-mounting boards from different tests [Upper left:control. Upper right: test 16. Lower left: in PC chassis for test 25. Lower right: in PC chassis for test 17.]

The comb pattern boards shown in Figure 5.10 are arranged according to the same tests as the boards in Figure 5.9, with soot discoloration more evident on these lighter colored printed circuit boards. Although the effects of different voltages are not evident in these reproductions, the higher voltage comb patterns (160 and 50 Vdc) collected more soot than the lower voltage patterns (5 and 0 Vdc). The voltage on the

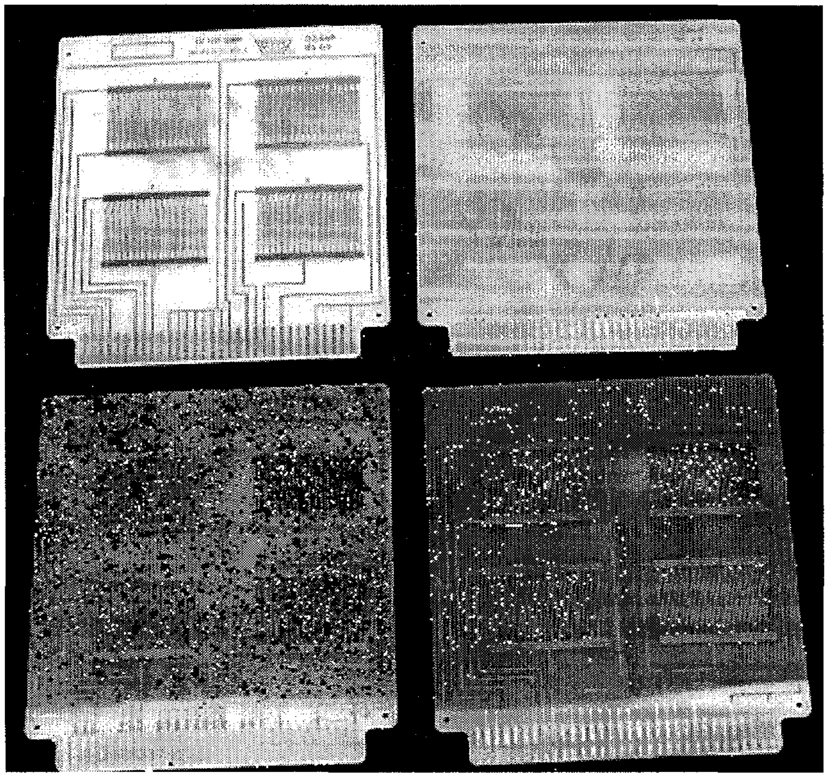


Figure 5.10 Exposure comb pattern boards [Arranged as in Figure 5.9]

160-Vdc comb pattern was sufficiently high so that when large pieces of soot landed on the bare board, sparks were observed.

The resistances of 44 components (7 types of chips and 4 combs in each of 4 configurations: bare, coated, in housing, and control) per test were measured for a 24-hour period. In this period, approximately 450 measurements were made on each component. Scatter plots were developed from these measurements in order to reduce this large amount of data into a manageable set. The scatter plots also provided a good intuitive grasp of the effects of smoke in general throughout these tests and showed the differences among the different protective measures for the boards. Also, to determine which of the smoke generation, environmental condition, or board condition factors were most significant, variances in resistances were analyzed using general linear models. Details of the analysis are given in reference 56. A summary of the results is given below:

Technology and Packaging

Digital I&C components are available with many different technologies and packages. Metal and ceramic packaging, which are hermetically sealed, tend to be more reliable than plastic packages. The data from the 16-K memory chips show that the ceramic packages were more robust than the plastic packages in a smoke environment. Differences between ceramic and plastic packages were not evident from the resistance measurements; therefore, the higher failure rate of plastic packages may be due to penetration of the plastic by smoke particles or moisture rather than shorting of contacts with soot. Most common digital electronics, however, use less expensive plastic packages. Hermetically sealed packages are significantly more expensive and are not typically available unless used for military applications.

The voltages at which the digital electronics operate vary according to the digital chip technology. Resistance measurements on the comb patterns indicate that higher voltage patterns are affected by smoke more than lower voltage patterns. The higher voltage lowers the resistance before the smoke is applied and continues to produce more leakage current throughout the exposure. Visually, soot tends to accumulate more around the high voltage patterns, and the 160-V pattern was observed to be arcing during the smoke exposure.

Two hex inverter chips were included on the chip mounting board to determine the difference between an SOIC package and a DIP. The statistical analysis that compared post-exposure averages showed no appreciable difference between these two packages except with respect to the *rate* of degradation at high fuel loads. When the fuel available for smoke production was high, both packages shorted; however, components with small contact spacing shorted earlier. Thus, the DIP package resisted shorting longer than the SOIC package. When the available fuel was low, resistance dropped for both packages slightly, and then recovered with little difference observed between the chip packages. A reason for not being able to determine differences may be that the low fuel loads were too low to cause much change in resistance.

These tests measured leakage currents that determined the change in resistance between contacts on components. Loss of resistance can cause problems in many components and circuits; for example, if the resistance between a contact to supply voltage and one to an input signal drops, a false signal may be received by the device input from the voltage supply. The likelihood of this happening depends on many factors such as the amount of smoke, location of the contacts, and humidity level. In general, loss of resistance between contacts will cause serious problems in any digital circuit.

Protection

Bare boards were highly affected by smoke while coated boards seemed to be less affected. Housing the boards in a PC chassis, which contained a fan, protected the boards only minimally. Visually, some of the boards that were placed within the chassis looked worse than those that were unprotected because clumps of soot were deposited on the board. For the high fuel load tests, however, virtually all components were shorted in these situations and little difference could be observed in the resistance measurements.

Significant Factors in Determining Circuit Bridging

Several observations can be made from the component tests; the most significant smoke generation factors are humidity, fuel level, and burn temperature. High humidity has been shown to affect the surface insulation resistance of printed circuit boards in environmental testing.[83] Other fire corrosivity tests which used comb patterns also showed that the resistance of exposed comb patterns is highly affected by humidity.[86]

As more fuel is burned, resistance drops. Smoke from plastic leaves a film, which is black and powdery if the plastic is burned in the flaming mode with adequate oxygen. The film is white and oily if produced without a flame and black and oily if produced with a flame, but the flame extinguishes due to lack of oxygen. For low fuel loads, the resistance generally dropped during the smoke exposure but recovered after the smoke was vented. This recovery was not often the case with the high fuel loads; once the circuit was shorted, it never recovered.

The burn temperature (flaming vs. smoldering) did not affect the resistance as much as the humidity or fuel. The burn temperature would be expected to change the smoke products in two ways: different chemical products can be produced at different temperature, and the mass loss rate of the fuel is slower if the fire is smoldering. Chemical analyses for Cl, Br and SO_4 showed a low correlation between burn temperature and the amount of these chemicals in the soot. Analysis of the amount of fuel that was burned shows that neither the burn temperature nor the fuel level alone determines the percentage of fuel that is burned. If a large amount of fuel was burned at a low temperature, approximately 20% of the fuel was consumed, while if a small amount of fuel was burned at either low temperature or a large amount of fuel was burned at high temperature, approximately 40-50% of the fuel was burned.

The circuit bridging tests showed that the synergistic effects of smoke and humidity are higher than for humidity alone.

PVC (included as part of the fuel load on the high fuel tests only) showed very little effect on resistance. Only a small proportion of the fuel was PVC in these tests and, with the high fuel load, many of the components shorted without PVC. There is also little correlation between the Cl deposition found by chemical analysis and the presence of PVC. Although the other cable materials did not contain PVC, some had high proportions of Cl and Br, which are typically used as fire retardants. No other cable materials were singled out for study in these tests.

The addition of CO_2 as a fire suppressant did not affect the resistance adversely, supporting results from the ORNL smoke exposures. The addition of CO_2 may be beneficial to the electronics by cooling the room and blowing away some of the soot deposition. These findings are supported by tests on the effect of CO_2 on computers.[87]

The galvanic metal was expected to trap Cl in the form of $ZnCl_2$, form a thick liquid, and drip onto the electronics.[85] Although a greasy film formed on the galvanic metal that was suspended in the smoke exposure chamber, the film never accumulated enough water to drip. Instead, the metal piece formed a surface upon which some of the smoke deposited. The overall effect was to reduce deposition on the surface of the electronics and reduce the negative effect of the smoke. On some high humidity tests, water appeared to be collecting at the base of the PC chassis. This water did not affect any of the components. Overall, these tests were found to be of an inadequate scale to properly assess the importance of this factor.

5.4.4 Conclusions from the SNL Study

Several conclusions may be drawn from the SNL smoke exposure studies. These include the following:

(1) Smoke causes circuit bridging in components. Circuit bridging increases leakage currents and can cause failures because stray currents cause errors in digital circuitry.

(2) Factors that affect circuit bridging are the amount of smoke, humidity level, and burning mode.

(3) Although surface deposits cause some circuit bridging, the presence of smoke in the air also causes increased leakage.

(4) The effect of circuit bridging on digital I&C equipment depends on the particular components and circuits. Component packaging (plastic, ceramic, or metal) and technology [CMOS, field effect

transistors (FETs), or fast schottky transistors] are only a few of the factors that determine the likelihood of survival of a circuit or component.

(5) Conformal coatings add significant protection to circuits.

(6) Mechanical protection may also protect circuits, depending on the presence of a ventilation fan. A fan may draw more smoke into the electronics.

The component test focused on circuit bridging in typical integrated circuits and the factors that can influence the (adverse) impact of the smoke exposure. These factors include the component technology and packaging, physical board protection, and environmental conditions such as the amount of smoke, temperature of burn, and humidity level. Hermetically sealed ceramic packages were less affected by smoke than plastic packages. Coating the boards with an acrylic spray provides some protection against circuit bridging. The most significant factors were humidity, fuel level, and burn temperature. The use of CO_2 as a fire suppressant, the presence of galvanic metal, and the presence of PVC did not significantly affect resistance measurements.

5.5 Stressors to be Considered During Qualification Testing of Digital I&C Safety Systems

One of the objectives of the studies described in this section is to provide the technical basis for determining whether additional environmental stressors should be explicitly included in a qualification program for safety-related digital I&C systems.

The first study sought to prioritize environmental stressors that can affect the reliability of digital equipment in nuclear power plants by comparing the relative risk-sensitivities of the stressors. The data and methods developed were applied to prioritize environmental stressors in an example plant, using a plant-specific PRA. The risk-screening results for the stressors in the example plant, subject to the bounding assumptions, indicate that humidity, EMI from lightning, and smoke can be potentially risk-significant. The risk-significance of EMI from lightning and smoke are sensitive to the periods before equipment failure is detected. If failures are detected only during the surveillance tests (assumed to be at intervals of 31 days), these stressors can be risk-significant even when only critical failures are considered and credit is given for detecting some failures through system self-diagnostics. For shorter detection periods, however, these two stressors may not be risk-significant. The results also show that the risk effects of some stressors, such as humidity, can be sensitive to the location of the equipment. For the levels of stressors analyzed, risk effects from temperature in digital I&C equipment locations, and that from assumed levels of vibration, appear to be insignificant.

The second study sought to identify/confirm the vulnerabilities of microprocessor-based technologies when a system is actually subjected to various environmental stressors, including temperature, humidity, EMI/RFI and smoke exposure. The study found that environmental stressor effects that do not result in permanent hardware failures may nonetheless cause intermittent upsets that would typically result in communication failure, 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). The greatest number of failures, as well as the most severe, were encountered during the EMI/RFI tests. With regard to temperature and humidity, the study found that the combination of high temperature at high relative humidity were the conditions to affect the EDSC, rather than temperature acting alone. For all the smoke tests, upsets were not encountered until approximately 1 hour into the exposure tests. The EDSC did not lose functionality when exposed to smoke equivalent to a large control room panel fire conditions (smoke density of about 3 g/m^3).[a] The solder mask on commercial electronic boards was found to be effective in preventing permanent failure of the boards in the EDSC used during the study, even when they were exposed to a reasonably high level of smoke (i.e., 160 g/m^3).

The third study sought to determine the impact of smoke on digital I&C equipment at the component and circuit board substrate level. The component tests focused on factors that could affect circuit bridging in typical digital electronic components. These factors include the component technology and packaging, circuit board protection with coatings or enclosures, and smoke generation factors. Hermetically sealed ceramic packages were found to be more resistant to smoke than plastic packages. Coating the boards with an acrylic spray provided significant protection against circuit bridging. The smoke generation factors that affected the resistance the most were humidity, fuel load, and burn temperature. The use of CO_2 as a fire suppressant, the presence of galvanic metal, and the presence of PVC in the material burned did not significantly affect the outcome of these results.

The following conclusions are made from the results of these studies:

(1) Smoke is an important stressor on safety equipment because of the possibility of multiple equipment failures. Nevertheless, the coatings on commercial electronic boards appear to be effective in preventing permanent failure of digital electronics boards, even when they are exposed to smoke from the most severe fire that is likely to be experienced in the control room.

(2) Research findings at present are not sufficient to justify including smoke exposure as part of qualification testing.

(3) There are currently no smoke exposure testing standards, so smoke exposure type testing is currently impractical.

(4) Currently, fire and its effects (smoke, heat, ignition explosions, toxic gases) on safety-related equipment is a fire protection concern that, in our opinion, is covered in GDC 3 of Appendix A of 10 CFR 50, IEEE Standard 384, "Independence of Class 1E Equipment and Circuits,"[88] and Appendix R of 10 CFR 50. GDC 3 requires that structures, systems, and components important to safety be located to minimize the probability and effects of fires and explosions. IEEE Standard 384 requires that an electrically generated fire in a Class 1E division shall not result in loss of function in the redundant Class 1E divisions. In addition to these requirements, Appendix R of 10 CFR 50 requires a defense-in-depth approach to be taken to (1) prevent fires from starting; (2) detect rapidly, control, and extinguish promptly those fires that do occur; and (3) provide protection for structures, systems, and components important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent safe shutdown of the plant. These practices should limit the chances of smoke exposure.

[a] A large control room panel fire has been postulated by Nowlen[81] as the most likely severe fire that might be experienced in the main control room. In this scenario, a whole panel burns, all equipment within the panel is destroyed, and the smoke from this fire is dispersed throughout the control room. Because the smoke under this scenario was postulated to be uniformly distributed throughout the entire main control room, this represents the smallest smoke density of the three fire scenarios postulated in the SNL study.

(5) The synergistic effect of high temperature in combination with high relative humidity is potentially risk-significant to digital I&C. Therefore, although high relative humidity is not as likely in the controlled environments where digital I&C are typically located (e.g., control room), the synergistic effect of these two stressors need to be considered on a case-by-case basis, especially for post accident monitoring equipment.

(6) There is a need for electromagnetic compatibility standard(s) to be applied in the nuclear power plant environment. For the locations in which I&C safety equipment are likely to be placed, stressor prioritization studies to date indicate that EMI has potentially higher risk-significance than smoke exposure or high temperature at high relative humidity. Also, during tests on the EDSC, the greatest number of errors, as well as the most severe (e.g., permanent module failure) occurred during the EMI/RFI tests.

6 RECOMMENDED TECHNICAL POSITION ON ENVIRONMENTAL QUALIFICATION OF DIGITAL I&C SYSTEMS

6.1 Introduction

The nuclear power industry is required to qualify safety-related equipment and systems to provide assurance that they will perform properly when required to do so throughout the life of the plant. The studies documented in this report have addressed issues that could impact environmental qualification for digital I&C systems. In this section, we present the technical position of the authors based on the results of these studies.

6.2 Application of Current Qualification Procedures to Digital I&C Safety Systems

It is the opinion of the authors that

(1) **Type testing** should continue to be the preferred test method for safety-related I&C systems.

(2) The state of the art does not warrant any changes to be made with regard to **aging methodologies** for digital systems in nuclear power plants.

(3) A stressor not previously considered for analog safety system qualification is **smoke exposure**. Research documented in this report confirms that smoke is a stressor that can adversely impact digital safety equipment. However, 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. Additional research into the susceptibility of digital components and modules to smoke-induced effects is on-going and should be continued. Based on existing research, present methodologies with regard to fire and its effects (smoke, heat, ignition, explosions, and toxic gases), which are addressed via GDC 3, IEEE 384,[88] and Appendix R of 10 CFR 50, should continue to be applied for digital I&C safety systems.

6.3 Application of Current Nuclear Qualification Standards to Digital I&C Safety Systems

Based on the comparative analysis of IEEE 323-1974[3] and IEEE 323-1983[35] performed in this section, we recommend that IEEE 323-1983 be endorsed (with some exceptions) for the following reasons:

(1) Methods for ongoing qualification are more clearly stipulated in the 1983 version than in the 1974 version of IEEE 323.

(2) The types of stressors and the sequential method of their application during preconditioning are more clearly stated in IEEE 323-1983. Although both standards are silent on how to address situations where synergistic effects may exist, we recommend that present methodologies continue to be applied until more is known about the aging sequence and possible synergistic effects on advanced digital technologies.

(3) The intent of the concept of "Significant Aging Mechanisms" (which enables the user to determine the conditions under which aging may *not* be considered necessary during type testing), is an extension of the provision in the 1974 version with regard to radiation aging. The 1974 version allows the exclusion of radiation during aging "if the required radiation level (necessary to simulate the equipment's expected end-of-qualified-life condition) can be shown to produce less effect than that which would cause loss of the equipment's Class 1E function." This concept appears to have been extended in the 1983 version to all aging mechanisms, rather than just radiation.

(4) The intent of the section on "Margin" is essentially the same in both versions of the IEEE standard. However, contrary to current practice, we are of the opinion that conservative qualification testing of I&C equipment requires that margin be applied to **both** the aging time, as has been done by some manufacturers in the past, and the type test parameters during DBE testing, as is suggested in IEEE 323-1983. The two margins address two separate issues. Margin on aging time seeks to compensate for uncertainties in the assumptions made in the use of the Arrhenius equation. On the other hand, margin on type test parameters during DBE testing seeks to compensate for variations in commercial production of equipment and their ability to satisfy a minimum operating time requirement during a DBE.

To enhance the usefulness of IEEE 323-1983, we recommend that the following exceptions be made:

(1) Locations at which preconditioning is not required should be more clearly defined. In this document, we have proposed one methodology to achieve this clarity by defining the location of a digital I&C safety system in an NPP as **Category A, B or C** (see the Appendix). Preconditioning before qualification testing must be performed for a (digital) safety system in a Category A location. For equipment in a category B location, preconditioning need not be used, but testing should include all DBE conditions. There should be a 10% margin on the **test duration** as well as for all test parameters for DBE testing. For example, if equipment is required to perform its function for 10 hours during a DBE, the system should be tested for 11 hours. For equipment in a category C location, preconditioning need not be used. In addition, unlike the case for a category B location, a 10% margin on the *test duration* is *not* required. However, a 10% margin is required for all test parameters under postulated DBEs.

(2) Methodologies for documenting qualification procedures should be augmented with the procedures proposed in this document.

6.4 Other Recommendations to Enhance I&C Qualification Methodologies

(1) It is recommended that the dynamic response of a *distributed* system under environmental stress be explicitly considered during type testing. In a microprocessor-based system, changes in component parameters (leakage current, signal rise and fall times, etc) due to some stressor can lead to intermittent upsets such as the inability of a component to trigger, the overall effect of which may be failure to communicate the correct data in a specified time (data flow failure). System response time is usually considered during design, but the sequential nature of digital processes (as opposed to the essentially instantaneous nature of analog processes) increases the significance of the potential of environmental stressors to cause intermittent upsets in subsystems, leading to degraded performance in the *total* system. Dynamic performance under environmental stress is especially important in PAM systems, which typically are required to function following a reactor trip or ESF actuation.

(2) There is a need for electromagnetic compatibility standard(s) to be applied to the NPP environment. For the locations in which I&C safety equipment are likely to be placed, stressor prioritization studies to date indicate that EMI has potentially higher risk-significance than smoke exposure or high temperature at high relative humidity. Also, during tests on the EDSC, the greatest number of errors, as well as the most severe (e.g., permanent module failure), occurred during the EMI/RFI tests.

It is recommended that information provided in the following reports be used as the basis for electromagnetic compatibility of I&C systems in NPPs:

NUREG/CR-6431, *Recommended Electromagnetic Operating Envelopes for Safety-Related I&C Systems in Nuclear Power Plants.*[89]

NUREG/CR-5941, *Technical Basis for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems.*[82]

NUREG/CR-6436, *Survey of Ambient Electromagnetic and Radio-Frequency Interference Levels in Nuclear Power Plants.*[90]

6.5 Additional Measures to Support the Use of High Quality Electronic Components

We suggest that the nuclear industry adopt a new philosophy of qualification, in which the assurance that a safety-related equipment will perform properly is "built-in" as well as being "tested-in." In this approach, assurance of equipment's quality starts at the **semiconductor component** level rather than at the system level. As a minimum, this can be achieved by encouraging the manufacturer of the safety-related I&C equipment to document the qualification standards used by the semiconductor manufacturer for stress testing. This approach is similar (but less stringent) to the U.S. military's QML methodology, which seeks to qualify ICs for high reliability and radiation hardness. The details of this methodology are defined in military specification MIL-PRF-38535.[59] In this approach, a production line is certified on a one-time basis, and all products from that line are subsequently qualified per the requirements of MIL-PRF-38535. Thus, the quality of a product from a QML line is defined by its conformance to MIL-PRF-38535. There are three phases to QML implementation: certification, qualification, and quality assurance. These phases use SPC of technology parameters relevant to radiation hardness, test structure to IC correlation, and extrapolation from laboratory to threat scenarios, to control factors affecting not only manufacturing yield, but also reliability and radiation hardness.

Note that unlike the military's QML certification process, the proposed approach does not involve certification of I&C vendors, nor does it require that military-grade components be used in the design of nuclear safetyrelated I&C equipment. Rather, the recommendation is that safety-related I&C system manufacturers document component qualification standards used by the semiconductor manufacturers. ICs are susceptible to long-term failure mechanisms under various environmental stressors. Examples of these failure mechanisms are electromigration and corrosion of metal interconnects. However, environmental testing and stress screening methodologies exist to enable the severity of these potential failures in a particular technology to be identified during manufacture. The use of components from high quality manufacturing processes, as demonstrated through manufacturer stress testing, can minimize that susceptibility to stressor effects. Thus, it is important that qualification of I&C systems begin at the IC-manufacturing level through the use of semiconductor components from product lines that have demonstrated their environmental compatibility through stress test screening.

7 REFERENCES

1. Electric Power Research Institute, "Advanced Light Water Reactor Utility Requirements Document," EPRI NP-6780, Revision 6, Palo Alto, CA, December 1993.

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

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

4. 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.

5. P.D. Ewing and D.E. Holcomb, *Relevance of U.S. Military Experience with EMI/RFI in Microprocessor-Based Systems to Nuclear Power Applications*, ORNL/NRC/LTR-95/7, Oak Ridge National Laboratory, March 1995.

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

7. J. M. Taylor, "Digital Computer Systems for Advanced Light-Water Reactors," Policy Issue SECY-91-292, U.S. Nuclear Regulatory Commission, September 16, 1991.

8. *Mc-Graw-Hill Encyclopedia of Science and Technology*, Vol. 9, McGraw-Hill Book Company, New York, pp. 254-271.

9. S. M. Sze, *VLSI Technology*, ISBN 0-07-062735-5, McGraw-Hill Book Company, New York.

10. J. R. Lloyd, "Electromigration," *Journal of Metals*, Vol. 36, no. 7, 1984, pp. 54-56.

11. L. Gallace and M. Rosenfield, "Reliability of Plastic Encapsulated Integrated Circuits in Moisture Environments," *RCA Review*, Vol. 45, no. 2, 1984, pp. 249-277.

12. A. P. Whitehead, P. K. Footner, and B. P. Richards, "ESD-Induced Electromigration; a New VLSI Failure Mechanism," *Proc. Intl. Symposium for Testing and Failure Analysis (ISTFA)*, 1984, pp. 214-220.

13. S. P. Bellier and R. F. Haythornthwaite, "A New Large-Scale Integrated Metallization Failure Mechanism," *Canadian Journal of Physics*, Vol. 63, no. 6, 1985, pp. 901-905.

14. M. Murtuza *et. al.*, "Flux Penetration and Pressure Cooker Fail Mechanism in Plastic IC Packages," *Proc. 36th Electronic Components Conf.*, 1986, pp. 616-621.

15. L. C. Wagner, "Failure Analysis of Metallization Corrosion," *Proc. of ASM's Third Conf. on Electronic Packaging*," 1987, pp. 275-282.

16. A. H. Johnston and R. E. Plaag, "Models for Total Dose Degradation of Linear Integrated Circuits," *IEEE Trans. on Nuclear Science*, Vol. NS-34, no. 6, pt. 1, 1987, pp. 1474-1480.

17. D. F. Farnholtz, "Operational Life Testing of Integrated Circuits," *Proc. Annual Reliability and Maintainability Symposium*, 1985, pp. 441-443.

18. O. Peyrard, "Highly Accelerated Stress Test on VLSI Plastic Components," *Proc. Intl. Symposium for Testing and Failure Analysis (ISTFA)*, 1988, pp. 167-172.

19. P. B. Ghate, "Electromigration-Induced Failures in VLSI Interconnects," *Solid State Technology*, 26, 1983, p. 113.

20. Kuan-Yu Fu, "Electromigration—A Reliability Concern for VLSI Interconnects and Interlevel Contacts," *Reliability and Quality Handbook*, 1993 Edition, Motorola Semiconductor Products Sector.

21. John Klema, "Wafer Level Dielectric Integrity," *Reliability and Quality Handbook*, 1993 Edition, Motorola Semiconductor Products Sector.

22. F. M. d'Heurle, "The Effect of Copper Additions on Electromigration in Aluminum Thin Films," *Metal. Trans.*, 2, 1971, p. 683.

23. N. Lycoudes, "The Reliability of Plastic Microcircuits in Moist Environments," *Solid State Technology*, October 1978.

24. Don VanOverloop, "An Investigation of Corrosion on Integrated Circuits via Pressure Temperature Humidity Bias Stressing," *Reliability and Quality Handbook*, 1993 Edition, Motorola Semiconductor Products Sector.

25. Nicholas Lycoudes, "The Reliability of Plastic Microcircuits in Moist Environments," *Reliability and Quality Handbook*, 1993 Edition, Motorola Semiconductor Products Sector.

26. G. C. Messenger and M. S. Ash, *The Effects of Radiation on Electronic Systems,* ISBN 0-442-25417-2, Van Nostrand Reinhold Company Inc., 1986, p. 294.

27. C. M. Hsieh *et. al.*, "Dynamics of Charge Collection from Alpha Particle Tracks in Integrated Circuits," *Reliability Physics, 19th Annual Proceedings*, 1981, pp. 38-42.

28. Electric Power Research Institute, "A Review of Equipment Aging Theory and Technology," EPRI NP-1558, Palo Alto, CA, September 1980.

29 G. P. Pecht, R. Agarwal, and D. Quearry, "Plastic Packaged Microcircuits: Quality, Reliability, and Cost Issues," *IEEE Trans. Reliability*, Vol. 42, No. 4, 1993.

30. M. Priore and J. Farrel, "Plastic Microcircuit Packages: A Technology Review," *Rept. CRTA-PEM*, Reliability Analysis Center, Rome, NY, March 1992.

31. *Texas Instruments Military Plastic Packaging*, Preliminary Handbook, Texas Instruments, 1992.

32. L. Condra *et. al.*, "Comparison of Plastic and Hermetic Microcircuits Under Temperature-Humidity Bias," *IEEE Trans. Components, Hybrids, and Manufacturing Technology*, Vol. 15, Oct. 1992 , pp. 640-650.

33. C. A. Lidback, "Plastic Encapsulated Products vs Hermetically-Sealed Products," *Summary report*, Motorola Inc., Govt. Electronics Group, January 1987.

34. R. J. Straub, "Automotive Electronic IC Reliability," *Proc. Custom Integrated Circuit Conf.*, 1990, pp. 92-94.

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

36. K. Spang, "Methodology for Artificial Aging of Electrical Components in Nuclear Power Plants: Results of Experimental Studies," SKI Technical Report 93:39, Sweden, 1993.

37. R. Lofaro *et. al.*, *Literature Review of Environmental Qualification of Safety-Related Electric Cables—Literature Analysis and Appendices*, NUREG/CR-6384, Vol 2, U.S. Nuclear Regulatory Commission, April 1996.

38. Ralph T. Johnson, Jr. *et. al., A Survey of the State-of-the-Art in Aging of Electronics With Application to Nuclear Power Plant Instrumentation*, NUREG/CR-3156, U.S. Nuclear Regulatory Commission, April 1983.

39. M. Subudhi, *Literature Review of Environmental Qualification of Safety-Related Electric Cables—Summary of Past Work*, NUREG/CR-6384, Vol. 1, U.S. Nuclear Regulatory Commission, April 1996.

40. James F. Gleason and Robert Hall, "Environmental Qualification of Nuclear Power Plant Control Equipment," *Instrumentation in the Power Industry*, Instr. Soc. of America, January 1978.

41. *Final Safety Analysis Report*, Grand Gulf Nuclear Station (BWR), Vol. 7, Section 3.11.

42. *Final Safety Analysis Report*, Vogtle Electric Generating Plant (PWR), Vol. 8, Section 3.11.

43. System 80^{+} CESSAR, Design Certification, Combustion Engineering, Vol. 4, App. 3.11A.

44. *Equipment Qualification Data Packages*, WCAP-8587, Westinghouse, 1978.

45. Electric Power Research Institute, "Radiation Effects on Organic Material in Nuclear Power Plants," EPRI NP-2129, Palo Alto, CA, November 1981.

46. James F. Gleason, "Aging and Seismic Performance for Safety-Related Equipment in a Mild Environment," *IEEE Trans. Nucl. Sc.*, Vol. NS-31, No. 1, February 1984.

47. G. C. Messenger and M. S. Ash, *The Effects of Radiation on Electronic Systems,* ISBN 0-442-25417-2, Van Nostrand Reinhold Company Inc., 1986, p. 296.

48. James R. Schwank, "Basic Mechanisms of Radiation Effects in the Natural Space Radiation Environment," SAND94-1580, Sandia National Laboratory.

49. G. C. Messenger and M. S. Ash, *The Effects of Radiation on Electronic Systems,* ISBN 0-442-25417-2, Van Nostrand Reinhold Company Inc., 1986, pp. 251, 294.

50. Takaaki Ohsaki, "Electronic Packaging in the 1990's–A Perspective From Asia," *IEEE Trans. On Components, Hybrids, and Manufacturing Technology*, Vol. 14, No. 2, June 1991, pp. 254-161.

51. Rao R. Tummala, "Electronic Packaging in the 1990's–A Perspective From America," *IEEE Trans. On Components, Hybrids, and Manufacturing Technology*, Vol. 14, No. 2, June 1991, pp. 262-271.

52. Herman Wessely *et. al.*, "Electronic Packaging in the 1990's–The Perspective From Europe," *IEEE Trans. On Components, Hybrids, and Manufacturing Technology*, Vol. 14, No. 2, June 1991, pp. 272-284.

53. K. Korsah, T. J. Tanaka, and 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.

54. Institute of Electrical and Electronics Engineers, IEEE 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," June 1987.

55. Institute of Electrical and Electronics Engineers, IEEE 334-1974, "IEEE Standard for Type Tests of Continuous Duty Class 1E Motors for Nuclear Power Generating Stations," March 1994.

56. 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.

57. Mahbubul Hassan and William E. Vesely, "Advanced Digital I&C Systems in Nuclear Power Plants: Risk-Sensitivities to Environmental Stressors," *1996 Amer. Nucl. Soc. Top. Mtg. On Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*,Vol. 2, pp 1197-1202.

58. U.S. Department of Defense, MIL-STD-810E, "Environmental Test Methods and Engineering Guidelines," July 1989.

59. U.S. Department of Defense, MIL-PRF-38535D, "General Specifications for Integrated Circuits (Microcircuits) Manufacturing," October 1995.

60. U.S. Department of Defense, MIL-STD-883, "Test Methods and Procedures for Microelectronics," November 1995.

61. International Organization for Standardization, ISO 9000, "Quality Management and Quality Assurance Standards," 1994.

62. Lennart Cider, "Cleaning and Reliability of Smoke-Contaminated Electronics," *Fire Technology*, Third Quarter, 1993.

63. *The Rome Laboratory Reliability Engineer's Toolkit,* Systems Reliability Division, Rome Laboratory, Griffiss Air Force Base, NY, April 1993.

64. *Reliability Analysis/Assessment of Advanced Technologies*, RADC-TR-90-72, Rome Air Development Center, Griffiss Air Force Base, NY, May 1990.

65. Pecht, M., and W. C. Ko, "A Corrosive Rate Equation for Microelectronic Metallization," *The Intl. Journal for Hybrid Microelectronics,* Vol. 13, No. 2, June 1990, pp. 41-51.

66. 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.

67. Willing, W.E., and N. P. Goldstein, "Combining Single-Event Latchup and Reliability Requirements for Space Vehicles," *Proc. Ann. Reliability & Maintainability Symp.*, IEEE Reliability Society, 1995, pp 445-449.

68. *Computer-Based Digital System Failures*, Technical Review Report, AEOD/T9-03, Reactor Analysis Branch, Safety Programs Division, Office of Analysis and Evaluation of Operational Data, U. S. Nuclear Regulatory Commission, July 1994.

69. *Aging Assessment of Surge Protective Devices in Nuclear Power Plants*, NUREG/CR-6340, U. S. Nuclear Regulatory Commission, January 1996.

70. *Verification and Validation Guidelines for High Integrity Systems*, NUREG/CR-6293, Vol. 2, U. S. Nuclear Regulatory Commission, March 1995.

71. *Standard Technical Specifications - Westinghouse Plants*, NUREG-1431, Vol. 2, U. S. Nuclear Regulatory Commission, September 1992.

72. M. P. Bohn *et. al.*, *Analysis of Core Damage Frequency, SURRY Unit 1, External Events*, NUREG/CR-4550, Vol. 3, Rev. 1, Part 3, U. S. Nuclear Regulatory Commission, December 1990.

73. SURRY Power Station Units 1 & 2, Updated Final Safety Analysis Report, July 1982.

74. Seabrook Station, Final Safety Analysis Report, Volume 8, May 1991.

75. R. D. Fowler *et. al.*, SURRY Unit 1 IRRAS Version 5.0 PRA Data Base, Idaho National Engineering Laboratory, April 28, 1993.

76. Edgar M. Brown, "System Operating Experience at ABB CE Plants," *Nuclear Plant Journal*, May-June, 1995, pp. 24-29.

77. R. J. Hanson, "Conducted Electromagnetic Transient-Induced Upset Mechanisms: Microprocessor and Subsystem Level Effects," *Proc. of EOS/ESD Symposium*, 1987, EOS-9, p. 104.

78. P. E. Gammil and J. M. Soden, "Latent Failures Due to Electrostatic Discharge in CMOS Integrated Circuits," *Proc. of EOS/ESD Symposium*, 1986, EOS-8, pp. 78-79.

79. U.S. Department of Defense, MIL-STD-461C, "Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility," August 1986.

80. U.S. Department of Defense, MIL-STD-462, "Measurement of Electromagnetic Interference Characteristics," July 1967.

81. Steve P. Nowlen, "Defining Credible Smoke Exposure Scenarios," Letter Report to U. S. NRC, Sandia National Laboratories, September 1994.

82. P.D. Ewing and K. Korsah, "Technical Basis for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems," NUREG/CR-5941, U. S. Nuclear Regulatory Commission, April 1994.

83. R. L. Iman, Burress, R. V., Anderson, D. J., et. al., 1995, "Evaluation of Low-Residue Soldering for Military and Commercial Applications– A Report from the Low Residue Soldering Task Force," Sandia National Laboratories, Albuquerque, NM.

84. L. Bustard and P. Holzman, "Low-Voltage Environmentally Qualified Cable License Renewal Industry Report; Revision 1," Electric Power Research Institute, 1994.

85. B. Reagor, "Smoke Corrosivity: Generation, Impact, Detection, and Protection," *Fire Sciences*, Vol. 10, 1992, pp. 169-179.

86. L. M. Caudill, J. T. Chapin, R. B. Comizzoli *et. al.*, "Current State of Fire Corrosivity Testing: Preliminary Electrical Leakage Current Measurements," *International Wire & Cable Symposium*, 1995, pp. 432-437.

87. M. Arvidson and H. Persson, "Koldioxids (CO_2) paverkan pa elektronik - slackning med laga koncentrationer. [Carbon Dioxide Suppression Systems - Risk of Damage to Electrical Equipment.]," Swedish National Testing and Research Institute, SR Report 1993:20.

88. Institute of Electrical and Electronics Engineers, IEEE 384-1981, "Independence of Class 1E Equipment and Circuits," September 1980.

89. P. D. Ewing and R. T. Wood, *Recommended Electromagnetic Operating Envelopes for Safety-Related I&C Systems in Nuclear Power Plants*, NUREG/CR-6431, U. S. Nuclear Regulatory Commission, January 1998.

90. S. W. Kercel, M. R. Moore, E. D. Blakeman, P. D. Ewing, and R. T. Wood, *Survey of Ambient Electromagnetic and Radio-Frequency Interference Levels in Nuclear Power Plants*, NUREG/CR-6436, U. S. Nuclear Regulatory Commission, November 1996.

APPENDIX: A METHODOLOGY FOR THE QUALIFICATION OF SAFETY-RELATED MICROPROCESSOR-BASED INSTRUMENTATION AND CONTROL EQUIPMENT FOR NUCLEAR POWER PLANTS

A.1 Introduction

In this Appendix we propose a methodology for environmental qualification of safety-related microprocessor-based instrumentation and control (I&C) equipment based on the technical basis established in this document. The methodology is based on the authors' recommendations that type testing should be the preferred method of qualification for microprocessor-based safety-related systems, that qualification of I&C systems should begin at the integrated-circuit-manufacturing level, an analysis of the effect of stressors on the equipment, and the expected normal and accident conditions in the location in which the equipment will be placed.

A.2 Proposed Methodology

(1) *The standards used by the integrated circuit (IC) manufacturer for component stress testing and qualification should be documented.*

ICs are susceptible to long-term failure mechanisms under various environmental stressors. Examples of these failure mechanisms are electromigration and corrosion of metal interconnects. However, environmental testing and stress screening methodologies exist to enable the severity of these potential failures in a particular technology to be identified during manufacture. Thus, it is important that qualification of I&C systems begin at the integrated-circuit-manufacturing level. That is, quality of I&C systems must be "built in" as well as "tested in." Built-in quality can be enhanced by assuring, among other process control methodologies, a minimum of stress tests aimed at enhancing component reliability.

As a minimum, qualification testing of the ICs shall include, but not limited to:

Temperature/Humidity Bias Tests
This is an environmental test designed to measure the moisture resistance of plastic encapsulated circuits, and is typically performed at a temperature of 85°C and a relative humidity (RH) of 85% for 1008 hours or more.

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

Temperature Cycle Tests
The goal of these tests 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 and 150°C respectively, with the test duration being 1000 cycles or more.

Autoclave Tests
This is an environmental test designed to measure device resistance to moisture penetration and the resultant effects of galvanic corrosion. Corrosion of the die is the expected failure mechanism, and typical test conditions are 121 °C at 100% RH and 0.205 MPa (15 psig). Typical test durations are 48 and 96 hours.

Low Temperature Operating Life Tests
This test is designed to accelerate hot carrier injection effects in metal oxide semiconductor (MOS) devices by exposing them to room temperature and applying biased operating conditions. Conditions for failure include threshold shifts and other parametric changes such as transconductance.

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

(2) *The location category of the safety I&C equipment should be identified.*

It is the primary role of qualification to ensure that Class 1E equipment can perform its safety function(s) with no failure mechanism that could lead to common cause failures under postulated service conditions. Semiconductor manufacturers' quality assurance (QA) activities generally ensure that maximum temperature ratings of industrial grade semiconductors exceed 176°F (80°C). Reliability stress tests routinely employed by semiconductor manufacturers to ensure component quality typically use temperature and humidity levels that exceed expected abnormal and accident conditions in the control room. These tests typically include the following: autoclave test (measures device resistance to moisture penetration and the resultant effect of galvanic corrosion), high temperature high humidity bias test (measures moisture resistance of plastic encapsulated devices), high temperature gate bias test (designed to electrically stress the gate oxide under a bias condition at high temperature), and high temperature storage life test (performed to accelerate failure mechanisms that are thermally activated through the application of extreme temperatures). Temperature in control room environments under *abnormal* [e.g., loss of heating, ventilation, and air-conditioning (HVAC)] conditions are not likely to exceed 120°F (49°C). [Normal temperature range in the control room is 60 to 80°F (16 to 27°C). Protection systems, which are typically located in the control room, are required to function for at least 12 hours under abnormal conditions.] Under these conditions, semiconductors are not likely to exhibit significant failure mechanisms caused by temperature. High humidity (above 85 %) is unlikely to be a problem unless it is accompanied by high temperature. In the environments proposed for digital safety I&C, such high humidity is likely only under accident conditions.

The above discussion suggests that certain locations in a nuclear power plant can be considered benign,[a] especially if a minimum level of qualification testing can be assured for the IC components, as is suggested in this methodology. The environment categories defined below can be used to identify whether aging should be considered during type testing of the microprocessor-based equipment:

[a] Section 49(c) of Title 10, part 50 of the *Code of Federal Regulations*; "A mild environment is an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences."

Location category A

Location category A is any location where the expected normal and abnormal service conditions with regard to environmental stressors are likely to be equal to, or exceed, the following:

Radiation	Normal gamma dose: $>10^4$ over 40 years.
Temperature	Normal: 32 to 49°C (90 to 120°F); abnormal and accident: >49°C (120°F).
Humidity	Normal: 20 to 90%; abnormal and accident: >95%.

Notes:

(1) There are areas inside containment where the integrated 40-year gamma dose is likely to exceed 10^4 rad. Examples include locations next to the reactor vessel, where the total dose may exceed 1.8×10^{10} rad in PWRs. However, such locations are not likely to house microprocessor-based I&C equipment.[1] The dose value used here represents the expected dose in the general area outside the reactor loop compartment wall.

(2) The temperature and humidity figures are average values estimated from the SAR and equipment data packages examined.

(3) Environmental qualification of equipment located in this area has typically included simulated aging.

Location category B:

Location category B is any location where the expected normal and abnormal service conditions with regard to environmental stressors are likely to correspond to the following:

Radiation	Normal total gamma dose: $>4 \times 10^2$ rad, but $<10^4$ rad, over 40 years.
Temperature	Normal: 27 to 41°C (80 to 105°F); Abnormal and accident: >41°C (105°F).
Humidity	Normal: 20 to 70%; Abnormal and accident: >95%.

Notes:

(1) Category B locations may be ventilated or nonventilated. Examples of such locations include pipe and electrical penetration rooms and parts of the auxiliary building containing equipment having safety-related functions.

(2) A category B location may be mild under normal conditions, but under accident conditions may experience high temperature, humidity, and/or radiation conditions comparable to containment in the event of a loss-of-coolant accident (LOCA) or high-energy line break (HELB).

(3) Environmental qualification of equipment located in this area has typically included simulated aging.

Location category C:

Location category C is any location where the expected normal and abnormal service conditions with regard to environmental stressors are likely to correspond to the following:

Radiation	Normal total gamma dose: $<4\times10^2$ rad over 40 years.
Temperature	Normal: 16 to 27°C (60 to 80°F); Abnormal and accident: >27°C (80°F) [49°C (120°F) maximum].
Humidity	Normal: 30 to 50%; Abnormal and accident: <95%.

Notes:

(1) Category C locations are typically air conditioned or ventilated. The control room is an example of a category C location.

(2) We define a *benign* environment to be identical to a category C location. In such a service environment, a seismic event is the only design basis event that can be expected to have catastrophic effect on all redundant safety equipment. Note that benign (category C) environments constitute a subset of category B locations.

(3) Environmental qualification of equipment located in this area has typically *not* included simulated aging. A total 40-year dose of less than 400 rad is quoted by reference[2] for RPS equipment located in the control room.

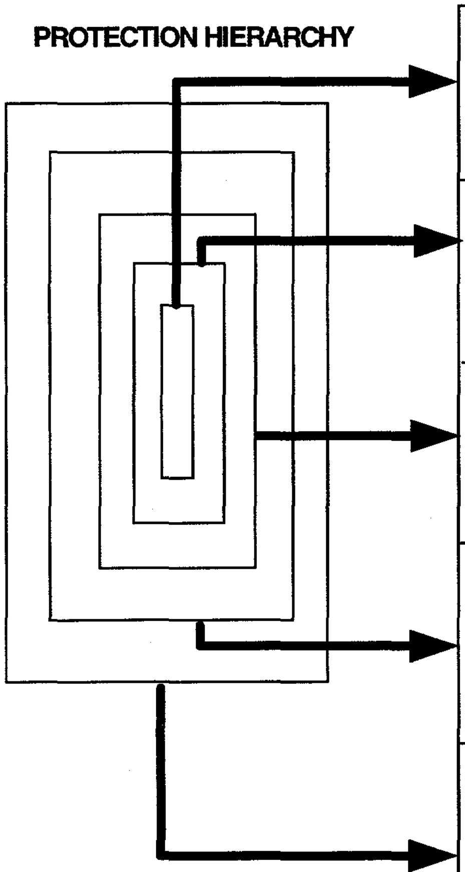
3. *Provide documentation to demonstrate how the safety I&C equipment is protected against environmental effects.*

Environmental reliability shall be built into the system at various levels. Fig. A.1 illustrates the various levels at which protection against the environment for the actual circuits/components performing a safety-related function can be assured.

The first level of environmental protection is provided by the HVAC system in the room or enclosure where the safety-related equipment is installed. While the HVAC system controls the environmental parameters such as humidity, temperature, and airborne particulates, the room itself may serve as a radiation shield for the equipment and a level of protection against the spread of smoke and fire in case a fire occurs.

The next level of protection for the safety system electronics is provided by the cabinet itself. Various design features such as fans, filters, and EMI/RFI shielding should be considered in the cabinet design. The fans and fan filters provide additional 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 help to prevent standing water if connections are made from the bottom of the cabinet.

Depending on the system design, the next level of protection may be modules, racks, or circuit boards inside the cabinet. Circuit boards may be mounted vertically 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 printed circuit board manufacturing techniques (e.g., use of solder mask, conformal coating, etc.) should provide significant defenses against short-term smoke exposure effects.



	Stressors	Environmental controls
Electronic component	• Radiation • Temperature • Humidity • EMI/RFI effects • Smoke, corrosive gases • Vibration	• Packaging (insertion mount, surface mount, chip-on-board • Circuit design (e.g., component ratings)
Circuit Board	• Radiation • Temperature • Humidity • EMI/RFI effects • Smoke, corrosive gases • Vibration	• Heat sinks • Shielding • Board layout • coating
Module/Rack	• Radiation • Temperature • Humidity • EMI/RFI effects • Smoke, corrosive gases • Vibration	• Fans • Shielding • Board enclosure design (e.g., inner foam cover)
Cabinet	• Radiation • Temperature • Humidity • EMI/RFI effects • Smoke, corrosive gases • Vibration	• Fans • Filters • Cabinet design • Shielding
Room	• Radiation • Temperature • Humidity • EMI/RFI effects • Smoke, corrosive gases • Vibration	• HVAC • Filtering • Fire protection • Shielding (gamma) • Location

Figure A.1 Illustrating levels of protection against environmental stressors for safety-related electronic hardware

The final level of environmental protection for system components is at the chip level. Thermal management problems at the chip level become increasingly significant as clock frequencies increase, while more circuitry is crammed onto microprocessors and other ICs. Moreover, as the number of on-chip input/outputs increase, new and often complex schemes must be used to make the necessary connections between closely packed circuits. This has led to increasingly sophisticated packaging technologies. Thermal protection at the microcircuit level, however, is the responsibility of chip design/packaging engineers. and not overall system design engineers. Thus the equipment qualifier only has to demonstrate that chips used for the design of a safety-related system have undergone adequate electronic stress screening tests, such as those identified under Section A.2.1.

4. *If the safety equipment is in a category A location, perform environmental qualification per IEEE 323-1983, subject to clarifications detailed below.*

For equipment in a Category A location, preconditioning (aging) shall be applied. In addition, a 10% margin shall be applied to all type test parameters for design basis event (DBE) testing. One reason for requiring preconditioning for Category-A-located equipment is the (possible) differences in aging times used during IC qualification testing on the one hand, and the expected service life of a safety equipment in a nuclear environment on the other. Since an I&C equipment in a category A environment will experience elevated radiation, temperature, and humidity under normal service conditions, it is important to ensure that the equipment will perform its safety function under DBE conditions *after* operating in the normal environment over a specified amount of time. It is the degradation with time (aging), followed by exposure to environmental extremes from design basis events, which presents a potential for causing common cause failures of safety equipment.

Rationale for Recommending IEEE 323-1983

The basis for the qualification of equipment important to safety comes from the *Code of Federal Regulations* (10 CFR 50.49). Regulatory Guide 1.89 describes methods acceptable to the NRC staff for complying with 10 CFR 50.49. IEEE Standard 323 establishes the basic requirements and methods for qualification. Regulatory Guide 1.89 endorses IEEE 323-1974 but does not endorse IEEE 323-1983. (This 1983 revision of IEEE 323 was reaffirmed in 1990 and 1996.) In this document, we recommend the use of the 1983 version (with appropriate clarifications as discussed in subsequent sections) for the following reasons:

(1) The methods of qualification—type testing, operating experience, and analysis—are identical in both versions.

(2) The reasons and concepts for aging are essentially the same in both versions.

(3) IEEE 323-1983 appears to have introduced the concept of "Significant Aging Mechanisms" so that the user of the standard can determine whether aging should be considered during type testing. While this concept is not explicitly stated in the 1974 version, it is important to note that the 1974 version does allow the exclusion of radiation during aging "if the required radiation level (necessary to simulate the equipment's expected end-of-qualified-life condition) can be shown to produce less effect than that which would cause loss of the equipment's Class 1E function." Thus, as in the 1983 version, the 1974 version allows an environmental stressor to be excluded in the aging program if its effect is "not significant."

(4) The types of stressors and the sequential method of their application during preconditioning are more clearly stated in IEEE 323-1983. However, neither standard addresses situations where synergistic effects may exist. In conformity with current applicable standards, the basic sequence followed in most programs is thermal aging, irradiation to aging-plus-accident dose, seismic test and main steam-line break (MSLB)/LOCA testing. However, this sequence is not necessarily the most conservative for microprocessor-based equipment and/or some packaging technologies. Since microprocessor-based safety systems are inherently more complex than their analog counterparts, it is important that aging methodologies increase, as much as possible, the assurance of their long term performance. It is suggested however, that present methodologies continue to be applied until more is known about the aging sequence and synergistic effects on advanced digital technologies. It is worth noting here that not all qualified equipment have followed the traditional methods. For example, on some cable specimens, Anaconda, Samuel Moore, and Raychem have qualified them using pre-aging with irradiation, followed by thermal aging. Also, ITT Suprenant, BIW, and Raychem have qualified some of their cables using simultaneous thermal and irradiation conditions during pre-aging.

(5) The intent of the section on "Margin" is essentially the same in both versions of the IEEE standard. However, the 1983 version provides further clarification by explicitly stating that "margin shall be applied to the type test parameters for DBE testing."

One difference between the two versions is that the 1983 version appears to imply that neither a qualification program, nor a test plan, is required for equipment located in a mild environment. We have proposed clarification by (1) defining three categories of geographical location in a nuclear power plant, and (2) suggesting documentation procedures in this methodology for the three geographical locations.

Documentation Procedures for Safety I&C Equipment in a Category A Location

The documentation requirements for a category A location is identical to the requirements in IEEE 323-1983. In particular, the user shall maintain a qualification file containing the following information:

(1) Identification of the equipment qualified
(2) Equipment specification
(3) Qualification program (Aging should be considered in the qualification program)
(4) Identification of any scheduled surveillance/maintenance, periodic testing, and any parts replacement required to maintain qualification
(5) Identification of safety functions to be demonstrated by test data
(6) Test plan
(7) Report of test results
(8) Summary and conclusions, including limitations and qualified life or periodic surveillance/maintenance interval determination.

Stressors

EMI/RFI

EMI/RFI and power surges should be considered in a qualification program. Generally, a qualification program must identify all environmental stressors under normal and abnormal service conditions. EMI/RFI and power surges are environmental stressors that can affect the performance of digital/computer-based equipment important to safety. Therefore, controlling electrical noise and the susceptibility of I&C

systems to EMI/RFI and power surges is a necessary step in meeting the intent of this methodology. Stressor prioritization studies summarized in this report indicate that EMI/RFI can be risk-significant even when only critical failures are considered and credit is given for detecting some failures through system self-diagnostics. Also, during tests conducted on the EDSC, the most prevalent stressor-induced upsets, as well as the most severe (e.g., permanent module failure) occurred during the EMI/RFI tests. A survey of LERs suggest that EMI/RFI also is a significant problem in current power plants.[1] The increased use of microprocessors and digital circuitry, combined with the use of higher clock frequencies, faster logic families, and lower-level logic voltages, may result in a greater susceptibility to upsets and malfunctions caused by the effects of EMI/RFI. While several standards exist and are used by reactor equipment manufacturers for EMI/RFI qualification of their digital equipment, no specific guidelines are presently available, to the authors' knowledge, that sets limits and criteria for the nuclear power plant environment. IEEE Standard 1050, *Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, was developed to provide guidance specific to a power generating plant for the design of grounding systems for I&C equipment. For the most part, IEEE 1050 is accurate in its treatment of electromagnetic compatibility (EMC) design and installation practices and applicable to the nuclear power plants environment. In addition, MIL-STD-461D, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference,* and MIL-STD-462, *Measurement of Electromagnetic Interference Characteristics*, are considered applicable to the needs of the nuclear industry. MIL-STD 461D and 462 were developed for use by the U.S. Department of Defense agencies to evaluate EMC. Applying to both equipment designs and procurement specifications, the purpose of the standards is to ensure that equipment and subsystems are compatible with their intended electromagnetic operating environment, and that EMI effects are considered early in the design process.

A standard applicable to the nuclear industry should include guidance on EMI, electromagnetic susceptibility, ESD, high-frequency transients, surge withstand, and lightning effects. A Regulatory Guide is currently being developed by the NRC for the nuclear industry. Until it is available, current standards such as IEEE 1050, MIL-STD 461D, MIL-STD 462 should continue to be used.

Smoke

A stressor not previously considered for safety system qualification is smoke exposure. Research findings documented in this report have shown that smoke is a stressor that can adversely impact digital safety equipment. However, research to date does not support the explicit inclusion of smoke exposure as a stressor during type testing. In addition there is no systematic, fully repeatable, test standard, so smoke exposure type testing is currently impractical. Currently, fire and its effects (smoke, heat, ignition explosions, toxic gases) on safety-related equipment is a fire protection concern that, in our opinion, are addressed in General Design Criteria (GDC) 3 of Appendix A of 10 CFR 50, IEEE 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," and Appendix R of 10 CFR 50. GDC 3 requires that structures, systems, and components important to safety be located to minimize the probability and effects of fires and explosions. IEEE Standard 384 requires that an electrically generated fire in a class 1E division shall not result in loss of function in the redundant Class 1E divisions. In addition to these requirements, Appendix R of 10 CFR 50 requires a defense-in-depth approach to be taken to (1) prevent fires from starting; (2) detect rapidly, control, and extinguish promptly those fires that do occur; and (3) provide protection for structures, systems, and components important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent safe shutdown of the plant. These practices should limit the chances of smoke exposure.

Margins

"Margin" is the difference between the most severe specified service conditions of the plant and the conditions used in type testing to account for normal variations in commercial production of equipment and reasonable errors in defining satisfactory performance. The margins recommended in IEEE 323-1983 are reasonable for digital I&C safety **systems** in a category A location, especially if a minimum of qualification testing at the **IC** level, as suggested in Section A.2.1, can be assured. Variations in commercial production of ICs is underscored by the results of tests performed by a major French origninal equipment manufacturer (OEM), under contract to the French Ministry of Defense.[3] The OEM subjected ten IC lots (from ten IC suppliers) of 30 molded devices each to extended testing. For two lots, there were no failures at the end of 3000 hours of testing. For one lot, there was only a single failure after 3000 hours. Two lots were removed from testing at 750 hours with failure rates nearing 100%. Four other lots were removed from testing at 1000 hours with 55% failures. For the last lot, there were no failures for the first 1000 hours, but at 1500 hours 28 out of the 30 devices failed.[3] The results show a wide variation among manufacturers, and underscores the importance of selecting a source of supply with great care for high integrity systems such as those required for nuclear power plants.

5. *If the safety equipment is in a category B location, perform environmental qualification per IEEE 323-1983, subject to the clarifications described below.*

For equipment in a category B location, preconditioning need not be used, but testing should include all DBE conditions. There should be a 10% margin on the **test duration** as well as for all test parameters for DBE testing. For example, if an equipment is required to perform its function for 10 hours during a DBE, the system should be tested for 11 hours. The following documentation shall be provided:

(1) Identification of the equipment qualified
(2) Equipment specification
(3) Identification of any scheduled surveillance/maintenance, periodic testing, and any parts replacement required to maintain qualification
(4) Identification of safety function(s) to be demonstrated by test data
(5) Test plan
(6) Report of test results
(7) Summary and conclusions, including limitations and qualified life or periodic surveillance/maintenance interval determination.

6. *If the safety equipment is in a category C location, perform environmental qualification per IEEE 323-1983, subject to the clarifications described below.*

For equipment in a category C location, preconditioning need not be used. In addition, unlike the case for a category B location, a 10% margin on the test duration is not required. However, a 10% margin is required for all test parameters under postulated DBEs. The following documentation shall be provided:

(1) Identification of the equipment qualified
(2) Equipment specification
(3) Identification of any scheduled surveillance/maintenance, periodic testing, and any parts replacement required to maintain qualification
(4) Identification of safety function(s) to be demonstrated by test data.

(5) EITHER:
(a) Test plan
(b) Report of test results

OR:

A certificate of compliance that the equipment supplied meets the requirements of the equipment specification.

7. *Address random and age-related failures using surveillance, on-line diagnostics, maintenance, and trending techniques.*

Wherever possible, advantage should be taken of the potential of microprocessor-based systems to perform advanced and on-line diagnostics, thereby improving the ability to detect both random and impending failures beyond present capabilities.

References

1. Korsah, K., 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. Herman Wessely *et. al.*, "Electronic Packaging in the 1990's–The Perspective From Europe," *IEEE Trans. On Components, Hybrids, and Manufacturing Technology*, Vol. 14, No. 2, June 1991, pp. 272-284.

3. *Navigator-Technology Direction for the MIL/AERO Community*, National Semiconductor, Vol. 8, Spring 1996.

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-6479
ORNL/TM-13264

2. TITLE AND SUBTITLE

Technical Basis for Environmental Qualification of Microprocessor-Based Safety-Related Equipment in Nuclear Power Plants

3. DATE REPORT PUBLISHED

MONTH	YEAR
January	1998

4. FIN OR GRANT NUMBER

L1798

5. AUTHOR(S)

K. Korsah, ORNL
R. T. Wood, ORNL
M. Hassan, BNL
T. J. Tanaka, SNL

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.)*

ORNL
P. O. Box 2008
Oak Ridge, TN
37831-6010

BNL
P. O. Box 5000
Bldg. 130
Upton, NY 11973

SNL
P. O. Box 5800
Albuquerque, NM
87185-0747

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

10. SUPPLEMENTARY NOTES

C. Antonescu, NRC Project Manager

11. ABSTRACT *(200 words or less)*

This document presents the results of studies sponsored by the Nuclear Regulatory Commission (NRC) to provide the technical basis for environmental qualification of computer-based safety equipment in nuclear power plants. The studies were conducted by Oak Ridge National Laboratory (ORNL), Sandia National Laboratories (SNL), and Brookhaven National Laboratory (BNL).

The studies address the following: (1) adequacy of the present test methods for qualification of digital I&C systems; (2) preferred (i.e., Regulatory Guide-endorsed) standards; (3) recommended stressors to be included in the qualification process during type testing: (4) resolution of need for accelerated aging for equipment to be located in a benign environment; and (5) determination of an appropriate approach for addressing the impact of smoke in digital equipment qualification programs.

Significant findings from the studies form the technical basis for a recommended approach to the environmental qualification of microprocessor-based safety-related equipment in nuclear power plants.

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

digital
EMI/RFI
environmental stressors
humidity
instrumentation and controls (I&C)
microprocessor
nuclear power plant
PRA
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