NUREG/CR-6406
ORNL/TM-13122

Environmental Testing of an Experimental Digital Safety Channel

Prepared by
K. Korsah, ORNL
T. J. Tanaka, SNL
T. L. Wilson, Jr., R. T. Wood, ORNL

Oak Ridge National Laboratory
Sandia National Laboratories

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555-0001

2. The Superintendent of Documents, U.S. Government Printing Office, P. O. Box 37082, Washington, DC 20402-9328

3. The National Technical Information Service, Springfield, VA 22161-0002

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC bulletins, circulars, information notices, inspection and investigation notices; licensee event reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the Government Printing Office: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grantee reports, and NRC booklets and brochures. Also available are regulatory guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG-series reports and technical reports prepared by other Federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions. *Federal Register* notices, Federal and State legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, Two White Flint North, 11545 Rockville Pike, Rockville, MD 20852-2738, for use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018-3308.

DISCLAIMER NOTICE

NUREG/CR-6406
ORNL/TM-13122

Environmental Testing of an Experimental Digital Safety Channel

Manuscript Completed: August 1996
Date Published: September 1996

Prepared by
K. Korsah, ORNL
T. J. Tanaka, SNL
T. L. Wilson, Jr., R. T. Wood, ORNL

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

Sandia National Laboratories
Managed by Lockheed Martin, Inc.

Oak Ridge National Laboratory
Oak Ridge, TN 37831-6010

Sandia National Laboratories
Albuquerque, NM 87185-0747

C. 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

ABSTRACT

This document presents the results of environmental stress tests performed on an experimental digital safety channel (EDSC) assembled at the Oak Ridge National Laboratory (ORNL) as part of the NRC-sponsored *Qualification of Advanced Instrumentation and Controls (I&C) System* program. The objective of this study is to investigate failure modes and vulnerabilities of microprocessor-based technologies when subjected to environmental stressors. The study contributes to the technical basis for environmental qualification of safety-related digital I&C systems.

The EDSC employs technologies and digital subsystems representative of those proposed for use in advanced light-water reactors (ALWRs) or for retrofits in existing plants. Subsystems include computers, electrical and optical serial communication links, fiber-optic network links, analog-to-digital and digital-to-analog converters, and multiplexers. The EDSC was subjected to selected stressors that are a potential risk to digital equipment in a mild environment. The selected stressors were electromagnetic and radio-frequency interference (EMI/RFI), temperature, humidity, and smoke exposure. The stressors were applied over ranges that were considerably higher than what the channel is likely to experience in a normal nuclear power plant environment. Ranges of stress were selected at a sufficiently high level to induce errors so that failure modes that are characteristic of the technologies employed could be identified.

Significant 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.

(2) Based on incidence of errors during testing, EMI/RFI, smoke exposure, and high temperature coupled with high relative humidity 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). Also, the effect of the stressor was typically immediate, whereas the occurrence of high temperature/humidity and smoke exposure effects was delayed for some interval (i.e., tens of minutes) after the application of the stressor.

(3) While 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.

(4) With regard to temperature and humidity, the study found that the combination of high temperature and high relative humidity (RH) were the conditions that affected the EDSC, rather than temperature alone. High RH is not as likely in a controlled environment such as a control room, but such conditions still need to be considered in qualification, especially for postaccident monitoring (PAM) 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 large control room panel fire conditions (smoke density of about 3 g/m^3). A large control room panel fire has been postulated by Steve Nowlen as the most severe fire that might be experienced in the main control room. This represents the *smallest* smoke density of the three fire scenarios postulated. Because of similarities between the EDSC and proposed advanced 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 large control room panel fire conditions. Given early detection of a fire and subsequent fire suppression, digital systems should maintain functionality (to allow safe shutdown) for about an hour following exposure, provided that the equipment is not directly exposed to the fire.

(7) The solder mask on commercial electronic boards appears to be effective in preventing catastrophic and/or permanent failure of the board even when the boards 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 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.)

The results of this study, along with results from related studies by Sandia National Laboratories and Brookhaven National Laboratory, will be used to develop the technical basis for possible enhancement of current qualification processes in a planned NUREG/CR report on an overall framework for the environmental qualification of digital safety-related I&C systems.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

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

The authors wish to acknowledge the contributions of several people in the Instrumentation and Controls Division of Oak Ridge National Laboratory in making this study possible. In particular, we wish to thank Gary Turner for his significant contributions during the initial hardware design and equipment procurement and Jim Mullens for developing the software used in the safety channel and in the engineered safety feature multiplexing unit. Jim's help during the many times we had to debug the integrated system is particularly appreciated. Thanks also go to José March-Leuba and David McMillan for their significant contributions during the development of the Host Computer software, particularly the data and error logging functions.

Mike Moore and Boyd Beets led the EMI/RFI tests, while Ed Reed led the temperature/humidity tests. The efforts of these colleagues are very much appreciated.

Special thanks are due Brian Swail, also of Oak Ridge National Laboratory, for helping to conduct the smoke tests at Sandia National Laboratories. His contributions were invaluable during the many times that we had to dismantle and reassemble equipment as well as perform "electronic sleuthing" to figure out what had gone wrong.

Daniel Ramirez of Sandia National Laboratories also deserves special mention. Without his technical expertise in setting up the smoke chamber and the tests in general, it would have been extremely difficult, if not impossible, to have brought this study to completion.

Finally, the authors wish to thank Linda Sparks, Janice Asher, and Sandra Lyttle for their help in preparing the manuscript.

ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
A/D	analog-to-digital
ALWR	advanced light-water reactor
AM	amplitude modulation
ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
CERDIP	ceramic dual-in-line package
CFR	Code of Federal Regulations
CMOS	complementary metal oxide semiconductor
CPU	central processing unit
CSPE	chlorosulfonated polyethylene
D/A	digital-to-analog
DAS	dual attached station
DTC	digital trip computer
EDSC	experimental digital safety channel
EMI/RFI	electromagnetic interference/radio-frequency interference
EPR	ethylene propylene rubber
EUT	equipment under test
ESF/MUX	engineered safety feature multiplexing unit
FDDI	fiber distributed data interchange
FOM	fiber-optic module (used interchangeably with fiber optic line driver)
GTEM	Gigahertz Transverse Electromagnetic
HOSTP	host processor (used interchangeably with host computer)
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and controls
IC	integrated circuit
I/O	input/output
IEEE	Institute of Electrical and Electronic Engineers
LISN	line impedance stabilization network
LWR	light-water reactor
MB	megabyte
NMOS	N-channel metal oxide semiconductor
NRC	U.S. Nuclear Regulatory Commission
ORNL	Oak Ridge National Laboratory
PAM	post-accident monitoring
PEM	plastic encapsulated microcircuit
PRS/MUX	process multiplexing unit
RAM	random access memory
RH	relative humidity
rms	root mean square
ROM	read-only memory
SVGA	super VGA
TC	test chamber
VGA	video graphics adapter
XLPE	cross-linked polyethylene

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:

Conformal coating. Complete coating (e.g., with silicones) over components and solder joints of a printed-circuit board (PCB) to provide insulation resistance as well as protection against contamination and degradation by moisture. Typically used for high-reliability PCBs.

Error.[a] A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

Fault.[a] An accidental condition that causes a functional unit to fail to perform its required function. A fault, if encountered, may cause a failure.

Large control room panel fire.[b] A scenario postulated to generate a smoke load of ~3 g/m^3.

Mild environment.[c] An environment expected as a result of normal service conditions and extreme (abnormal) in-service conditions where a seismic event is the only design basis event of consequence. Synonymous with benign as used in this document.

Nibble. Four bits of digital data. In comparison, a group of eight bits makes one byte of digital data.

Significant fires in general plant areas.[b] A scenario postulated to generate a smoke load of ~20 g/m^3.

Small in-cabinet fire.[b] A scenario postulated to generate a smoke load of ~160 g/m^3.

Solder mask. An epoxy barrier applied to the printed-circuit surface of a board. Prevents solder bridges from forming during the component assembly wave soldering operation.

---

[a] *IEEE Standard Glossary of Software Engineering Terminology.*

[b] Nowlen, Steve, *Defining Credible Smoke Exposure Scenarios*, Letter Report to USNRC, Sandia National Laboratories, September 1994. See also Sect. 6.1.

[c] IEEE Standard 323-1983, "IEEE Standard for Qualification of Class 1E Equipment for Nuclear Power Generating Stations."

1 INTRODUCTION

1.1 Motivation for Digital I&C Qualification Research

Rising maintenance costs, coupled with lack of spare parts for instrumentation and control (I&C) systems no longer supported by the original manufacturer, are forcing an increasing number of utilities to consider upgrading with newer, more readily available technology such as fiber optic transmission and microprocessor-based systems. In addition, advanced light-water reactor (ALWR) manufacturers will make even more extensive use of such technologies in the design of both control and safety (Class 1E) systems. While the application of new technology in the nuclear environment is generally encouraged by the U.S. Nuclear Regulatory Commission (NRC),[1] the introduction of such new technology, either as retrofits in existing nuclear power plants or in the next generation of light-water reactors (LWRs), may require development of testing and acceptance criteria and new or revised qualification standards and guidelines. Accordingly, NRC initiated the confirmatory research program, *Qualification of Advanced Instrumentation and Control (I&C) Systems*, at the Oak Ridge National Laboratory (ORNL) to assess the impact of environmental stressors on I&C hardware.

Recognition that the use of computers in safety systems poses challenges different from those of analog systems prompted the development of IEEE Std 7-4.3.2-1993, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*.[2] 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 analysis must be performed to ensure that the system has a high "correct response probability" and that the probability of common cause failure (e.g., due to environmental stressors such as electromagnetic interference and/or inherent age-related degradation mechanisms) is reduced to an acceptable level. The NRC is obligated to examine new I&C innovations as they emerge and are applied to nuclear safety systems. The ongoing study is necessary to ensure that the nuclear industry can take advantage of the new technology while maintaining the extraordinarily high requirements for reliability needed in nuclear safety applications.

1.2 Motivation for Conducting Experimental Tests

A number of studies were performed to identify approaches that could be used in enhancing digital I&C qualification for the nuclear power plant environment (see Appendix A). In particular, ORNL sought to identify (1) environmentally related I&C system failure and reliability information in both the nuclear and nonnuclear industries; (2) literature on survivability of digital I&C equipment subjected to smoke exposure in nuclear power plant or similar environments; (3) literature and standards on qualification methodologies for digital I&C in nuclear power plants; and (4) foreign nuclear plant experience with digital I&C. The following conclusions were made from these studies:

(1) Experimental investigation of digital I&C environmental susceptibility was needed to fully determine the efficacy of digital qualification methodologies since no comprehensive database having sufficient detail to allow digital I&C system failures to be accurately related with causative mechanisms currently exists for either the nuclear or nonnuclear industries.

(2) Although some earlier work[3] had indicated that through-hole electronics can be reconditioned, with good results, after deposition of up to 100 μg chloride/cm^2, very few tests had been performed to determine the reliability of microprocessor-based electronic equipment in a smoke-filled environment.

(3) Smoke from an electrical fire had not previously been considered as a stressor for analog safety system qualification. To help resolve the question of whether smoke should be included in a qualification program, a study of the severity of system failures as a function of various environmental stressors, including those explicitly identified in current qualification standards for nuclear power plant environments, was needed. No such studies could be identified.

The tests documented in this report were performed to address the above issues.

1.3 Project Objective and Goal

One objective of this study into environmental compatibility is to identify failure modes and vulnerabilities that are unique to advanced digital systems. Therefore, this task was undertaken to determine experimentally the characteristic effects caused by environmental stressors using a system that is *representative* of advanced safety system designs. The tests performed in this work examine advanced digital components to determine susceptibility to various environmental stressors and to identify the failure modes and severity of consequences for advanced safety systems. The purpose is thus to enhance the regulatory process and provide guidance on the necessary level of testing for qualifying digital systems. The study focuses on advanced digital components, including fiber-optic network interface systems, serial communication links (optical fiber and copper transmission), analog-to-digital converters, multiplexers, and microprocessor-based trip systems when subjected to environmental stressors, including smoke, electromagnetic interference/radio-frequency interference (EMI/RFI), temperature, and humidity.

The study, along with smoke impact and stressor prioritization studies being performed by Sandia National Laboratories and Brookhaven National Laboratory, respectively, will support the development of the technical basis for the potential enhancement of current qualification processes. The interrelated research effort conducted by the three national laboratories is depicted in Figure 1.1.

1.4 Rationale for Design Choices During the Development of the Experimental Digital Safety Channel

This investigation seeks to address the following:

(1) What failure modes do the new technologies proposed for use in advanced safety systems exhibit when stressed beyond normal operating conditions?

(2) How are failures of certain subsystems (e.g., communication interfaces) likely to affect system performance (i.e., by determining the safety consequences of system-level effects)?

(3) How can these findings contribute to establishing and strengthening the technical basis for current regulatory guidelines?

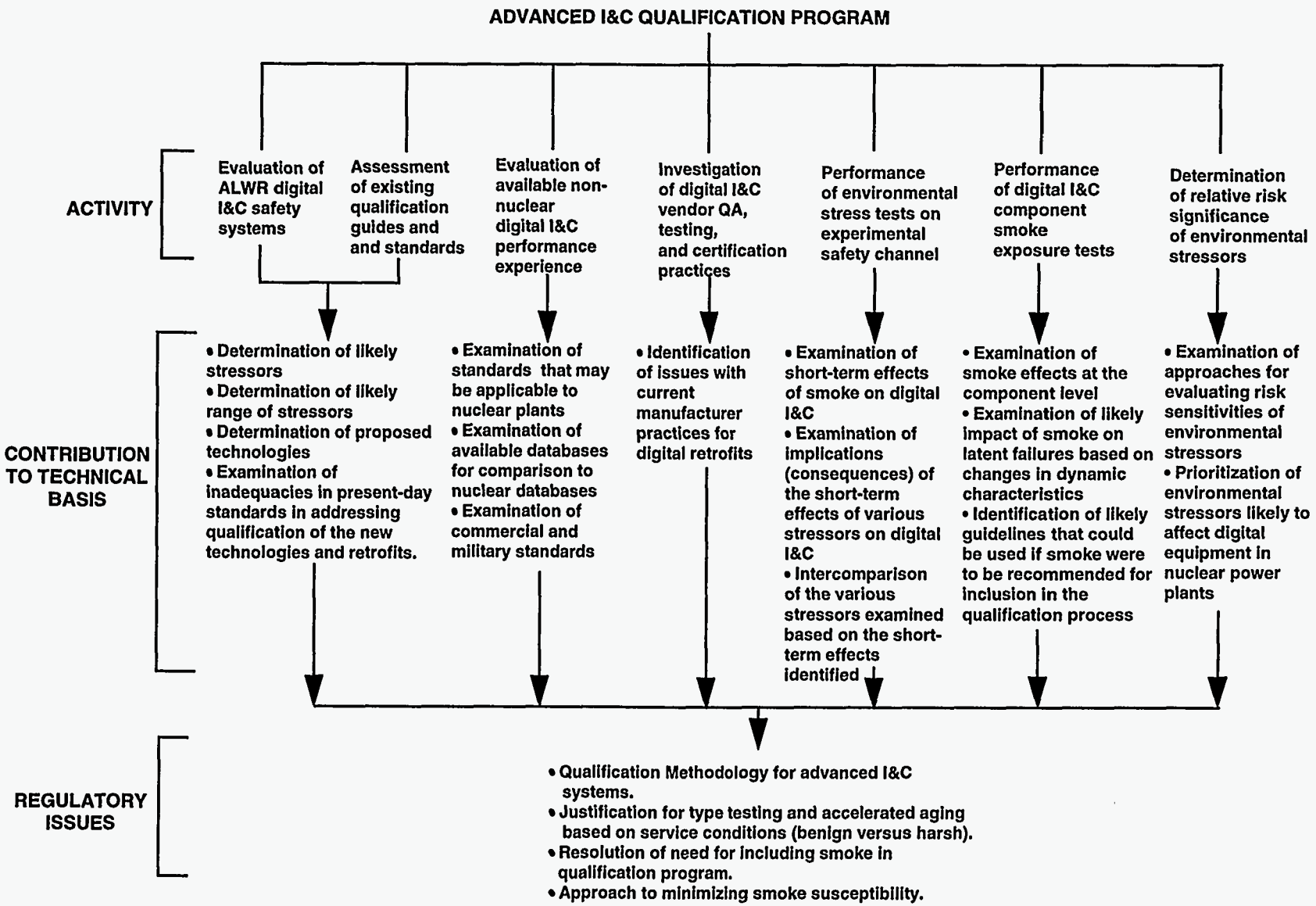


Figure 1.1 Developing the technical basis for potential enhancement of current qualification process

The goal of the project is *not* to perform qualification testing of any particular manufacturer's advanced safety system, and, in fact, it is impractical for this program to test *every* digital safety system design. Thus, the approach for this investigation is to test representative hardware and identify characteristic failure modes by accomplishing the following steps:

(1) Identify the new forms of technology present in the advanced systems being proposed by reactor manufacturers.

(2) Assemble for environmental testing an experimental digital safety channel (EDSC) incorporating the advanced technologies and system functionality identified in step 1.

(3) Test the subsystems of the EDSC to stress levels beyond the projected service conditions to determine environmental susceptibilities and likely failure scenarios.

The reactor trip designs for the *AP600* (Westinghouse), the *ABWR* (General Electric), and the *System 80+* (Combustion Engineering) were reviewed to identify technologies that are different from present-day safety system implementations. Descriptions of the three designs can be found in NUREG/CR-5904, *Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors.*[4]

Advanced technologies proposed for these systems include fiber-optic interface systems, microprocessor-based modules, multiplexers, and fiber distributed data interchange (FDDI) networks. Whereas reactor trip systems are typically implemented as four separate divisions, ORNL's EDSC implemented only one division. The trip information from the other three divisions is simulated by a Host Processor. This approach is necessary to meet budgetary constraints but does not compromise the objectives of the task, since the safety channel implemented incorporates a full complement of the various technologies of interest, namely, microprocessor-based analog-to-digital converters, multiplexers, computers, fiber-optic line drivers, an FDDI network, and optical/electrical interfaces.

Since the design of the EDSC and the selection of its constituent hardware are intended to represent the surveyed commercial systems, test results from the EDSC allow generalizations to be made from the data obtained. The approach and reasoning are as follows:

(1) The system design is typical of ALWR trip systems or some proposed retrofits in the chip fabrication technology used.

The complementary metal oxide semiconductor (CMOS), N-channel metal oxide semiconductor (NMOS), and bipolar integrated circuits (ICs) are the chip technologies proposed for ALWRs. These chips are most likely to be plastic encapsulated microcircuits (PEMs) rather than hermetically sealed microcircuits. A PEM 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.

Traditionally, PEMs have been used primarily in commercial and telecommunication electronics. In fact, PEMs comprise about 97% of the market share of worldwide microcircuit sales.[5,6] However, the military has typically employed hermetic packages because of the perception that they are more reliable than PEMs. Some studies show that the reliability of plastic ICs is comparable to that of ceramic ICs. For example, a

comparison of failure rate data for PEMs and hermetically packaged devices shows that from 1978 to 1988, both types of packaged devices improved by a factor of 10 in early life failure rates. 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 compares closely with figures for hermetic parts.[7] In comparative tests of plastic surface mount devices [small outline integrated circuits (SOICs)] and ceramic dual-in-line packages (CERDIPs) in which the tests were designed to simulate a worst-case avionics environment (–40°C to +85°C, 98% RH), the failure rate for the PEMs was found to be as low as 1.6% per 10^6 h. In contrast, the failure rate for the hermetic parts was 6.1% per 10^6 h. The significant difference in failure rates was attributed to the loss of hermeticity of glass seals. (The failure mechanism for both PEMs and hermetic parts was metalization damage due to moisture.)

All modules/computers purchased for the environmental tests employed a mix of plastic encapsulated chip technologies. A representative list of these components is given in Appendix B.

(2) The system is typical of ALWR trip systems or some proposed retrofits in the board fabrication technology currently used.

Nuclear equipment manufacturers typically purchase or fabricate electronic boards to industrial standards rather than to military standards. Thus the industrial-grade boards used for the EDSC tests were expected to have similar fabrication materials (similar plating, soldering, and coating materials) and to have similar responses to the stressors that were examined (i.e., temperature, humidity, EMI/RFI, and smoke). For example, the use of solder masks or other coatings on circuit boards appears to provide a degree of protection from smoke contamination by reducing current leakage and loss of signal level. Some of the modules relied on plastic housings encasing the circuit boards to provide protection from contaminants. This afforded the opportunity to investigate the effect smoke and other environmental stressors could have on the subsystems as well as on the experimental system as a whole.

(3) The system components are typical of ALWR safety systems and proposed retrofits in temperature ratings and reliability stress tests used during component quality assurance procedures.

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°C to 70°C (32°F to 158°F). For industrial-grade components, this range is between 0°C to 85°C (32°F to 185°F), and the ratings for military-grade components is –55°C to 130°C (–67°F to 266°F). The EDSC was assembled with commercial- and industrial-grade components representing over 400 components from over 10 different manufacturers.

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 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).

(4) The system design is typical of ALWR trip systems or some proposed retrofits in functionality and communication protocols used.

In the ALWR systems examined, each division will typically perform trip/no trip calculations for each process variable in one subsystem and send the data over fiber-optic serial data lines to equivalent subsystems in the other divisions for voting. Also, divisions typically employ analog-to-digital (A/D) multiplexing modules to transmit field data to trip calculation units. For the EDSC, the multiplexed data are sent via a network to simulate the advanced hardware and software communication protocol proposed for some manufacturers' protection systems.

(5) The system design is typical of ALWR trip systems or some proposed retrofits in memory/board density.

While current digital safety systems such as the Westinghouse *Eagle 21* employ 16-bit processors, 32-bit processors are more common in commercial and nonnuclear industries, with 64-bit processors soon to arrive. This rapid pace of technology movement will almost certainly lead to obsolescence of the earlier processors in the nuclear industry. Also, memory size and density have risen. This is true not only in the commercial sector, but also in the nuclear industry because of sophisticated online diagnostics and monitoring software requirements of ALWRs and digital retrofits. The effect of increased memory requirements on data reliability is twofold. First, they propel the market toward increased memory densities. This means that the effective size of each memory cell is reduced, resulting in a decrease in the threshold to alpha particle susceptibility (susceptibility to alpha particles is a primary source of "soft" errors). While most packaging materials supply adequate protection against environmental alpha particles, certain package materials emit alpha particles, thereby increasing the probability of soft errors for some chips.[8] Because soft errors can also be caused by environmental disturbances and high-energy radiation other than alpha particles, an increase in the overall board memory can also cause a higher system error rate. For the same reasons, the probability of "hard" errors (e.g., processor lockup) also increases with increasing memory size.

The processor boards in the computers used in the EDSC employed 4-MB random access memory (RAM). This memory density is comparable to requirements in digital retrofits and ALWRs.

(6) The system design enables investigation of the functional behavior of a distributed system under applied environmental stress.

Manufacturers are likely to qualify a distributed system by qualifying each individual subsystem separately (e.g., field process multiplexing system, programmable logic controller, trip subsystems, etc.). The EDSC design simulates a "distributed system" and therefore enables the environmental vulnerabilities of such a system, including its interfaces, to be investigated as a total integrated system.

It should be noted that the results of system performance in this study are not necessarily limited to protection systems but could be generalized to all I&C systems using similar technologies. For example, the behavior of a communication link in response to environmental stress would be largely the same for a control system as for a protection system.

1.5 Background

The basis for protection system qualification comes from the *Code of Federal Regulations* (CFR). 10 CFR 50.49(d)(3) and 10 CFR 50.55a(h)–IEEE 279 (Ref. 9) provide a list of stressors that must be considered for qualification of Class 1E equipment. The list includes temperature, pressure, humidity, chemicals,

radiation, and submergence. Under a separate heading, the regulations also require seismic qualification. IEEE 323-1974 (Ref. 10) gives essentially the same list of stressors, adding vibration and mechanical wear. Since all digital hardware currently in service or proposed from vendors is designed for a habitable, mild environment (e.g., control room or cable spreading room), the environmental stressors selected for testing in this study are those stressors important in a mild environment. Submergence, elevated pressure, and radiation can be considered physically prevented from occurring in the mild location where the digital equipment is located; therefore, these stressors are not addressed in this study. Another consideration in the selection is the need for additional information. Digital systems have different failure modes and fail at different levels of stress than analog components. For an analog system, the effect of temperature rising from 24°C to 49°C (75°F to 120°F) is often merely a loss of calibration accuracy. Digital systems, on the other hand, can suffer more serious effects, including failure to perform their functions at all, because of communication failure or lockup of the central processor. These factors led to selecting elevated temperature, humidity, EMI/RFI, and smoke as the subjects of this study. Additionally, these stressors have the potential for affecting more than one division of a safety channel and are thereby a potential source of common cause error.

Equipment situated in a control room environment is not affected by a reactor system's design basis events and anticipated abnormal occurrences. Rather, the potential initiating events for equipment stress are from an entirely different set of events. For increasing temperature, the primary initiating event is a loss of heating, ventilating, 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, or spurious emissions from other electronic equipment. An electrical equipment fire is the primary initiator for smoke.

Seismic vibration and operationally induced vibration are not considered in this study. 10 CFR 50, Appendix A, Criterion 2, identifies earthquakes as a design basis event for a protection system, and seismic vibration must be considered for any digital protection system equipment regardless of its location in a nuclear plant. However, seismic qualification of digital components does not appear to pose any unique qualification issues. Surface-mounted integrated components are recognized as rugged components and are routinely used in applications such as automobiles, aircraft, and portable electronic equipment in which accelerations typically exceed that of a design basis earthquake. Based on an investigation of existing failure information[11] and discussions with nuclear-qualified I&C system suppliers,[12] digital systems for nuclear safety applications should require no special seismic or vibration design consideration beyond normal industry practice. Therefore, seismic qualification for digital equipment should be treated in the same manner as for analog equipment in accordance with existing standards such as IEEE 344-1987.[13] Thus, no special testing of the EDSC for vibration susceptibility is considered in this study.

A stressor not previously considered for analog safety system qualification is smoke from an electrical fire. During the Advisory Committee on Reactor Safeguards (ACRS) meeting on October 8–10, 1992, regarding environmental qualification requirements for digital I&C systems, the ACRS voiced concern about vulnerabilities of digital I&C to smoke. ACRS recommended that certain elements of the equipment qualification research program be reassessed to include the effects of smoke as a stressor on advanced I&C system hardware.

Aging is a consideration for qualification required by 10 CFR 50 and IEEE 323-1974. However, components for this study were not preconditioned by natural or artificial aging to their end-of-installed-life conditions. Aging does not appear to pose a significant design concern for digital systems because the equipment is installed in a mild environment and because it is accessible for monitoring, calibration, and

replacement. Consequently, the equipment can be expected to be serviced or replaced as necessary throughout the plant life. The installed equipment can thus be assumed to have like-new performance.

2 EXPERIMENTAL DIGITAL SAFETY CHANNEL DESIGN DESCRIPTION

2.1 System Design Considerations

The experimental digital safety channel (EDSC) assembled for this study is representative of advanced safety system designs proposed for ALWRs.[4] The functional configuration and digital technologies employed for the EDSC are based on proposed ALWR safety system designs. The system itself is a composite of commercial- and industrial-grade versions of hardware components used in advanced protection systems. In fact, the digital hardware used in the EDSC represents more than 400 semiconductor components from over 10 different manufacturers. It is therefore expected that the EDSC will exhibit vulnerabilities and failure modes that are characteristic of an advanced safety system.

A reactor protection system typically consists of four divisions of process channels that are usually interconnected in a configuration that uses 2-out-of-4 voting for final safety system actuation. On the other hand, the EDSC consists of *one* division of the trip system fully implemented in hardware. **The functions typically performed by the other three divisions are implemented by a single computer or host processor (HOSTP). Implementing the system in this way enabled one complete channel, its interfaces, and its interactive behavior with other channels to be tested while at the same reducing the cost of the EDSC.**

Rather than build the EDSC, another alternative would have been to purchase for testing one or more of the systems reviewed in NUREG/CR-5904.[4] However, several considerations make such an approach impractical. First, the cost of each system would be much higher than that of the EDSC. Also, some advanced systems are still in the design stage and are not yet available for testing. Even when purchasing a system, the error detection and logging requirements of the test program would require implementing custom software and potentially custom hardware. The modifications would add to the cost, and, after modification, the system would not be identical to the manufacturer's design. For the increase in expense and complexity, the test program would not yield significantly different or improved information regarding failure modes.

The system is selected and assembled to represent a typical hardware configuration of a single channel of advanced modules running a program that simulates protection system software. The system hardware has representative modules for data acquisition, serial communication, network communication, and information processing. The software has features for simulating protection system software and for monitoring itself to detect and log errors. The components are industrial-grade electronics, typical of components that would be dedicated to nuclear application. **An actual system would differ in many details, but the overall design is typical, as are the failure modes and their consequences.**

An important point about the failure modes detected in this study is that, although they are abnormal events for the system, the majority of these errors would not result in a failure of the protection system to perform its mission. Self-diagnosis and redundancy in the protection system prevent individual abnormal events from causing the system either to fail to trip when required or to trip when not required. Generally, a second failure of some sort must occur for the event to result in a system failure. The second failure can be an identical failure in a parallel division (common mode failure), a different failure due to the same stressor (common cause), or a defect in the self-diagnosis features of the system to handle the event in a fail-safe manner (with a concomitant failure in the verification and validation program to identify the deficiency). The stressors considered in this study

have the potential for affecting multiple channels and causing common mode and common cause failures. **The experimental program looked for the failure modes, the stress level required to cause failure, repeatability of failures, and impact/severity of failure on system operation.**

The physical geometry of the EDSC is not typical of a digital protection system since it is not a rack-mounted cabinet installation. The central processing units (CPUs) and their associated communication boards are each mounted in an industrial-grade, aluminum case (individual cases for each of the four computers in the EDSC). The D/A modules are mounted on a backplane that is external to the computers. The fiber-optic line drivers are external devices in separate cases. **Physically separate devices, rather than a rack-mounted system, permit the components to be subjected to stress individually.** This capability is necessary to identify the source of some communication failures. Although the physical geometry is admittedly atypical of a reactor protection channel, no special considerations regarding the observed failure modes are thought necessary.

Although the EDSC components were not qualified and tested according to the requirements of IEEE 323, the component specifications have been evaluated for suitability in the mild environment of a nuclear safety system. The EDSC components are rated for the same or more severe operating ranges of temperature and humidity as the typical environmental specifications. The typical temperature and humidity specifications for nuclear plant instrumentation in mild environments are 5°C to 49°C (40°F to 120°F) and 5% to 95% RH. All the components selected for the EDSC are rated for at least these ranges. In one instance, testing showed equipment failures within the rated operating temperature range, indicating the need to confirm the manufacturer's advertised ratings for commercial-grade components through qualification. Components, particularly power supplies, are rated for RF emissions (FCC Class B Standards). Typically, no specifications are given regarding susceptibility to radiated or conducted EMI/RFI. The computer manufacturer's bus architecture description gave the following information regarding EMI and RFI noise immunity:

> The 10-slot backplane is constructed of four layers, with internal ground and power planes, for RFI and EMI noise immunity and low trace capacitance. The signal traces are located on layers 1 and 4 (the outer layers). Layer 2 is the Ground plane. Layer 3 is the Power plane.

Overshielding can distort signals by lengthening the rise and fall times of the signal edges. Some card options can have problems driving high-capacitance lines. The 10-slot board is constructed with ground dipoles between signal traces to minimize crosstalk while keeping trace capacitance to the lowest practical value. Noise in overshielded backplanes can become a problem in relatively low-noise environments.

Each (power) input is filtered by one or more large electrolytic capacitors for low-frequency line noise rejection. Ceramic bypass filter capacitors of 0.1 μF improve high-frequency noise immunity. All four input voltages have bypass capacitors.

No component manufacturer provided any specification regarding tolerance to smoke or other airborne contaminants. The computers are rated for light industrial use. The CPU boards have solder masks but no conformal coatings. This level of environmental protection, while not necessarily as effective as conformal coating, nevertheless appeared to be sufficient to prevent catastrophic and/or permanent failure of the boards even when exposed to a high level of smoke during the tests.

Product specifications, copied from the manufacturer's data sheets, are given in Appendix C. Manufacturers' names have been intentionally deleted so as not to advertise either the positive or negative attributes of the products selected.

2.2 System-Level Design Description

A block diagram of the EDSC is shown in Figure 2.1. The EDSC consists of two major functional subsystems: the test system (i.e., the equipment under test) and the test control system. The test system represents a single channel of an advanced reactor protection system, based on ALWR designs, and consists of the process multiplexing unit (PRS/MUX), a digital trip computer (DTC), and an engineered safety feature multiplexing unit (ESF/MUX). To be more representative of actuation reactor protection system implementations, the test system software is implemented in firmware for each subsystem. The test control system simulates the test scenarios (i.e., generates analog signals corresponding to various 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 HOSTP performs the test control functions. The following sections discuss hardware and software features of the EDSC and the considerations in the design and selection of hardware that are important to obtain representative failure modes due to temperature, humidity, EMI/RFI, and smoke.

2.2.1 Process Multiplexing Unit

The PRS/MUX subsystem of the EDSC represents the process signal conditioning, data acquisition, multiplexing, and remote data communication elements of advanced reactor protection system designs. The subsystem configuration is shown in Figure 2.2. The function of the PRS/MUX is to acquire process analog signals, digitize these data, and format them into frames suitable for transmission over an FDDI network. In the EDSC implementation, the signals are generated by a 16-channel D/A plug-in card inside the HOSTP, which simulates the actual field instrumentation such as transmitters.

The data acquisition component of the PRS/MUX consists of microcomputer-based modules plugged into a multiplexer backplane. Each data acquisition module performs signal conditioning, isolation, ranging, A/D or D/A conversion, and digital communications. Interconnection between modules is via an RS-485 bidirectional serial bus standard. Communication between a module and the PRS/MUX can be configured as an RS-232 or RS-485 link. The rated operating temperature range of the A/D modules is –25°C to 85°C (–13°F to 185°F). The sampling rate per module is nine samples per second at 12-bit accuracy. Absolute accuracy including temperature effects is ±0.05%. The input modules are designed to process low-level signals in harsh environments. The modules provide 1500 Vrms continuous isolation. The isolation prevents ground loops, protects against transients, and eliminates common mode voltage problems. The modules provide a high level of noise rejection. The input modules provide 160 dB of common mode rejection and 50 dB of normal mode rejection.

A common approach in multiplexed data acquisition systems in nuclear power plants is a board-based analog multiplexer and an A/D converter module. The microprocessor-based data acquisition modules used in the EDSC are an advancement that provides a considerable increase in flexibility to process many types of signals with a single module. The microprocessor-based module is likely to be used by advanced protection systems. It should be noted that the response of microprocessor-based designs to stressors may not be typical of conventional board-based components because the

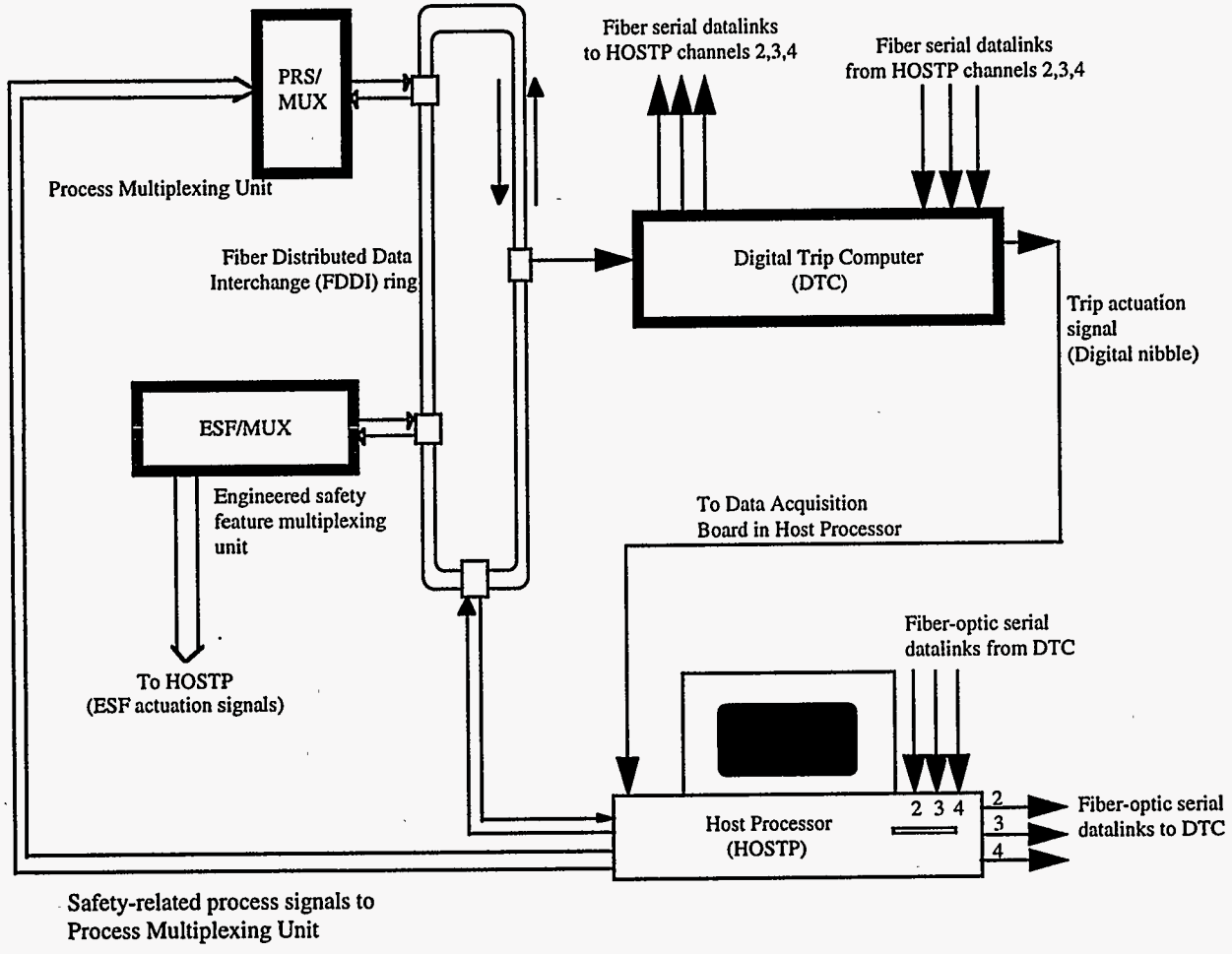


Figure 2.1 Functional block diagram of the experimental digital safety channel

Figure 2.2 PRS/MUX subsystem of the EDSC.

individual containers provided for the data acquisition modules offer some protection against the effects of smoke and humidity and also significant shielding against radiated EMI.

The processor component of the PRS/MUX consists of an industrial computer employing a full-featured, single-board design with an Intel 486DX-33 central processor unit. The computer is rated for an operating temperature range of 5°C to 50°C (41°F to 122°F) and 5% to 95% relative humidity (noncondensing). The computer board is mounted in an aluminum alloy chassis. The PRS/MUX software resides in a 4.2-MB read-only memory (ROM) disk. The PRS/MUX computer also contains an FDDI network adapter that communicates formatted data from the data acquisition system to the HOSTP and DTC via a dual attached station (DAS).

The FDDI network is an example of advanced network hardware with commercial error detection and correction software for communicating information both internally within the protection system and externally to devices such as posttrip monitors or digital control systems. The FDDI adapter is connected to the network via a bypass module. If a network node fails, the bypass module connects the network loop around the failed node.

2.2.2 Digital Trip Computer

The DTC subsystem of the EDSC represents the process variable trip calculation and channel trip logic elements of advanced reactor protection system designs. The subsystem configuration is shown in Figure. 2.3. The DTC polls the network to acquire the digital values of the process signals from the PRS/MUX. It then compares individual process variables 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 HOSTP sends trip/no-trip information for

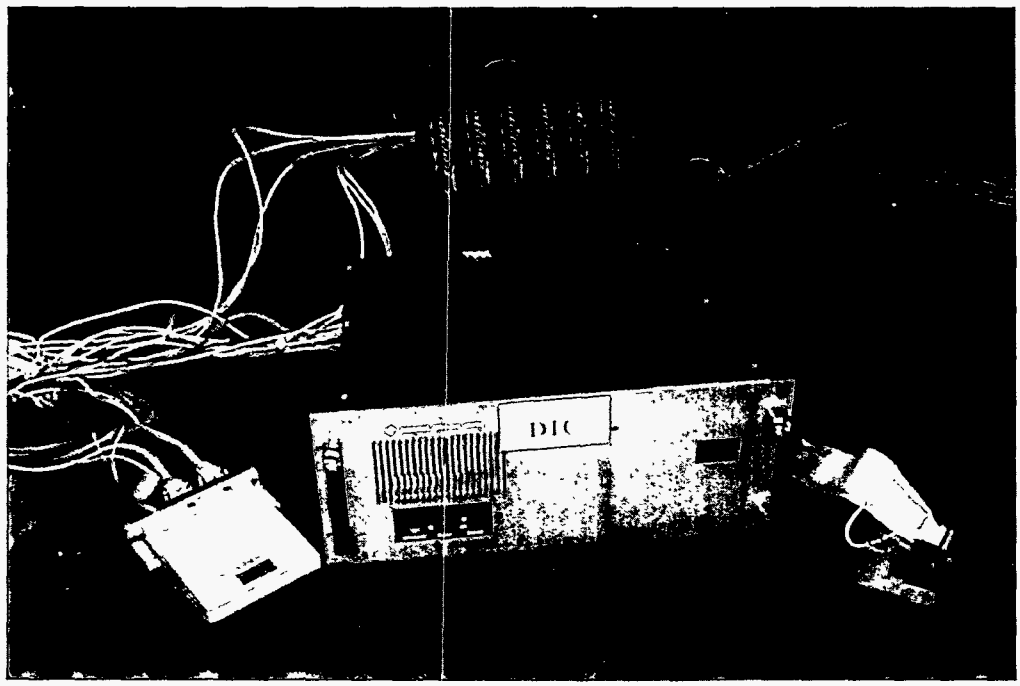


Figure 2.3 DTC subsystem of the EDSC.

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 channel trip result is then communicated to the HOSTP as a digital trip actuation signal via a parallel communication interface.

The DTC consists of an industrial-grade digital computer identical to the PRS/MUX computer. The DTC software resides in a 4.2-MB ROM disk. As with the PRS/MUX computer, the DTC is equipped with an FDDI network adapter. In addition, the DTC contains two serial communications boards, each having RS-485 ports. These communications boards are connected externally to fiber-optic line drivers, representing communications with the other divisions of the safety system (three input drivers on the first card and three output drivers on the second).

Fiber-optic signal transmission is expected to be used extensively in advanced digital protection systems because of its inherent isolation properties and resistance to EMI and RFI. The serial-optical line drivers and the FDDI network represent two different implementations of fiber-optic transmission, thereby giving representative behavior and failure modes for both types of communication technologies.

2.2.3 Engineered Safety Feature Multiplexing Unit

The ESF/MUX subsystem of the EDSC represents the ESF actuation command processing and data communication elements of advanced reactor protection system designs. The subsystem configuration is shown in Figure 2.4. The ESF/MUX demultiplexes the digital information sent by

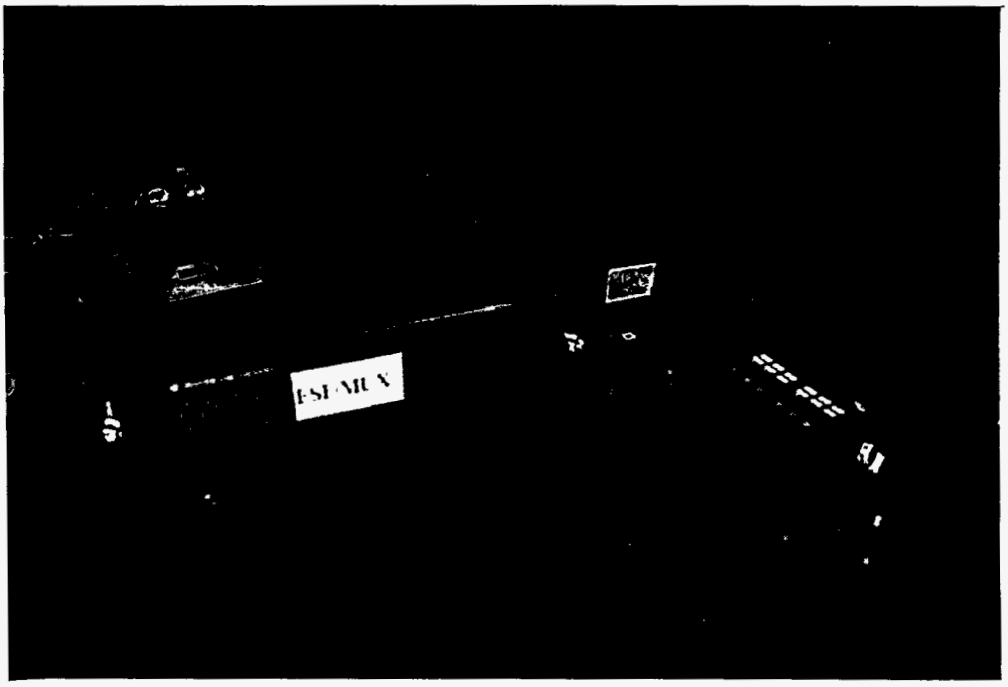


Figure 2.4 ESF/MUX subsystem of the EDSC.

the HOSTP via the FDDI network into the appropriate analog signals. In this way, it simulates ESF actuation signals. The ESF/MUX consists of a computer with a multiplexer backplane on which are mounted D/A modules, each with a 4- to 20-mA signal output. The current outputs are converted to voltage outputs using precision resistors, and the signals are then transmitted to a conventional board-mounted data acquisition system in the HOSTP. As with the PRS/MUX and DTC computers, ESF/MUX software resides in a 4.2-MB ROM disk.

2.2.4 Host Processor

The HOSTP system serves as the test control system. The system configuration is shown in Figure 2.5. The HOSTP acts as a test monitoring and error logging system but also simulates the data communication and interface functions typically performed by 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 reducing the cost of the experimental system. The data acquisition, error logging, and user interface software was developed using LABVIEW™ from National Instruments.

The HOSTP is a 486DX2-66 computer of the same family as the DTC and PRS/MUX computers. However, its clock speed is twice as fast (66 MHz in the HOSTP vs 33 MHz in the others). Plug-in cards include an FDDI network adapter identical to those described for the DTC and PRS/MUX systems and serial communication cards with port connections to the fiber-optic line drivers. Others are an A/D card for monitoring signals from the ESF/MUX and a D/A card for generating the analog test signals for the PRS/MUX. The HOSTP is also equipped with a 270-MB hard disk for storing the system software and recording results. The user interface includes a standard keyboard, a mouse, and a 53-cm super video graphics adapter (SVGA) monitor.

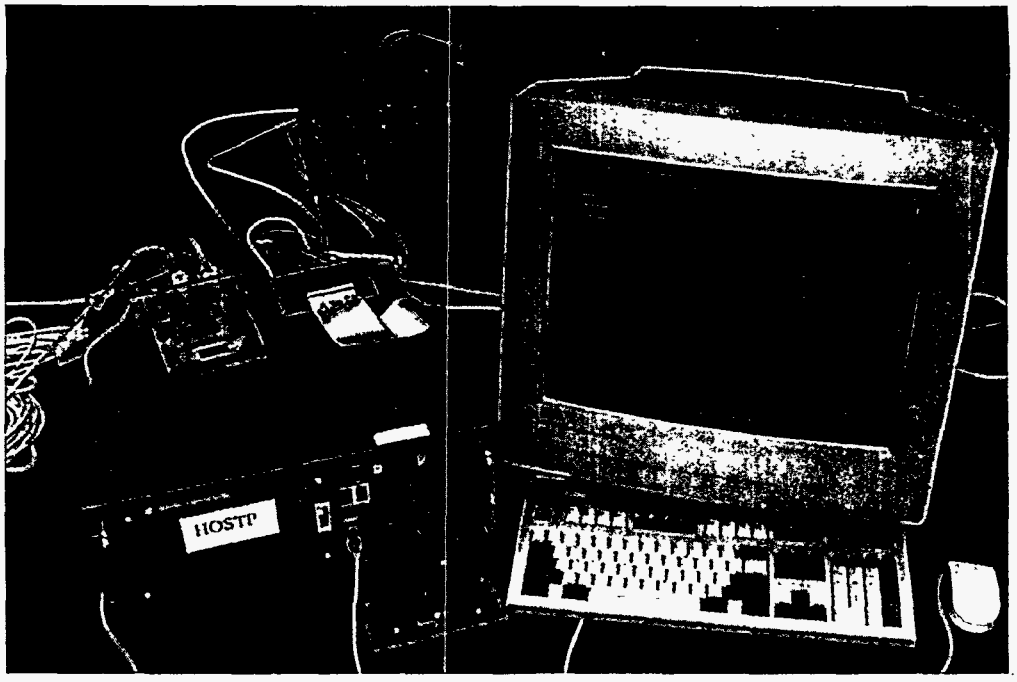


Figure 2.5 HOSTP system of the EDSC.

The main functions performed by the HOSTP may be summarized as follows:

(1) It generates process signals typical of either normal or accident conditions for each test scenario. These signals are hardwired to the PRS/MUX.

(2) It sends a command via the network to the PRS/MUX, requesting it to begin data acquisition at the start of a test scenario.

(3) It acquires the digitized process signals sent over the FDDI network by the PRS/MUX. (Note that the data from the PRS/MUX are also acquired by the DTC.) In this way the HOSTP verifies that the process data (analog signals) it sent to the PRS/MUX have not been corrupted during acquisition or communication (e.g., by the PRS/MUX itself).

(4) It simulates the trip functions of three other divisions by generating trip/no-trip data for each of the process signals and sends them via fiber-optic serial datalinks to the DTC.

(5) It performs 2-out-of-4 voting based on the internally generated trip/no-trip information corresponding to each simulated channel and the trip/no-trip information sent from the DTC via the serial datalinks and compares the voting result with the channel trip actuation signal generated by the DTC.

(6) It provides specified pump, valve, and other ESF actuation signals digitally to the ESF/MUX via the FDDI network.

(7) It monitors the ESF/MUX command outputs of analog actuation signals via a plug-in A/D card inside the HOSTP.

(8) It performs test system error logging functions and displays test system status.

Test scenarios are used to stimulate the safety function of the EDSC test system. Each test scenario corresponds to a fixed set of process signal values that are typical of either normal or accident conditions. A test cycle consists of 10 test scenarios. During each environmental test, the test cycle is continuously repeated to allow the functional performance of the EDSC to be monitored.

3 SYSTEM BEHAVIOR AND FAILURE IDENTIFICATION METHODOLOGY

3.1 Generic Environmental Stress-Related Failures in Digital Systems

Several failure modes are associated with ICs and circuit boards, some of which include open circuit due to cracked substrate, loss of hermetic seal, short circuits, and decrease in volume resistance (circuit boards) after exposure to high humidity.[14] Most failures of electronics components and systems fall into one of the following categories:[15–17] (a) hard failures; (b) upsets; and (c) latent failures.

Hard failures are permanently damaged parts, where replacements must be installed to restore the system to normal operation. The lethal damage may be due to a broken connection on the microchip in an area smaller than one-tenth the cross section of a human hair,[15] or it may be due to overstress (e.g., from heat, electrostatic discharge, EMI/RFI, nonthermal smoke) of several components on a board simultaneously.

Upsets are temporary or intermittent malfunctions that have the potential for causing serious consequential damage.[15] For example, an upset may cause a microprocessor to retrieve instructions that do not correspond to the software written for it to execute. This may cause the microprocessor to output address, data, and status signals that are not defined by the software written for the microprocessor, resulting in a potentially disastrous response of the system.[16]

Latent failures refer to devices that have been over stressed and are slightly degraded but continue to function[15] until some future date (perhaps months or years later), when they become hard failures. For example, it has been reported that one latent failure in a satellite system did not surface for 5 years.[17] Component degradation that can lead to latent failures may often take the form of changes in leakage currents, noise margins, rise and fall times, and changes in other component parameters that nevertheless remain sufficiently within tolerance for the affected channel to perform normally. It was impractical in our study to thoroughly investigate latent failure effects, so the focus is therefore limited to upsets and hard failures.

While the reliability of ICs has improved considerably over the past two decades, environmentally related hard failures and upsets at the component level are still to be expected and do, of course, happen. At the board or system level, however, the effect of upsets includes data errors due to bit changes in memory cells, board failures due to processor lockup, and interface failures (e.g., timeouts on serial interfaces). Therefore, the EDSC test setup was designed to investigate the following general categories of failures that are typical of distributed digital systems:

- Serial Communication Errors
  There are a variety of serial data communication standards and protocols, among the more common of which are RS-232, RS-422, RS-423, and RS-485. Some proposed ALWR safety system designs will employ either RS-232 or RS-485 datalinks. Error detection schemes for such data communication technologies are typically limited to the ability to detect single-bit (parity) errors in the data. In the EDSC, both RS-232 or RS-485 datalinks were used. The tests were designed to log datalink timeouts, parity errors, and overrun errors as a result of environmental stress, without halting the overall test cycle.

- Network-Related Errors
  As in the case of serial communication systems, many network architectures, protocols, and standards exist. Some network communications are deterministic in nature, which means that every node is guaranteed a fixed time for communication, and control actions must take place in the allotted time. Other network communications are nondeterministic (e.g., Ethernet). For obvious reasons, however, all network communication protocols used within any part of a safety system must be deterministic. Some ALWR designs that were investigated will employ FDDI network(s) with a deterministic, token-passing protocol. Error detection schemes for the EDSC tests were designed to identify and log generic errors such as failure of a node to acknowledge receipt of data, data corrupted in transit, and inability of a node to send a data packet.

- Loss of Data Accuracy
  In a traditional analog safety system, errors may result from process signal drifts from transmitters. In a digital system, another source of error may come from the A/D modules as a function of environmental stressors. The temperature drift of the A/D modules used in the EDSC was specified as $\pm 0.3\ \mu V/°C$, but the possible contribution from nonthermal effects (e.g, smoke) was not specified, nor is it a typical specification for any A/D modules. In the environmental tests, we attempted to investigate thermal, humidity, and smoke-related data inaccuracies by monitoring the difference between the voltage sent to, and that transmitted by, the PRS/MUX for all the process signals as each stressor was applied. All voltage differences greater than the arbitrarily selected value of 100 mV were reported.

- Unintended Digital Actuation Errors
  A feature common to most trip systems is that the output leading to actuation units (e.g., solid state relays) is a discrete signal. The EDSC simulates one proposed ALWR implementation in which the output is a digital nibble (i.e., four bits of data). The digital output to load drivers is arguably one of the more vulnerable parts of a digital safety system, since its malfunction may either cause a spurious trip of the channel or it may prevent the channel from performing its final actuation function. We investigated the effect of various environmental stressors on the digital output to final actuation circuitry by monitoring the nibble output from the DTC and comparing it to the expected value.

- Permanent Board Failures
  At the system level, many component failures (e.g., damage to a memory cell, processor lockup) may also lead to corrupted data and communication timeouts. However, such manifestations will typically be permanent and will persist even after power-down and restart of the affected node or module. The EDSC tests were designed to detect persistent/permanent errors but not necessarily to identify the malfunctioning component. In the case of a permanent malfunction, subsequent examination and troubleshooting of the affected board/module were conducted to identify the malfunctioning component.

The foregoing identifies general error categories anticipated in the environmental tests in terms of generic characteristics of microprocessor-based distributed systems. Also, since the modules contained a mix of different chip technologies (CMOS, NMOS, bipolar, etc.), the overall system response to a particular environmental stressor, and therefore the results of the tests, was not unique to a particular chip technology. Finally, although the various environmental stressors were performed on the same set of equipment, age-related effects were unlikely because of the relatively short exposure times (several hours rather than months or years). In any case, any possible synergistic effect of a previously applied stressor

was addressed by performing a baseline test prior to applying the next stressor. This and other assumptions made (see Sect. 7) allowed conservative stressor intercomparisons to be made.

3.2 Generic Digital System Upsets and Their Consequences in Safety Systems

To relate the system upsets and failures observed in the tests to generic potential *consequences* in a digital safety system, we 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 is considered to be the most serious, while failure category E is the least serious. As explained below, failure categories A and B can result in loss of functionality, that is, loss of the ability of the module, channel, or subsystem to perform its intended function. Failure categories C and D may not necessarily result in loss of functionality, and failure category E *will not* result in loss of functionality since the implication is that the system is designed to fail safe upon the occurrence of the upset. It is important to recognize 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 can 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 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 would likely prevent a channel from performing its function. However, the adverse effect of such an upset can usually be offset in a typical power plant safety system through engineering design. For example, during the tests, a number of serial and network communication timeouts occurred because of parity and overrun errors. In an actual safety system, the most serious consequences of such timeouts can 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 is able to recover in time for the required function to be performed without exceeding the channel response time requirements. For example, during the tests, the DTC had to retransmit data on the network on several occasions because of a lack of acknowledgment by the receiver for messages sent. A conditionally safe failure, if it persists, may 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 limited period of time.

(E) Fail-Safe Failure

This is an upset in a component or module that puts the channel in a tripped or safe state.

During the course of the tests, some errors or effects arose that were strictly limited to the performance of the HOSTP and not related to the channel (equipment) under test. These were EDSC-specific failures and were noted as potential stressor effects on digital equipment but were not included in the assessment of microprocessor-based safety system vulnerabilities to environmental stressor effects. For example, the HOSTP video display was observed to alternately blank OFF and ON during the magnetic field tests. The phenomenon was due to the close proximity of the HOSTP to the equipment under test owing to space limitations.

Table 3.1 illustrates generic environmental stressor-induced upsets in digital systems and their potential consequences in terms of the classification scheme used in this study. The table also lists some specific examples of the generic stressor-induced upsets that were observed with the EDSC.

Table 3.1 Generic environmental stressor-induced upsets in digital systems and their potential consequences

Generic stressor-induced errors in digital systems	Some plausible or actual examples observed with EDSC	Consequence classification used in study
Permanent component/board failures and upsets that lead to unintended and unsafe digital actuation errors.	EMI-induced upset caused digital actuation nibble to give erroneous result.	Critical Failure
Component/module upsets that would usually prevent a channel from performing its function, but whose adverse effect in an actual plant safety system can be offset through engineering design.	Serial and network communication timeouts occurred because of 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 is able to recover in time for the required function to be performed.	The digital trip computer (DTC) had to retransmit data on the network on several occasions because of a lack of acknowledgment of messages sent.	Conditionally Safe Failure

Table 3.1 (continued)

Generic stressor-induced errors in digital systems	Some plausible or actual examples observed with EDSC	Consequence classification used in study
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 long after the stressor has been removed.	Changes in leakage currents, noise margins, pulse rise and fall times, and other component parameters that nevertheless remain sufficiently within tolerance for the affected channel to continue to perform normally. (NOTE: The tests were not designed to thoroughly investigate latent failures.)	Latent Failure
Component/module upsets that place 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

3.3 Environmental Stressor-Induced Errors in the EDSC

This section lists the errors encountered during the environmental testing of the EDSC. Note that this list includes not only the errors actually observed, but also plausible errors that *could have* occurred.

(a) *Timeout by DTC on attempt to read data from HOSTP channel 2 fiber-optic serial datalink.* This indicates that the DTC never received the data it was expecting from the channel 2 serial port of the HOSTP. This is a potentially unsafe error.

(b) *Timeout by DTC on attempt to read data from HOSTP channel 3 fiber-optic serial datalink.* This is a potentially unsafe error.

(c) *Timeout by DTC on attempt to read data from HOSTP channel 4 fiber-optic serial datalink.* This is a potentially unsafe error.

(d) *Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 2.* This indicates that the HOSTP never received the data it was expecting from the channel 2 serial port of the DTC. This is a potentially unsafe error.

(e) *Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 3.* This is a potentially unsafe error.

(f) *Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 4.* This is a potentially unsafe error.

(g) *Corrupted data from HOSTP channel 2 fiber-optic serial link to DTC.*
This indicates that the data received by the DTC were corrupted (e.g., parity error, no expected delimiter, etc.). In an actual plant design a node may request the data to be retransmitted, and the upset, if it persists, may eventually result in a timeout of the serial datalink. This is a conditionally safe error.

(h) *Corrupted data from HOSTP channel 3 fiber-optic serial link to DTC.*
The points made in (g) are also applicable here. This is a conditionally safe error.

(i) *Corrupted data from HOSTP channel 4 fiber-optic serial link to DTC.*
This is a conditionally safe error.

(j) *Channel trip error.*
This occurs when an incorrect trip nibble is transmitted between the DTC and the HOSTP. This problem may be due to noise or other problems with the cable connection between the DTC and the HOSTP. In this case, the actual nibble communicated to the HOSTP might have been a "do not trip" nibble when there should have been a trip, or it might have signified a "trip" when no trip should result. This is a critical error since there is no way to tell how the bits could change in an actual power plant trip system.

(k) *Timeout by PRS/MUX computer on attempt to read from the PRS/MUX communication port.*
This implies failure of the common communication port between the process multiplexer backplane and its computer. This type of fault will occur if (a) ***none*** of the input/output (I/O) modules on the PRS/MUX backplane can communicate with the PRS/MUX computer or (2) the common communication port itself between the PRS/MUX backplane and its computer has failed. This is a potentially unsafe error.

(l) *Corrupted data read from at least one I/O module from the PRS/MUX backplane.*
When the signal value from an I/O module is requested, several characters are typically sent. These characters include the value of the actual analog signal as well as some control characters. An error is reported when the PRS/MUX computer does not receive the expected number of characters from the module or if the data are found to be corrupted (overrun error, framing error, parity error, etc.). In an actual plant system, this constitutes a conditionally safe error, unless the error persists, thus generating a timeout.

(m) *Timeout on attempt to read data from one or more of the PRS/MUX I/O modules.*
This is a potentially unsafe error.

(n) *DTC had to retransmit data to HOSTP.*
The DTC sends error messages to the HOSTP after every test cycle. If the message is not acknowledged, the DTC will retransmit the data. This retransmission is performed at a lower level than the application. Thus the latter will typically continue to perform its normal functions. However, in an actual plant, a persistent error may eventually lead to a potentially unsafe situation because the (safety) information may not be received in a timely manner. This is therefore categorized as a potentially unsafe error.

(o) *PRS/MUX had to retransmit data on network.*
The PRS/MUX sends process data to the DTC as well as error messages to the HOSTP. If the receipt of information sent to either the DTC or to the HOSTP is not acknowledged, the information is retransmitted. This retransmission is performed at a lower level than the application. Thus the latter will typically continue to perform its normal functions. However, in an actual plant, a persistent error may eventually lead to a potentially unsafe situation because the (safety) information may not be received in a timely manner. This is therefore a conditionally safe error.

(p) *ESF/MUX had to retransmit data onto network.*
ESF actuation signals are sent to the ESF/MUX by the HOSTP. At the end of data transfer to the ESF/MUX, a "*message received*" command is sent to the HOSTP by the ESF/MUX. If the ESF/MUX never receives an acknowledgment back from the HOSTP, the ESF/MUX retransmits the "*message received*" command. This retransmission is performed at a lower level than the application. Thus the latter will typically continue to perform its normal functions. However, the scenario postulated in (n) or (o) may also occur. This constitutes a conditionally safe error.

(q) *HOSTP had to retransmit data to ESF/MUX.*
ESF actuation signals are sent to the ESF/MUX by the HOSTP. If the HOSTP never receives an acknowledgment back from the ESF/MUX that it did receive these data, the HOSTP will retransmit the data. If this error occurred in an actual plant, it would constitute a conditionally safe error for the same reasons cited in (n).

(r) *Difference between voltage sent to, and that transmitted by, the PRS/MUX for one or more process signals.* (Digitized values of hardwired analog process signals sent to the PRS/MUX by the HOSTP are echoed back to the HOSTP via the FDDI network).
This type of error is reported whenever the voltage difference is greater than 100 mV. This constitutes a loss of data accuracy and is classified as a potentially unsafe failure. In a typical reactor trip system, signal validating methodologies can be used to check for out-of-range values, drifts, etc.

(s) *Difference between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals.* (Digital voltage actuation signals sent to the ESF/MUX by the HOSTP via the FDDI network are echoed back to the HOSTP via hardwired connections).
This constitutes a loss of data accuracy and is classified as a potentially unsafe failure.

(t) *Total network transmission failure.*
A total network failure will prevent the DTC from receiving process information from the PRS/MUX. In an actual power plant safety system implementation, the software can be designed to put the channel in a tripped state if the latter does not receive information from the PRS/MUX in a specified time. This is therefore categorized as a potentially unsafe failure.

(u) *Failure on attempt by HOSTP to initialize fiber-optic serial write link on channel 2.*
Initialization typically involves establishing the protocol to be used through software (e.g., number of stop bits, even or odd parity, etc.). This is an EDSC-specific error since it originates in the HOSTP (the serial card referred to is a part of the HOSTP).

(v) *Failure on attempt by HOSTP to initialize fiber-optic serial write link on channel 3.*
This is an EDSC-specific failure.

(w) *Failure on attempt by HOSTP to initialize fiber-optic serial write link on channel 4.*
This is an EDSC-specific failure.

(x) *Failure on attempt by DTC to initialize fiber-optic serial write link to HOSTP channel 2.*
Unlike error type (u), this is related to the channel under test (the serial card referred to is in the DTC). It is a potentially unsafe failure because in an actual protection system, a channel can be placed in a tripped state on the occurrence of such failure.

(y) *Failure on attempt by DTC to initialize fiber-optic serial write link to HOSTP channel 3.*
This is a potentially unsafe failure.

(z) *Failure on attempt by DTC to initialize fiber-optic serial write link to HOSTP channel 4.*
This is a potentially unsafe failure.

(aa) *DTC could not receive data from the PRS/MUX in specified time.*
The DTC must receive process signals from the PRS/MUX and serial data from the HOSTP. When it finds that it has received complete input from either source, it will wait for an additional specified time for the other input. If this interval passes, it will declare an error, flush one measurement's worth of byte from the buffer allocated for the PRS/MUX network input, and flush all bytes from the buffer allocated for the HOSTP serial data input. It then sends appropriate error messages to the HOSTP. This is a potentially unsafe failure.

(bb) *Network data packet could not be sent by PRS/MUX.*
This usually indicates a network hardware fault in the PRS/MUX node and is classified as a potentially unsafe failure.

(cc) *Network data packet could not be sent by DTC.*
This usually indicates a network hardware fault in the DTC node and is classified as a potentially unsafe failure.

(dd) *Error in data packet received by PRS/MUX.*
The HOSTP computer sends a command via the network to the PRS/MUX computer to start each test. This fault type indicates that the PRS/MUX network hardware detected an error in the resulting data packet, such as the packet being too small. In an actual plant, a node can request the packet to be resent. However, if the error persists, it can result in a timeout. Accordingly, this is a conditionally safe error.

(ee) *Error in data packet received by DTC.*
The only data the DTC receives via the network are process signals from the PRS/MUX. This failure type indicates that the DTC network hardware detected an error in the resulting data packet, such as the packet being too small. The arguments raised in (dd) are also applicable here. This is a conditionally safe error.

(ff) *HOSTP monitor continuously blanked OFF and ON.*
This is classified as an EDSC-specific failure. The phenomenon was attributable to the close proximity of the HOSTP to the equipment under test owing to space limitations.

(gg) *PRS/MUX power supply failure.*
This is a potentially unsafe failure because an actual power plant protection system can be designed so that the affected channel is placed in a tripped state upon loss of power.

(hh) *DTC power supply failure.*
This is a potentially unsafe failure because an actual power plant protection system can be designed so that the affected channel is placed in a tripped state upon loss of power.

4 ELECTROMAGNETIC/RADIO-FREQUENCY INTERFERENCE TESTS

4.1 Rationale

EMI/RFI tests were performed on the EDSC according to applicable test criteria and methods stipulated in MIL-STD-461C[18] and MIL-STD-462,[19] respectively. MIL-STD-461 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 system-level EMI/RFI-induced upsets and failure modes in microprocessor-based safety systems. The tests also enabled comparisons to be made with other environmental stressors, including smoke exposure, based on a common testing subject representing a nuclear safety application. The tests were not intended to ascertain whether the EDSC met emissions criteria. Therefore, only susceptibility test methods and criteria were used in the experimental investigation. The tests performed are the following:

CS01—Conducted Susceptibility, Low Frequency;
CS02—Conducted Susceptibility, High Frequency;
CS06—Conducted Susceptibility, Spikes;
RS01—Radiated Susceptibility, Magnetic Fields;
RS02—Radiated Susceptibility, Spikes; and
RS03—Radiated Susceptibility, Electric Fields.

Details of the test methods are given below.

4.2 CS01: Conducted Susceptibility, Low Frequency

The CS01 test ensures that equipment under test (EUT) is not susceptible to EMI/RFI present on the power leads in the frequency range 30 Hz to 50 kHz. The test is applicable to ac and dc power leads, including grounds and neutrals, that are not grounded internally to the equipment under test. The test is not applicable at frequencies within ±5% of the power line frequency (i.e., 57 to 63 Hz in the United States).

The first series of tests consisted of connecting an audio power amplifier in series with the phase power lead so that the sinusoidal audio interference signal output "rode" on the main power that was applied to the EUT. The audio voltage output ranged from 1 to 5 Vrms, with a frequency range of 30 Hz to 50 kHz.

The second series of tests was similar to the first, except that the sinusoidal interference signal output was connected to the neutral lead.

4.2.1 CS01 Test Procedure

Table 4.1 lists the test equipment used for the CS01 tests. The test setup is shown in Figure 4.1. Note that a line impedance stabilization network (LISN) is employed on each ungrounded power lead to prevent conducted coupling through the power source. A detailed description of the test procedure follows.

Table 4.1 CS01 test equipment

Equipment	Manufacturer	Model Number	Serial Number
Power sweep generator	Solar Electronics	6550-1	822527
Oscilloscope	Tektronix	2465	B025650

Interference on Phase Line

(1) The test equipment is connected as shown in Figure 4.1, with the series interference voltage impressed on the line by connecting the audio transformer secondary in series with the phase lead.

(2) Power is applied to the EUT by closing a switch on the test panel, the EDSC is initialized, and the HOSTP software is started.

(3) The test equipment is energized and the function generator is set to provide a 30-Hz driving signal.

(4) The magnitude of the voltage on the line is slowly increased to 5 Vrms, and any EDSC malfunctions are observed. The EDSC's performance is continuously monitored by the HOSTP, and error messages are displayed by the HOSTP. If a malfunction occurs, the corresponding conditions are noted. Then the voltage is reduced to zero and increased again to determine if the error is repeatable. Typically, the voltage at which a malfunction occurs is maintained for at least 10 s.

(5) Step 4 is repeated for frequency settings of 50 Hz, 100 Hz, 200 Hz, 500 Hz, and 1 kHz.

(6) The test frequency is set to 2 kHz and step 4 is repeated, except that the test voltage limit is now 4 Vrms.

(7) The test frequency is set to 5 kHz and step 4 is repeated, except that the test voltage limit is now 3 Vrms.

(8) The test frequency is set to 10 kHz and step 4 is repeated, except that the test voltage limit is now 2 Vrms.

(9) The test frequency is set to 20 kHz and step 4 is repeated, except that the test voltage limit is now 1.5 Vrms.

(10) The test frequency is set to 50 kHz and step 4 is repeated, except that the test voltage limit is now 1 Vrms.

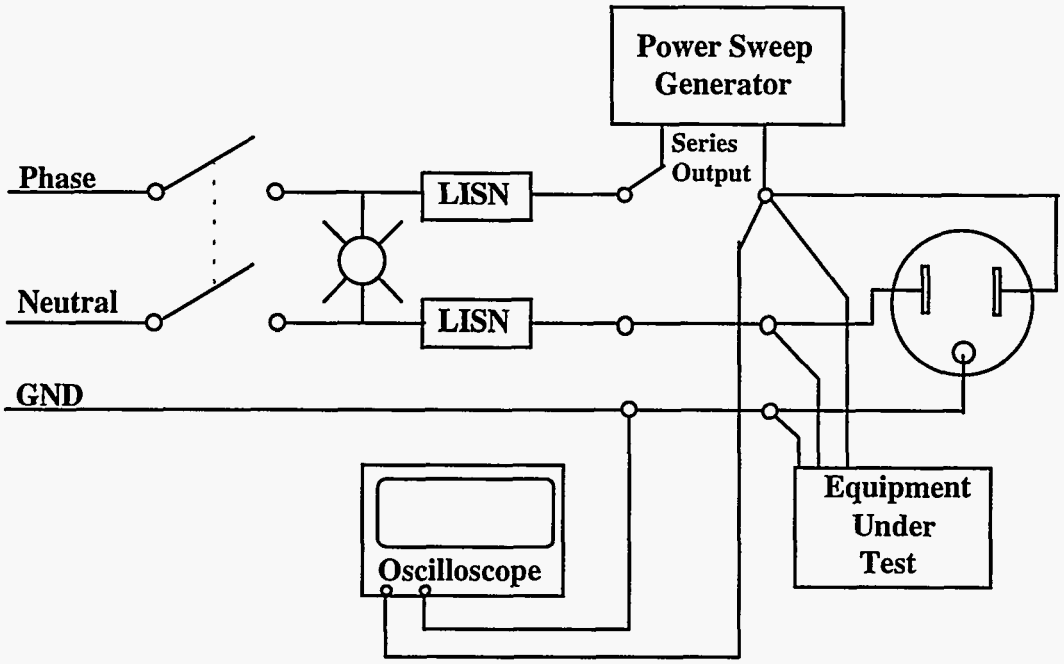


Figure 4.1 CS01 test setup

(11) The HOSTP software is stopped, and the test equipment and EDSC are powered down.

Interference on neutral line

(1) The test equipment is connected as shown in Figure 4.1, except that the audio transformer secondary is connected in series with the neutral lead rather than the phase lead.

(2). Steps 2 to 11 above are repeated.

4.2.2 CS01 Test Results

The HOSTP automatically recorded error messages and time stamps for all detected anomalies in error log files. Actual trip/no-trip and voltage levels were recorded in data files. Tables 4.2 and 4.3 present the test results with the PRS/MUX as the EUT, and Tables 4.4 and 4.5 present the test results with the DTC as the EUT.

Table 4.2 CS01 test results—interference on phase lead of PRS/MUX

Frequency (Hz)	Voltage (Vrms)	Errors
30	5	none
50	5	none
100	5	none
200	5	none
500	5	none
1000	5	none
2000	4	none
5000	3	none
10000	2	none
20000	1.5	none
50000	1	none

Table 4.3 CS01 test results—interference on neutral lead of PRS/MUX

Frequency (Hz)	Voltage (Vrms)	Errors
30	5	none
50	5	none
100	5	none
200	5	none
500	5	none
1000	5	none
2000	4	none
5000	3	none
10000	2	none
20000	1.5	none
50000	1	none

Table 4.4 CS01 test results—interference on phase lead of DTC

Frequency (Hz)	Voltage (Vrms)	Errors
30	5	none
50	5	none
100	5	none
200	5	none
500	5	SOME*
1000	5	none
2000	4	none
5000	3	none
10000	2	SOME*
20000	1.5	none
50000	1	none

*See text for discussion.

Table 4.5 CS01 test results—interference on neutral lead of DTC

Frequency (Hz)	Voltage (Vrms)	Errors
30	5	none
50	5	none
100	5	none
200	5	none
500	5	none
1000	5	none
2000	4	none
5000	3	none
10000	2	none
20000	1.5	none
50000	1	none

4.2.3 Analysis of CS01 Test Results

As can be seen from Tables 4.2 and 4.3, no errors were recorded with the PRS/MUX as the EUT, either with the phase lead tests or with the neutral lead tests.

With the DTC as the EUT, no errors were observed during the neutral lead tests. However, during the phase lead tests, timeout errors and network data retransmits were recorded at the test voltages and frequencies of 5 Vrms, 500 Hz and 2 Vrms, 10 kHz. The errors encountered are illustrated in Figure 4.2. It is interesting to note that none of these errors could be made to recur under identical test conditions. Therefore, these errors were attributed to random effects and underscore the complex nature of the susceptibility of digital electronics to EMI. The CS01 test does not specify a maximum time limit for application of the test signal. A time limit of 5 min was used for these tests with the exception of the 5-Vrms, 500-Hz test. The assumption made was that errors or malfunctions due to conducted noise signals in the power line are expected to arise during the initial seconds to minutes of the occurrence of the noise signal. During the test at 5 Vrms, 500 Hz, however, it was decided to test the effect of a longer application time on the system. The test signal was applied for more than 15 min, and the faults occurred close to the end of this interval. However, as mentioned above, the errors could not be repeated when the test signal was reduced to zero and reapplied for approximately the same amount of time. It was concluded that the error was a random effect, and, for subsequent tests, the test application time was limited to 5 min.

Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 2 (error type d).			*					
Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 3 (error type e).			*					
Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 4 (error type f).			*					
DTC had to retransmit data (error type n).							*	
PRS/MUX had to retransmit data (error type o).							*	
DTC could not receive data from PRS/MUX in specified time (error type aa).							*	
	0.100 5.0	0.200 5.0	0.500 5.0	1.0 5.0	2.0 4.0	5.0 3.0	10.0 2.0	20.0 kHz 1.5 Vrms

Note that no errors occurred with the neutral lead tests. Also, no errors occurred with either the phase lead tests or the neutral lead tests with the PRS/MUX as the EUT.

Figure 4.2 CS01 phase lead test results (DTC is the EUT)

4.3 CS02: Conducted Susceptibility, High Frequency

The CS02 test is similar to the CS01 test except that it covers the higher frequency range from 50 kHz to 400 MHz. The CS02 test is applicable to ac and dc power leads, including grounds and neutrals, that are not grounded internally to the equipment under test.

4.3.1 CS02 Test Procedure

Table 4.6 lists the test equipment used for the CS02 tests. The test setup is shown in Figure 4.3. A detailed description of the test procedure follows.

Table 4.6 CS02 test equipment

Equipment	Manufacturer	Model Number	Serial Number
Signal Generator	Hewlett Packard	8656A	2312A04388
Amplifier	Amplifier Research	75A220	15706
RF Coupler	Solar Electronics	7415-1	821062
Oscilloscope	Tektronix	2465	B025650

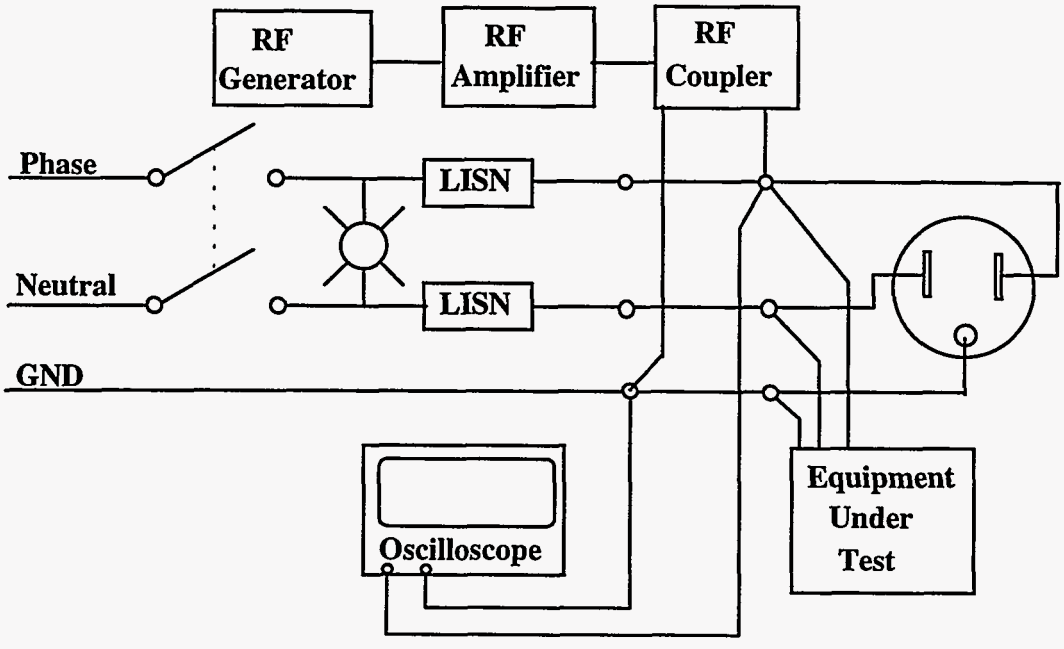


Figure 4.3 CS02 test setup

Interference on phase line

(1) The test equipment is connected as shown in Figure 4.3, with the interference voltage injected into the power line phase lead in parallel through a coupling network whose impedance is high at 60 Hz and low above 50 kHz.

(2) The interference voltage impressed on the power line is monitored using the RF coupler and the oscilloscope, and the test equipment controls are adjusted for zero output voltage.

(3) The EUT is energized, the EDSC is initialized, and the HOSTP software is started.

(4) The signal generator is set for 50% amplitude modulation (AM) at 1 kHz and a signal frequency of 100 kHz.

(5) The RF coupler is calibrated using the procedure described in Appendix D. (NOTE: Since the response of the coupler is not completely flat, it has to be calibrated at each frequency at which it is to be used.)

(6) The magnitude of the voltage on the line is slowly increased to 1 Vrms and held for 5 min or to equipment malfunction. The EDSC's performance is continuously monitored by the HOSTP, and error messages are displayed by the HOSTP. If a malfunction occurs, the corresponding conditions are noted. Then the voltage is reduced to zero and increased again to determine if the error is repeatable.

(7) If errors do not occur in step 6, the coupling voltage is increased to 2 Vrms and held for 5 min or to equipment malfunction. If a malfunction occurs, the voltage is reduced to zero and increased again to determine if the error is repeatable.

(8) If errors do not occur in step 7, the coupling voltage is increased to 4 Vrms and held for 5 min or to equipment malfunction. If a malfunction occurs, the voltage is reduced to zero and increased again to determine if the error is repeatable.

(9) Steps 5 to 8 are repeated with frequency settings of 200 kHz, 500 kHz, 1 MHz, 2 MHz, 5 MHz, 10 MHz, 20 MHz, 50 MHz, 100 MHz, and 200 MHz (each with 50% AM at 1 kHz).

(10) The HOSTP software is stopped, and the test equipment and EDSC are powered down.

Interference on neutral line

(1) The test equipment is connected as shown in Figure 4.3 except that the interference voltage is injected into the power line neutral lead in parallel through a coupling network whose impedance is high at 60 Hz and low above 50 kHz.

(2) Steps 2 to 10 above are repeated.

4.3.2 CS02 Test Results

The HOSTP automatically recorded error messages and time stamps for all detected anomalies in error log files. Actual trip/no-trip and voltage levels were recorded in data files. Tables 4.7 and 4.8 present the results for the PRS/MUX as the EUT, and Tables 4.9 and 4.10 present the results for the DTC as the EUT.

Table 4.7 CS02 test results—interference on phase lead of PRS/MUX

Frequency (MHz)	Voltage (Vrms)	Errors
0.1	1	none
0.1	2	none
0.1	4	none
0.2	1	none
0.2	2	none
0.2	4	none
0.5	1	none
0.5	2	none
0.5	4	none
1	1	none
1	2	none
1	4	none
2	1	none
2	2	none
2	4	none
5	1	none
5	2	none
5	4	none
10	1	none
10	2	none
10	4	SOME*
20	1	none
20	2	none
20	4	none
50	1	none
50	2	none
50	4	none
100	1	none
100	2	none
100	4	none
200	1	none
200	2	none
200	4	none

*See text for discussion.

Table 4.8 CS02 test results—interference on neutral lead of PRS/MUX

Frequency (MHz)	Voltage (Vrms)	Errors
0.1	1	none
0.1	2	none
0.1	4	none
0.2	1	none
0.2	2	none
0.2	4	none
0.5	1	none
0.5	2	none
0.5	4	none
1	1	none
1	2	none
1	4	none
2	1	none
2	2	none
2	4	SOME*
5	1	none
5	2	none
5	4	none
10	1	none
10	2	none
10	4	SOME*
20	1	none
20	2	none
20	4	none
50	1	none
50	2	none
50	4	none
100	1	none
100	2	none
100	4	none
200	1	none
200	2	none
200	4	none

*See text for discussion.

Table 4.9 CS02 test results—interference on phase lead of DTC

Frequency (MHz)	Voltage (Vrms)	Errors
0.1	1	none
0.1	2	none
0.1	4	none
0.2	1	none
0.2	2	none
0.2	4	none
0.5	1	none
0.5	2	none
0.5	4	none
1	1	none
1	2	none
1	4	none
2	1	none
2	2	none
2	4	SOME*
5	1	none
5	2	none
5	4	none
10	1	none
10	2	none
10	4	none
20	1	none
20	2	none
20	4	none
50	1	none
50	2	none
50	4	none
100	1	none
100	2	none
100	4	none
200	1	none
200	2	none
200	4	none

*See text for discussion.

Table 4.10 CS02 test results—interference on neutral lead of DTC

Frequency (MHz)	Voltage (Vrms)	Errors
0.1	1	none
0.1	2	none
0.1	4	none
0.2	1	none
0.2	2	none
0.2	4	none
0.5	1	none
0.5	2	none
0.5	4	none
1	1	none
1	2	none
1	4	none
2	1	none
2	2	none
2	4	SOME*
5	1	none
5	2	none
5	4	none
10	1	none
10	2	none
10	4	SOME*
20	1	none
20	2	none
20	4	none
50	1	none
50	2	none
50	4	none
100	1	none
100	2	none
100	4	none
200	1	none
200	2	none
200	4	none

*See text for discussion.

4.3.3 Analysis of CS02 Test Results

The faults recorded are shown in Figures 4.4 to 4.7 for the different test configurations. For the PRS/MUX phase lead tests, faults occurred at a frequency of 10 MHz when the applied test voltage reached 4 Vrms. For the neutral lead test, faults occurred at 2 MHz and also at 10 MHz.

Some of the faults were due to the inability of some of the I/O modules on the multiplexer backplane to communicate in a timely manner with the PRS/MUX computer, resulting in a timeout error. These faults were intermittent, because the affected modules appeared to recover during some test cycles and were able to send their voltage values to the PRS/MUX computer. Another type of fault that occurred in some of the I/O modules resulted in the affected modules reporting incorrect voltage to the PRS/MUX computer. In an actual plant, an error of this nature may be observed in the control room if zero or out-of-range values are observed on display panels. Drift problems may be seen only by comparison with corresponding signals in other channels. It is interesting to note that the voltage errors experienced by the TRP/MUX also occurred with the ESF, even though the latter was not under test. This problem is hypothesized to be due to radiated noise coupling into the ESF/MUX because of its proximity to the EUT.

Similar faults occurred at 2 MHz and at 10 MHz when the DTC was subjected to the same test conditions.

In summary, the errors that occurred in both cases (i.e., PRS/MUX and the DTC) fall into the following generic error types: Serial Datalink Errors, Network-Related Errors, and Loss of Data Accuracy. No hard (permanent) failures occurred.

	0.1	0.2	0.5	1	2	5	10	20	50	100	200 MHz
Timeout on attempt to read data from one or more of the PRS/MUX I/O modules (Error type m).							*				
Diff. between voltage sent to, and that transmitted by, the PRS/MUX for one or more process signals (Error type r).							*				
							4 V	(Minimun voltage at which error occurred)			

Figure 4.4 CS02 phase lead test results (PRS/MUX is the EUT)

	0.1	0.2	0.5	1	2	5	10	20	50	100	200 MHz
Timeout on attempt to read data from one or more of the PRS/MUX I/O modules (error type m).							*				
Diff. between voltage sent to, and that transmitted by, the PRS/MUX for one or more process signals (error type r).							*				
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).					*						
					4 V		4 V (Minimum voltage at which error occurred)				

Figure 4.5 CS02 neutral lead test results (PRS/MUX is the EUT)

	0.1	0.2	0.5	1	2	5	10	20	50	100	200 MHz
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).					*						
					4 V (Minimum voltage at which error occurred)						

Figure 4.6 CS02 phase lead test results (DTC is the EUT)

	0.1	0.2	0.5	1	2	5	10	20	50	100	200 MHz
Timeout on attempt to read data from one or more of the PRS/MUX I/O modules (error type m).							*				
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).					*		*				
					4 V		4 V (Minimum voltage at which error occurred)				

Figure 4.7 CS02 neutral lead test results (DTC is the EUT)

4.4 CS06: Conducted Susceptibility, Spikes

The CS06 test evaluates the response of the EUT to spikes on the power leads. That is, it determines if the EUT is susceptible to voltage transients introduced on the equipment power leads at spike amplitudes less

than the specified acceptance criteria. CS06 is applicable to both ac and dc power leads, including grounds and neutrals, that are not grounded internally to the equipment or subsystem.

4.4.1 CS06 Test Procedure

Table 4.11 lists the test equipment used to perform the CS06 tests. The test setup is shown in Figure 4.8. Note that an LISN is employed on each ungrounded power lead to prevent EMI/RFI from being transmitted back into the power source. Detailed description of the test procedure follows.

Table 4.11 CS06 test equipment

Equipment	Manufacturer	Model	Serial number
Spike generator	Solar Electronics	7054-i	129148
Oscilloscope	Tektronix	2465	B025650

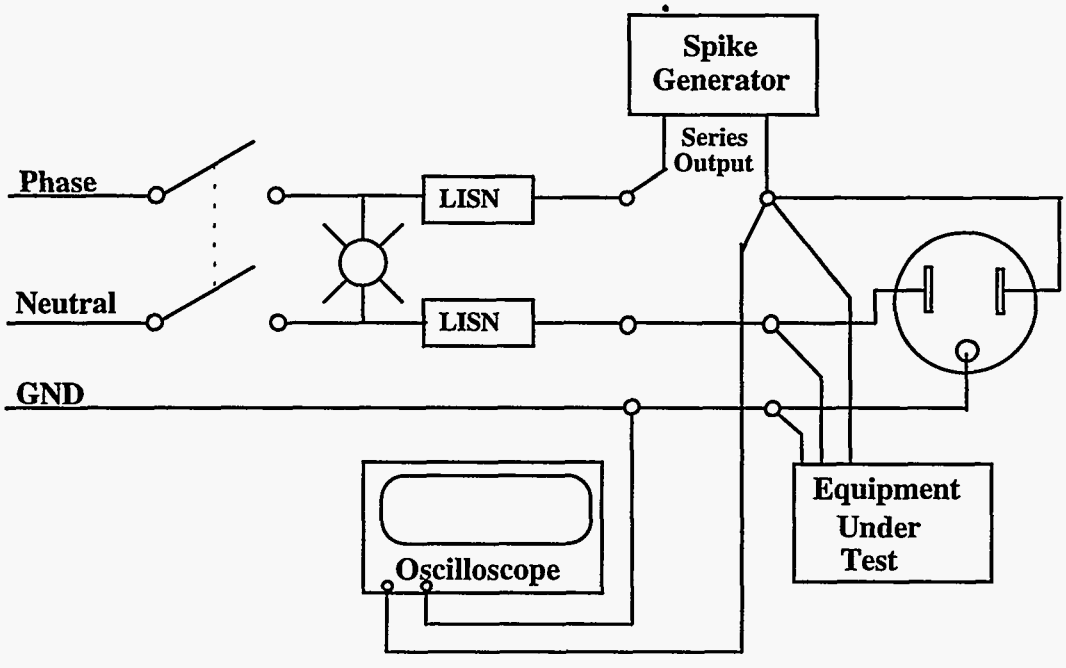


Figure 4.8 CS06 test setup

Spikes on AC power phase lead

(1) The spike generator is connected in series with the power line phase lead using the *series output* of the generator.

(2) The spike generator output is adjusted for minimum amplitude using an X100 probe, with one channel of the oscilloscope connected to monitor the amplitude of the spike applied to the phase lead. (The oscilloscope probe ground clip is placed on the green wire safety ground, not on any of the spike generator output terminals.)

(3) The test equipment is energized and the polarity of the low amplitude spikes is observed to ensure that *positive* spikes are applied on the phase line.

(4) The EUT is energized, the EDSC is initialized, and the HOSTP software is started.

(5) The spike voltage is synchronized with the power line voltage at 0° phase angle.

(6) Starting from 0 V, the spike amplitude is increased to 400 V in 100-V increments. At each voltage increment, the system performance is observed for at least 10 test cycles (~15 s) before the next incremental voltage is applied. The EDSC's performance is continuously monitored by the HOSTP, and error messages are displayed by the HOSTP. If a malfunction occurs, the corresponding conditions are noted. Then the voltage is reduced to zero and increased again to determine if the error is repeatable.

(7) If errors occur at a specific voltage level, no tests are performed at higher voltage levels. If the EUT is not susceptible below 400 V, the final condition of 400 V is maintained for 5 min.

(8) The spike amplitude is reduced to zero.

(9) Steps 6 to 8 are repeated with the spike synchronized with the power line waveform at 90° phase angle.

(10) Steps 6 to 8 are repeated with the spike synchronized with the power line waveform at 180° phase angle.

(11) Steps 6 to 8 are repeated with the spike synchronized with the power line waveform at 270° phase angle.

(12) The spike generator is set up to "free run" and the spike rate is varied for 1 min to observe any malfunctions under these conditions.

(13) The HOSTP software is stopped and the test equipment and EUT are de-energized.

(14) The spike generator leads are reversed to apply *negative* spikes to the EUT. Then steps 4 to 10 are repeated, with the negative voltage spikes applied to the phase lead.

Spikes on ac power neutral lead

(1) The spike generator is connected in series with the power line neutral lead using the *series output* of the generator.

(2) The spike generator output is adjusted for minimum amplitude. Using an X100 probe, one channel of the oscilloscope is connected to monitor the amplitude of the spike applied to the neutral lead. (The oscilloscope probe ground clip is placed on the green wire safety ground, not on any of the spike generator output terminals.)

(3) Steps 3 to 13 above are repeated, except that the generator is connected in series with the neutral lead rather than the phase lead.

(4) The spike generator leads are reversed to apply negative spikes to the EUT. Then steps 3 to 13 above are repeated, with the negative spikes applied to the neutral lead.

4.4.2 CS06 Test Results

The HOSTP automatically recorded error messages and time stamps for all detected anomalies in error log files. Actual trip/no-trip and voltage levels were recorded in data files. Tables 4.12 to 4.15 present the test results with the PRS/MUX as the EUT, and Tables 4.16 to 4.19 present the test results with the DTC as the EUT.

PRS/MUX as EUT

Table 4.12 CS06 test results—positive spikes on phase lead of PRS/MUX

Phase (degrees)	Voltage (V)	Errors
0	100	none
0	200	none
0	300	SOME*
90	100	none
90	200	SOME*
180	100	none
180	200	SOME*
270	100	none
270	200	SOME*

*See text for discussion.

Table 4.13 CS06 test results—negative spikes on phase lead of PRS/MUX

Phase (degrees)	Voltage (V)	Errors
0	–100	none
0	–200	none
0	–300	none
0	–400	SOME*
90	–100	none
90	–200	none
90	–300	none
90	–400	SOME*
180	–100	none
180	–200	none
180	–300	none
180	–400	SOME*
270	–100	none
270	–200	SOME*

*See text for discussion.

Table 4.14 CS06 test results—positive spikes on neutral lead of PRS/MUX

Phase (degrees)	Voltage (V)	Errors
0	100	none
0	200	none
0	300	none
0	400	SOME*
90	100	none
90	200	SOME*
180	100	none
180	200	none
180	300	none
180	400	SOME*
270	100	none
270	200	SOME*

*See text for discussion.

Table 4.15 CS06 test results—negative spikes on neutral lead of PRS/MUX

Phase (degrees)	Voltage (V)	Errors
0	–100	none
0	–200	none
0	–300	none
0	–400	SOME*
90	–100	none
90	–200	SOME*
180	–100	none
180	–200	none
180	–300	SOME*
270	–100	none
270	–200	none
270	–300	none
270	–400	SOME*

*See text for discussion.

DTC as EUT

Table 4.16 CS06 test results—positive spikes on phase lead of DTC

Phase (degrees)	Voltage (V)	Errors
0	100	none
0	200	none
0	300	none
0	400	SOME*
90	100	none
90	200	none
90	300	none
90	400	none
180	100	none
180	200	none
180	300	none
180	400	none
270	100	none
270	200	none
270	300	none
270	400	SOME*

*See text for discussion.

Table 4.17 CS06 test results— negative spikes on phase lead of DTC

Phase (degrees)	Voltage (V)	Errors
0	–100	none
0	–200	none
0	–300	none
0	–400	SOME*
90	–100	none
90	–200	none
90	–300	none
90	–400	SOME*
180	–100	none
180	–200	none
180	–300	none
180	–400	SOME*
270	–100	none
270	–200	none
270	–300	none
270	–400	none

*See text for discussion

Table 4.18 CS06 test results—positive spikes on neutral lead of DTC

Phase (degrees)	Voltage (V)	Errors
0	100	none
0	200	none
0	300	none
0	400	none
90	100	none
90	200	none
90	300	none
90	400	SOME*
180	100	none
180	200	none
180	300	none
180	400	SOME*
270	100	none
270	200	none
270	300	none
270	400	none

*See text for discussion.

Table 4.19 CS06 test results—negative spikes on neutral lead of DTC

Phase (degrees)	Voltage (V)	Errors
0	–100	none
0	–200	none
0	–300	none
0	–400	SOME*
90	–100	none
90	–200	none
90	–300	none
90	–400	none
180	–100	none
180	–200	none
180	–300	none
180	–400	SOME*
270	–100	none
270	–200	none
270	–300	none
270	–400	SOME*

*See text for discussion.

4.4.3 Analysis of CS06 Test Results

The results of the CS06 tests are shown graphically in Figures 4.9 to 4.16. With the PRS/MUX as the EUT, the errors were similar to those of the CS02 tests. Most errors were due to temporary failure of some of the I/O modules to transfer data to the PRS/MUX computer. These communication errors typically occurred at 400 V (both positive and negative spikes) and at all phase angles tested.

With the DTC as the EUT, many of the errors that occurred were timeouts due to temporary failure of the DTC serial datalink ports. Many of these occurred at a test voltage amplitude of 400 V, but the phase angle at which the errors occurred did not demonstrate an identifiable pattern.

No permanent failures occurred during these tests.

Corrupted data read from at least one I/O module from the PRS/MUX backplane (error type l).			*		*		*		*
Timeout on attempt to read data from one or more of the PRS/MUX I/O modules (error type m).			*		*		*		*
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).					*				
	100	200	300	100	200	100	200	100	200 V
	Spike synchronized with power voltage a 0° phase angle			Spike synchronized with power voltage at 90° phase angle		Spike synchronized with power voltage at 180° phase angle		Spike synchronized with power voltage at 270° phase angle	

Figure 4.9 CS06 tests with positive spikes on phase lead of PRS/MUX

Timeout by DTC on attempt to read data from HOSTP channel 2 fiber-optic serial datalink (error type a).									*			
Corrupted data read from at least one I/O module from the PRS/MUX backplane (error type l).			*			*			*		*	
Timeout on attempt to read data from one or more of the PRS/MUX I/O modules (error type m).			*			*			*		*	
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).						*						
	–100	–200	–400	–100	–200	–400	–100	–200	–400	–100	–200	–400 V
	Spike synchronized with power voltage at 0° phase angle			Spike synchronized with power voltage at 90° phase angle			Spike synchronized with power voltage at 180° phase angle			Spike synchronized with power voltage at 270° phase angle		

Figure 4.10 CS06 tests with negative spikes on phase lead of PRS/MUX

Corrupted data read from at least one I/O module from the PRS/MUX backplane (error type l).			*		*				*		*	
Timeout on attempt to read data from one or more of the PRS/MUX I/O modules (error type m).			*		*				*		*	
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).											*	
	100	200	400	100	200	400	100	200	400	100	200	400 V
	Spike synchronized with power voltage at 0° phase angle			Spike synchronized with power voltage at 90° phase angle			Spike synchronized with power voltage at 180° phase angle			Spike synchronized with power voltage at 270° phase angle		

Figure 4.11 CS06 tests with positive spikes on neutral lead of PRS/MUX

Timeout by DTC on attempt to read data from HOSTP channel 2 fiber-optic serial datalink (error type a).								*			
Corrupted data read from at least one I/O module from the PRS/MUX backplane (error type l).			*		*			*			*
Timeout on attempt to read data from one or more of the PRS/MUX I/O modules (error type m).					*			*			*
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).											
	−100	−200	−400	−100	−200	−100	−200	−300	−100	−200	−400 V
	Spike synchronized with power voltage at 0° phase angle			Spike synchronized with power voltage at 90° phase angle		Spike synchronized with power voltage at 180° phase angle			Spike synchronized with power voltage at 270° phase angle		

Figure 4.12 CS06 tests with negative spikes on neutral lead of PRS/MUX

Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 2 (error type d).			*									
Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 3 (error type e).			*									
Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 4 (error type f).			*									
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).												*
	100	200	400	100	200	400	100	200	400	100	200	400 V
	Spike synchronized with power voltage at 0° phase angle			Spike synchronized with power voltage at 90° phase angle			Spike synchronized with power voltage at 180° phase angle			Spike synchronized with power voltage at 270° phase angle		

Figure 4.13 CS06 tests with positive spikes on phase lead of DTC

Timeout by DTC on attempt to read data from HOSTP channel 2 fiber-optic serial datalink (error type a).									*			
Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 2 (error type d).									*			
Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 3 (error type e).									*			
Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 4 (error type f).									*			
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).			*			*						
	–100	–200	–400	–100	–200	–400	–100	–200	–400	–100	–200	–400 V
	Spike synchronized with power voltage at 0° phase angle			Spike synchronized with power voltage at 90° phase angle			Spike synchronized with power voltage at 180° phase angle			Spike synchronized with power voltage at 270° phase angle		

Figure 4.14 CS06 tests with negative spikes on phase lead of DTC

Timeout by DTC on attempt to read data from HOSTP channel 2 fiber-optic serial datalink (error type a).									*			
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).						*			*			*
	100	200	400	100	200	400	100	200	400	100	200	400 V
	Spike synchronized with power voltage at 0° phase angle			Spike synchronized with power voltage at 90° phase angle			Spike synchronized with power voltage at 180° phase angle			Spike synchronized with power voltage at 270° phase angle		

Figure 4.15 CS06 tests with positive spikes on neutral lead of DTC

Timeout by DTC on attempt to read data from HOSTP channel 2 fiber optic serial datalink (error type a).									*			
Diff. between voltage received by, and that transmitted to, the ESF/MUX for one or more ESF system signals (error type s).			*						*			
	–100	–200	–400	–100	–200	–400	–100	–200	–400	–100	–200	–400 V
	Spike synchronized with power voltage at 0° phase angle			Spike synchronized with power voltage at 90° phase angle			Spike synchronized with power voltage at 180° phase angle			Spike synchronized with power voltage at 270° phase angle		

Figure 4.16 CS06 tests with negative spikes on neutral lead of DTC

4.5 RS01: Radiated Susceptibility, Magnetic Fields

The RS01 test ensures that equipment and subsystems are not susceptible to radiated magnetic fields in the range 30 Hz to 50 kHz. A Merritt coil set, consisting of four rectangular coils oriented so as to produce linearly polarized horizontal magnetic fields, is used to generate the required magnetic fields. The EUT is placed within the radiating loop of the Merritt coil set.

4.5.1 RS01 Test Procedure

Table 4.20 lists the test equipment used for the RS01 tests. The test setup is shown in Figure 4.17. A detailed description of the test procedure follows.

NOTE: Calibration of power sweep generator:

To determine the settings of the Solar sweep generator for the required field strengths specified in MIL-STD-461C (see step 6 below), an FW Bell model 9640 Gauss meter was used. For frequencies from 30 to 200 Hz, the output of the power sweep generator was increased until the Gauss meter indicated the desired field strength for each frequency. At each frequency, the voltage swing (Vpp)

Table 4.20 RS01 test equipment

Equipment	Manufacturer	Model	Serial Number
Power sweep generator	Solar Electronics	6550-1	X151231
Merritt coil	Electric Research	1318.001	9501
Oscilloscope	Tektronix	TEK2465	X170968
Gauss meter	F. W. Bell	9640	239554

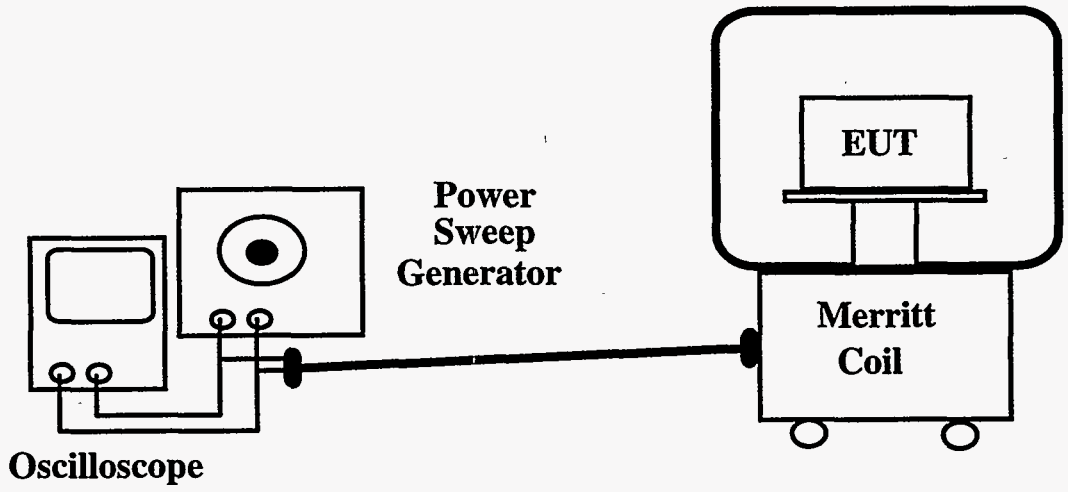


Figure 4.17 RS01 test setup

was recorded from the oscilloscope display. The required voltage swing for the higher frequencies was extrapolated from these readings.

Magnetic field tests

(1) The EUT is placed inside the radiating loop of a Merritt coil, and connections are made to the power sweep generator and the oscilloscope, as shown in Figure 4.17.

(2) The EUT is energized, the EDSC is initialized, and the HOSTP software is started.

(3) The power sweep generator output control is adjusted for a minimum amplitude and energized.

(4) The power sweep generator is set to a frequency of 30 kHz.

(5) Using an X100 probe, one channel of the oscilloscope is used to monitor the amplitude of the voltage applied to the Merritt coil.

(6) The magnitude of the power sweep generator output is slowly increased until the voltage corresponding to the required magnetic field strength as specified in MIL-STD-461C (limit for RS01) is reached. The EDSC's performance is continuously monitored by the HOSTP, and error messages are displayed by the HOSTP. If a malfunction occurs, the corresponding conditions are noted. Then the voltage is reduced to zero and increased again to determine if the error is repeatable.

(7) Steps 5 and 6 are repeated with frequency settings of 60 Hz, 100 Hz, 200 Hz, 500 Hz, 1 kHz, 2 kHz, 5 kHz, 10 kHz, 20 kHz, and 50 kHz.

(8) The HOSTP software is stopped, and the test equipment and EUT are de-energized.

4.5.2 RS01 Test Results

The HOSTP automatically recorded error messages and time stamps for all detected anomalies in error log files. Actual trip/no-trip and voltage levels were recorded in data files. Table 4.21 presents the test results with the PRS/MUX as the EUT, and Table 4.22 presents the test results with the DTC as the EUT.

PRS/MUX as EUT

Table 4.21 RS01 test results—radiated magnetic fields on PRS/MUX

Frequency (Hz)	RS01 limit (dBpT)	RS01 limit (Oe)	Scope Setting (Vpp)	Errors
30	160	1	20.6	none
60	148	0.25	10.2	none
100	140	0.1	6.2	none
200	128	0.025	3.9	none
500	112	0.004	1.4	none
1000	106	0.002	1.4	none
2000	100	0.001	1.4	none
5000	94	0.0005	1.8	none
10000	86	0.0002	1.4	none
20000	80	0.0001	1.4	none
50000	76	0.00006	2.2	none

Table 4.22 RS01 test results—radiated magnetic fields on DTC

Frequency (Hz)	RS01 limit (dBpT)	RS01 limit (Oe)	Scope Setting (Vpp)	Errors
30	160	1	20.6	none
60	148	0.25	10.2	none
100	140	0.1	6.2	none
200	128	0.025	3.9	none
500	112	0.004	1.4	none
1000	106	0.002	1.4	none
2000	100	0.001	1.4	none
5000	94	0.0005	1.8	none
10000	86	0.0002	1.4	none
20000	80	0.0001	1.4	none
50000	76	0.00006	2.2	none

4.5.3 Analysis of RS01 Test Results

No errors were observed with either the PRS/MUX or the DTC as the EUT.

4.6 RS02: Radiated Susceptibility, Spikes

The RS02 test evaluates the response of the equipment under test to radiated magnetic and electric fields generated by spikes and power line frequency current. The RS02 test is applicable to signal cables and enclosures, but power input and output leads are exempt. Only the spike generator portion of the tests was performed since the required generating equipment was not available for the 60-Hz test.

4.6.1 RS02 Test Procedure

Table 4.23 lists the test equipment used for the RS02 tests. The test setup is shown in Figure 4.18. Detailed description of the test procedure follows.

Spike test

(1) An inducing wire is wrapped around the signal cable between the EUT and the associated equipment, as shown in Figure 4.18. (Note: Care should be taken to ensure that there is no excess wire length or coils in the inducing wire.)

Table 4.23 RS02 test equipment

Equipment	Manufacturer	Model number	Serial number
Spike generator	Solar Electronics	7054-1	X155039
Oscilloscope	Tektronix	TEK2465	X170968

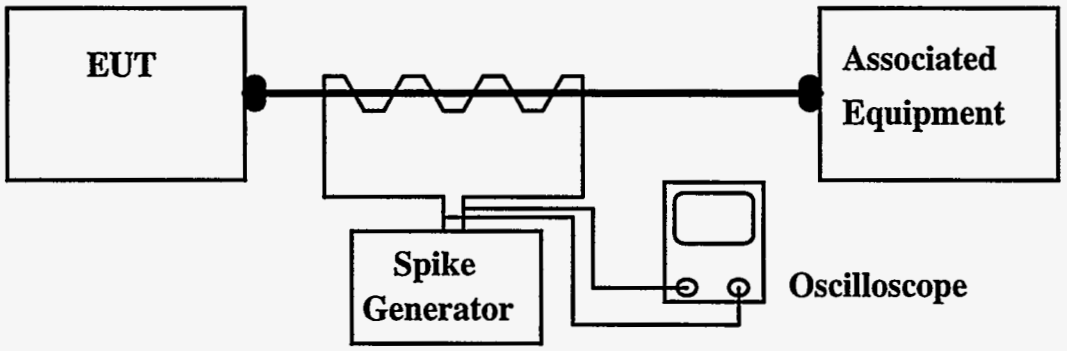


Figure 4.18 RS02 setup for signal cable test

(2) The ends of the inducing wire are connected to the series output of the spike generator.

(3) The spike generator output control is adjusted for minimum amplitude, and the spike generator is energized.

(4) The EUT is energized, the EDSC is initialized, and the HOSTP software is started.

(5) Using an X100 probe, one channel of the oscilloscope is used to monitor the amplitude of the spike applied to the inducing wire. The polarity of the spikes is observed to ensure that positive spikes are applied on the inducing wire.

(6) The spikes are synchronized with the power line frequency at 0° phase angle, and the spike amplitude is increased to 400 V. The EDSC's performance is continuously monitored by the HOSTP, and error messages are displayed by the HOSTP. If a malfunction occurs, the corresponding conditions are noted. Then the voltage is reduced to zero and increased again to determine if the error is repeatable.

(7) If a malfunction does not occur until the 400-V spike amplitude is reached, the final condition of 400 V is maintained for 5 min.

(8) The spike amplitude is reduced to zero.

(9) Steps 6 to 8 are repeated, with the spike synchronized to the power line frequency at 90° phase angle.

(10) Steps 6 through 8 are repeated with the spike synchronized to the power line frequency at 180° phase angle.

(11) Steps 6 to 8 are repeated, with the spike synchronized to the power line frequency at 270° phase angle.

(12) The spike generator is set up to free run, and the spike rate is varied for 1 min to observe any malfunctions under these conditions.

(13) The spike amplitude control is reduced and the test equipment is de-energized before switching spike polarity.

(14) The leads at the spike generator output are reversed to apply negative spikes to the inducing wire. The test equipment is then energized.

(15) Steps 6 to 12 are repeated with negative voltage spikes applied.

(16) The HOSTP software is stopped and the test equipment and EUT are de-energized. Then the inducing wire is disconnected from the cable and spike generator.

Tests with equipment case wrapped

(1) At least four turns of wire are wrapped around the EUT enclosure in the X-Y plane, taped in place, and connected to the series output of the spike generator, as shown in Figure 4.18.

(2) Steps 3 to 16 above are repeated.

(3) Steps 1 and 2 of this list are repeated with the inducing wire in the Y-Z plane.

(4) Steps 1 and 2 of this list are repeated with the inducing wire in the X-Z plane.

Figure 4.19 shows the Cartesian coordinate system used to define directions in the EUT wrap-around tests.

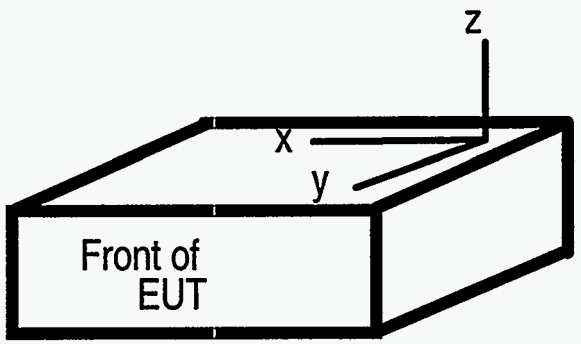


Figure 4.19 Cartesian coordinate sytem used to define RS02 test

4.6.2 RS02 Test Results

The HOSTP automatically recorded error messages and time stamps for all detected anomalies in error log files. Actual trip/no-trip and voltage levels were recorded in data files. Tables 4.24 to 4.27 present the test results with the PRS/MUX as the EUT, and Tables 4.28 to 4.31 present the test results with the DTC as the EUT.

PRS/MUX as EUT

Table 4.24 RS02 test results—spikes applied to PRS/MUX signal cable

Spike Polarity	Max Applied Spike Voltage (V)	Errors
Positive	400	none
Negative	400	none

Table 4.25 RS02 test results—X-Y enclosure wrap test on PRS/MUX

Spike Polarity	Max Applied Spike Voltage (V)	Errors
Positive	400	none
Negative	400	none

Table 4.26 RS02 test results—Y-Z enclosure wrap test on PRS/MUX

Spike Polarity	Max Applied Spike Voltage (V)	Errors
Positive	400	none
Negative	400	none

Table 4.27 RS02 test results—X-Z equipment wrap test on PRS/MUX

Spike Polarity	Max Applied Spike Voltage (V)	Errors
Positive	400	none
Negative	400	none

DTC as EUT

Table 4.28 RS02 test results—spikes applied to DTC signal cable

Spike Polarity	Max Applied Spike Voltage (V)	Errors
Positive	400	none
Negative	400	none

Table 4.29 RS02 test results—X-Y enclosure wrap test on DTC

Spike Polarity	Max Applied Spike Voltage (V)	Errors
Positive	400	none
Negative	400	none

Table 4.30 RS02 tests results—Y-Z enclosure wrap test on DTC

Spike Polarity	Max Applied Spike Voltage (V)	Errors
Positive	400	none
Negative	400	none

Table 4.31 RS02 test results—X-Z enclosure wrap test on DTC

Spike Polarity	Max Applied Spike Voltage (V)	Errors
Positive	400	none
Negative	400	none

4.6.3 Analysis of RS02 Test Results

The results of the RS02 tests are shown in Figures 4.20 and 4.21. With the PRS/MUX as the EUT and with the test wire wrapped around the PRS/MUX copper signal cable, the HOSTP's monitor was observed to flash continuously (i.e., the screen would alternately blank out and come back on at a frequency of about 1 Hz) when negative polarity spikes were applied. The flashing stopped when the test voltage spike was reduced from 400 to 250 V. This phenomenon was attributed to the close proximity of the HOSTP monitor to the EUT, resulting from limited space for the test environment. In any case, the problem was not "safety related," since the monitor was not part of the channel under test. However, it does underscore the fact that magnetic fields may interfere with computer displays and could thereby prevent an abnormal occurrence from being observed early and thus prevent a safety-related manual corrective action from being taken in a timely manner.

No other errors were observed with either the positive or negative polarity tests when the test wire was wrapped around either the X-Y, Y-Z, or X-Z plane of the PRS/MUX.

With the test wire wrapped around the DTC signal cables, no errors were observed when positive polarity spikes were applied. However, when negative polarity spikes were applied, the HOSTP's monitor was observed to flash continuously, as in the previous case. The screen stopped flashing when the test voltage spike magnitude was reduced to 300 V.

No errors were observed with either the positive or negative polarity tests when the test wire was wrapped around either the X-Y, Y-Z, or X-Z plane of the DTC.

HOSTP continuously blanked OFF and ON (error type ff).		*						
	+ve spike (400 V)	−ve spike (400 V)	+ve spike (400 V)	−ve spike (400 V)	+ve spike (400 V)	−ve spike (400 V)	+ve spike (400 V)	-ve spike (400 V)
	Test wire around signal cable		Test loop parallel to X-Y plane		Test loop parallel to Y-Z plane		Test loop parallel to X-Z plane	

Figure 4.20 RS02 test results with PRS/MUX as the EUT

HOSTP continuously blanked OFF and ON (error type ff).		*						
	+ve spike (400 V)	−ve spike (400 V)	+ve spike (400 V)	−ve spike (400 V)	+ve spike (400 V)	−ve spike (400 V)	+ve spike (400 V)	−ve spike (400 V)
	Test wire around signal cable		Test loop parallel to X-Y plane		Test loop parallel to Y-Z plane		Test loop parallel to X-Z plane	

Figure 4.21 RS02 test results with DTC as the EUT

4.7 RS03: Radiated Susceptibility, Electric Fields

The RS03 test ensures that equipment under test is not susceptible to radiated electric fields in the frequency range from 14 kHz to 1 GHz. The fields are produced with a Gigahertz Transverse Electromagnetic (GTEM) cell.

4.7.1 RS03 Test Procedure

Table 4.32 lists the test equipment used for the RS03 tests. The test setup is shown in Figure 4.22.

Table 4.32 Test equipment for RS03

Equipment	Manufacturer	Model	Serial No.
Signal Generator	Hewlett Packard	8656A	2312A04388
Function Generator	Hewlett Packard	3325A	1748A15807
RF Power Amplifier	Amplifier Research	75A220	15706
Broadband Power Amplifier	EATON	15100B	0508-02272
Field probe	EMCO	7122	9406-1201
Interface Unit	EMCO	7122 7110	9410-1278
GTEM Cell	EMCO	7122 5311	1131

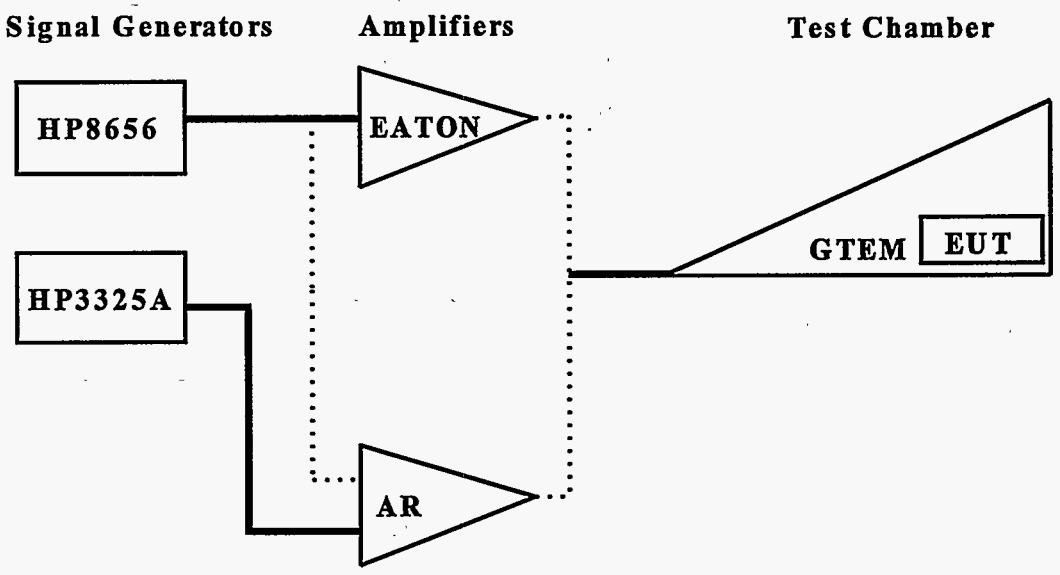


Figure 4.22 RS03 test setup

The following points should be noted:

The following basic generating system was used to provide the fields recorded in the tables below: The HP3325A function generator was used for 0.02–0.05 MHz, and the HP8656 signal generator was used for 0.1–990 MHz. The EATON amplifier was used for 500 and 990 MHz, and the Amplifier Research (AR) amplifier was used for all other frequencies. No modulation was used on the 20- to 50-kHz fields because the low-frequency generator does not provide modulation.

In general, field strengths of about 10 V/m, 20 V/m, and the maximum field strength obtainable were tested. However, in some cases the maximum level obtainable was at or below 20 V/m, so only two field strengths were tested.

To obtain the desired field strength of ~20 V/m at 2 MHz, the gain control was kept at maximum, and fractional dBm settings were used. This change was made to allow a better correlation at a later time.

For the PRS/MUX tests (50 MHz and above), the multiplexer backplane that was inside the GTEM cell was brought outside and swapped with the ESF/MUX multiplexer backplane, because the 20-MHz, 106-V/m test resulted in a permanent failure of the initial EUT's multiplexer power supply.

A detailed description of the test procedure follows.

(1) The EUT is placed in the GTEM cell and connections are made as shown in Figure 4.22. The amplifier output is connected to the GTEM input.

(2) The EUT is energized, the EDSC is initialized, and the HOSTP software is started.

(3) The signal generator output is connected to the amplifier input, and both pieces of equipment are powered.

(4) The frequency output of the signal generator is set to 20 kHz.

(5) The signal generator modulation is turned off, and the voltage across the antenna input connector is adjusted until the field strength as measured by the EMCO Model 7122 antenna is approximately ~10 V/m.

(6) The signal generator modulation is turned on and adjusted for 80% AM with the internal 1-kHz source.

(7) The field strength is maintained for 200 test cycles (~5 min), while the EDSC's performance is continuously monitored by the HOSTP. If a malfunction occurs, the corresponding conditions are noted. Then the field strength is reduced to zero to determine if the system will recover. If the system recovers, the particular test is performed again to determine if the errors are repeatable. If a permanent failure occurs at a particular field strength, the tests are suspended and the cause of the malfunctions is determined. The malfunctioning component is then replaced and the tests are continued.

(8) At the same selected frequency, the field strength is set to 20 V/m; then steps 6 and 7 are repeated.

(9) With the selected frequency remaining fixed, the field strength is increased gradually, while repeating steps 6 and 7, until errors occur or the maximum ratings of the test equipment are reached, whichever comes first.

(10) Before changing frequency, the voltage amplitude is reduced to zero.

(11) The frequency is set to 50 kHz and steps 5 to 10 are repeated.

(12) The test equipment is shut down, and the HP3325A function generator is replaced with the HP8656 signal generator.

(13) The frequency is set to 100 kHz and steps 5 to 10 are repeated.

(14) The frequency is set to 200 kHz and steps 5 to 10 are repeated.

(15) The frequency is set to 500 kHz and steps 5 to 10 are repeated.

(16) The frequency is set to 1 MHz and steps 5 to 10 are repeated.

(17) The frequency is set to 2 MHz and steps 5 to 10 are repeated.

(18) The frequency is set to 5 MHz and steps 5 to 10 are repeated.

(19) The frequency is set to 10 MHz and steps 5 to 10 are repeated.

(20) The frequency is set to 20 MHz and steps 5 to 10 are repeated.

(21) The frequency is set to 50 MHz and steps 5 to 10 are repeated.

(22) The frequency is set to 100 MHz and steps 5 to 10 are repeated.

(23) The frequency is set to 200 MHz and steps 5 to 10 are repeated.

(24) The test equipment is powered down, and the AR amplifier is replaced with the EATON amplifier.

(25) The frequency is set to 500 MHz and steps 5 to 10 are repeated.

(26) The frequency is set to 900 MHz and steps 5 to 10 are repeated.

(27) The HOSTP software is stopped and the test equipment and EUT are de-energized.

4.7.2 RS03 Test Results

The HOSTP automatically recorded error messages and time stamps for all detected anomalies in error log files. Actual trip/no-trip and voltage levels were recorded in data files. Table 4.33 presents the test results with the PRS/MUX as the EUT, and Tables 4.34 presents the test results with the DTC as the EUT.

PRS/MUX as EUT

Table 4.33 RS03 test results with PRS/MUX as the EUT

Frequency (MHz)	Field Strength (V/m)	Errors
0.02	10	none
0.02	20	none
0.02	65	none
0.05	10	none
0.05	20	none
0.05	65	none
0.1	10	none
0.1	20	none
0.1	70	none
0.2	10	none
0.2	20	none
0.2	82	none
0.5	10	none
0.5	20	none
0.5	69	none
1	10	none
1	20	none
1	65	none
2	10	none
2	20	none
2	62	none
5	10	none
5	20	none
5	68	SOME*
10	10	none
10	20	none
10	68	none
20	10	none
20	20	none
20	72	SOME*
50	10	none
50	20	none
100	10	none
100	20	none
100	34	SOME*
200	10	none
200	20	none
200	32	SOME*
500	10	none
500	20	none
500	22	SOME*
990	10	none
990	12	none

*See text for discussion.

Table 4.34 RS03 test results with DTC as the EUT

Frequency (MHz)	Field Strength (V/m)	Errors
0.02	10	none
0.02	20	none
0.02	66	none
0.05	10	none
0.05	20	none
0.05	85	none
0.1	10	none
0.1	20	none
0.1	85	none
0.2	10	none
0.2	20	none
0.2	82	none
0.5	10	none
0.5	20	none
0.5	69	none
1	10	none
1	20	none
1	65	none
2	10	none
2	20	none
2	62	none
5	10	none
5	20	none
5	51	none
5	60	none
10	10	none
10	20	none
10	50	none
10	68	SOME*
20	10	none
20	20	none
20	68	SOME*
50	10	none
50	20	none
50	40	SOME*
100	18	none
100	34	none
100	85	none
200	17	none
200	32	none
200	73	none
500	11	none
500	20	none
990	12	none
990	18	none

*See text for discussion.

4.7.3 Analysis of RS03 Test Results

The results of the RS03 tests are shown in Figures 4.23 and 4.24. With the PRS/MUX as the EUT, temporary failures were recorded at 5 MHz [68 V/m], 20 MHz [72 V/m], 100 MHz [34 V/m], 200 MHz [32 V/m], and 500 MHz [22 V/m]. These temporary failures resulted in system-level errors such as (1) inability to read data from a PRS/MUX I/O module (timeout error) and loss of data accuracy in the process variables transmitted across the network by the PRS/MUX. While the system was able to recover from these errors in all cases, the power supply of the original PRS/MUX multiplexer backplane under test inside the GTEM cell failed permanently after the 20-MHz, 72-V/m test. This multiplexer was swapped with the ESF/MUX multiplexer backplane so that the failed power supply could be replaced with a functionally equivalent one. Throughout all the EMI/RFI tests, this is the only hard or permanent failure that occurred. The minimum field strength at which temporary errors occurred with the PRS/MUX as EUT was 22 V/m.

With the DTC as the EUT, temporary failures were recorded at 10 MHz [68 V/m], 20 MHz [68 V/m], and 50 MHz [40 V/m]. The temporary failures resulted in system-level errors such as (1) timeout errors and (2) failure on attempt to initialize a serial datalink, indicating temporary problems with the serial cards in the HOSTP. The latter errors are EDSC-specific (the EDSC was not under test), and it is hypothesized that radiative coupling due to the limited space available for the tests caused the temporary malfunction in the HOSTP serial cards. The minimum field strength at which temporary errors occurred with the DTC was 40 V/m.

4.8 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 nuclear power plant 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) compared to low-voltage, sinusoidal 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.

While 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

Corrupted data read from at least one I/O module from the PRS/MUX backplane (error type l).	68		72					
Timeout on attempt to read data from one or more of the PRS/MUX I/O modules (error type m).	68		72					
Difference between voltage sent to, and that transmitted by, the PRS/MUX for one or more process signals (error type r).	68		72		34	32	22	
PRS/MUX power supply failure (error type gg).			72					
	5	10	20	50	100	200	500	900 MHz

(NOTE: No errors occurred at frequencies below 5 MHz. Also, numbers in table cells indicate the minimum field strength in volts per meter at which the particular errors occurred).

Figure 4.23 RS03 test results with the PRS/MUX as the EUT

Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 2 (error type d).		68						
Failure on attempt by HOSTP to initialize fiber-optic serial write link on channel 2 (error type u).		68						
Failure on attempt by HOSTP to initialize fiber-optic serial write link on channel 3 (error type v).			68	40				
	5	10	20	50	100	200	500	900 MHz

(NOTE: No errors occurred at frequencies below 10 MHz. Also, numbers in table cells indicate the minimum field strength in volts per meter at which the particular errors occurred).

Figure 4.24 RS03 test results with the DTC and fiber-optic modules as the EUT

susceptibility of particular systems can be mitigated by grounding, shielding, isolation, and surge withstand practices.

The results of all the tests, as a function of the failure classifications established in this document, are shown in Figure 4.25.

(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 4.25 Summary of EMI/RFI test results as a function of failure classification

5 TEMPERATURE/HUMIDITY TESTS

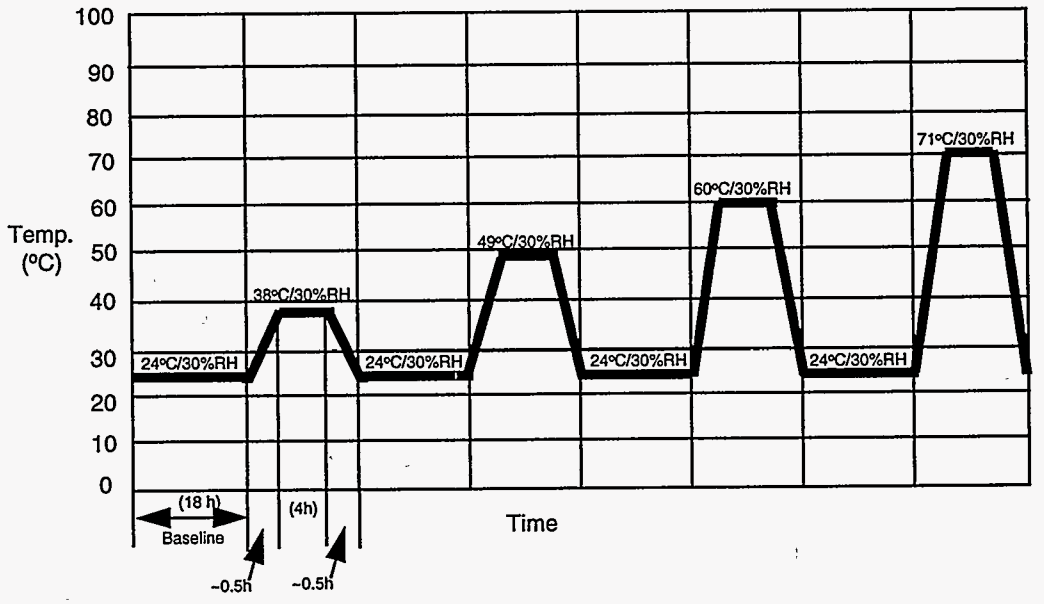
5.1 Introduction

The temperature/humidity cycles used in the environmental tests were selected after careful review of current nuclear, commercial, and military environmental and qualification testing standards and practices.[20-30] A total of 16 elevated temperature/humidity tests was performed; 8 of these were performed with the PRS/MUX as the EUT and 8 with the DTC as the EUT. With the process multiplexing unit as the EUT, temperature tests at 30% relative humidity (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 temperatures, but at a relative humidity of 85%. Both test sequences were then repeated using the DTC as the equipment under test.

A maximum temperature of 71°C (160°F) was considered adequate for the tests for three reasons. First, this value is sufficiently high (taking into account the operating limits of the systems comprising the EDSC) to induce errors so that failure modes characteristic of the technologies employed could be identified. Second, it is well beyond what the channel is likely to experience in a normal nuclear power plant (control room) environment. Third, it is comparable to 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 is typically about 75°C (167°F). This qualification methodology is typical of reactor manufacturers and suppliers.

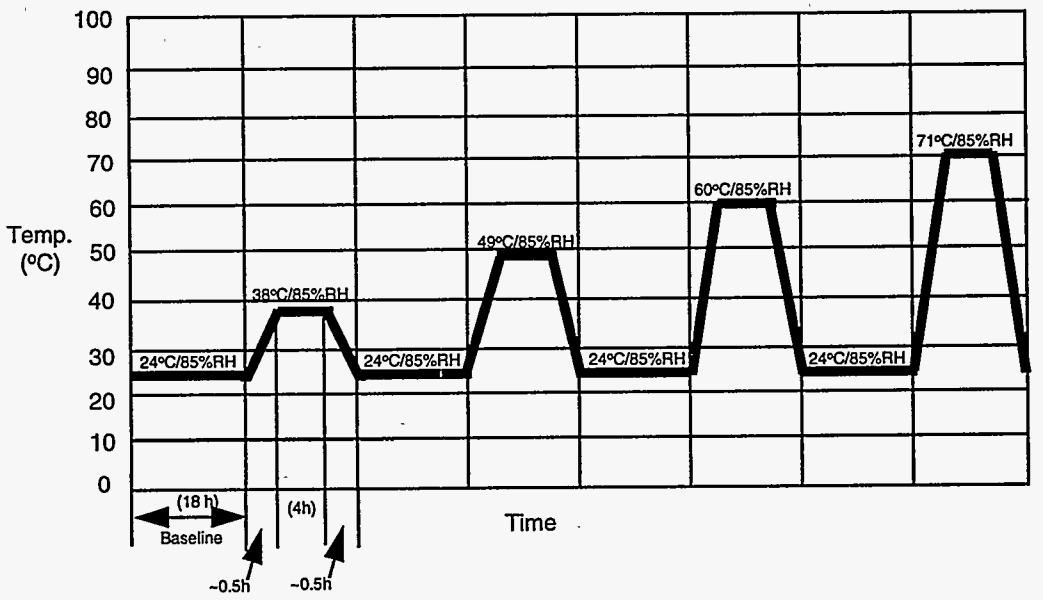
The general procedure followed was to obtain data for about 18 h at the baseline temperature and humidity and then increase only the temperature to the next test value. The EUT was then monitored at this new steady-state test value for a period of 4 h. The temperature was then reduced to the baseline value, and monitoring was continued for an additional 18 h, after which the temperature was raised to the next test value. These test sequences are shown in Figures. 5.1 and 5.2. 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.

The fiber-optic modules (FOMs) were not subjected to the elevated temperature tests. Prior functional testing of the EDSC had demonstrated the system-level interaction characteristics resulting from FOM failures due to temperature. In particular, the FOMs exhibited communication failures (i.e., parity errors, framing errors, timeouts) at about 38°C, well below the maximum test temperature (71°C) to which the EDSC would be subjected. It was decided that no additional failure information could be obtained by subjecting the FOMs to higher temperatures since the FOMs could either be damaged or their failure characteristics could obscure other failure modes for the entire system. They were therefore not subjected to the temperature stresses in order that actual temperature-induced errors related to other subsystems or modules of the EDSC could be more clearly established.



NOTES:
(1). All baseline tests were 18h in duration.
(2). All temperature ramp-ups and ramp-downs reached steady state values within 0.5h.
(3). All elevated temperature tests were 4h in duration.

Figure 5.1 Temperature cycles at 30% RH used during tests



NOTES:
(1). All baseline tests were 18h in duration.
(2). All temperature ramp-ups and ramp-downs reached steady state values within 0.5h.
(3). All elevated temperature tests were 4h in duration.

Figure 5.2 Temperature cycles at 85% RH used during tests

5.2 General Test Procedure

The general procedure adopted for all the tests was as follows:

(1) The *equipment under test* (EUT) is placed in the test chamber (TC). The TC is maintained at a temperature of 24°C (75°F) and an RH of 30%.

(2) The EUT is energized, the EDSC is initialized, and the HOSTP software is started.

(3) The EUT is monitored at this temperature and relative humidity for ~18 h.

(4) The TC temperature is increased to 38°C over a ramp time of ~0.5 h. The RH is maintained at the baseline value.

(5) The EUT is monitored at the new steady-state value for 4 h.

(6) The TC temperature is brought back to baseline conditions as in (1). This condition is maintained for a period of 18 h while constantly monitoring the EUT to obtain new baseline data.

(7) The TC temperature is increased to 49°C, and steps 5 and 6 are repeated.

(8) The TC temperature is increased to 60°C, and steps 5 and 6 are repeated.

(9) The TC temperature is increased to 71°C, and step 5 is repeated.

(10) The TC temperature is returned to a new baseline condition of 24°C and 85% RH. This condition is maintained for a period of 18 h while constantly monitoring the EUT to obtain new baseline data.

(11) The TC temperature is increased to 38°C over a ramp time of ~0.5 h. The RH is maintained at the baseline value.

(12) The EUT is monitored at the new steady state value for 4 h.

(13) The TC temperature is returned to baseline conditions as in (10). This condition is maintained for a period of 18 h while constantly monitoring the EUT to obtain new baseline data.

(14) The TC temperature is increased to 49°C, and steps 12 and 13 are repeated.

(15) The TC temperature is increased to 60°C, and steps 12 and 13 are repeated.

(16) The TC temperature is increased to 71°C, and steps 12 and 13 are repeated.

(17) The HOSTP software is stopped, and the EUT is de-energized.

5.3 Analysis of Temperature/Humidity Test Results

With the PRS/MUX as the EUT, no errors were recorded for all the temperature cycle tests run at 30% relative humidity. Figure 5.3 shows the errors recorded during tests performed at 85% RH. Errors were recorded at 49°C, 60°C, and 71°C. The "voltage difference" errors (type "r" faults) were due to intermittent hardware faults with one of the I/O modules on the PRS/MUX backplane. This resulted in the voltage reported by the I/O module (zero volts) being less than the analog input voltage sent to that I/O module by the HOSTP. This type of error is classified in this study as a potentially unsafe error since in a typical reactor trip system, signal validation methodologies can be used to check for such "out-of-range" values, drifts, etc.

	24°C/ 85%RH (18 h) (Baseline)	38°C/ 85%RH (4 h)	24°C/ 85%RH (18 h) (Baseline)	49°C/ 85%RH (4 h)	24°C/ 85%RH (18 h) (Baseline)	60°C/ 85%RH (4 h)	24°C/ 85%RH (18 h) (Baseline)	71°C/ 85%RH (4 h)
Corrupted data read from at least one I/O module from the PRS/MUX backplane (error type l).								*
PRS/MUX had to retransmit network data (error type o).								*
Difference between voltage sent to, and that transmitted by, the PRS/MUX for one or more process signals (error type r).				*		*		*

(No errors occurred at 30% RH).

Figure 5.3 Temperature tests at 85% RH, with PRS/MUX as EUT

Errors generally increased as a function of temperature. For example, at the highest test temperature (71°C), errors that occurred in addition to the type "r" faults included corrupted data from some of the I/O modules (parity error, framing error, etc.). The PRS/MUX network card also appeared to have been temporarily affected, as is evidenced by the node having to retransmit data across the network (type o errors).

High humidity can, of course, increase the severity of observed I&C failures. This is evidenced by the fact that the PRS/MUX had no errors at 30% RH but exhibited degraded performance at the 85% RH level. In addition, temperature is seen to act as an accelerating factor through the occurrence of the observed errors at high temperature. The postulated mechanism for the temperature/humidity interaction is an expansion of microcracks in the circuit board due to increased temperature, followed by moisture ingress that results in intermittent circuit failures. However, as in the case of the EMI/RFI tests, all the above faults are classified as either potentially unsafe or conditionally safe failures. In other words, the system can be designed to result in fail-safe conditions given such upsets.

No errors were encountered for any of the temperature tests at either 30% or 85% RH with the DTC as the EUT. This is not unexpected considering that most of the errors for the PRS/MUX were related to the I/O modules and relatively exposed PRS/MUX multiplexer backplane and that the DTC had no equivalent components.

In summary, observations from these tests appear to indicate that the reliability of current microprocessor *components* is such that upsets, rather than hard failures, are 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.

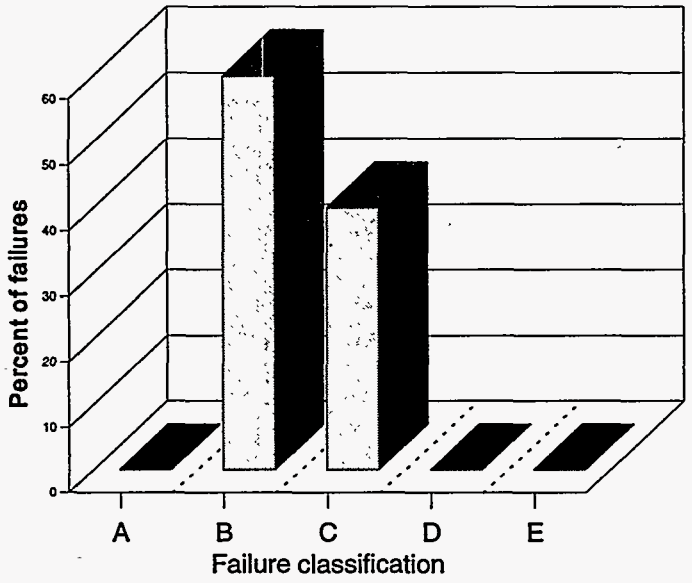
5.4 Summary of Temperature/Humidity Tests

The major subsystems of the EDSC—the industrial computers, the fiber-optic line drivers, and the A/D modules of the process multiplexing 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 45°C (114°F). At the higher relative humidity (85%), some of the A/D modules in the PRS/MUX failed temporarily when test temperatures reached 49°C (120°F), which is 11°C (20°F) below their maximum rated operating value [60°C (140°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.

The failures encountered during the tests are depicted graphically in Figure 5.4 as a function of the failure classifications used in the document. Three conclusions are suggested from this and the preceding discussions:

(1) 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, elevated temperature (e.g., due to loss of 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.

(2) 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



(a)

Failure classifications used in (a)

Failure Catetory	Description	Number of Errors in Failure Category	Percent of Errors in Failure Catetory
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)

(NOTE: All failures occurred at 85% RH.)

Figure 5.4 Summary of temperature/humidity test results as a function of failure classification

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.

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

6 SMOKE TESTS

6.1 Smoke Exposure Environment

Smoke is a known hazard for electronic equipment; however, very few tests have been developed to determine the reliability of electronic equipment in a smoky atmosphere. The actual contents of smoke can vary in many ways depending upon not only the material being burned, but also the method of production. Fire properties such as burn temperature, oxygen availability, and whether the fire is smoldering or openly flaming can affect the smoke products generated. Other important considerations are the smoke density, the material burned, the humidity, and possible presence of fire suppression chemicals. All of these properties may influence the impact of smoke on electrical equipment performance.

In order to produce smoke in a standardized manner, the American Society for Testing and Materials (ASTM) draft corrosivity test standard produced by the subtask group E5.21.70 was followed. This draft standard is based on a standard toxicity test that has been in use for many years. The primary measurement of the draft corrosivity standard is the loss of metal from a corrosion probe as a function of the various materials burned. Although the objective of the draft standard (relative corrosivity) is different from our objective of testing electronic components in a smoke environment, the methods of smoke production and the time of exposure of the smoke recommended by the standard were adopted to produce a "standard" smoke environment and test scenario.

The mode of burning for this test was radiant heat from tungsten-quartz lamps aided by ignition from either an electrical spark or a butane pilot flame. The fuel was placed inside a cylindrical quartz combustion chamber illuminated by the lamps. The smoke production and exposure equipment is illustrated in Figure 6.1. The radiant heat lamps are adjusted so that a fixed heat flux of 50 kW/m^2 is produced at the fuel surface. The heat flux was measured with a Schmidt-Boelter (thermopile) heat flux meter prior to each test to determine the amount of heat that was incident on the fuel at the beginning of the test. Small variations in the positions of the lamps can affect the heat flux that is incident on the sample. As smoke is produced, the quartz chamber becomes coated with some soot, thus reducing the heat flux.

Nowlen[31] has evaluated the types and sizes of fires that are most likely at nuclear power plants and, based on both testing and plant experience, has defined typical smoke loads for the most common fire types. The smoke load is defined as the ratio of the mass of fuel available to burn to the volume of air into which the fire products are dispersed. Based on information in the Nowlen report, three different smoke loads corresponding to three different fire threat scenarios were used for our tests. The smoke loads used are defined as follows:

Small In-Cabinet Fire: The highest smoke load postulated occurs when electronic equipment is located within the same electrical panel as a small panel 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 noninvolved 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 power plant control panels. A smoke load of 26–560 g/m^3 was identified for this scenario. For our tests, a moderate smoke load of 160 g/m^3 was used.

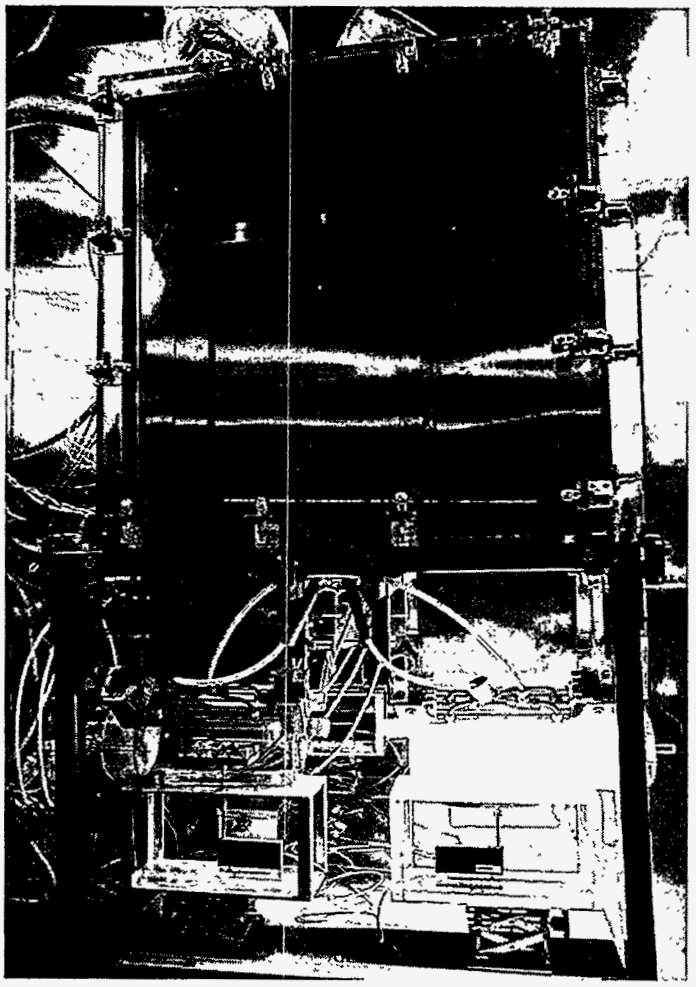


Figure 6.1 Smoke chamber The combustion chambers (four quartz cylinders) are shown underneath the exposure chamber.

Earlier work had 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.[3] The lower limit 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.

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 a 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 case to be

from 2.8–11.2 g/m^3. For our tests, a smoke load of ~3 g/m^3 was used to simulate this scenario. Analysis of the smoke deposition showed the chloride content 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 previous two scenarios. As in the large control room panel fire scenario, a fully involved electrical control panel fire is postulated. However, general plant areas tend to be somewhat smaller, on average, than main control rooms. Hence, the smoke load cited by Nowlen for this scenario was 14–56 g/m^3. For our tests, a smoke load of 20 g/m^3 was used to simulate this scenario. Analysis of the smoke deposition showed the chloride content to be about 57 μg chloride/cm^2.

The volume of the exposure chamber was 1 m^3, so the magnitude of the smoke load used was equal to the amount of fuel burned. For example, a smoke load of 20 g/m^3 corresponds to 20 g of burnable fuel. In a nuclear power plant, there are many sources of fuel for an accidental fire, but the most abundant source in terms of mass is cable insulation. The type of fuel determines how destructive the smoke will be. In a power plant, there are many different qualified cables used for instrumentation and control. In a typical fire, different types of cables may be affected. Because the scope of these tests is limited by the equipment available to test, a mixture of cable types was burned to provide the smoke for these tests. This mixture included cables that are commonly used in plants.[32] The percentages of nuclear power plants that use these types of cables are also listed in Ref. 14, and this was used in determining the percentage (by weight) of each cable type to include in the mixture. The cables include Rockbestos Firewall III, Anaconda Flameguard, Brand Rex, and Samuel Moore cables. Common materials used for insulation and jacketing for these cables include ethylene propylene rubber (EPR), chlorosulfonated polyethylene (CSPE), neoprene, cross-linked polyethylene (XLPE), and ethylene propylene diamer (EPDM).

The amount of cable material to burn was determined by stripping the insulation from a sample cable and determining the fraction of the total weight of the cable that is made up by the insulation. Typically, the insulation material constituted 50 to 75% of the total mass of the cable. Lengths of cable that corresponded to the desired weight of insulation were loaded into the combustion cell on aluminum trays. The loaded trays were weighed before and after the burn to determine the amount of fuel actually burned. A list of the cable materials used in the smoke exposures for each of the tests is given in Table 6.1.

The conditions of each of the eight smoke exposures varied according to the type of environment that was to be simulated, as shown in Table 6.1. For tests simulating conditions outside the control room, humidity was added as a test parameter. The logic behind this choice is that, although temperature and humidity in a control room are well controlled, humidity may be high in other areas of a plant either because it is uncontrolled or because water may be used to extinguish a fire that might occur. To simulate such a high-humidity condition, steam was added to the smoke exposure chamber immediately after the fuel was burned. A standard amount of water, 34 g, was converted to steam in a combustion chamber by 15 min of heating with the radiant heat lamps.

Table 6.1 Smoke exposure test parameters

Test Number	Equipment Under Test	Fuel (Plastic) Burned (g)	Cable Mixture Burned	Total Grams (Plastic and wire)	Notes	Summary of Errors
1	Process Multiplexing Unit (PRS/MUX)	3.3	Rockbestos Firewall III Insulation: FRXLPE Jacket: CSPE	2	No added humidity. Used electric sparkers to help ignite cables.	**Baseline test:** No errors. **Smoke test:** Occasional network retrans-missions from DTC.
			Anaconda Flameguard Insulation: EPR Jacket: CSPE	1.23		
			Kerite HTK Insulation: Unknown Jacket: Unknown	1.937		
			Raychem XLPE Insulation: XLPE	0.53		
			Dekoran Dekorad Insulation: EPDM Jacket: CSPE	0.923		
			Rockbestos Coax (le) Insulation: Unknown Jacket: Unkown	0.59		
2	PRS/MUX	2.8	Rockbestos Firewall III Insulation: FRXLPE Jacket: CSPE	1.922	Steamed off 34 mL of water imme-diately after burning to simulate humidity. Relative humidity inside exposure chamber reached 85%.	**Baseline test:** Occasional network retrans-missions from DTC. **Smoke test:** Occasional network retrans-missions from DTC.
			Anaconda Flameguard Insulation: EPR Jacket: CSPE	1.336		
			Kerite HTK Insulation: Unknown Jacket: Unknown	1.159		
			Raychem XLPE Insulation: XLPE	0.384		
			Dekoran Dekorad Insulation: EPDM Jacket: CSPE	0.601		
			Rockbestos Coax (le) Insulation: Unknown Jacket: Unknown	0.58		

Table 6.1 (continued)

Test Number	Equipment Under Test	Fuel (Plastic) Burned (g)	Cable Mixture Burned	Total Grams (Plastic and wire)	Notes	Summary of Errors
3	Digital Trip Computer (DTC), without Fiber-Optic Modules (FOMs)	2.63	Rockbestos Firewall III Insulation: FRXLPE Jacket: CSPE Anaconda Flameguard Insulation: EPR Jacket: CSPE Kerite HTK Insulation: Unknown Jacket: Unknown Raychem XLPE Insulation: XLPE Dekoran Dekorad Insulation: EPDM Jacket: CSPE Rockbestos Coax (le) Insulation: Unknown Jacket: Unkown	1.726 1.054 1.219 0.396 0.91 0.47	No added humidity.	**Baseline:** No errors. **Smoke test:** Channel trip error during ignition of fuel prior to exposure test (EMI/RFI-related). See text.
4A	Digital Trip Computer (DTC), without Fiber-Optic Modules (FOMs).	None	None	None	CO_2 only test (no smoke). Amount of CO_2 used was 1.2 kg. Test performed to determine the probable effect of CO_2 on microprocessor-based equipment in the control room.	**Baseline:** Occasional network retransmissions from DTC. **CO_2 test:** Occasional network retransmissions from DTC.

Table 6.1 (continued)						
Test Number	Equipment Under Test	Fuel (Plastic) Burned (g)	Cable Mixture Burned	Total Grams (Plastic and wire)	Notes	Summary of Errors
4B	Digital Trip Computer (DTC), without Fiber-Optic Modules (FOMs).	2.8	Rockbestos Firewall III Insulation: FRXLPE Jacket: CSPE Anaconda Flameguard Insulation: EPR Jacket: CSPE Kerite HTK Insulation: Unknown Jacket: Unknown Raychem XLPE Insulation: XLPE Dekoran Dekorad Insulation: EPDM Jacket: CSPE Rockbestos Coax (le) Insulation: Unknown Jacket: Unknown	1.803 1.351 1.385 0.313 0.777 0.497	Test was designed to determine the effect of CO_2 suppression on digital equipment exposed to smoke equivalent to a postulated control room fire (see text). The smoke was added immediately after 4A.	**Smoke test:** Timeouts from serial datalinks.

Table 6.1 (continued)

Test Number	Equipment Under Test	Fuel (Plastic) Burned (g)	Cable Mixture Burned	Total Grams (Plastic and wire)	Notes	Summary of Errors
5	Digital Trip Computer (DTC), without Fiber-Optic Modules (FOMs).	20.39	Rockbestos Firewall III Insulation: FRXLPE Jacket: CSPE	10.64	No added humidity. Had problems with program initially. Sparkers (EMI/RFI) suspected. Sparkers plugged in individually.	**Baseline:** No errors. **Smoke test:** Occasional network retrans-missions from DTC.
			Anaconda Flameguard Insulation: EPR Jacket: CSPE	4.96		
			Kerite HTK Insulation: Unknown Jacket: Unknown	4.75		
			Raychem XLPE Insulation: XLPE	2.7		
			Dekoran Dekorad Insulation: EPDM Jacket: CSPE	3.54		
			Rockbestos Coax (le) Insulation: Unknown Jacket: Unknown	3.69		
			Brand Rex XLPE Insulation: XLPE Jacket: CSPE	5.27		
			Okonite Okolon Insulation: EPR Jacket: CSPE	4.23		
			BIW Insulation: EPR Jacket: CSPE	2.1		
			Kerite FR Insulation: Unknown Jacket: Unknown	1.81		
			PVC Insulation: PVC Jacket: PVC	1.4		

Table 6.1 (continued)

Test Number	Equipment Under Test	Fuel (Plastic) Burned (g)	Cable Mixture Burned	Total Grams (Plastic and wire)	Notes	Summary of Errors
6	PRS/MUX	19.97	Rockbestos Firewall III Insulation: FRXLPE Jacket: CSPE	10.34	Water boiled off in chamber to simulate high-humidity conditions after fire suppression by water. Humidity inside exposure chamber reached 85%. Butane lighters used for this and all subsequent tests.	**Baseline test:** Occasional network retransmissions from DTC. **Smoke test:** 1. Occasional network retransmissions from DTC. 2. Failure of PRS/MUX to transmit correct analog voltage.
			Anaconda Flameguard Insulation: EPR Jacket: CSPE	4.938		
			Kerite HTK Insulation: Unknown Jacket: Unknown	4.92		
			Raychem XLPE Insulation: XLPE	2.63		
			Dekoran Dekorad Insulation: EPDM Jacket: CSPE	3.2		
			Rockbestos Coax (le) Insulation: Unknown Jacket: Unkown	3.58		
			Brand Rex XLPE Insulation: XLPE Jacket: CSPE	5.24		
			Okonite Okolon Insulation: EPR Jacket: CSPE	4.42		
			BIW Insulation: EPR Jacket: CSPE	2.22		
			Kerite FR Insulation: Unknown Jacket: Unknown	1.79		
			PVC Insulation: PVC Jacket: PVC	1.27		

Table 6.1 (continued)

Test Number	Equipment Under Test	Fuel (Plastic) Burned (g)	Cable Mixture Burned	Total Grams (Plastic and wire)	Notes	Summary of Errors
7	PRS/MUX	160.13	Rockbestos Firewall III Insulation: FRXLPE Jacket: CSPE	139.49	No humidity added. Butane lighters used to ignite cables.	**Baseline:** Occasional network retrans-missions from DTC. **Smoke Test:** Occasional network retrans-missions from DTC.
			Anaconda Flameguard Insulation: EPR Jacket: CSPE	48.42		
			Kerite HTK Insulation: Unknown Jacket: Unknown	44.92		
			Raychem XLPE Insulation: XLPE	28.02		
			Dekoran Dekorad Insulation: EPDM Jacket: CSPE	45		
			Rockbestos Coax (le) Insulation: Unknown Jacket: Unkown	47.66		
			Brand Rex XLPE Insulation: XLPE Jacket: CSPE	71.33		
			Okonite Okolon Insulation: EPR Jacket: CSPE	53.41		
			BIW Insulation: EPR Jacket: CSPE	21.3		
			Kerite FR Insulation: Unknown Jacket: Unknown	21.04		
			PVC Insulation: PVC Jacket: PVC	14.72		

Table 6.1 (continued)

Test Number	Equipment Under Test	Fuel (Plastic) Burned (g)	Cable Mixture Burned	Total Grams (Plastic and wire)	Notes	Summary of Errors
8A	FOMs only; two of them without cover so that the PC board was directly exposed to the smoke.	2.43 (Tray 1 only).	Rockbestos Firewall III Insulation: FRXLPE Jacket: CSPE	40.66	Env. Chamber conditions: 13°C (55°F); 43% RH. 1. Cables in tray 1 burned; then system left running for 1 h. 2. Cables in tray 2 burned without venting chamber. Thus, total smoke density was approxi-mately 17.88 g/m^3. System continued running for additional 1 h 3. Cables in trays 3 and 4 burned without venting chamber. Thus, total smoke density was approxi-mately 64.3 g/m^3. System continued running for additional 1 h.	No errors.
			Anaconda Flameguard Insulation: EPR Jacket: CSPE	18.52		
			Kerite HTK Insulation: Unknown Jacket: Unknown	17.52		
			Raychem XLPE Insulation: XLPE	8.77		
8B		15.45 (Tray 2 only)	Dekoran Dekorad Insulation: EPDM Jacket: CSPE	8.93		Timeout on serial read ports. Problem was from the exposed FOMs.
			Rockbestos Coax (le) Insulation: Unknown Jacket: Unkown	13.68		
			Brand Rex XLPE Insulation: XLPE Jacket: CSPE	20.01		
			Okonite Okolon Insulation: EPR Jacket: CSPE	16.62		
			BIW Insulation: EPR Jacket: CSPE	8.05		
8C	Replaced open FOMs that failed. The replacements were closed this time and placed **outside** the environmental chamber.	46.42 (Tray 3 and tray 4)	Kerite FR Insulation: Unknown Jacket: Unknown	6.92		No errors.
			PVC Insulation: PVC Jacket: PVC	4.62		

6.2 Smoke Test Procedure

A total of 10 tests was performed on the PRS/MUX, the DTC subsystem, and the FOMs. This 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 was as follows:

(1) The EUT is placed in the exposure chamber. Then the EUT is energized, the EDSC is initialized, and the HOSTP software is started.

(2) Baseline data are obtained over a period of ~3 h. The environmental chamber is maintained at 24°C (75°F) and 30% RH during this time.

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

(4) In the case where the test calls for humidity as well as smoke, a predetermined amount of water is boiled off inside the exposure chamber, 15 min into the test, to provide 85% RH.

(5) The EUT is exposed to the smoke or smoke/steam mixture for a total of 1 h. The smoke is then exhausted from the exposure chamber.

(6) The EUT is left in the exposure chamber and performance monitoring is continued for ~20 h. The environmental chamber temperature is maintained at ~24°C and 30% RH.

(7) The HOSTP software is stopped and the EUT is de-energized.

(8) The EUT is examined for damages/malfunctions and thoroughly cleaned. (Cleanup consisted of first removing the electronic boards and blowing the deposited, nonsticky 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 and dried with compressed air. The exposure chamber was also thoroughly cleaned and made ready for the next test.)

The cable mixture was burned by placing the mixture in a tray and exposing it to the tungsten-quartz radiant heat lamps. During this entire period, a sparker, located 2.5 cm above the fuel, continuously sparked to provide an ignition source for hot gases produced by the radiant heat lamps. The resulting hot gases and smoke rose by natural convection up the 30-cm-long stainless steel chimney to the Lexan exposure chamber. After the burnup period, the chimney damper was closed, and a fan within the test chamber continuously mixed the smoke vapors. Since this was a static smoke exposure, the smoke was not allowed to leave the exposure chamber for the first hour of the test. The smoke chamber was sealed as well as possible to prevent smoke leaks; to allow for the expansion of gases because of heat and production of smoke, an empty plastic bag was placed over one of the ports. After a total of one hour of equipment exposure to the smoke, the smoke was exhausted from the test chamber. However, monitoring of system performance continued for several hours, after which the system was shut down, thoroughly cleaned, and reassembled for the next test.

Previous tests had indicated that the FOMs were very susceptible to elevated temperatures and would, in fact, begin to malfunction at ambient temperatures above about 32°C (90°F). To investigate the effect of smoke alone on the FOMs, smoke tests were performed with only the FOMs inside the exposure chamber (Tests number 8A through 8B in Table 6.1) while keeping the exposure chamber temperature below 27°C (80°F). In this case, the smoke exposure tests were performed in the following manner:

(1) Burn fuel in one cable fuel tray to simulate the smallest smoke density used for the other smoke exposure tests.

(2) Monitor system performance for a period of 1 h.

(3) Without venting the environmental chamber, burn additional fuel in the second cable fuel tray to simulate the medium smoke density used for the other smoke exposure tests.

(4) Monitor system performance for a period of 1 h.

(5) Without venting the environmental chamber, burn additional fuel in the third and fourth cable fuel trays to simulate the highest smoke density used for the other smoke exposure tests.

(6) Monitor system performance for a period of 1 h.

Pertinent data regarding each of the smoke exposure tests are given in Table 6.1.

6.3 Analysis of Smoke Exposure Test Results

The results of the smoke exposure tests are shown in the fifth column of Table 6.1 and in Figure 6.2. A few general observations can be made: First, the severity of the errors generally increased as the density of the smoke increased. Second, communication errors were observed at all levels of smoke density, ranging from network retransmissions at low smoke densities to serial link timeout errors at higher smoke densities. Another general observation was that once the various units had been exposed to smoke, the baseline tests were no longer error free. This observed behavior underscores the potential difficulty of thoroughly ridding a previously exposed board of all residual smoke particulates through cleaning and may point to the need to replace all exposed circuit boards after a fire as a matter of policy.

The most significant error that occurred during the environmental testing of the EDSC took place during the fuel ignition phase prior to test number 3. Several electric sparking devices were used to ignite the cable samples for smoke generation to initiate the exposure test. It is hypothesized that significant electromagnetic emissions were generated by the combined effect of four sparkers. The observed error, a channel trip error (failure type j), occurred before significant amounts of smoke had been generated, and so it appears to have resulted from EMI effects through the parallel ribbon cable that conveys the digital trip signal from the DTC. When butane lighters were substituted for the sparking devices in subsequent tests, these critical EDSC failures did not recur. However, it was not possible to reproduce this error in subsequent laboratory tests. Appendix E documents the investigation of the electromagnetic emissions from one of the sparking devices.

	B1 (18 h)	S1 (1 h) PRS/ MUX	B2 (18 h)	S2 (1 h) PRS/ MUX w/HI RH (85%)	B3 (18 h)	S3 (1 h) DTC w/o FOMs	B4 (18 h)	S4A (2 h) DTC CO_2 only	S4B (1 h) DTC w/o FOMs, w/CO_2	B5 (18 h)	S5 (1 h) DTC w/o FOMs	B6 (18 h)	S6 (1 h) PRS/ MUX w/HI RH (85%)	B7 (18 h)	S7 (1 h) PRS/ MUX	S8 (3h) FOMs only
Timeout by HOSTP on attempt to read data from DTC fiber optic serial datalink to channel 2 (error type d).									*							*
Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 3 (error type e).									*							*
Timeout by HOSTP on attempt to read data from DTC fiber-optic serial datalink to channel 4 (error type f).									*							*
DTC had to retransmit data to HOSTP (error type n).		*	*	*			*	*			*	*	*	*	*	
Difference between voltage sent to, and that transmitted by, the PRS/MUX for one or more process signals (error type r).													*			

LEGEND:
B = Baseline test.
S = Smoke test (i.e., EUT was subjected to smoke during this time).
For the actual smoke tests (S1 through S8), the number in parentheses indicates the smoke exposure time, after which the test chamber was vented. The failures indicated occurred within this 1-h window.
For the baseline tests the numbers in parentheses indicate the test duration (the EUT was not subjected to smoke during this time).

Figure 6.2 Results of smoke exposure tests
(Baseline data were acquired prior to each smoke exposure test).

According to the error consequence classification scheme used in this document, the least severe error encountered involved the DTC having to retransmit data over the FDDI network because the DTC did not receive an acknowledgment for data it had sent previously. This problem occurred during most of the smoke exposure tests and also during some baseline tests. Probable causes are postulated to be DTC network card problems due to smoke particulates getting into the fiber connector interfaces or temporary circuit bridging through the circuit board edge connections from smoke particulates, sufficient to cause only temporary errors.

There were timeout errors (failure types d, e, and f) when the DTC was the EUT and also when the FOMs were tested. It appears that in both cases circuit bridging on the edge connectors of electronic cards probably was the cause of the failures. Indeed, circuit bridging studies of uncoated boards performed at Sandia National Laboratories showed a marked decrease in insulation resistance a few minutes after the beginning of smoke exposure.

It is noteworthy that the computers under test exhibited no failures (e.g., processor lockups) resulting from smoke particle deposition, although soot was spread throughout each chassis by the computer cooling fans. On the other hand, the communication interfaces of the FOMs were found to be vulnerable to smoke deposition when their circuit boards were directly exposed (Note: The FOM circuit boards for the EDSC are encased in individual plastic shells that have limited ventilation, so direct exposure was accomplished by removing module covers.) The boards in both the computers and the FOMs used solder masks but did not have any conformal coating. However, a significant difference between the two was that the computers used industrial-grade components while the FOMs used commercial-grade components, although there is no conclusive evidence to confirm that this difference alone accounts for the superior resistance to smoke exposure effects demonstrated by the computers.

During tests in which only the FOMs were exposed to smoke (test number 8 in Figure 6.2), the covers of two of the FOMs were removed so that the circuit boards would be exposed directly to the smoke, as would be likely for a cabinet implementation of optical datalinks. To investigate the effect of board orientation, one module was positioned vertically while the other was positioned horizontally. No errors were recorded during the first burn (smoke density of 2.43 g/m^3). The timeout errors recorded occurred toward the end of the second exposure (smoke density of 15.45 g/m^3). These occurred with the FOMs that were directly exposed to the smoke. However, since the failures occurred with both the vertically positioned and horizontally positioned modules, there is indication that board orientation was not a factor to the malfunctions. One conclusion suggested from the FOM tests is that certain packaging and printed circuit board manufacturing techniques (e.g., use of solder mask, conformal coating, etc.) may provide important defenses against short-term smoke exposure effects. Further tests in this regard are currently being performed at Sandia National Laboratories.[33]

Several fire suppression simulations were included in the smoke tests. These included the addition of humidity in the form of steam and CO_2 from a fire extinguisher. When humidity was added during the smoke exposure, the objective was to reach 80% RH. This was accomplished using a simple calculation of the amount of water required in the chamber to raise the humidity to this level, given the temperature that was expected at the end of the exposure. The actual relative humidity reached in both cases in which water was boiled off was 85%. The results of the humidity tests (test numbers S2 and S6) show that humidity may be an important factor in creating temporary short circuits, and its adverse effect on digital boards is likely to increase with the severity of the smoke exposure. The addition of CO_2 was accomplished with a test of CO_2 alone from the fire extinguisher. By itself, the CO_2 had little or no effect on the performance of the equipment, although the temperatures in the exposure chamber dropped drastically as a result of its addition.

6.4 Summary of Smoke Exposure Tests

Failures encountered during the smoke exposure tests, as a function of the failure classifications used in the document, are shown in Figure 6.3. Several conclusions are suggested by the smoke test results:

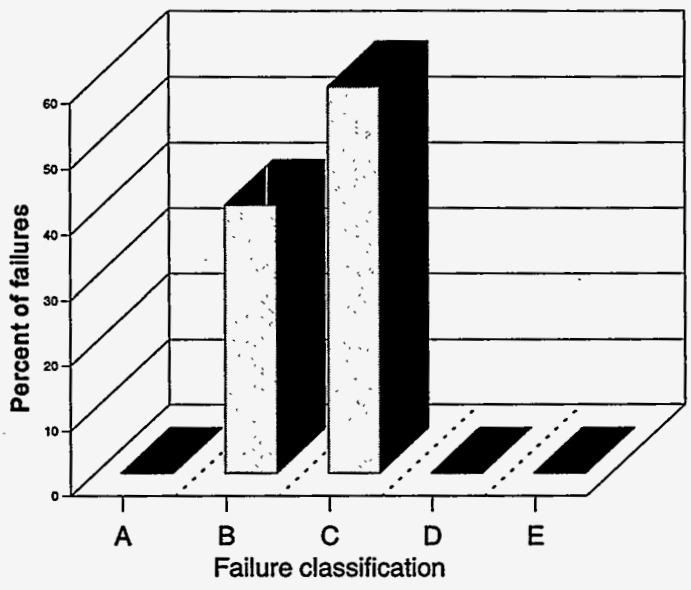
(1) Smoke can cause circuit bridging and thereby affect the operation of digital equipment. Because the circuit board edge connections and interfaces are typically uncoated, the most likely effect of the smoke is to impede communication and data transfer between subsystems. These effects are likely to 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 . A companion program at Sandia National Laboratories is continuing further tests on the impact of smoke on digital equipment.[33]

(3) 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 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[31] as the most severe fire that might be experienced in the main control room. This represents the *smallest* smoke density of the three fire scenarios postulated. Because of similarities between the EDSC and proposed advanced 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 when exposed to smoke equivalent to large control room panel fire conditions. Given early detection of a fire and subsequent fire suppression, digital systems should maintain functionality (to allow safe shutdown) for about an hour 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.



(a)

Failure classifications used in (a)

Failure Category	Description	Number of Errors in Failure Category	Percent of Errors in Failure Cateogory
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 6.3 Summary of smoke exposure test results as a function of failure classification

7 SUMMARY AND CONCLUSIONS

Several tests were performed on an experimental digital safety channel (EDSC) to investigate failure modes and vulnerabilities of microprocessor-based technologies when subjected to environmental stressors potentially present in a nuclear power plant control room environment. The EDSC was subjected to selected stressors that pose a potential risk to digital equipment located in a mild environment. Thus, equipment aging was not a consideration. The selected stressors were EMI/RFI, temperature, humidity, and smoke exposure, in that order. Any potential synergistic effects were accounted for by running the system in the absence of environmental stressors for several hours between tests (baseline data).

7.1 Failure Types Encountered

Most of the failures encountered during the tests were categorized as either *potentially unsafe* failures or *conditionally safe* failures. No critical failures were encountered during the EMI/RFI tests. (These tests were performed according to MIL-STD susceptibility standards.) However, a comparison of the failure types for all the stressors show that more severe EDSC errors were encountered during the EMI/RFI tests than during the tests involving other stressors. For example, the EMI tests produced the only permanent failure of the EDSC (i.e., power supply). In addition, during the initiation of one of the smoke tests, EMI/RFI generated by sparking devices used to ignite cables for smoke generation appears to be the cause of a critical failure in the EDSC performance. The fewest number of failures occurred during the temperature and humidity tests.

7.2 EMI/RFI

Of the six different EMI/RFI susceptibility tests performed, the system 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 produced by the conducted spike tests (CS02 and CS06). Errors also occurred with the radiated electric field tests (RS03). However, these errors typically occurred at values that are higher than called for in the MIL-STD specifications used as guidelines for the tests. In general, the EDSC exhibited greater susceptibility to conducted EMI. It should be noted that the relative susceptibility of particular systems can be mitigated by grounding, shielding, isolation, and surge withstand practices.

High-voltage spikes on power leads were found to cause a greater number of upsets and within a relatively short time (i.e., seconds) compared to low-voltage, sinusoidal 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.

7.3 Elevated Temperature

The different temperature ratings among the various subsystems of the EDSC afforded an opportunity to investigate the effect of temperature/humidity stressors on various I&C subsystems and their interfaces as they approached and exceeded their rated temperature/humidity specifications. Some subsystems (i.e., the FOMs) experienced temporary failure about 8°C (15°F) or more *below* manufacturers' ratings, while others did not fail even when they were stressed more than 17°C (30°F) above manufacturers' ratings. These observations underscore the need to qualify commercial-grade components despite manufacturers' advertised ratings. There is evidence to suggest that design flaws were responsible for the equipment that failed below manufacturer's rating. Partly because of 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.

7.4 Smoke

Subsystems of the EDSC were operated while being subjected to various levels of smoke that approximate credible control room fire scenarios (a control panel fire, a general area fire, and a small in-cabinet fire). The focus was on the performance of the system while under exposure to smoke. This corresponds to the need for safety systems to be functional during a fire, presuming that manual plant shutdown and fire suppression will be the response following discovery of the fire. For these smoke exposure tests, a 1-h exposure was selected as an appropriate test interval. Communication link errors were observed at all levels of smoke density, ranging from a few network retransmissions at low smoke densities to serial communication timeout errors at higher smoke densities.

The severity of the errors generally increased as the smoke concentration increased. Communication errors were observed at all levels of smoke, ranging from network retransmissions at low smoke densities to serial link timeout errors at higher smoke densities. Another observation was that once the various units were exposed to smoke, the baseline tests were no longer error free. This observed behavior underscores the potential difficulty of thoroughly ridding a previously exposed board of all residual smoke particulates through cleaning and may point to the need to replace all exposed circuit boards after a fire as a matter of policy.

It is noteworthy that the computers under test exhibited no permanent failures or serious upsets such as processor lockups resulting from smoke particle deposition, although soot was spread throughout each chassis by the computer's fan. On the other hand, the communication interfaces of the FOMs were found to be vulnerable to smoke deposition when the circuit boards were directly exposed.

Several fire suppression simulations were included in the tests. This included the addition of humidity in the form of steam and CO_2 from a fire extinguisher. The results of the humidity (85% RH) tests showed that humidity may be an important factor in creating temporary shorts, and its adverse effect on digital boards is likely to increase with the severity of the smoke exposure. The CO_2 had very little effect on the equipment, although the temperature in the chamber dropped drastically.

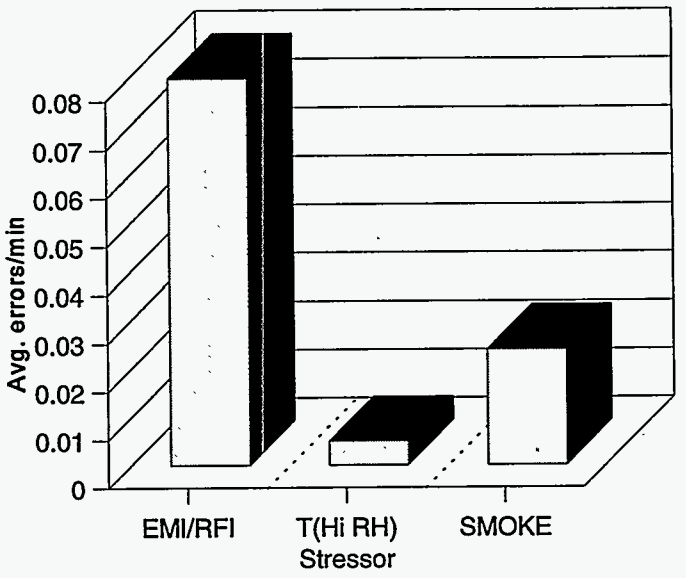
7.5 Stressor Intercomparisons: Assumptions

While the nature of these environmental tests does not permit a rigorous statistical comparison of the effects of the various stressors, the authors have attempted to make a conservative comparison by making the following assumptions: (1) all errors observed during a test are attributable to the stressor being applied (i.e., no residual effects); (2) all errors encountered were classified as potentially unsafe errors for the purposes of this comparison; (3) errors that occurred at the higher smoke densities were conservatively assumed to be attributable to smoke exposure in general (i.e, at all levels tested). Finally, since the test durations were different for each environmental stressor, an average number of errors per unit time was calculated separately for each stressor. Figure 7.1 shows the results of this comparison. [To obtain the average error rates shown in Figure 7.1(a), the total number of faults attributable to each stressor was divided by the total time the EDSC was exposed to the corresponding stressor.] The results show that EMI/RFI upsets had the most severe effect on the EDSC, followed by smoke exposure and then elevated temperature at high relative humidity.

7.6 Reliability of Data Communications

Using the same assumptions made in the previous section, the proportion of errors that were due to serial and network communications was computed for each stressor and is shown graphically in Figure 7.2. It is observed that a significant fraction of all errors resulting from the application of the stressors is communication errors. Many of these errors were timeout errors or corrupted transmissions, indicating failure of a computer to receive data from an associated multiplexer, optical serial link, or network node.

It should be noted that the fabrication and packaging technologies employed in the manufacture of the EDSC components (e.g., microprocessor chips, circuit boards, etc.) are very similar to those for actual or proposed safety-related digital systems. In addition, all microprocessor-based safety systems are likely to have some type of communication, either at the board level (bus communication and transfer of data) or at the system level (serial or network data transfers). Thus, it is reasonable to postulate that while the main source of malfunction in a specific digital safety system might be different, stressor-induced communication errors can, in general, be expected to be of significance in digital safety systems. A method of improving the reliability of data communications is to use *data redundancy*. This simply involves adding some redundancy to the data bits, which is then used to check the validity of the data every time the latter is referenced. For low error rates and small memory applications (below 1 MB), parity checking is a good choice. A parity error indicates data corruption but is limited to the detection of only single-bit errors. The more sophisticated Hamming code can detect two-bit errors and correct one-bit error in a word. Hamming code-based error detection and correction technologies are well suited to moderately noisy systems, which includes microprocessor-based systems with more than 4 MB of main memory.[8]

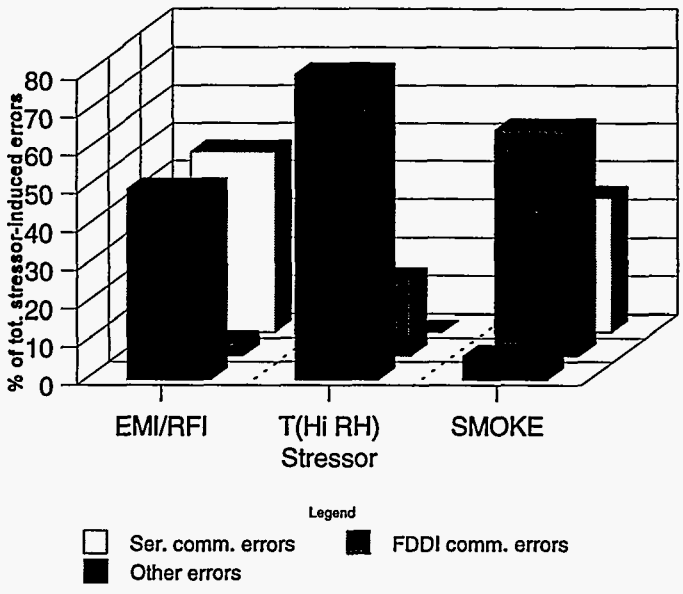


(a)

	STRESSOR								
	EMI/RFI						TEMPERATURE		SMOKE
	CS01	CS02	CS06	RS01	RS02	RS03	(30% RH)	(85% RH)	
No. of faults	6	9	57	0	1	12	0	5	17
Total exposure time (min)	80	240	465	110	80	80	960	960	720
Avg. error per minute	0.080						0.005		0.024

(b). Data used in plotting (a).

Figure 7.1 Comparison of stressor-induced faults for the environmental stressors studied



(a)

	STRESSOR								
	EMI/RFI						TEMPERATURE		SMOKE
	CS01	CS02	CS06	RS01	RS02	RS03	(30%RH)	(85%RH)	
Serial communication errors	3	3	31	0	0	3	0	0	6
Serial communication errors (percent of total errors for stressor)	47 %						0 %	0 %	35 %
FDDI network communication errors	2	0	0	0	1	0	0	1	10
FDDI network communication errors (percent of total errors for stressor)	3.5 %						0 %	20 %	59 %
Other errors	1	6	26	0	0	9	0	4	1
Other errors (percent of total for stressor)	49.5 %						0	80 %	6 %
Total errors	6	9	57	0	1	12	0	5	17

(b). Data used in plotting (a).

Figure 7.2 Fractional contribution of communication errors for the EDSC testing

7.7 Summary

In summary, significant overall findings from the environmental tests performed in this study 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.

(2) Based on incidence of errors during testing, EMI/RFI, smoke exposure, and high temperature coupled with high relative humidity 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). Also, the effect of the stressor was typically immediate, whereas the occurrence of high temperature/humidity and smoke exposure effects were delayed for some interval (i.e., tens of minutes) after the application of the stressor.

(3) While 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.

(4) With regard to temperature and humidity, the study found that the combination of high temperature at high RH was the condition to affect the EDSC, rather than temperature acting alone. High RH is not as likely in a controlled environment such as a control room but still needs to be considered in qualification, especially for PAM 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 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[31] as the most severe fire that might be experienced in the main control room. This represents the *smallest* smoke density of the three fire scenarios postulated. Because of similarities between the EDSC and proposed advanced 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 when exposed to smoke equivalent to large control room panel fire conditions. Given early detection of a fire and subsequent fire suppression, digital systems should maintain functionality (to allow safe shutdown) for about an hour following exposure, provided that the equipment is not directly exposed to the fire.

(7) The solder mask on commercial electronic boards appears 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[3] 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.)

The results of this study, along with results from related studies by SNL and BNL, will be used to develop the technical basis for possible enhancement of current qualification processes in a planned NUREG/CR on an overall framework for the environmental qualification of digital safety-related I&C systems.

8 REFERENCES

1. U. S. Nuclear Regulatory Commission, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems in Nuclear Power Plants," Regulatory Guide 1.152, November 1985.

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

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

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, Oak Ridge National Laboratory, April 1994.

5. G. M. Pecht, R. Agarwal, and Dan Quearry, "Plastic Packaged Microcircuits: Quality, Reliability, and Cost Issues," *IEEE Transactions on Reliability*, 42(4):513–517 (December 1993).

6. "Texas Instruments Military Plastic Packaging," Preliminary Handbook, Texas Instruments, 1992.

7. Lloyd Condra et. al., "Comparison of Plastic and Hermetic Microcircuits Under Temperature Cycling and Temperature Humidity Bias," *IEEE Transactions on Components, Hybrids, and Manufacturing Technology*, 15(5):640–650 (October 1992).

8. Anupama Hedge, "Detect/Correct Errors to Improve Data Reliability," *Electronics Design*, pp. 75–82, (June 11, 1992).

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

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

11. T. L. Wilson and R. T. Wood, "Investigation of Information Resources on Qualification and Reliability of Digital Instrumentation and Control Systems in Non-Nuclear Industries," ORNL/NRC/LTR-96/4, Letter Report to the U.S. NRC, January 1996.

12. T. L. Wilson and R. T. Wood, "Evaluation of Vendor Test Programs for Instrumentation and Control Systems," ORNL/NRC/LTR-95/27, Letter Report to the U.S. NRC, September 1995.

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

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

15. O. M. Clark and R. E. Gavender, "Lightning Protection for Microprocessor Based Electronic Systems," pp. 197–203 in *Proceedings of the EOS/ESD Symposium*, 1989.

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

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

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

19. U.S. Department of Defense, MIL-STD-462, "Test Method Standard for Measurement of Electromagnetic Interface Characteristics," July 1967.

20. Institute of Electrical and Electronics Engineers, IEEE Standard 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," approved June 23, 1983, reaffirmed September 28, 1990.

21. Electronic Industries Association, JEDEC Standard No. 22-B, "Test Methods and Procedures for Solid State Devices Used in Transportation/Automotive Applications," September 1987.

22. Electronic Industries Association, JEDEC Standard JESD22-A104-A, "Temperature Cycling," December 1989.

23. Electronic Industries Association, JEDEC Standard No. 22-A101-A, "Steady-State Temperature Humidity Bias Life Test," July 1988.

24. Electronic Industries Association, EIA/TIA-455-3A, (FOTP-3), "Procedure to Measure Temperature Cycling Effects on Optical Fibers, Optical Cable, and Other Passive Fiber Optic Components," May 1989.

25. Electronic Industries Association, EIA/TIA-455-A, "Standard Test Procedure for Fiber Optic Fibers, Cables, Transducers, Sensors, Connecting and Terminating Devices, and Other Fiber Optic Components," August 1981.

26. Electronic Industries Association, EIA/TIA-455-188 (FOTP-188), "Low Temperature Testing of Fiber Optic Components," January 1992.

27. Electronic Industries Association, EIA/TIA-455-5A (FOTP-5), "Humidity Test Procedure for Fiber Optic Connecting Devices," June 1990.

28. Electronic Industries Association, EIA Component Bulletin CB9-F, "Reference Guide for Fiber Optic Test Procedures," March 1987.

29. U.S. Department of Defense, MIL-STD-883D, "Test Methods and Procedures for Microelectronics," approved November 15, 1991.

30. U.S. Department of Defense, MIL-STD-810E, "Environmental Test Methods and Engineering Guidelines," approved July 14, 1989.

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

32. L. Bustard and P. Holzman, "Low-Voltage Environmentally Qualified Cable License Renewal Industry Report," EPRI TR-103841, Rev. 1, Electric Power Research Institute, July 1994.

33. T. J. Tanaka, K. Korsah, and C. Antonescu, "Preliminary Studies on the Impact of Smoke on Digital Equipment," pp. 85–99 in *23rd Water Reactor Safety Information Meeting*, Bethesda, Maryland, October 1995.

APPENDIX A–RESEARCH ACTIVITIES LEADING TO PRESENT TESTS

Prior to conducting the environmental tests, a number of tasks were performed to identify approaches that could be used in enhancing digital I&C qualification for the nuclear power plant environment. In particular, we sought to identify (1) environmentally related instrumentation and control (I&C) system failure rate information in both the nuclear and nonnuclear industries; (2) literature on survivability of digital I&C equipment to smoke exposure in nuclear power plant environments; (3) literature and standards on qualification methodologies for digital I&C in nuclear power plants; and (4) foreign nuclear plant experience with digital I&C. The findings are discussed in Chap. 1. This appendix briefly describes these research activities.

Reactor and Safety-Related I&C Manufacturers Interviewed

Industry representatives from Westinghouse, General Electric, the Foxboro Company, and Combustion Engineering were interviewed. The information acquired formed the basis for ascertaining the extent to which advanced technology will be used in the design of proposed safety systems for advanced light-water reactors (ALWRs).

(1) GE Nuclear Energy. Contact persons: Barry Simon, Principal Engineer; Monty A. Ross, Manager, Electrical Systems and Equipment Design; Timothy J. O'Neil, Principal Engineer.

(2) Westinghouse Electric Corporation: J. B. Reid, Manager, Plant Instrumentation and Control Systems; D. J. Vaglia, Senior Engineer, Plant Instrumentation and Control Systems; Joseph Bersa, Senior Engineer, Plant Instrumentation and Control Systems.

(3) Foxboro Company: David R. Ringland, Senior Power Specialist; J. T. Keiper, Business Manager, Nuclear Energy Systems.

(4) Combustion Engineering: Tom Starr; William J. Gill; Stan Ritterbusch.

First Literature Search of IEEE and COMPENDEX Databases

A literature search of the INSPEC and COMPENDEX databases of published research from 1987 to 1992 was performed. This search was accomplished using search rules designed to focus on qualification and susceptibility of digital I&C systems to environmental stresses such as temperature, humidity, and electromagnetic interference/radio-frequency interference (EMI/RFI). This search returned 1060 titles. A manual review of the titles reduced the scope to approximately 50 titles. About 30 of these were obtained for a more detailed analysis. Many of the articles had limited applicability because they dealt with aspects of digital I&C reliability at the component level rather than at the system level. For example, many of the articles addressed chip packaging issues, EMI/RFI effects on microprocessors, electronic stress screening, etc.

Nuclear Databases Investigated

The frequency of reactor trips and engineered safety feature (ESF) actuations attributable to environmentally related faults in I&C systems was investigated. The motivation was to estimate qualitatively the effectiveness of current qualification procedures in reducing the frequency of protection system I&C failures caused by environmental stressors. Two of the most widely used databases for various aspects of nuclear plant data were investigated:

(5) Licensee Event Reports (LERs).
(6) Nuclear Plant Reliability Data System (NPRDS).

Study of Optical Fiber Reliability and Qualification

The failure modes and degradation mechanisms of optical fiber cables and transmission components were reviewed in the literature, and interviews were conducted with cognizant Bellcore personnel. In addition, relevant optical fiber qualification standards were studied. The following phone contacts were made:

(7) Thomas C. Tweedie, Bellcore.
(8) Samuel V. Lisle, Fujitsu Network Transmission Systems Group.

Nonnuclear Industries Visited

Interviews were held with cognizant personnel of selected nonnuclear industries where the environment for I&C equipment is similar to that of nuclear power plants:

(9) Olin Corporation (chemical industry).
(10) Duke Power Company (Allen Steam Station).

Investigation of the Military Experience with EMI/RFI-Related Problems with Microprocessor-Based Equipment

Cognizant individuals from the U.S. Army, Navy, and Air Force were surveyed with regard to nonclassified U.S. Department of Defense experience with EMI/RFI that may be relevant to digital equipment in nuclear power plants:

(11) Ltc. J. W. Delk, Electromagnetic Compatibility Center (ECAC), Department of Defense, Adelphie, MD.
(12) Bob Snyder, ECAC.
(13) Homer Riggins, ECAC.
(14) Jerry M. Daughdill, Air Force Communications Command, 1839th Engineering Installation Group.
(15) David Cofield, Army Communications Electronics Command (CECOM).
(16) Paul Major, CECOM.
(17) Kenneth Proctor, CECOM.

(18) Charles Brown, Head of I&C Division, Nuclear Propulsion Directorate, Naval Sea Systems Command.
(19) Jeff Lucas, Naval Electronics Systems Engineering Center.
(20) Michael O. Hatfield, Naval Surface Warfare Center.
(21) Stephen Caine, Space and Naval Warfare Systems Command.
(22) John Tatum, Army Research Laboratory, Nuclear and Directed Energy Division.

Foreign Research Organizations and Nuclear Power Plants Visited

Discussions were held with personnel in five organizations in three European countries with regard to the qualification/application of microprocessors and other "advanced" technologies in the protection systems of nuclear power plants. In addition, discussions were held with EMI experts in four European countries to exchange information about technical approaches to control EMI/RFI and power surges in nuclear power plants:

(23) Framatome, Paris, France: Alan Parry.
(24) AEA Technology, Winfrith, England: Keith McMinn, Ian Smith, Derek Bardsley.
(25) Siemens, Erlangen, Germany: Warner Aleite.
(26) Siemens AG, Frankfurt, Germany: Heinz-Wilheim Bock.
(27) Institute for Safety Technology, Munich, Germany: Werner Bastl.
(28) Chooz B Nuclear Power Plant: Cottel Robert.
(29) Nuclear Protection and Safety System Institute, Paris, France: Guy Gauthier.
(30) EMC '94, ROMA, University of Rome "La Sapienza," Rome, Italy: Mauro Feliziani.
(31) Schneider Electric SA, Paris, France: Jacques Delaballe.

Instrument Vendors Interviewed

A follow-up survey of instrument vendors for nuclear and nonnuclear industries was performed to supplement the information previously ascertained and documented in NUREG/CR 5904.[1] In particular, four instrument technologies not currently used in nuclear power plants were identified through the survey of advanced instrumentation manufacturer and I&C system researchers as having potential for use in the nuclear power industry. The findings on these technologies are reported in ORNL/NRC/LTR-95/23.[2] The companies included in the survey are the following:

(32) Triconix Corporation (fault-tolerant computer systems).
(33) Ottotec Corporation (Intelligent transmitters).
(34) Heraeus Sensor (resistance temperature detectors and other temperature sensors).
(35) August Systems Incorporated (fault-tolerant computer systems).
(36) The Foxboro Company (protection systems and instrument manufacturer).
(37) K-Tech Corporation.
(38) Thermal Instrument Company (flow meters and temperature sensors).
(39) Weed Instrument Company, Inc. (instrument manufacturer).
(40) Computer Application System, Inc.
(41) Westinghouse, Inc. (Reactor manufacturer, safety-related systems).
(42) Bailey Instruments (instrument manufacturer).
(43) Pepperel+Fuchs, Inc. (manufacturer of various instruments).

(44) Ottotec Corporation (intelligent transmitters).
(45) Motorola (single chip pressure sensors).
(46) Panametrics (ultrasonics-based devices).

Nuclear Vendor Qualification Study

Representatives of the nuclear safety system vendors were surveyed for information regarding digital system qualification databases. The industry contacts included the following:

(47) Jim Scecina, B&W Nuclear Technologies, Lynchburg, VA
(48) Barry Simon, General Electric Nuclear, San Jose, CA
(49) Jim Keiper, Foxboro Company, Foxboro, MA
(50) Ed Brown, ABB Combustion Engineering, Windsor, CT
(51) Carl Vitalbo, Westinghouse Electric Company, Pittsburgh, PA
(52) Ray Torok, Electric Power Research Institute, Palo Alto, CA

Second Literature Search of IEEE INSPEC and COMPENDEX Databases

The purpose of this search was to acquire information on qualification, reliability, or testing of electronics in nonnuclear industries. Potential sources having high-reliability requirements similar to those of the nuclear industry are the military, space, automotive, and commercial aviation industries. The approach was to conduct a literature search of abstracts and a search of Internet sites for related research on reliability, qualification, or testing of electronics.

This literature search covered the years 1988 through 1995 using the COMPENDEX and IEEE INSPEC databases of scientific abstracts. A three-level search strategy was developed to identify relevant articles from the roughly 500,000 abstracts contained in the databases. The search looked for information on qualification, testing, reliability, or failures of digital (or microprocessor or electronic, etc.) components due to the stressors cited in IEEE 323 (temperature, humidity, pressure, EMI/RFI, surge withstand, etc.) This search returned 1000 titles. A manual review of these titles reduced the scope to ~70 titles. Reading the abstracts from these articles identified 23 articles on specific aspects of reliability that had some degree of applicability. We followed up the literature search by contacting four of the authors to determine if any additional data are available for use in nuclear safety system qualification methodologies. The interviews identified two main resources of general information: the Reliability Analysis Center (RAC) at the Rome Laboratories and databases of major suppliers of microprocessors (Texas Instruments, Motorola, National Semiconductor). Representatives from these places were also contacted. They provided summaries of the types of data kept at their sites and the uses that they had for the data. The RAC has more than 37,000 bibliographic references in their reliability library. The industry databases contain qualification data from all the manufactured products. Many of these records involve large sample sizes and can be used for statistical estimation of component reliability. Both resources are clearly useful for qualifying advanced digital components for nuclear safety and control applications.

The Internet search looked for industries or military entities that published home pages related to qualification or reliability. A number of promising Web sites for the Navy, Army, Federal Aviation Administration (FAA), and the National Aeronautics and Space Administration were browsed, but no particularly useful sites were identified. The FAA Service Difficulty Report database allows the reader to

search for specific failures in aircraft. A search for avionics or autopilot or printed circuit board failures identified a number of occurrences; the usefulness of the information for reliability estimates in nuclear business seems questionable, primarily because of the limited amount of data recorded about the failed components. Web sites with a listing of DOE reports or laboratory reports turned up frequent citations of work performed by this program but little other relevant work.

References

1. K. Korsah, R. L. Clark, and R. T. Wood, "Functional Issue and Environmental Qualification of Digital Protection System of Advanced Light-Water Nuclear Reactors," NUREG/CR-5904, Oak Ridge National Laboratory, April 1994.

2. D. E. Holcomb, K. Korsah, and R. T. Wood, "Survey of Advanced Instrumentation with Potential Applicability to Safety-Related Systems at Nuclear Power Plants," ORNL/NRC/LTR-95/23, Oak Ridge National Laboratory, June 1995.

APPENDIX B–REPRESENTATIVE LIST OF COMPONENTS USED IN ENVIRONMENTAL TESTS

The table below lists components on five of the integrated circuit boards used in the experimental digital safety channel (EDSC). We have not included components on *all* boards in the EDSC because many boards are identical. For example, there are four SK-NET FDDI-FE network interface boards in the EDSC, one in each computer.

Board Name: SK-NET FDDI-FE
S/N: 60-10-026-001
Part A

U#	Manufacturer	Part I.D.	Function	Footprint
U1	TEXAS INSTRUMENTS	ALS133	13 INPUT NAND GATE	16-pin SOIC
U12	NATIONAL SEMICONDUCTOR	74FR240	INVERTING OCTAL TRI-STATE BUF	20-pin SOIC
U13	NATIONAL SEMICONDUCTOR	74FR244	OCTAL TRI-STATE BUFFER	20-pin SOIC
U14	ADVANCED MICRO	PAL16R8-7JC	PAL HSREQ	20-pin PLCC
U16,U17,U18,U19,U20	MOTOROLA	F245	OCTAL TRI-STATE TRANSCEIVER	20-pin SOIC
U21,U22	ADVANCED MICRO	AM29C821ASC	10 BIT TRI-STATE D FLIP-FLOP	24-pin SOIC
U23	ADVANCED MICRO	AM29C823ASC	9 BIT TRI-STATE D FLIP-FLOP	24-pin SOIC
U24	VX	8113	50.000 MHz OSCILLATOR	4-pin DIP
U25	ADVANCED MICRO	AM28FO10-120JC		36-pin PLCC
U27,U45	MOTOROLA	F74	DUAL D FLIP-FLOPS w/ PRE, CLR	14-pin SOIC
U28	ADVANCED MICRO	PAL16R8-7JC	PAL w/CLOCK	20-pin PLCC
U29,U34	MOTOROLA	F138	3 TO 8 LINE DECODER	16-pin SOIC
U3,U15,U35,U42,U46, U54,U55,U56	NATIONAL SEMICONDUCTOR	GAL16V8-15	GENERIC ARRAY LOGIC	20-pin PLCC
U32	ADVANCED MICRO	AM79865JC	FDDI	20-pin PLCC
U33	ADVANCED MICRO	AM79866JC	FDDI	20-pin PLCC
U37	ADVANCED MICRO	AM79C830AKC	COMMUNICATIONS PROCESSOR	168-pin SOIC
U36	ESS TECH	3354	COMMUNICATIONS PROCESSOR	120-pin SOIC
U38,U39,U40	MOTOROLA	ACT245	OCTAL TRI-STATE TRANSCEIVER	20-pin SOIC
U4	MOTOROLA	F00	QUAD 2 INPUT NAND	14-pin SOIC
U41,U43	MOTOROLA	ACT273	OCTAL D FLIP-FLOP w/ CLEAR	20-pin SOIC
U44	ADVANCED MICRO	AM79C864KC	COMMUNICATIONS PROCESSOR	168-pin SOIC
U47	MOTOROLA	F08	QUAD 2 INPUT AND GATE	14-pin SOIC
U49,U50,U51	NATIONAL SEMICONDUCTOR	74F373	OCTAL LATCH w/ TRI-STATE OUT	20-pin SOIC
U5,U57	MOTOROLA	F02	QUAD 2 INPUT NOR GATE	14-pin SOIC
U52,U53	TEXAS INSTRUMENTS	F245	OCTAL TRI-STATE TRANSCEIVER	16-pin SOIC
U59	ADVANCED MICRO	PAL16L8-7JC	PAL FPBUG	20-pin PLCC
U6	SUMITOMO	SDM3181-XF	FDDI TRANSCEIVER	Connector
U7	MOTOROLA	FI74	HEX D FLIP-FLOPS w/ CLEAR	16-pin SOIC
U8,U9,U10,U11	TOSHIBA	TC55328AJ	32K x 8 HSSRAM	28-pin PLCC
U26	ADVANCED MICRO	PALCE16V8H	PAL DFIFO	20-pin PLCC
U30		402186	ASIC	16-pin DIP
U52	TEXAS INSTRUMENTS	ALS174	HEX D FLIP-FLOPS w/ CLEAR	16-pin SOIC
U31	MOTOROLA	F244	OCTAL TRI-STATE BUFFER	20-pin SOIC
U48	OKI	3202105	DSP	28-pin PLCC

Part B

U#	Manufacturer	Part I.D.	Function	Footprint
U1	ADVANCED MICRO	AM79865	FDDI	20-pin PLCC
U2	ADVANCED MICRO	AM79866	FDDI	20-pin PLCC
U3	TEXAS INSTRUMENTS	75462	DUAL PERIPHERAL DRIVERS	8-pin SOIC
U4	ADVANCED MICRO	CE22V10Q	PAL COSTA	28-pin PLCC
U5	ADVANCED MICRO	79C864KC	COMMUNICATIONS PROCESSOR	168-pin SOIC
U7	SUMITOMO	SDM3181-XF	FDDI TRANSCEIVER	Connector
U8	ADVANCED MICRO	74C841ASO	10 BIT D-TYPE LATCHES	24-pin SOIC

Board Name: Romdisk PCE/2
Manufacturer: Curtis, Inc.

Quantity	Manufacturer	Part I.D.	Function	Footprint
10	Intel	28FO10	128K x 8 CMOS FLASH MEMORY	32-pin Plastic Dip
2	ST	T74LS245	OCTAL TRI-STATE TRANSCEIVER	20-pin Dip
1	ST	T74LS374	TRI-STATE OCTAL D FLIP-FLOP	20-pin Dip
3	ST	T74LS138	3 to 8LINE DECODER	16-pin Dip
2	ST	T74LS175	QUAD D FLIP-FLOP w/ CLEAR	16-pin Dip
2	ST	T74LS244	OCTAL TRI-STATE BUFFER	20-pin Dip
1	National Semiconductor	LM357	OP-AMP	8-pin Dip
2	National Semiconductor	P9336	PROGRAMMABLE LOGIC DEVICE	20-pin Dip
3	LSI	GAL20XV10B	PROGRAMMABLE LOGIC DEVICE	24-pin Dip

Board Name: 440-0135-001 REV F
Manufacturer: WIDGET WORLD

U#	Manufacturer	Part I.D.	Function	Footprint
U1,U2	PHILLIPS	LM311N	OP-AMP	8-pin Dip
U3,U4,U5	HARRIS	CD74HCT4053	TRIPLE 2-CHANNEL ANALOG MUX	16-pin Dip
U6,U7	PHILLIPS	74HCT02	QUAD 2-INPUT NOR	14-pin Dip
U8,U9	TEXAS INSTRUMENTS	SN75176B	DIFFERENTIAL BUS TRANSCEIVER	8-pin Dip
U10	HARRIS	CD74HCT04	HEX INVERTER	14-pin Dip
U11	HEWLETT-PACKARD	4100	OPTO-ISOLATOR	8-pin Dip
U12	HEWLETT-PACKARD	4200	OPTO-ISOLATOR	8-pin Dip
U13	LINEAR TECHNOLOGY	LT1281	QUAD OP-AMP	16-pin Dip
U14	HARRIS	CD74HCT4538	DUAL MULTIBRATOR	16-pin Dip

Board Name: 92-005173-OX
REV: D-A-04
S/N: 1065

U#	Manufacturer	Part I.D.	Function	Footprint
U28,U29,U30,U38,U45,U57, U58,U59,U60,U61,U62,U63, U64,U71,U72,U73	TEXAS INSTRUMENTS	74F245	OCTAL TRI-STATE TRANSCEIVER	20-pin SOIC
U21,U32,U33,U49,U50,U51, U52	TEXAS INSTRUMENTS	74F244	OCTAL TRI-STATE BUFFER	20-pin SOIC
U10,U11,U12,U13,U15,U16, U17,U18	CYPRESS SEMICONDUCTOR	CY7C199-20VC	STATIC RAM	28-pin PLCC
U53	F	9405	RAM 72 pin SIMM	72-pin SIMM
U9,U14,U34,U35,U36	TEXAS INSTRUMENTS	74F573	TRI-STATE OCTAL D-TYPE LATCH	20-pin SOIC
U19	CYPRESS SEMICONDUCTOR	CY7C187-15VC	STATIC RAM	24-pin PLCC
U8	TEXAS INSTRUMENTS	74F125	TRI-STATE QUAD BUFFERS	14-pin SOIC
U20	PARADIGM	PDM41256SA15SO	STATIC RAM	28-pin PLCC
U75	OPTI	82C683	PERIPHERAL INTERFACE PROCESSOR	168-pin SOIC
U44	OPTI	82C686	PERIPHERAL INTERFACE PROCESSOR	168-pin SOIC
U27	OPTI	82C681	PERIPHERAL INTERFACE PROCESSOR	168-pin SOIC
U40	OPTI	82C688	PERIPHERAL INTERFACE PROCESSOR	168-pin SOIC
U26	MOTOROLA	74F00	QUAD 2 INPUT NAND GATE	14-pin SOIC
U25	DALLAS SEMI	DS1232	MICRO-PROCESSOR SUPPORT	8-pin DIP
U66	DALLAS SEMI	DS1233	MICRO-PROCESSOR SUPPORT	4-pin SOIC
U1	MOTOROLA	74F32	QUAD 2 INPUT OR GATE	14-pin SOIC
U77	MOTOROLA	74LS32	QUAD 2 INPUT OR GATE	14-pin SOIC
U6	TEXAS INSTRUMENTS	74F04	HEX INVERTER	14-pin SOIC
U7	TEXAS INSTRUMENTS	74F74	DUAL D FLIP-FLOP	14-pin SOIC
U5	McGuirk ELEC.	SG531PH	66 MHz CLOCK	4-pin DIP
U48	LSI	GAL16V8B	GENERAL ARRAY LOGIC	20-pin PLCC
U41	KYOCERA	HC1-TS	14.318 MHz OSCILLATOR	4-pin
U39	MOTOROLA	74F11	TRIPLE 3 INPUT AND GATE	14-pin SOIC
U3	INTEL	A80486DX-33	INTEL PROCESSOR	PROCESSOR
U23	JBM	L-51-56	DELAY LINES	8-pin DIP

U31	PERICOM SEMI	PI74FCT640TS	INVERTING OCTAL TRI-STATE TRANSEIVER	20-pin SOIC
U46	PERICOM SEMI	PI74FCT244TS	OCTAL TRI-STATE BUFFER	20-pin SOIC
U67	CHIPS	F82C721	MICROPROCESSOR SUPPORT	100-pin SOIC
U24	AMERICAN MEGA.	AMIBIOS	486DX EISA BIOS	28-pin DIP
U70	ST	1489DI		14-pin SOIC
U43	NATIONAL SEMICONDUCTOR	DM74ALS05AM	HEX INVERTER (OPEN DRAIN)	14-pin SOIC
U68,U69	TEXAS INSTRUMENTS	75C1406	TRIPLE DRIVER RECEIVER	16-pin SOIC
U42	MEGATRENDS	MEGA-KB-H-Q	BIOS MEMORY	44-pin PLCC

APPENDIX C—EDSC SYSTEM SPECIFICATIONS

The following tables list the specifications of the plug-in boards, modules, and subsystems used for the implementation of the experimental digital safety channel (EDSC).

Table C.1. Manufacturer's specifications for serial optical line drivers

Speed	Transparent through 20 kbits/s on 20-mA current loop port, 64 Kbps on RS-232 port, 128 kbits/s on RS-485 port
Operation	Network Mode or Master/Slave Mode, half-duplex
Indicators	(10) LEDs
Interface	RS-232 DCE/DTE, RS-485, 20-mA current loop–active or passive transmit and receive, fiber-optic transmit and receive
Connectors	(1) DB9, (4) ST or SMA, (1) screw terminal block
Power	115 Vac, 60/50 Hz
Size	1.8 in. H × 8.5 in. D (4.6 × 14 × 21.6 cm)
Weight	2 lb (0.9 kg)

Table C.2. Manufacturer's specification for serial-optical communications port controllers

Environmental Conditions	
Condition	**Values**
Air Temperature: System on System off	 0°C to 70°C –65°C to 150°C
Humidity: System on System off	 8% to 80% 20% to 80%
Altitude	0 to 10,000 ft 0 to 3,048 m

Controller Specifications	
Function	**Specification**
I/O ports/expansion slot	4 ports per slot
Controllers per system	Up to 4 (space and operating system permitting)
Power requirements +5 Vdc +12 Vdc -12 Vdc	4-Port 0.720 A 0.054 A 0.0060 A
Heat output 4-port	12.3 Btu/h
Interface	RS-232/422 (4-port)
I/O port address *The default address conflicts with COM2 and COM4.*	Set with SW1 or ADDRESS SELECT switch Default set to 2E0
Hardware interrupt (Default is 3)	RJ45: Set with SW2 switch IRQ 2, 3, 4, 5, 10, 11, and 12 RJ11: Set with IRQ SELECT SWITCH IRQ 2, 3, 4, 5, 7, 10, and 11

Table C.2 (continued)

Controller Specifications (continued)	
Function	**Specification**
Baud rate	50 through 115.2 kbit/s
Data bits	5, 6, 7, or 8
Stop bits	1, 1.5, or 2
Modem control	RJ45: RTS, CTS, DSR, DCD, and DTR RJ11: CTS, DCD, and DTR
UL recognition	RJ11 only
Dimensions	RJ45: 10 × 4 in. RJ11: 8.56 × 4.5 in.

Table C.3 Manufacturer's specifications for D/A and A/D modules for PRS/MUX and ESF/MUX systems

Input Module Specifications	
Input Ranges	Thermocouple, mV V, mA
Output	RS-485
Accuracy	±0.05% or better
Zero Drift	±0.3 μV/°C
Span Drift	±3 ppm/°C (±25 ppm/°C max)
Common Mode Voltage, Input to Output	1500 Vrms continuous
Common Mode Rejection @ 50 Hz or 60 Hz 1-kΩ Source Imbalance	160 dB
Normal Mode Rejection @ 50 Hz or 60 Hz	58 dB
Differential Input Protection	240 Vrms continuous
Input Transient Protection (CMV)	IEEE-Std 472 (SWC)
Input Resistance	100 MΩ
Bandwidth	4 Hz
Conversion Rate	9 samples/s
Power Consumption	1.2 W

Table C.3 (continued)

Output Module Specifications	
Output	
Ranges	0–20 mA, 4–20 mA
Overage	±2 mA
Initial Accuracy	
Output Offset	±5 μA (±15 μA max)
Span	±0.02% FSR (= 0.05% FSR max)
Accuracy vs Temperature	
Output Offset TC	±1 μA/°C
Gain TC	±50 ppm/°C
Resolution	±0.02% FSR
Nonlinearity	±0.02% FSR
Bandwidth	100 samples/s
Settling Time	1 ms to 0.1% FSR
Noise (100 Hz Bandwidth)	1 μA pk-pk
Load Resistor	0 to 750 Ω
Normal Mode Protection	240 Vrms
Slew Rate	Step Response Plus 0.125–128 mA/s in Eleven Binary Ranges
Read back	
Initial Accuracy	±100 μA
Output Offset	±0.5% FSR
Span	
Accuracy vs Temperature	
Output Offset TC	±5 μA/°C
Gain TC	±200 ppm/°C
Resolution	±0.5% FSR
Nonlinearity	±0.5% FSR
Isolation	
Common Mode Voltage Input to Output	1500 Vrms
CMR @ 60 Hz	90 dB min
Transient Protection	IEEE-Std 472 (SWC)
Power Consumption	1.2 W

Table C.3 (continued)

Common Module Specifications	
Power Supply Voltage, Operating	 –5 V ± 5%
Size	2.3 × 3.1 × 0.75 in. (58.4 × 78.7 × 19.1 mm)
Environmental Temperature Range Rated Performance Storage Relative Humidity (MIL-STD-883C, Method 1004.4)	 –25°C to +85°C –40°C to +85°C 0 to 95.5% @ 60°C

Table C.4 Manufacturer's specifications for computers (HOSTP, PRS/MUX, ESF/MUX, and DTC)

Power Supply	250 W 26 A @ +5 Vdc 0.5 A @ -5 Vdc 9.0 A @ +12 Vdc 0.5 A @ -12 Vdc
Power Requirement	115/220 Vac +13%/–20%, 49–61Hz
Operating Temperature	+5 to +50°C, 5 – 95% RH Non-condensing
Storage Temperature	–5 to +75°C, 5 – 95% RH Noncondensing
FCC Classification (Power Supply)	Class B Standards
UL/CSA Ratings (Power Supply	UL 1012, CSA C22.2
Construction Chassis Front Panel	 0.055-in. aluminum alloy, gold zinc finish 0.125-in. aluminum alloy, medium texture paint Sherwin Williams paint #F63-A-3080
Fans, Filtration Card Cage Area	Optional, 1, 106 CFM, 4.68-in. fan, filtered to 45 PPI
Connectors, External	Keyboard 5 pin DIN connector, front Accessory power outlet plug, rear
Switches	Power on, CPU reset, front panel
Drive Capacity	Rack and Bench Mount–Four half-height or two half-height and one full-height, 5.25-in. device bays Floor Mount–Three half-height or one full-height and one half-height, 5.25-in. bays
Weight	35 lb (16.0 kg) (Shipping—45 lb (20.5 kg)
Dimensions	18.25 in. D × 7.0 in. × 19 in. W 46.35 cm D × 17.78 cm H × 48.26 cm W
Backplane	10 slot, 4 layer, low-capacitance backplane, all AT ISA (16 bit) slots. Different configurations available on special request.

Table C.5 Manufacturer's specifications for FDDI network adapters

EISA-bus FDDI Network Adapter	
Dimensions	Base board: approx. 5 × 10.8 in. (127 × 275 mm) DAS Adapter board: 3.8 × 6.4 in. (99 × 162 mm)
Bus interface	EISA bus (32-bit DMA slave)
Network Interface	Compatible with the FDDI ANSI X3T9.5 specifications
LAN controller	AMD FORMAC Plus
RAM	32 kB or 128 kB CMOS RAM
FLASH memory	128 kB, 16 pages of 8 kB each can be addressed with page specifications
Shared memory	8 kB, one of 15 start addresses, ranging from 0xC0000 to 0xDC000 can be selected using the EISA configuration utility
I/O addresses	Slot-specific I/O address range
Interrupts	Four interrupts available with both edge triggering or level triggering, each selectable by using the configuration utility Interrupts: 1, 10, 9, 5
DMA	Four channels available, selectable by using the EISA configuration utility DMA channels: 7, 6, 5, 0
Timer	Two channels clocked at a maximum of 6.25 MHz
Power dissipation	DAS @5 V max 2.3A @12 V max 30mA

Table C.6 Manufacturer's specification for host processor's plug-in board

Number of Channels	16
ADC Resolution (Bits)	12
Gains	1, 10, 100, 500
Range (V)	0 to + 10, ±5, ±10
Input FIFO (words)	16
Hardware Analog Trigger	No
Fully Software Configurable	No

Table C.7 Manufacturer's specifications for FDDI bypass module

Optical Performance	
Insertion Loss	1.2 dB typical, 1.7 dB maximum
	3–6 dB on loopback or as specified
Switching Time	22 ms maximum
Cross-Talk	–80 dB maximum
Durability	10^7 cycles minimum
Repeatability	0.03 dB maximum

Electrical Requirements	
Switching Voltage	4.2 Vdc minimum, 6.0 Vdc maximum
Switching Current	130 mA to switch, 30 mA to hold (2X)
Connector	6 pin mini-DIN, standard DIN, MTE, or RJ jack

Environmental Specifications	
Operating Temperature	–10°C minimum to +55°C maximum
Storage Temperature	–20°C minimum to +65°C maximum
Humidity	Noncondensing

Electrical Connections	
PIN 1	Secondary Switch Positive (+5 Vdc)
PIN 2	Primary Switch Positive (+5 Vdc)
PIN 3	Primary Switch Ground
PIN 4	Secondary Switch Ground
PIN 5	Power Loopback
PIN 6	Power Loopback

Table C.8 Manufacturer's specifications for host processor's digital I/O plug-in board

I/O Signal Ratings		
Absolute maximum voltage rating	–0.5 to + 7.0 V with respect to GND	
Input Signal Specifications	**Minimum**	**Maximum**
Input logic high voltage	2.0 V	5.25 V
Input logic low voltage	0.0 V	0.8 V
Maximum input current ($0 < V_{in} < V$)	—0 μA	10 μA
Output Signal Specifications		
Pin 49 (at +5 V)	0.5 A maximum	
Pin 99 (at +5 V)	0.5 A maximum	
Output Logic High Voltage	**Minimum**	**Maximum**
At $I_{out} = -200$ μA	2.4 V	5.0 V
Output Logic Low Voltage		
At $I_{out} = 1.7$ mA	0.0 V	0.45 V
Darlington drive current		
($R_{EXT} = 750\ \Omega$ $V_{EXT} = 1.5$ V)	–1.0 mA	–4.0 mA
Operating Environment		
Temperature	0°C to 70°C	
Relative humidity	5% to 90% noncondensing	
Storage Environment		
Temperature	–55° to 150°C	
Relative humidity	5% to 90% noncondensing	
Physical		
Dimensions	3.9 in. by 6.5 in.	
I/O connector	100-pin male, ribbon-cable connector	
Power Requirement (from PC I/O Channel)		
Typical power	0.45 A at 5 VDC (±5%)	
Maximum power	1.2 A at 5 VDC (±5%)	

APPENDIX D–RF COUPLING FACTORS FOR CS02 TESTS

The RF coupler for the CS02 tests was calibrated in accordance with the MIL-STD-462 test specifications, and the coupling factors are shown in Table D.1. These factors are used to calculate the correspondence between oscilloscope readings and actual amplifier output. The two right-hand columns give the voltages (in dBmVp-p and in mVp-p respectively) that should appear on the oscilloscope in order to have 1 Vrms (2.8 Vp-p) present at the coupler output.

Table D.1 RF coupling factors

Frequency (MHz)	Input (dBm)	Coupler (dBm)	Difference (dB)	Scope	
				(dBmVp-p)	(mVp-p)
0.1	–60	0	60	9	3
0.2	–60	–4	56	13	4.5
0.5	–60	–11	49	20	10
1	–60	–16	44	25	18
2	–60	–20	40	29	28
5	–60	–23	37	32	40
10	–60	–27	33	36	63
20	–60	–25	35	34	50
50	–60	–27	33	36	63
100	–59	–30	29	40	100
200	–58	–27	31	38	79

APPENDIX E—EMI EVALUATION OF SPARK GENERATOR

This section documents the electromagnetic interference (EMI) signature of one of the spark generators used to ignite cables during some of the earlier smoke tests. (During later tests, butane lighters were used.)

Summary

The highest field strengths recorded were about 100 mV/m (see Figure E.8 at 60 MHz). Most of the energy was concentrated between dc and 20 MHz. However, there were significant peaks/bands of energy at frequencies up to about 900 MHz. There were several peaks in the 10–30-mV/m range, but most of the peaks were below 10 mV/m.

Introduction

The spectra were recorded using the SAS1D broadband antenna S/N 341 from Amplifier Research. Typically, the analyzer was set to the frequency span and bandwidth (BW) indicated for that figure, and then Max Hold was pressed. The analyzer was allowed to record for 5–10 min before the resulting peak amplitute spectrum was stored.

Data and Results

As shown in Figure E.1, the spark generator produces significant energy between dc and 20 MHz. For most of the spectrum the noise floor was about 37 dB μV/m. The highest peaks (other than the dc artifact portion of the spectrum) are in the 80–90-dB μV/m range or about 10–30 mV/m.

Next, the dc to 50-MHz portion of the spectrum was recorded. As shown in Figure E.2, the number of peaks above the noise floor greatly decreases above about 20 MHz. Here again, we have the 10–30-mV/m peaks below 2 MHz. The highest level recorded above 2 MHz was about 9 mV/m at about 46 MHz.

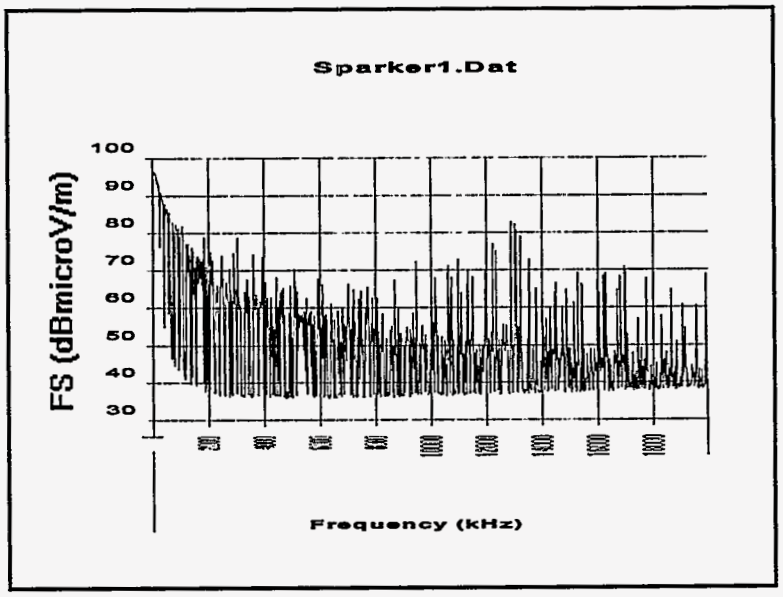


Figure E.1 Sparker1.Dat, 100-kHz BW, 0–20-MHz span, antenna on low band

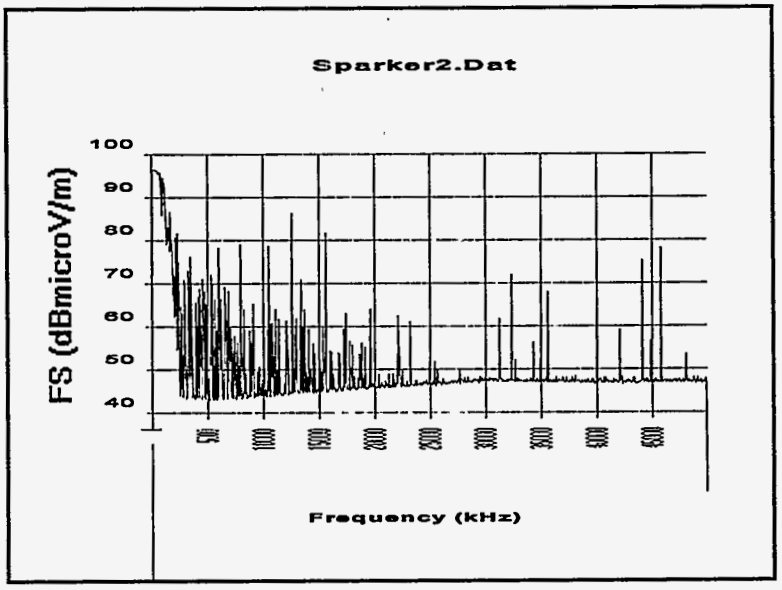


Figure E.2 Sparker2.Dat, 1-MHz BW, 0–50-MHz span, antenna on low band

A third spectrum was recorded using the low band of the antenna, covering 25–75 MHz. As shown in Figure E.3, there were several peaks of about 10–30-mV/m amplitude in the 50–60-MHz range.

In Figures E.4 and E.5, the antenna was set to the high band. Field strengths as high as about 5 mV/m were recorded at frequencies up to about 140 MHz, as shown in Figure E.4.

As shown in Figure E.5, the energy generated by the spark generator has very few peaks above 500 MHz.

The 2–20-MHz portion of the spectrum was then investigated using 1-MHz BW. The results are shown in Figure E.6. The spark generator tips were moved closer together so that the sparks would occur more frequently. This, however, may cause the amplitudes to decrease.

We also experimented by alternately pushing the generator tips together and pulling them apart and recording what is probably the worst-case fields. As shown in Figure E.7, the field strengths reached about 98 dB μV/m at about 12 MHz, which is equivalent to 80 mV/m.

Next, we recorded the higher frequencies, as shown in Figure E.8, using the high band of the SAS1D. The highest field was about 100 mV/m at about 60 MHz.

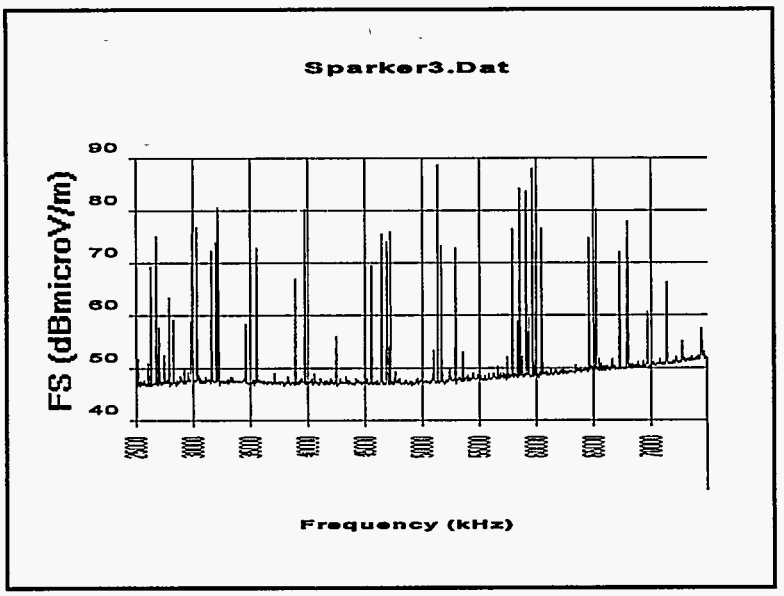


Figure E.3 Sparker3.Dat, 1-MHz BW, 25–75-MHz span, antenna on low band

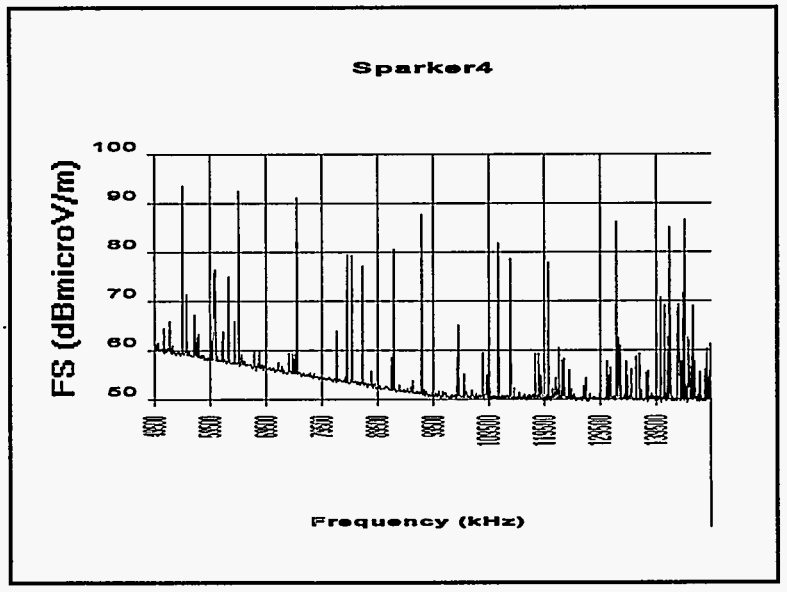


Figure E.4 Sparker4.Dat, 1-MHz BW, 50–150-MHz span, antenna on high band

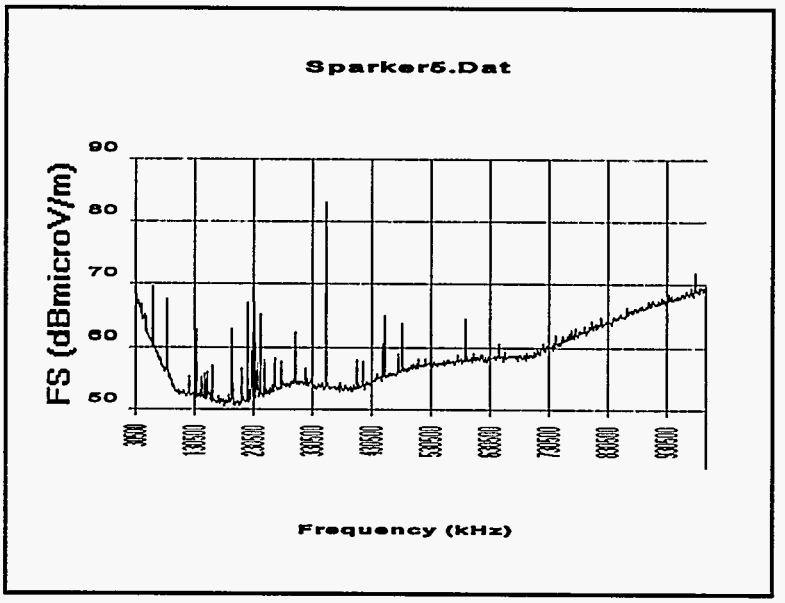


Figure E.5 Sparker5.Dat, 1-MHz BW, 100–1000-MHz span, antenna on high band

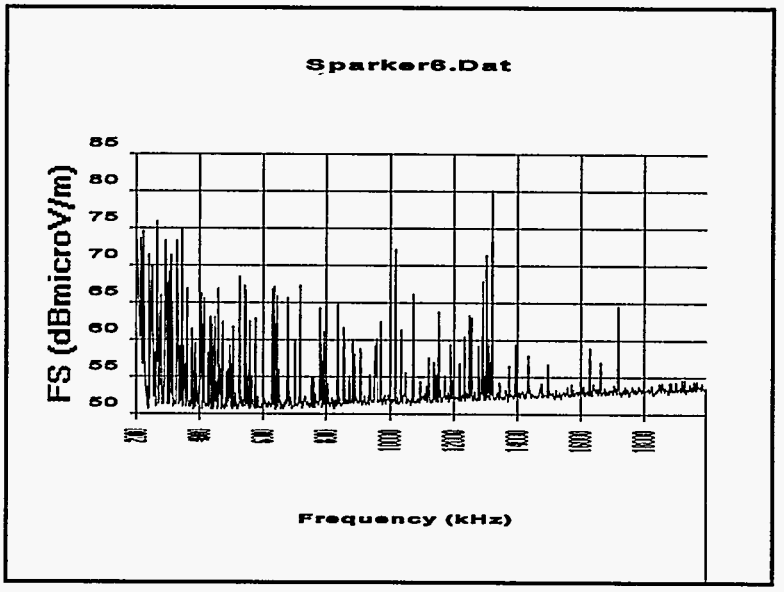


Figure E.6 Sparker6.Dat, 1-MHz BW, dc–20-MHz span, antenna on low band

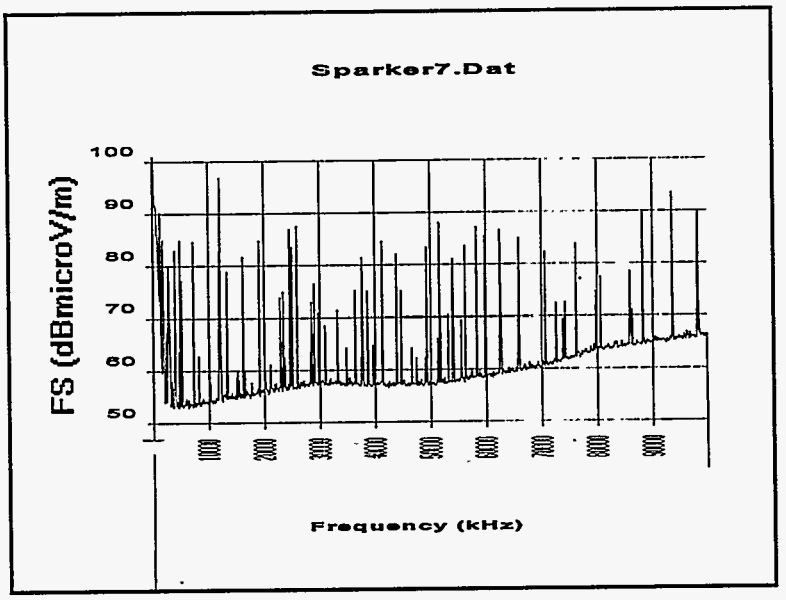


Figure E.7 Sparker7.Dat, 1-MHz BW, dc–100-MHz span, antenna on low band

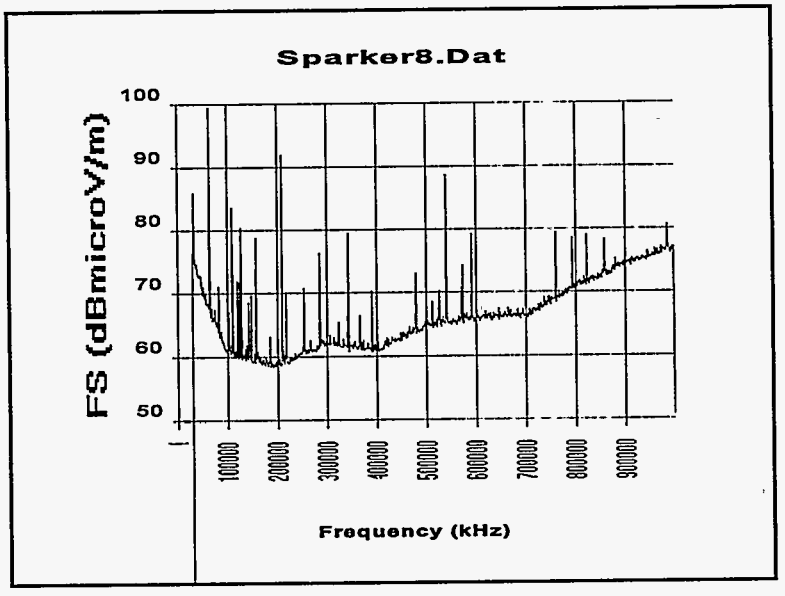


Figure E.8 Sparker8.Dat, 1-MHz BW, dc–1000-MHz span, antenna on high band

INTERNAL DISTRIBUTION

1.	G. T. Alley	20.	B. K. Swail
2.	R. E. Battle	21.	R. E. Uhrig
3.	D. F. Craig	22.	J. D. White
4.	P. D. Ewing	23.	T. L. Wilson, Jr.
5.	D. N. Fry	24-32.	R. T. Wood
6.	D. E. Holcomb	33-34.	Central Research Library
7.	S. W. Kercel	35.	Y-12 Technical Reference Department
8-16.	K. Korsah	36-37	Laboratory Records Department
17.	D. W. McDonald	38.	Laboratory Records–Record Copy
18.	C. E. Pugh	39.	ORNL Patent Section
19.	J. O. Stiegler	40.	I&C Division Publications Office

EXTERNAL DISTRIBUTION

41. Christina Antonescu, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Program Manager, Control Instrumentation and Human Factors Branch, MS T-10E33, 2 White Flint North, 11545 Rockville Pike, Rockville, MD 20852
42. Matthew Chiramal, U.S. Nuclear Regulatory Commission, NRR/HICB, MS O-8H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
43. Franklin D. Coffman, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Chief, Control Instrumentation and Human Factors Branch, MS T-10E33, 2 White Flint North, 11545 Rockville Pike, Rockville, MD 20852
44. M. Wayne Hodges, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Director, Division of Systems Technology, MS T-10E33, 2 White Flint North, 11545 Rockville Pike, Rockville, MD 20852
45. Joseph P. Joyce, U.S. Nuclear Regulatory Commission, NRR/HICB, MS O-8H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
46. Thomas L. King, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Deputy Director, Division of Systems Technology, MS T-10E33, 2 White Flint North, 11545 Rockville Pike, Rockville, MD 20852
47. Eric J. Lee, U.S. Nuclear Regulatory Commission, NRR/HICB, MS 8-H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852

48. Evangelos C. Marinos, U.S. Nuclear Regulatory Commission, NRR/HICB, MS O-8H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
49. Jerry L. Mauck, U.S. Nuclear Regulatory Commission, NRR/HICB, MS O-8H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
50. David L. Morrison, U.S. Nuclear Regulatory Commission, Director, Office of Nuclear Regulatory Research, MS T-10F12, 2 White Flint North, 11545 Rockville Pike, Rockville, MD 20852
51. William T. Russell, U.S. Nuclear Regulatory Commission, Director, Office of Nuclear Reactor Regulation, MS O-12G18, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
52. Themis P. Speis, U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Chief, Instrumentation and Controls Branch, MS T-10F12, 2 White Flint North, 11545 Rockville Pike, Rockville, MD 20852
53. Ashok C. Thadani, U.S. Nuclear Regulatory Commission, NRR/ADT, MS O-12G8, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
54. Jit P. Vora, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Electrical, Materials and Mechanical Engineering Branch, MS T-10E10, 2 White Flint North, 11545 Rockville Pike, Rockville, MD 20852
55. Jared S. Wermiel, U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Chief, Instrumentation and Controls Branch, MS O-8H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
56. Richard Blauw, Commonwealth Edison Information Services, 125 S. Clark, Room 1139, Chicago, IL 60603
57. Mahbubul Hassan, Brookhaven National Laboratory, P. O. Box 5000, Bldg. 130, Upton, NY 11973
58. Albert J. Machiels, Electric Power Research Institute, 3412 Hillview Avenue, P. O. Box 10412, Palo Alto, CA 94303
59. D. R. Miller, Ohio State University, Mechanical Engineering Department, 206 W Eighteenth Ave, Columbus, OH 43210
60. Ron Moore, The RM Group, 12024 Broadwood Drive, Knoxville, TN 37922
61. David Norton, Houston Advanced Research Center, 4800 Research Forest Drive, The Woodlands, TX 77381
62. Maurice M. Sevik, Carderock Division, Naval Surface Warfare Center, Code 1900, Bethesda, MD 20084-5000
63. Barry H. Simon, General Electric Co., ABWR Program, 175 Curtner Ave, MC 788, San Jose, CA 95125
64. Ernesto Suarez, Pratt & Whitney, P. O. Box 109600, MS 716-87, West Palm Beach, FL 33410
65. Tina J. Tanaka, Sandia National Laboratories, Organization 6449, P. O. Box 5800, Albuquerque, NM 87185-0737
66. Robert M. Taylor, Capital Controls Company, 3000 Advance Lane, Colmar, PA 18915
67. C. D. Wilkinson, Electric Power Research Institute, 3412 Hillview Avenue, P. O. Box 10412, Palo Alto, CA 94303

68-69. Office of Scientific and Technical Information, U.S. Department of Energy, P. O. Box 62, Oak Ridge, TN 37831

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-6406
ORNL/TM-13122

2. TITLE AND SUBTITLE

Environmental Testing of an Experimental Digital Safety Channel

3. DATE REPORT PUBLISHED

MONTH	YEAR
September	1996

4. FIN OR GRANT NUMBER

L1798

5. AUTHOR(S)

K. Korsah, ORNL
T. J. Tanaka, SNL
T. L. Wilson, Jr., ORNL
R. T. Wood, ORNL

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

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

Oak Ridge National Laboratory
P. O. Box 2008
Oak Ridge, Tennessee 37831-6010

Sandia National Laboratories
P. O. Box 5800
Albuquerque, NM 87185-0737

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 environmental stress tests performed on an experimental digital safety channel (EDSC) assembled at the Oak Ridge National Laboratory (ORNL) as part of the NRC-sponsored *Qualification of Advanced Instrumentation and Controls (I&C) System* program. The objective of this study is to investigate failure modes and vulnerabilities of microprocessor-based technologies when subjected to environmental stressors. The study contributes to the technical basis for environmental qualification of safety-related digital I&C systems for nuclear power plants.

The EDSC employs technologies and digital subsystems representative of those proposed for use in advanced light-water reactors (ALWRs) or for retrofits in existing plants. It was subjected to selected stressors that are a potential risk to digital equipment in a mild environment. The selected stressors were electromagnetic and radio-frequency interference (EMI/RFI), temperature, humidity, and smoke exposure. The stressors were applied over ranges that were considerably higher than what the channel is likely to experience in a normal nuclear power plant environment. Stressor-induced errors were logged so that failure modes that are characteristic of the technologies employed could be identified.

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

digital
EMI/RFI
environmental testing
environmental stressors
failure modes
fiber-optic communications
humidity
instrumentation and controls (I&C)
microprocessor
multiplexing equipment
qualification
reactor protection system
smoke
temperature

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page) Unclassified

(This Report) Unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program