
Digital I&C Systems in Nuclear Power Plants

Risk-Screening of Environmental Stressors and a Comparison of Hardware Unavailability With an Existing Analog System

Manuscript Completed: December 1997
Date Published: January 1998

Prepared by
M. Hassan, Brookhaven National Laboratory
W.E. Vesely, Science Applications International Corporation

Brookhaven National Laboratory
Upton, NY 11973-5000

Science Applications International Corporation
655 Metro Place South, Suite 745
Dublin, OH 43017

C.E. Antonescu, NRC Project Manager

Prepared for
Division of Systems Technology
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code W6542



NUREG/CR-6579
BNL-NUREG-52536

Digital I&C Systems in Nuclear Power Plants

Risk-Screening of Environmental Stressors and a Comparison of Hardware Unavailability With an Existing Analog System

Prepared by
M. Hassan/BNL
W. E. Vesely/SAIC

Brookhaven National Laboratory

Science Applications International Corporation

Prepared for
U.S. Nuclear Regulatory Commission



20081201042

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

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

ABSTRACT

In this report, we present a screening study to identify environmental stressors for digital instrumentation and control (I&C) systems in a nuclear power plant (NPP) which can be potentially risk-significant, and compare the hardware unavailability of such a system with that of its existing analog counterpart. The stressors evaluated are temperature, humidity, vibration, radiation, electro-magnetic interference (EMI), and smoke. The results of risk-screening for an example plant, subject to some bounding assumptions and based on relative changes in plant risk (core damage frequency impacts of the stressors), indicate that humidity, EMI from lightning, and smoke can be potentially risk-significant. Risk from other sources of EMI could not be evaluated for a lack of data. Risk from temperature appears to be insignificant as that from the assumed levels of vibrations. A comparison of the hardware unavailability of the existing analog Safety Injection Actuation System (SIAS) in the example plant with that of an assumed digital upgrade of the system indicates that system unavailability may be more sensitive to the level of redundancy in elements of the digital system than to the environmental and operational variations involved. The findings of this study can be used to focus activities relating to the regulatory basis for digital I&C upgrades in NPPs, including identification of dominant stressors, data-gathering, equipment qualification, and requirements to limit the effects of environmental stressors.

TABLE OF CONTENTS

	<i>Page</i>
ABSTRACT	iii
LIST OF FIGURES	vii
LIST OF TABLES	vii
EXECUTIVE SUMMARY	ix
ACRONYMS	xiii
ACKNOWLEDGMENTS	xv
1 INTRODUCTION	1-1
1.1 Background	1-1
1.2 Objectives	1-1
1.3 Issues in Risk and Reliability Evaluations of Digital Upgrades	1-2
1.4 Risk-Sensitivity-Based Approach for Evaluating the Effects of Stressors	1-3
1.5 Scope of the Study	1-3
1.6 Organization of the Report	1-4
2 REVIEW OF INFORMATION ON THE EFFECTS OF ENVIRONMENTAL STRESSORS ON ADVANCED DIGITAL I&C DEVICES AND SYSTEMS	2-1
2.1 Introduction	2-1
2.2 Military Data and Information	2-1
2.2.1 Military Documents Reviewed	2-2
2.2.2 Organization and Reporting of Data in the Military Documents	2-2
2.2.3 Military Application Environments and Stressors	2-3
2.2.4 Approach to Modeling Stressor Effects in the Military Documents	2-4
2.3 NPP Operational Experience	2-4
2.3.1 AEOD Report on Digital System Failures	2-5
2.3.2 ABB-Combustion Engineering Experience	2-5
2.3.3 NPRDS Data	2-6
2.4 Other Environmental Stressor Vulnerabilities of Digital I&C Systems Reported in Literature	2-6
2.5 Review Summary	2-8
3 FAILURE MODES OF DIGITAL I&C SYSTEMS	3-1
3.1 Introduction	3-1
3.2 Failure Modes of Digital Devices	3-3
3.3 Failure Modes of Digital Systems	3-5
3.3.1 Experience at U.S. Nuclear Power Plants	3-5
3.3.2 Other Experience of Digital Control System Failure	3-6
3.4 Summary	3-7

TABLE OF CONTENTS

(continued)

		<i>Page</i>
4	APPROACHES FOR EVALUATING RISK-SENSITIVITY OF ENVIRONMENTAL STRESSORS	4-1
4.1	Introduction	4-1
4.2	Risk-Sensitivity of a Stressor	4-1
4.3	Basic Steps in Determining the Risk-Sensitivities of Stressors	4-3
5	ASSEMBLING DATA FOR EVALUATING RISK-SENSITIVITY OF STRESSORS	5-1
5.1	Basic Objectives and Approach	5-1
5.2	Temperature	5-2
5.3	Humidity	5-3
5.4	Vibration and Shock	5-4
5.5	Radiation	5-5
5.6	EMI	5-6
5.7	Smoke	5-8
5.8	Assumptions on Locations and Environments of I&C Equipment in NPPs	5-10
6	RISK-SCREENING OF ENVIRONMENTAL STRESSORS IN AN EXAMPLE PLANT	6-1
6.1	Example Case	6-1
6.2	Risk-Sensitivities to Temperature	6-4
6.3	Risk-Sensitivities to Temperature-Humidity	6-6
6.4	Risk-Sensitivities to Vibration	6-7
6.5	Risk-Sensitivities to EMI from Lightning	6-8
6.6	Risk-Sensitivities to Smoke	6-8
6.7	Risk-Screening of Environmental Stressors	6-9
6.8	Sensitivity of the Stressor Risk-Screening Results to Specific Assumptions	6-11
7	A COMPARISON OF HARDWARE UNAVAILABILITY IN A DIGITAL-VERSUS ANALOG-I&C SYSTEM	7-1
7.1	System Description	7-1
7.2	Safety Injection Actuation System Models	7-3
	7.2.1 System Definition for Modeling	7-3
	7.2.2 Analog SIAS	7-3
	7.2.3 Digital SIAS	7-5
	7.2.4 SIAS Logic Models	7-6
7.3	SIAS Hardware Failure Data	7-7
7.4	SIAS Fault-Tree Quantification	7-9
7.5	System Unavailability Results	7-10

TABLE OF CONTENTS

(continued)

		<i>Page</i>
8	SUMMARY AND CONCLUSIONS	8-1
	REFERENCES	R-1
	APPENDIX A Effects of Environmental Stressors on I&C Devices and Systems	A-1
	APPENDIX B Calculations of Environmental Stressor Risk-Sensitivity	B-1
	APPENDIX C Fault-Tree Diagrams	C-1

LIST OF FIGURES

3.1	Basic Digital I&C System	3-2
6.1	Risk-Sensitivities to Temperature	6-6
6.2	Risk-Sensitivities to Temperature-Humidity	6-7
6.3	Risk-Sensitivities of Environmental Stressors in Example Plant	6-10
7.1	Simplified Block Diagram of One Train of ESFAS in SURRY	7-2
7.2	Block Diagram of Analog SIAS Used in Evaluations of System Unavailability	7-4
7.3	Block Diagram of Digital SIAS Used in Evaluations of System Unavailability	7-6
7.4	Block Diagram of the Four-Train Digital SIAS	7-10

LIST OF TABLES

2.1	Digital System Failure Events Reported in LERs (1990-1993)	2-5
2.2	Digital System Performance at ABB-CE Plants	2-6
3.1	Typical Programmable Electronic Device Failure Modes	3-4
3.2	Digital I&C System Failure Events in U.S. NPPs	3-6
3.3	Common-Cause Failures of Multiple Channels in an Assortment of Ten Digital Systems	3-7
5.1	Temperature Conversion Factors	5-3
5.2	Factor Reduction in Digital Microcircuit Device Time-to-Failure Due to Corrosion	5-4
5.3	Failure Rates of Selected Digital Equipment	5-5
5.4	SURRY Fire Initiating Event Frequencies in Control Room	5-9
5.5	Estimated I&C Unavailabilities from Smoke Events in Control Room	5-9
5.6	Environmental Conditions in Selected Areas of the Example PWR	5-10

CONTENT

(continued)

	<i>Page</i>
6.1 I&C Basic Events Modeled in Surry PRA	6-2
6.2 Estimates of Core Damage Frequency (CDF)	6-4
6.3 I&C Cutsets Identified at a Frequency Truncation Level of 1.0E-10	6-5
6.4 Risk-Sensitivities to Vibration	6-7
6.5 Risk-Sensitivities to EMI from Lightning	6-8
6.6 Risk-Sensitivities to Smoke in Control Room	6-9
6.7 Risk-Screening of Environmental Stressors in Example Plant	6-11
6.8 Sensitivity of Stressor Risk-Screening Results to Assumptions in Example Plant	6-13
7.1 Safety Injection Actuation Initiating Parameters and Logic	7-2
7.2 Failure Data for Analog SIAS Components	7-7
7.3 Failure Data for Digital SIAS Components	7-8
7.4 Analog SIAS Unavailabilities	7-10
7.5 Digital SIAS Unavailability For Different Application Data and Failure Detection Intervals	7-11
7.6 Sensitivity of Digital SIAS Unavailability to System Architecture	7-12
7.7 Sensitivity of Digital SIAS Unavailability to Common-Cause Factors	7-12

EXECUTIVE SUMMARY

This report presents a screening study to identify environmental stressors for advanced digital instrumentation and control (I&C) systems in a nuclear power plant which can be potentially risk-significant, and compares the hardware unavailability of such a system with that of its analog counterpart. The risk-screening is based on estimated risk-sensitivities of the stressors, which are the changes they cause in plant risk, and are quantified by estimating their effects on the occurrences of I&C failure and the consequent increase in risk in terms of core damage frequency (CDF). The study included reviewing and collecting data on the effects of environmental stressors on digital I&C failures, developing approaches for estimating risk-sensitivities of stressors based on available data, and then applying these data and methods to screen stressors in an example plant (a NUREG-1150 Pressurized Water Reactor), using its specific PRA. The study of system unavailability is based on one system of a PWR (the Safety Injection Actuation System or the SIAS) and included developing simplified logic models of digital and analog systems, collecting data to support the models, and performing sensitivity studies on some key data and modeling assumptions.

We reviewed the literature, including military documents, records of operational events in nuclear power plants, and journal publications on the performance of digital equipment in other industries to assemble information to assess the potential effects of environmental stressors on digital I&C performance, and to estimate reliability and risk parameters. We found that data are sparse, both in terms of the environmental effects and the reliability of digital equipment. Further, there are uncertainties in the estimates of both of these due to variations in parameters associated with the application of stressors, such as their levels and duration, and the diversity of the equipment and operational conditions. Therefore, the data can only be used to broadly compare system unavailabilities, or risks from different stressors, based on estimated ranges of potential effects or bounds on potential effects.

In evaluating the failure modes of digital I&C systems, we identified several incidents of their spurious operations in the literature, including those in NPPs, and initiated by an environmental stressor (Electro-Magnetic Interference, or EMI). However, these events generally led to more conservative plant configurations through the inadvertent operations of safety systems. None caused the system to fail to perform its essential safety functions. In other reported environmental stressor-related events, one system failure was due to loss of air-conditioning and others were due to lightning damaging microprocessor-based hardware. In some instances, multiple redundant equipment was affected by the stressors. Such failures can be a concern from risk considerations because of possible loss of redundancy in safety systems through common-cause effects.

The stressors evaluated for risk effects are temperature, humidity, vibration, radiation, EMI from lightning, and smoke. EMI effects from other sources could not be evaluated because of a lack of data. Radiation does not appear to be a significant stressor at I&C cabinet locations. In estimating risk-sensitivities of environmental stressors, the effects of stressors on digital I&C are introduced in the PRA, either by modifying the failure rates of the equipment and incorporating the likelihood factors for stressor effects to occur, or by estimating equipment unavailabilities based on the frequencies of the stressor events. The PRA then is used to recalculate the change in CDF. An increase in risk due to specific I&C failures is determined by the importance of the equipment, as modeled in the PRA.

The risk effects of stressors presented in this report are based on two categories of assumptions in risk quantifications:

EXECUTIVE SUMMARY

1. assuming a likelihood of 1.0 for exposure of digital I&C equipment to temperature, humidity, and vibration at the levels noted, and
2. assuming a failure probability of 1.0 for digital I&C equipment for potential common-cause type events, such as for lightning-induced EMI and smoke.

The first assumption is made because present information suggests the relevant stressors and exposures are plausible. The second assumption is made to bound the stressor's risk effects, necessitated by a lack of data, to resolve the relationship between their occurrences and the corresponding probability of equipment failure, particularly for smoke events. The sensitivity of the risk-screening results to uncertainty in the occurrence frequency of this second category of stressor events, and to the delay in detecting failure of equipment following such events is evaluated. A sensitivity study also is performed considering only those fractions of digital I&C failures which could be critical for system function and which may not be detected by system self-diagnostics, to evaluate their effect on the results of stressor risk-screening.

The results for the stressors in the example plant, subject to the bounding assumptions, indicate that humidity, EMI from lightning, and smoke can be potentially risk-significant. The risk-significance of EMI from lightning and smoke, however, are sensitive to detection periods for equipment failure following the events. The results also show that the effects of some stressors, such as, humidity, can be sensitive to the location of the equipment. For the levels of the stressors analyzed, risk effects from temperature in digital I&C equipment locations, and from assumed levels of vibrations, appear to be insignificant.

We compare the hardware unavailability of the existing analog Safety Injection Actuation System (SIAS) in a PWR with that of an assumed digital upgrade of the system. The results indicate that with proper design and surveillance, advanced digital systems should be able to meet or improve on the hardware unavailability of current analog systems. The effects of different environments and operational variations on digital hardware unavailability is analyzed using failure data from NPP and offshore platform applications, and theoretical estimates of failure probabilities in an industrial environment, based on military data. The environmental effects are included in basic component-failure probabilities and are not separately available. The analysis includes random or independent failures, and common-cause or dependent failures of hardware. The effects of test and maintenance are not modeled. The limited study shows that system unavailability may be more sensitive to the architecture of the digital system than to the environmental and operational variations considered.

There are several limitations to this study. The risk-estimates used existing I&C models in the PRA; that is, estimated environmental effects on the failure probabilities of digital system are applied to the I&C basic events currently modeled. Also, where data are sparse, bounding approaches are employed, such as in evaluating EMI and smoke effects, giving conservative risk estimates. Evaluations of system unavailability lacked common-cause data for digital components groups. To estimate such parameters, a significant amount of information is needed on the performance of the system as well as careful data evaluations. Lacking it, a sensitivity approach is taken to include the common-cause effects. The unavailability results represent system unavailabilities due to hardware failures, based on data from three different applications. However, differences in the unavailability of the example system are not all due to environmental factors as these data also include additional effects, such as, differences in hardware quality, duty cycling, the device's complexity and technology. Only one plant is used in the risk-screening

EXECUTIVE SUMMARY

study, and the comparison of unavailability is based on hardware failures in one system. For digital systems, failures of software and human-machine interface can be significant contributors to unavailability.

Nevertheless, the risk-screening application demonstrates the usefulness of the approach in identifying environmental stressors which can be potentially risk-significant. The system unavailability study provides a comparison of digital versus analog system hardware-performance, as well as showing the dependence of digital system's unavailability on different parameters. The failure data from different applications give a measure of variability in the expected system unavailability.

Based on this study, detailed modeling and information requirements can be specified for improving assessments of risk effects of stressors in a NPP using digital I&C. Such risk depends not only on the stressors' physical effects on the equipment and their likelihoods, but also on the specific equipment that is affected, its failure modes and risk-importance. Consequently, to more accurately estimate the risk contributions of digital I&C systems in NPPs, including the effects of stressors, will require extending current I&C models in the PRA to reflect the characteristics of the digital system, and also having adequate reliability data to support these models, both for normal operating conditions and for off-normal operations. A case in point is the urgent need for developing data on common-cause failure for digital systems in NPPs. Risk significant I&C components also can be identified from these extended models, so that data-gathering, evaluations of stressors, and qualification of equipment can be more efficiently focused on these risk-significant components.

ACRONYMS

A/D	analog-to-digital
ABB-CE	ABB Combustion Engineering
AEOD	Analysis and Evaluation of Operational Data
AFW	auxiliary feedwater
ALU	arithmetic logic unit
CCF	common-cause failure
CDF	core damage frequency
CE	Combustion Engineering
DMA	direct memory access
DoD	Department of Defense
EMI	electro-magnetic interference
ESF	emergency safety feature
ESFAS	emergency safety features actuation system
I&C	instrumentation and control
INPO	Institute for Nuclear Power Operations
IPE	individual plant examination
IRQ	interrupt request
LER	Licensee Event Report
LOCA	loss-of-coolant-accident
LOOP	loss-of-offsite-power
MCS	minimal cutset
MOS	metal-oxide semiconductor
MTBF	mean-time-between-failures
MTTF	mean-time-to-failure
NASA	National Aeronautics and Space Administration
NPP	nuclear power plant
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
ORNL	Oak Ridge National Laboratory
PES	programmable electronic system
PRA	Probabilistic Risk Assessment
PWR	pressurized-water reactor
R&M	reliability and maintainability
RAC	Reliability Analysis Center
RADC	Rome Air Development Center
RFI	radio-frequency interference
RPS	reactor protection system
SEL	single event latchup
SIAS	safety injection actuation system
SSPS	solid-state protection system
TS	technical specification

ACKNOWLEDGMENTS

The authors wish to thank the NRC Program Manager, Christina Antonescu, for her help in initiating and planning this study, and to Franklin Coffman, NRC Branch Chief, Instrumentation, Control, and Human Factors Branch, for many insightful comments throughout this work. Thanks also go to Dr. Kofi Korsah of the Oak Ridge National Laboratory for assistance in interpreting the implications of digital-device failure modes to system effects. The authors wish to acknowledge the contributions of Dr. S. Wong in identifying I&C equipment modeled in the PRA and their locations, and Mr. S. Kasturi and Mr. M. Villaran in analyzing NPRDS data on digital hardware failure. Special thanks to Mr. G. Martinez-Guridi, Dr. P.K. Samanta, Mr. J. Taylor, and Mr. M. Villaran for reviewing the report and providing suggestions for improvement. Finally, thanks to Barbara Roland for her expertise in preparing this manuscript.

1 INTRODUCTION

1.1 Background

Advanced digital systems based on microprocessors are proliferating in the area of process instrumentation and control (I&C) because of their increased capabilities and superior performance compared to the I&C systems based on analog devices. This technology also is being implemented in nuclear power plants (NPPs) in the United States to replace aging and obsolete analog I&C systems. To date, digital I&C upgrades have been made for selected systems in more than two dozen plants including protection, safety, process control, and monitoring applications.

A concern with using advanced digital I&C systems in NPP applications, particularly for safety-critical systems, is their potential vulnerabilities to NPP environments and the consequent effects on plant risk. A related concern is the reliability performance of digital I&C systems in NPP environments vis-a-vis existing analog systems. Such concerns arise from the limited experience with digital I&C systems in NPPs. Stressor-related failures of digital equipment have been reported [1] which are unique for such systems, and are not experienced by corresponding analog systems.

Digital technology was introduced relatively recently in the nuclear power industry, mostly in non-critical control applications. In general, very little information is available on the performance of advanced digital I&C systems in NPPs, and specifically, there is no data on the effects of NPP environments on these equipment.

A large variety of microprocessor-based digital I&C equipment currently is available with significant differences in semiconductor or packaging technology, the complexity of the devices, their ruggedness, and quality. Military experience shows that significant differences can be expected in reliability performance depending on the choice of the equipment and the particular application [2].

A systematic evaluation of risk effects of stressors is important for understanding the relative risk impacts of various stressors and to focus further research on important environment-related vulnerabilities. The lack of experience with digital equipment in NPP environments requires that the risk and reliability evaluations involving such systems draw upon relevant experience with the equipment available from other uses. However, although digital systems enjoy a very wide application base across the industries and substantial operational experience with them has accumulated, there is very little organized or independent data available to perform risk and reliability studies on these systems except for those provided by the U.S. military in unclassified reports. The approach we have taken in this study is to combine and use all relevant information and data on digital I&C systems to evaluate their associated reliability and environmental risk effects in NPP applications.

1.2 Objectives

The purpose of this study is to contribute to developing the technical basis for regulatory guidance on environmental qualification of advanced microprocessor-based digital upgrades of safety I&C systems in NPPs. The study is intended to provide information on the risk effects of environmental stressors, and the expected reliability performance of digital I&C systems in NPP environment. The following are the objectives of this study:

1 INTRODUCTION

1. to develop approaches to evaluate risk from potential stressors associated with digital I&C systems in nuclear power plants
2. to collect information and data which can be used to support stressor risk evaluations
3. to apply the approaches and information to the best extent possible to screen the potential stressors for risk-significance
4. to compare the hardware unavailability of a microprocessor-based advanced I&C system to that of an existing analog system.

1.3 Issues in Risk and Reliability Evaluations of Digital Upgrades

From considerations of plant risk in upgrading to digital I&C hardware, the questions of interest are the failure modes and mechanisms of such equipment, and its expected reliability performance in the operating environment. The risk-significance of the failure of specific equipment is another important issue since the frequencies of failure in different modes and the risk-consequences of such failures determine the overall plant risk. If environmental stressors have a detrimental effect on risk-significant equipment, or cause such equipment to fail in an unsafe manner, plant risk can be significantly increased. Plant risk can also be significantly increased if environmental stressors cause redundant equipment to fail simultaneously, known as common-cause failures or dependent failures.

For most digital hardware in benign environments, random (independent) failures are not necessarily an issue as the mean time between failures (MTBF) (generally better than $1.0E+6$ hours) most often exceeds the requirements of the application. Rather, it is the specific operational and environmental conditions which may degrade the performance of digital equipment that are of concern. The failure mechanisms for digital devices, reported in Ref. 2, indicate that these are accelerated by stressors which can be characterized by operational and environmental conditions. These stressors can contribute towards the same failure modes for a device, or to different failure modes specific to either conditions. Further, the operational and environmental conditions can be characterized by parameters which are within the normal operating range, i.e., within specifications, or by abnormal/accident conditions, i.e., parameters beyond specifications. The operational conditions refer to such parameters as the device's supply voltage, the junction temperature, and duty cycles. The environmental conditions refer to such parameters as ambient temperature, humidity, vibration, radiation, smoke, and EMI/RFI (electromagnetic interference/radio-frequency interference). In risk-evaluation of environmental stressors, both short-term stressor effect, such as, sudden changes in their levels or sudden application of stressors, and long-term effects, such as sustained operation in a given stressor environment, may need to be considered.

Information is needed, therefore, on the physical effects of different environmental stressors on digital equipment in order to estimate their potential negative impact, and consequent plant risk. Data on performance are needed at both system and component level in different stressor environments. System-level information can be used, for example, to identify any peculiar or unique system failure mode related to stressors which can be important from a NPP's risk perspective. Component-level information is useful to establish the vulnerabilities of individual I&C components to specific stressors; it also is needed to develop system reliability models for specific systems.

The primary difficulty in risk and reliability evaluations of digital upgrades, however, lies with the data. Although digital control systems have been used for many years in different industries, digital microcircuit technology has been continuously evolving with new material, fabrication technology, and increasing complexity. Moreover, there are many different manufacturers offering a wide variety of these products with significant variations in their operational characteristics. Development of information on failures related to the effects of environmental stressors on these devices is hindered by a lack of a sufficient number of any one type in use in a specific application. Further, environmental effects in operational data are generally not separated out when the equipment's failure rates are presented because they often are difficult to separate from other effects. Environmental effects are often synergistic which also makes it problematic to transfer or validate operational experience across applications.

Digital I&C systems can vary widely in terms of system complexity, system architecture, hardware, software, and human interface. Consequently, it is not possible to predict from a generic study how a particular system will fail. System-specific analysis is necessary to define failures and identify applicable failure modes based on functional requirements on the system for safe plant operation. System-specific analysis is also necessary to determine the risk-significance of specific equipment. A generic study, however, can be useful for assessing overall system performance and for identifying broad categories of failures and risk and how these can be influenced by environmental stressors.

1.4 Risk-Sensitivity-Based Approach for Evaluating the Effects of Stressors

The risk effects due to a stressor can be expressed in terms of the risk-sensitivity of the plant to that particular stressor. The risk-sensitivity of a stressor is the change in plant risk which occurs given its presence. The risk sensitivity to a stressor is evaluated by determining its effect on the occurrences of I&C failure and the effect of these failures on risk. If the effects of the stressor on I&C failure rates can be determined or bounded, then the different possible I&C failure rates can be input to a Probabilistic Risk Assessment (PRA) to determine the resulting risk sensitivity. As an upper-bound evaluation, the I&C equipment which can be affected by the stressor can be assumed to fail, and the resulting increase in risk determined. The risk increase which is determined also can be multiplied by the likelihood of the stressor occurring to produce an expected impact. Risk-sensitivities to stressors so determined can be used to screen the stressors for risk-significance.

1.5 Scope of the Study

The I&C systems in NPPs associated with reactor protection and safety-system actuations typically consist of several elements, such as process sensors, transmitters, sensing lines, and cabling as well as various logic units and switching devices. The upgrades are implemented primarily by using various digital microcircuits, including microprocessors, to replace analog logic and switching functions in the I&C systems. However, the existing sensors, transmitters, and cabling in the I&C systems are expected to remain the same, at least in the near future, although fiber-optic cables and components eventually may replace much of this equipment. Consequently, in the present context, in evaluating the risk associated with digital upgrades due to environmental stressors, the impact of NPP operating environments on various digital microcircuit devices are most relevant. The risk-sensitivities discussed in this study are based on the effects of environmental stressors on these elements of the digital I&C systems.

I&C equipment in NPPs generally can be found in all major plant locations, such as the control building, the auxiliary building, and the containment. However, the logic and switching equipment associated with safety-

1 INTRODUCTION

critical I&C are primarily located in the control building, and some, possibly, in the auxiliary building. Depending on the specific plant, the control building areas where I&C cabinets may be located are the control room, relay room, cable-spreading room, and switchgear room. Presently, there is no indication that nuclear utilities have any plans to locate microprocessor-based equipment in the harsh environments of the containment. The templates presented in Ref. 3 on advanced reactor I&C involving digital systems indicate that microprocessor-based equipment may be located in the control building and auxiliary building only. Consequently, in our analysis we assumed that the digital I&C equipment is located in these plant areas.

In this study, the environmental stressors are screened for risk-significance based on plant risk-sensitivities to them. The risk-sensitivities refer to changes in the plant's core-damage frequency due to negative effects of the stressors on digital I&C equipment. Plant risk-sensitivities are investigated for temperature, humidity, vibration, radiation, EMI/RFI, and smoke, these six environmental stressors being identified from a literature review as having the potential to have an impact on the digital microcircuits' reliability, and consequently, on the reliability of the digital system. Where appropriate, normal operating conditions as well as abnormal and accident conditions in the plant are considered. A PRA-based approach is taken to quantify any changes in plant risk due to the effects of environmental stressors using existing I&C models in the PRA. The effects of environmental stressors are introduced in the PRA calculations by modifying the occurrences of system failure.

The assessments of system unavailability presented in this report compare the hardware unavailability of the analog Safety Injection Actuation System (SIAS) in the example plant with that of an assumed digital upgrade. The environmental effects are included in basic component failure probabilities used in system unavailability evaluations, and are not separately available. The analysis includes random or independent failures, and common-cause or dependent failures of hardware. The effects of test and maintenance on system unavailability are not modeled.

1.6 Organization of the Report

This report is organized as follows. Chapter 1 is an overview of the risk issues associated with digital I&C upgrades in NPPs. Data and modeling needs for evaluating a stressor's risk sensitivity in NPPs also are discussed. Chapter 2 reviews the information available on the effects of environmental stressors on advanced digital I&C equipment. The failure modes of digital I&C devices and systems identified from literature are presented in Chapter 3, including those experienced during the recent environmental testing of an experimental digital safety system by Oak Ridge National Laboratory (ORNL). In Chapter 4, approaches are developed for assessing the risk-sensitivity of environmental stressors. Chapter 5 discusses data on environmental stressors assembled from various sources for calculating risk-sensitivity. Environmental stressor risk-sensitivity results for an example plant, obtained using the approaches and data developed earlier, are presented in Chapter 6. The risk-sensitivity results are used to screen the stressors for risk-significance, also in Chapter 6. In Chapter 7, hardware unavailability of a microprocessor-based I&C system is compared with that of an existing analog system performing the same functions. Our key findings, conclusions, and recommendations for further work are contained in Chapter 8. Appendices A, B, and C contain some additional detailed data and results.

2 REVIEW OF INFORMATION ON THE EFFECTS OF ENVIRONMENTAL STRESSORS ON-ADVANCED DIGITAL I&C DEVICES AND SYSTEMS

In this chapter, we review information on the effects of stressors on digital I&C devices and systems. Information from the literature is discussed, including failure experiences with these systems. The results of an analysis of failures of digital equipment in NPPs is also presented.

2.1 Introduction

An important task in this study was collecting information and data on the effects of environmental stressors on advanced digital I&C equipment for evaluating their risk impacts. Data was also needed for evaluating the reliability of digital systems. Information was sought on stressor effects, system failures, and equipment reliability performance from across the industries to supplement the limited nuclear operating experience with this equipment. Although radiation-related stress is unique to NPP environments, other environmental stressors identified in this study for NPPs, i.e., temperature, humidity, vibration, EMI/RFI, and smoke from potential fires, are common in most industries. Radiation is considered an important stressor in the application of advanced digital I&C systems in space; therefore, such information was also sought which could be related to NPP operating environments.

In published literature on the reliability of electronic systems, military documents are more frequently cited as information sources; this is partly due to the detailed database maintained by the military and partly due to public accessibility of these documents. Military documents were one of the main targets in our data collection activities. These documents provided information on the performance of digital I&C equipment at the component level. Information at system level was obtained from NPP operational experience reported in the Licensee Event Reports (LERs). Experience with digital equipment in NPP environments reported in NPRDS (Nuclear Plant Reliability Data System) were analyzed to estimate the equipment's failure rates to compare with other experiences. Additional information on the performance of digital systems was obtained from journal publications.

2.2 Military Data and Information

Digital control systems involving microcircuits were used most widely in the past by the U.S. military in a wide range of environments in land, sea, air, and space. The U.S. military also systematically tested and reviewed this equipment to provide guidance on its performance and reliability in various applications. Military data on equipment reliability generally are available through publications of the Rome Laboratory (formerly known as the Rome Air Development Center or RADC), located at Griffis Air Force Base, Rome, New York. Information also is available from the U.S. Department of Defense (DoD) Information Analysis Center at Rome,

2 REVIEW OF INFORMATION

New York, known as the Reliability Analysis Center (RAC), which is chartered to collect, analyze, and disseminate reliability information on electronic systems and parts.

2.2.1 Military Documents Reviewed

To identify military documents on the effects of stressors on digital I&C hardware, the list of military publications on the reliability and maintainability (R&M) discipline was scrutinized and a bibliographic search was conducted of the RAC database using keywords. The search included technical reports, standards, handbooks, and other publications. Several documents were targeted for detailed review. The following contained relevant information on the reliability of digital device and the effects of environmental stressors on these devices:

- The Rome Laboratory Reliability Engineer's Toolkit [2]
- Reliability Prediction of Electronic Equipment [4]
- NASA Parts Application Handbook [5].
- Reliability Analysis/Assessment of Advanced Technologies [6]

These documents were published or updated between 1988 and 1993 and represent the most recent, detailed reliability information available on digital equipment. The data sources in these documents generally are based on historical information on the devices' failures. In addition to the microcircuit database maintained by the RAC, data from industry and from the open literature were used, as well as data on accelerated life tests. The information contained in these documents are discussed in the following sections.

2.2.2 Organization and Reporting of Data in the Military Documents

The military publications containing information on digital equipment, generally are reports intended for providing guidance on the application and usage of a wide range of electronic equipment needed by the armed services. Digital microcircuit devices constitute a small subset of this population. Information generally is grouped by functional categories. Digital devices, however, were identified by semiconductor technology, such as bipolar, and metal-oxide semiconductor (MOS), as well as by their functional categories, such as microprocessors, logic arrays, and by the complexity of the devices, such as number of gates.

Information, analyses, and predictive models on different aspects of the reliability of digital microcircuits are presented in these documents, along with qualitative and quantitative information on the effects of environmental stressors. Although several different sources of raw data were used to derive estimates of the devices' performance parameters, these sources are not always explicitly identified.

In some cases, microcircuit data on stressor effects are grouped by the type of device; otherwise data were lumped together with the derived environmental performance data based on several devices, including, analog, digital, and discrete semiconductor devices. Although there is material overlap among some military documents, each report is focussed towards a different objective and contains unique specific details.

2 REVIEW OF INFORMATION

Statistics on microcircuit device failures are available from military reports for different failure mechanisms. Table A1 in Appendix A shows an example of information on failure modes and mechanisms. For each type of equipment, failure mechanisms are listed, followed by the corresponding failure statistics, modes, and accelerating factors. Microcircuits are categorized by type, such as digital, memory, linear, and hybrid. The memory units also are likely to be digital equipment although they are separated out from the digital category. The factors accelerating failure include both operational conditions and environmental factors. The environmental accelerating factors include temperature, moisture, vibration, and shock. In terms of accelerating factors for failure, digital equipment appears to suffer from the same stressors as other microcircuit devices. However, the relative effects of different environmental stressors and thresholds for reliability degradation may be different, as suggested by the differences in the failure statistics. The application environments in which they are applied also may be different for different categories of devices.

Information on radiation effects on digital devices was identified in Ref. 5 (Mil-HDBK-978B). This document is a basic technical reference developed for the National Aeronautics and Space Administration (NASA) to improve the agency's selection of electronic, electro-mechanical, and electrical components, and to support failure analyses of systems employing these components for different applications. Volume 3 of this document has information on microcircuits including digital microcircuit devices. However, this information focuses on the technical details of the various technologies in each category of device, and does not explicitly give reliability effects. Detailed information on the effects of environmental stressors is limited to the effects of radiation on microcircuit devices although other stressor effects are briefly discussed. The types of functional faults or failures expected due to radiation-induced damage in such devices are elaborated. There is a table, shown as Table A2 in Appendix A, which classifies radiation effects by microcircuit technology. Quantitative ranges are given for total dose hardness levels for different devices, while qualitative judgments have been made about their susceptibility to radiation effects known as "single event upset." The total dose hardness level refers to the sensitivity of the microcircuit device to the cumulative effects of radiation, expressed as the absorbed dose in silicon. The "single event upset" is due to the passage of a single ionizing particle, such as an alpha particle, through the device; this also is referred to as a "soft error" as it does not permanently damage the device, but may trigger a change in its logic state (bit error). Single heavy ions also can cause "latch up" in some devices resulting in a massive number of bit errors so that the device eventually may be permanently damaged.

2.2.3 Military Application Environments and Stressors

An important piece of information available from military documents is the evaluation of the reliability effects of environmental stressors. The reliability effects are also quantified, except for radiation-induced stresses, through a single "environmental factor" for each type of device and for each category of equipment use in that environment. The environmental categories are classified by military applications, such as ground fixed, ground mobile, naval, and airborne application. Depending on the document, between eleven and fourteen different environment categories are identified covering major areas of equipment use by the military services. Mostly qualitative but some quantitative descriptions of these environments can be traced to other military documents. Table A3 in Appendix A is reproduced from Ref. 4 which describes these environments. In general, these

2 REVIEW OF INFORMATION

categories represent different levels of control on the equipment's environment, such as temperature and humidity control using heating/cooling equipment, limited temperature control through ventilation around the equipment with no humidity control, or no control at all, such as, for unsheltered equipment.

2.2.4 Approach to Modeling Stressor Effects in the Military Documents

Probably the most popular reference for many years on failure rates for electronic devices has been the military handbook 217 and its updates. Through Ref. 6, the military made efforts to revise the prediction models for the failure rate in MIL-HDBK-217 for existing equipment using available information, and to develop new reliability-prediction models for emerging technology devices; these included advanced digital microcircuit devices, such as VLSI/ULSI including microprocessors and gate-array devices, memory devices including programmable logic devices, and digital GaAs devices.

Reliability issues associated with microcircuit devices were categorized as early-, middle-, and end-life, and models were developed to predict the reliability of the device at different stages of its life. In this approach, random failure is assumed for early- and middle-life, while the end-life failures are assumed to be due to wear out. The latter are associated with environmental effects, and were considered to be particularly important for advanced technologies because of the increased complexity of these devices, along with their physical compactness.

Failure mechanisms during operating life are analyzed with references to failure-accelerating factors, such as environmental stresses and other operating conditions. Failure mechanisms are categorized into two broad categories a) those related to electrical failures, and, b) those related to the failures of packages for multichip devices which generally are mechanical. To simplify the models, all non-electrical failures of microcircuit devices were considered to be package failures.

Table A4 in Appendix A reproduces the potential mechanisms for end-life electrical failures identified in Ref. 6 for VLSI/ULSI microcircuit devices. The corresponding failure modes are also listed, along with various environmental and other failure-accelerating stressors. However, the frequency of failure occurrence in each mode is not given. The temperature effects refer to the junction temperature within the device.

The report identifies corrosion as one of the most important failure mechanisms and dedicates a considerable portion to analyzing various corrosion processes. A plot is given (shown as Figure A1 in Appendix A) of the temperature-humidity relationship to corrosion, expressed through the environmental acceleration factor which is the inverse to the multiplier to the Mean-Time-To-Failure (MTTF) due to corrosion. The higher the temperature and the humidity, the larger is this factor, resulting in rapid decrease in the MTTF due to corrosion.

2.3 NPP Operational Experience

We mentioned earlier that NPPs in the United States have been using some digital I&C systems for several years, including microprocessor-based systems. NRC's office of Analysis and Evaluation of Operational Data

(AEOD) published a review report (AEOD/T94-03) [7] on events involving digital I&C system failures based on LERs for 1990-1993. Experience with a specific digital safety system in NPPs (the Combustion Engineering Core Protection System) has been reported in the literature by sources associated with the vendor [8]. Information on equipment failures in NPPs also are documented in the database of the Nuclear Plant Reliability Data System (NPRDS) [9]. In this section, we discuss this reported experience with digital I&C systems in NPPs.

2.3.1 AEOD Report on Digital System Failures

This AEOD report [7] identified 79 LERs involving digital equipment failures from 1990 to 1993. These failures generally were categorized as originating from errors in the software, human-machine interface, EMI, and from random component failures. Table 2.1, reproduced from Ref. 7, breaks up the events by cause category. Section 4.3.1 further categorizes the events by failure modes. For environmental stressors, the EMI events are relevant. Some of the failures categorized as 'random' may also have been influenced by environmental stressors. However, we cannot isolate such effects from LER descriptions alone. Although the information contained in this document provides important insights on the causes of failure of digital systems, it does not yield any data for evaluating stressor risk.

Table 2.1 Digital System Failure Events Reported in LERs (1990-1993)

Category	Number of Events
Software Error	30
Human-Machine Interface Error	25
Electromagnetic Interference	15
Random Component Failure	9
Total	79

2.3.2 ABB-Combustion Engineering Experience

Since 1980, Combustion Engineering plants have been using digital computer-based systems along with analog systems for reactor protection functions. The system was initially based on 16-bit computers but a more recent version uses 32-bit hardware. Table 2.2, edited from Ref. 8, shows the performance statistics of digital elements of the system based on 67 reactor years of operating experience. The failures are not separated by either modes or causes. Failure rates are approximately $4.6E-6$ per hour for processors and memory units, and $1.2E-5$ per hour for input/output. Failures that are non-self-indicating refer to hardware failures which are not detected by the self-diagnostic feature of this system. ABB-CE reported one EMI event, originating from a lightning strike, which resulted in a reactor trip in 67 reactor years of operation, or an occurrence frequency of approximately $1.5E-2$ per year. Also, there was one software deficiency event which prevented one trip output from being set as

2 REVIEW OF INFORMATION

required. However, a redundant trip output was available to trip the channel. The data in this paper were used in evaluating digital system reliability, reported in Chapter 7.

Table 2.2 Digital System Performance at ABB-CE Plants

System Element	Cumulative Hours of Operation	Number of Failures Non-self Indicating
Processors and Memory	1,084,752	5
Input/Output	1,084,752	13

2.3.3 NPRDS Data

Since the early 1980s, NPPs have used digital systems which have hardware (e.g., microprocessors, logic arrays, application specific integrated chips) similar to that in current technology digital systems. As part of this work, we reviewed NPP operating experience with the digital systems currently in use, and attempted to estimate failure rate from it. Details of the analysis are given in Ref. [10].

The data analysis included downloading failure data from the Nuclear Plant Reliability Data System operated by INPO (Institute for Nuclear Power Operations) into a spreadsheet, validating the records as representing a failure of a digital system, categorizing them by the type of failure, and evaluating their environments. Generally, the type of failures involved functional failure of the component (mostly circuit cards) and/or the associated instrument channel. The failures were generally detected by malfunction alarms/indications in the control room or during surveillance testing. In the sample reviewed, no software related failures or spurious actions were noted. At the circuit card level, most of the failures appeared to be from passive circuit components rather than I&Cs or microprocessor chips. But caution is warranted, since the NPRDS failure narrative is generally insufficient to draw firm conclusions in this regard.

From reviewing the failure records, we determined that, with few exceptions, discrete digital electronic systems and components are located in temperature- and humidity-controlled environments. The few exceptions are components that are part of a sensor or A/D (analog-to-digital) converters, such as those for digital radiation monitoring systems, rod position indicating systems, or nuclear instrumentation. The failure rates for digital equipment were estimated to be $1.76E-6$, and represent averages over all digital equipment currently in use in NPPs under all operational conditions and at all locations.

2.4 Other Environmental Stressor Vulnerabilities of Digital I&C Systems Reported in Literature

Clark and Gavender [11] reported damage and failures of microprocessor-based I&C systems caused by lightning-induced transient voltage spikes in the energy production, manufacturing, and petrochemical industries.

2 REVIEW OF INFORMATION

Electromagnetic coupling has been cited as the most frequent means of electrical energy from lightning entering I&C systems. Low voltage data and control line interface components are most frequently damaged. The authors argue that electrical storms do not have to be directly overhead to cause damage, especially when instrumentation signal lines are active. The paper presents the electrical field generated by lightning as a function of distance to strike and the corresponding induced voltages in 1 meter of wire. These values range from 110 volts per meter vertical electric field and 20 volts induced in 1 meter of wire for a strike distance of 10 kilometers to a vertical field of 11000 volts per meter and 2000 volts induced for a strike distance of 0.1 kilometer. The range of vulnerabilities in terms of induced voltage spike for different devices also are given; these range from a low threshold for failure of 30 volts (for VMOS devices) to as high as 1000 volts (for Schottky TTL). For common devices such as EPROMS and CMOS, which may also be used in NPP I&C systems, these thresholds for failure respectively are 100 volts and 250 volts. This paper, however, did not contain any data on -frequencies of equipment failure and stressor effects which could be used for prioritizing stressor risk. Instead, information on the frequencies of thunderstorm occurrence reported in this paper for different parts of the United States, along with the frequency of lightning-induced I&C perturbations and failure events in NPPs reported in Ref. 12 for existing systems, as reported in section 5.6, was used in our evaluations.

Extensive facility-wide damage to telecommunications equipment from smoke following fires have been reported [13]. This paper also cited Factory Mutual data on large, nonthermal damages (i.e. from smoke and fire-suppression agents) across the industries. Smoke effects on equipment are caused by the transport and deposition of the products of combustion, such as carbon soot and other chemical products, including many corrosive chemical compounds. Smoke particles, deposited on microcircuit devices, can cause contact failures, contact bridging, and corrosion. Some of these processes can further be enhanced in the presence of other environmental factors, such as high relative humidity. While there is increasing interest in the insurance industry in studying the effect of smoke and other nonthermal damage to electronic equipment, including computer-based equipment, because of the large costs associated with losses, much of the work done on the subject is considered proprietary, such as that by Factory Mutual. We did not identify any data on smoke-related failure of digital equipment in the literature, which could be used in stressor risk-sensitivity evaluations. Instead, assumptions were made about smoke effects based on fire frequencies in NPPs and limited laboratory tests conducted as part of the NRC's environmental test program for digital I&C equipment as discussed in section 5.7.

Paula and Roberts [14] reported failure experiences of fault-tolerant digital control systems from several industries in the United States and in Europe including chemical, petrochemical, and nuclear. Information is generally provided on a total of 20 systems including a number of single-channel and overall system failures, although information is spotty on some systems. For a subset of ten of these systems (systems 1 through 10 as identified in Table 7 of Ref. 14) about which there is more complete information. A total of 35 system failure events are reported for an operating period of 90 system-years. During the same period, there were an additional 279 single channel failures. One system suffered no failure in a ten-year operating period. Software failures is the leading cause for all system failures and include all software deficiencies, followed by power supply interruptions and disturbances, and human-interaction errors during operation or maintenance. Spurious failures are system failures caused by spurious signals generated within the system, such as through EMI. Additionally, two other environment-related failures of multiple channels of these systems are reported, one failure from high-temperature due to loss of air-conditioning and the other from lightning. The causes of a significant number of system failures (~30%) were not identified. It is interesting to note that software failures and Human-Machine interface errors

2 REVIEW OF INFORMATION

are also identified from NPP operational events (Table 2.1) to be the two leading causes of digital system failures. Additionally, the paper reported the failure rates of digital equipment (processors, memory, input and output) in offshore platform environment and the estimated failure rates of the same in an industrial environment. The environmental effects are not available separately but are included in basic equipment failure rates reported for the applications. The data is used in our analysis of digital system reliability presented in Chapter 7.

Willing and Goldstein [15] discuss radiation effects on the reliability of digital devices associated with the phenomena known as single event latchup (SEL). The latchup of a device involves a massive number of bit errors. The bit errors originate from the upset of a memory bit caused by the passage of ionizing radiation through the device. A bit error is also known as 'soft error' as it causes no permanent damage to the device. In case of latchup, however, the device draws excessive supply current and eventually may suffer permanent damage through overheating. The device operation may experience a lock up, or the device may burnout from such an event. The paper discusses estimating changes in device failure rates as a function of rates of occurrence of SEL. Reliability performance of some example devices in space applications also is discussed.

2.5 Review Summary

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

Our review of NPP operating experience identified EMI/RFI as a stressor. The principal sources of these EMI/RFI were lightning, welding near I&C equipment, sources internal to the equipment, and poor grounding as a causal factor. Furthermore, the failure rates of digital equipment in NPPs appear to be higher than those reported by the military. However, the differences could not be attributed to any specific factor since the quality requirements for military hardware are generally higher than those for commercial-grade equipment used in NPPs. For electronic equipment in general, the military reported a factor of 5 difference in MTBF between military quality equipment and commercial equipment [2], with the latter having the shorter MTBF; this translates roughly into a factor of 5 higher expectation in failure rates of commercial equipment compared to military quality equipment. An overall estimate of failure rate of all digital equipment in NPP environment from NPRDS data shows that this estimate is comparable to the ABB-CE experience, with a factor of approximately 3 lower for processors and memory, and a factor of approximately 7 higher for input and output units.

Information from other published sources yielded qualitative and some quantitative data on stressor effects on the reliability of digital hardware. These are used in stressor risk and system reliability analysis, as appropriate, in the following chapters.

3 FAILURE MODES OF DIGITAL I&C SYSTEMS

In this chapter, we discuss the failure modes of digital I&C systems caused by all sources including environmental stressors. A digital I&C system can be a programmable controller or microprocessor- or computer-based distributed control system. Digital I&C systems function differently than older analog systems and their failure modes can be different. The purpose here is to provide information on the ways in which digital systems can fail and their relevance to plant safety. The focus is on the safety function applications of I&C systems (such as, the reactor protection system (RPS) or the emergency safety features actuation system (ESFAS) in a nuclear power plant, and not on continuous process control applications. Our current task further focusses on the hardware aspects of system failures, although failures from all causes are discussed.

We discuss the failure modes of digital devices identified in literature, and analyze available digital system failure experience in terms of system failure modes. We also discuss some of the failure modes experienced during the recent environmental testing of an experimental digital safety system [16], performed by the ORNL as part of the U.S. NRC's ongoing environmental qualification program for digital I&C.

3.1 Introduction

For safety I&C applications, irrespective of analog or digital implementation of the system, the basic system failure modes of interest are:

1. those which prevent the I&C system from performing its required protection or safety functions on demand, and,
2. those which actuate protection or safety systems without a demand, also known as spurious operation.

System failures belonging to the first type are the most critical since they can lead to unsafe or dangerous plant or process states. Such a situation can arise, for example, from a stuck-on or stuck-off critical output point which prevents the system from responding to a demand. Some potentially critical fault, such as failure of diagnostic of a critical output point, in combination with other faults also can lead to system failure mode of the first type. The second of these two failure modes may or may not be critical. An example for this category would be a component fault resulting in spurious system actuation which leads to unneeded but safe plant shutdown, or which, coupled with other faults or failures, causes process transients and leads to potentially unsafe plant conditions. The question then is how digital-device or -subsystem failures contribute to these I&C system failure modes.

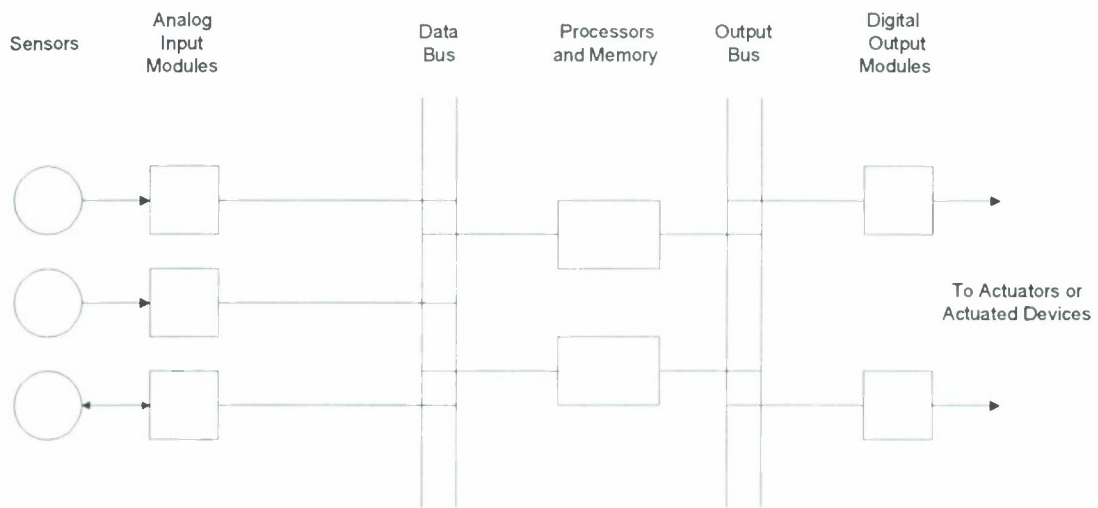
Digital I&C systems can vary widely in terms of system complexity, system architecture, hardware, software, and human interface. Consequently, a generic study cannot predict how a particular system will fail. System-specific analysis is necessary to define failures and identify the applicable failure modes based on functional requirements on the system for safe plant operation. However, a generic study is useful for identifying broad categories of failures which provide insight on some possible, though not necessarily exhaustive, ways digital systems can fail.

While digital systems can be very different in their implementations, the basic hardware elements are

3 FAILURE MODES OF DIGITAL I&C SYSTEMS

essentially the same, process sensors, input and output modules, data processing and logic units, data and communication networks, and actuators. Figure 3.1 shows a simple digital I&C system. Sensors and actuators in a digital system are generally the same as those in analog systems. Consequently, the hardware differences between the digital I&C systems and their analog counterparts lie in the rest of the system building blocks. Failures of digital systems are the results of physical or functional failures of these basic system elements. Section 3.2 discusses typical failure modes of key digital system elements.

Figure 3.1 Basic Digital I&C System



From a system perspective, an important difference between the digital and analog systems is in the architecture. Analog systems generally do not share hardware elements between redundant channels, and a desired level of system reliability is achieved through replication of the needed number of independent channels. Digital systems, however, often rely on components, such as processors, data and communication networks, to process or to transmit multiple signals. Failure of such a key element can lead to critical system failure since multiple channels can be simultaneously affected.

Redundancy in digital systems is often implemented through the concept of "fault-tolerance" which prevents isolated faults or failures from causing overall system failures. For safety systems, redundancy is required to meet regulatory requirements. Fault-tolerance is generally achieved by sharing multiple redundant hardware and by using self-diagnostic features to identify faults and to reconfigure the system once a fault occurs. However, the level of redundancy can vary at different levels of a particular system and some elements of the system may not be truly redundant. For example, undetected failure in a key diagnostic feature, or in the hardware or software used to reconfigure a faulted system, can lead to critical system failure. Reference 17 indicates that in the case of redundant microprocessors with automatic fault-detection and "switch-over" circuitry, the overall reliability may not be any higher than the reliability of the "switch-over" circuitry. The author also raises the issue that faults in such a

3 FAILURE MODES OF DIGITAL I&C SYSTEMS

common module have the potential to prevent both microprocessors simultaneously from functioning properly. For redundant systems, common-cause failures are another concern which can occur from systematic faults in identical hardware and software, and which can defeat the purpose of redundancy. Digital system failure modes are discussed in section 3.3.

3.2 Failure Modes of Digital Devices

Table 3.1, reproduced from Ref. 18, lists the typical failure modes of programmable electronic systems (PES) and input/output devices which should be recognized during the design of the system. The PES includes programmable controllers, distributed control system controllers, or application-specific stand-alone microcomputers. Reference 18 cautions that the PES may have many failure modes which are difficult to recognize and some of which can be unsafe.

It is difficult to predict generically what the effects of individual device failure modes will be on overall system function since the ultimate effects will depend on the system characteristics, such as its architecture and/or self-diagnostic capabilities. A particular system may be able to diagnose and isolate specific faults thus allowing for fault-tolerance, and the system reconfigured based on available resources. Some of the failure modes cited in Table 3.1 can be critical or potentially critical for system function. For example, the effects of Arithmetic Logic Unit (ALU) faults or stuck input/output bits in PES can both be severe. ALU faults will typically result in errors in calculations involving data, and may prevent the system from performing its designated function. However, the impact of ALU faults can be reduced by engineering design, such as using software logic to check the calculations and rejecting any inconsistent output. On the other hand, generally it is impossible to predict the effect of a stuck bit because it depends on where the failure occurs in the system. The impact of the stuck bit will also depend on whether it is in the data path or in the final actuation logic. A stuck bit can cause system failure if it occurs at a critical output point. Error-checking codes may be able to detect this problem; redundant output may be another solution.

Some of the failure modes listed in Table 3.1 can also be triggered by stressors as was observed during environmental testing of an experimental digital safety system by Oak Ridge National Laboratory [16]. Among these were parity generator fault, timeout, loss of input/output communication, and frame fault/buffer overrun. A brief discussion of the faults and their potential implications on system function follows.

A parity generator fault may allow single-bit errors to go undetected, resulting in communication of erroneous data which may prevent the system from performing its necessary functions. A timeout typically indicates that a communication port (e.g., serial, network) may have waited for a specified amount of time without receiving the desired information. If this information is critical to the system's operation, it may result in system failure, but its impact can be reduced by introducing redundant channels in system design. Loss of input/output communication will typically result in no data being input to the system, or no data being output; the result may be a loss of system function. Again, the impact can be reduced by designing redundant input/output. A frame fault/buffer overrun typically occurs in data communication (e.g. serial data communication). Systems can be designed to detect such errors. Problems of this type may result in communication failure.

3 FAILURE MODES OF DIGITAL I&C SYSTEMS

**Table 3.1 Typical Programmable Electronic Device Failure Modes
(Reproduced from Reference 18)**

Device(s)	Failure Mode	Device(s)	Failure Mode
PES	stuck bit/multiple bits dynamic faults/x-talk instruction time/wait states/stall μ Code/macro code Arithmetic Logic Unit (ALU) faults access time wait state logic access time stuck Interrupt Request (IRQ) stuck/loss of timing device specific (custom IC) stuck Input/Output bit x-talk on Input/Output lines wrong Input/Output line data direction fault (I/O Port) signal too fast/slow (I/O Port) lost bit/byte/message (comm) wrong sender/receiver/message timeout/multidrop conflict deadlock (comm) parity generator fault frame fault/buffer overrun stuck Direct Memory Access (DMA) x-talk (DMA) loss of Input/Output communication Bus request stuck (DMA) Transfer time incorrect (DMA) wrong sample time timer register fault wrong timer timeout/overrun timebase fault set/reset fault IRQ/poll fault (timer) trigger pattern (WDT) trigger too early/late (WDT)	INPUT	stuck on/off upscale/downscale/conversion fault drift/calibration unstable Input isolation Fault linearization/compensation
		OUTPUT	stuck on/off/conversion fault upscale/downscale drift/calibration unstable output isolation fault linearization/compensation

3.3 Failure Modes of Digital Systems

Operational experience with digital I&C systems in NPPs show that various failure causes of hardware, software, human interactions, and of environmental stressor origin contribute to system failures. Failure events in digital I&C systems also can be categorized as independent or random failures and dependent or common-cause failures. Hardware failures can be random or systematic due to common flaw in manufacturing or due to external factors, such as the operating environment. Random failure of hardware, as discussed in the earlier section, seldom causes overall system failures in fault-tolerant digital systems. Software failures can be termed functional failures, that is system failure occurs only under a specific set of operating conditions. Under all other circumstances, the system can perform the required functions. Reference 14 states that even a single failure in a software has the potential to disable an otherwise redundant digital I&C system. Human interaction-related failure occurs in interfacing with the system during operation or maintenance. Hardware redundancy as a means of achieving high system reliability can be offset through human-interaction errors since such errors have the potential to affect multiple channels of the system. Environmental stressors can also impair multiple channels when physically located in the same or a similar environment. The following three sections summarize failure experience with digital I&C systems documented in the literature, and failure experienced during recent environmental testing of an experimental digital control system.

3.3.1 Experience at U.S. Nuclear Power Plants

Reference 7 lists digital system failures from 1990 to 1993, identified from Licensee Event Reports (LERs). The systems involved in the events included plant protection and safety systems as well as various control and monitoring systems. Both independent (random) failures and dependent failures (common-cause) are included. Although the systems involved in the events are not all relevant for plant protection and safety, and are not always redundant systems, the events provide insight on the ways digital I&C systems can fail.

Table 3.2 categorizes the events in terms of system functions. The categories are somewhat arbitrary but are based on descriptions of events and keeping in mind the system failure modes of interest described in Section 3.1. The events are broken down into categories for each failure cause, such as hardware, software, human interactions, and environmental stressor (EMI).

The first column in Table 3.2 lists causes for the failures as identified in Ref. 7. The next five columns show the number of failure events by types. The failure types are self-explanatory from the column headings except for the heading "others" that includes miscellaneous failures which could not be categorized.

3 FAILURE MODES OF DIGITAL I&C SYSTEMS

Table 3.2. Digital I&C System Failure Events in U.S. NPPs

Cause	Number of Events			
	Spurious Trips and System Actuations	Loss of Monitoring or Control Function	Incorrect or Incomplete Parameter Evaluation	Others
Hardware	4	5	0	0
Software	2	7	5	15
Human Interaction	6	8	2	10
EMI	10	4	0	1
Total	22	24	7	26

The events under the "spurious trips and system actuations" category include protection and safety system actuations when such actions were not needed. Most of these events were caused by EMI which introduced spurious signals in the system or caused by some key system component, such as a microprocessor, to malfunction. Human interaction errors were also a key contributor to event frequency in this category. Single points of hardware failures and malfunctions which caused spurious trips or system actuations point to a lack of adequate hardware redundancy in some of these systems.

Several events in the "loss of monitoring or control function" category also were due to the unavailability of a critical system component, such as a microprocessor or a computer. Loss of monitoring or control function can be critical for plant safety, particularly under abnormal or accident conditions and if such failures remain unannounced. A frequent causal event for human interaction error in this category was incorrect entry in software. Software configurations, as well as, software verification and validation errors, were also frequent contributors to the loss of monitoring and control functions category.

Incorrect or incomplete parameter evaluation is another concern for digital systems since they can remain undetected and have the potential to lead to critical system failure, such as not providing trip signal when the process parameter levels required such a trip to assure plant safety. Events under this category were caused by software errors and by human-interaction errors; these included incompatible software and hardware, corrupted data, inadequate procedure, and misoperation.

The bulk of the events under the "others" category included violations of technical specification (TS) requirements. Inappropriate or nonconservative setpoint settings (human interaction error) were responsible for system failures in three cases.

3.3.2 Other Experience of Digital Control System Failure

Paula and Roberts [14] reported 35 common-cause failure (CCF) events affecting multiple channels from a collection of 10 fault-tolerant digital control systems from a diverse group of industries. The CCF experience was

3 FAILURE MODES OF DIGITAL I&C SYSTEMS

based on a cumulative operating history of 90 system-years. The systems are generally redundant but use identical hardware and software on redundant channels. Nine out of these 10 systems are 1-out-of-2 redundancy type, while the other one is a 2-out-of-4 high-integrity protection system. Table 3.3 summarizes these failures for relevant common-cause events.

Software failures lead all CCFs followed by operations/maintenance. The hardware common-cause event reported was in the high-integrity protection system with an operating history of 3 years; the CCF was caused by common hardware defect in redundant channels. The system also suffered seven single channel failures during the same period. The "other" category contains two failures caused by environmental stressors, one from high-temperature due to the failure of air-conditioning, and the other from lightning disabling multiple computer equipment. The rest of the events in this category are associated with power supply failures. It is not clear whether these failures are due to common power supply or to common-cause affecting multiple power supplies. The failure cause for 11 of the CCF events were not identified. Additionally, 23 events are reported which are not included in Table 3.3 and which are failures in common hardware including network and data storage equipment. One of the ten systems experienced no CCF nor any other failure during operation for 10 years.

Table 3.3 Common-Cause Failures of Multiple Channels in an Assortment of Ten Digital Systems (data from Ref. 14)

Common Cause	Number of Events
Hardware	1
Software	9
Operational/Maintenance	7
Other	7
Unidentified	11

3.4 Summary

In reviewing failure modes of digital I&C systems, our study identified several incidents of spurious operation of such systems in NPPs. However, these events generally led to more conservative plant configurations through inadvertent and unneeded operations of safety systems. None of these events has resulted in failure of the system to perform its essential safety functions. In only one event identified in Ref. 8, a software deficiency in a digital I&C-based protection system caused the system to fail to set a trip output. Nevertheless, the trip was accomplished through a redundant trip output. In some instances of stressor effects, multiple redundant equipment were affected. Such failures are an important concern for plant risk considerations because of the possibility of loss of redundancy in safety systems.

4 APPROACHES FOR EVALUATING RISK-SENSITIVITY OF ENVIRONMENTAL STRESSORS

In this chapter, we present approaches for evaluating the risk-sensitivity of environmental stressors. The results are used to screen the stressors. The steps in determining the risk-sensitivities are discussed.

4.1 Introduction

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

4.2 Risk-Sensitivity of a Stressor

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

1. The likelihood of the stressor,
2. The components affected by the stressor,
3. The increase in failure rates of the affected components, and
4. The risk contribution from the affected components.

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

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

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

4 APPROACHES FOR EVALUATING RISK-SENSITIVITY

then

$$C' = LF^N C \quad (4.1)$$

In words, this relationship can be expressed as

$$\begin{matrix} \text{Plant Risk Including} \\ \text{Stressor Effects} \end{matrix} = \left\{ \begin{matrix} \text{Stressor} \\ \text{Likelihood} \end{matrix} \right\} \times \left\{ \begin{matrix} \text{I\&C Failure} \\ \text{Rate Increase} \end{matrix} \right\}^N \times \left\{ \begin{matrix} \text{I\&C Risk} \\ \text{Contribution} \end{matrix} \right\} \quad (4.2)$$

The increase in CDF contributions due to a stressor then can be obtained by quantifying or estimating ranges for L and F. The equation applies for stressors which systematically degrade equipment and cause their failure rate to increase. When the stressor is assumed to occur, i.e. L=1, equation 4.1 reduces to

$$C' = F^N C \quad (4.3)$$

We assumed that the stressor has the same effect on failure rates of all relevant components. However, if these effects differ, then the term F^N in Equation 4.1 is substituted by $\prod F_i$, where

$$\prod F_i = \begin{matrix} \text{the product of factor increases, } F_i, \in \\ \text{failure rates of individual} \\ \text{I\&C basic events, } i, \text{ affected by the stressor.} \end{matrix} \quad (4.4)$$

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

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

then

$$C' = (fpT_i/2)C/\prod u_i \quad (4.5)$$

where the term in the parenthesis is the unavailability of the I&C basic events in the cutset affected by the stressor, and where $\prod u_i$ is the product of the unavailabilities of the affected I&C basic events in the cutset .

In general, equations 4.1, 4.3, and 4.5 apply where there is one dominant combination of equipment failures (i.e. one dominant minimal cutset) which contributes to the CDF. If there are several dominant

4 APPROACHES FOR EVALUATING RISK-SENSITIVITY

combinations, then C' is determined from each combination, i.e. each minimal cutset, using the above formula and then summed over the contributions.

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

$$S = (C' - C) / C_{\text{TOTAL}} \quad (4.6)$$

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

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

The risk-sensitivities for a set of stressors can be presented by determining S for each stressor using the estimated values for L , C , F , and N . The relative risk-sensitivities for different stressors can then be compared, or the results can be used to identify risk-significant stressors. This approach is demonstrated in chapter 6 for an example NPP.

4.3 Basic Steps in Determining the Risk-Sensitivities of Stressors

The following are the basic steps involved in determining the risk-sensitivities of stressors:

1. Identify potential stressors
2. Evaluate the likelihood of each stressor
3. Evaluate the stressor effects on the occurrences of I&C failure
4. Determine the risk contributions, i.e. the impact of components failures caused by stressors

Identify potential stressors

Potential stressors are identified in this step which can affect the performance of digital instrumentation and control equipment. Sources of information can be manufacturers specifications, historical operating experience with both digital and analog equipment, test and research studies, and expert opinion. Identification should include a

4 APPROACHES FOR EVALUATING RISK-SENSITIVITY

description of the stressor, the environments or situations in which it can arise, and its effects on the equipment, including physical characterizations. Bases for the information should be given, including any documented and historical data.

Evaluate the likelihood of each stressor

The likelihood should be estimated of each stressor occurring during plant operation including normal operation and possible abnormal or accident conditions. The estimates of probabilities of occurrence should include historical data, engineering knowledge, and expert opinion.

The likelihood of a given stressor can be separated into two factors. The first is the likelihood of the environment or the operational conditions which can give rise to the stressor. The second is the likelihood of the stressor actually occurring in the environment. If more than one environment or situation can give rise to the stressor, then the product of the two factors is summed for the different environments.

Evaluate the stressor effects on the occurrences of I&C failure

This step consists of two intermediary steps:

1. identify the I&C components which can be affected by the stressor.
2. model the effects of the stressor on the component's reliabilities or failure rates.

Identifying the I&C components affected by the stressors involves identifying, for each stressor, the types of I&C components which can be affected and the environments and activities in which the stressor can occur. Each I&C component in the plant (or in the Probabilistic Risk Assessment (PRA), if a PRA is used) then is evaluated to determine if it is of the type affected and is in the stressor-inducing environment. Instead of evaluating individual components, the I&C components in the plant or PRA can be grouped by similar design and environment and the groups evaluated. The result will be a set of potentially susceptible I&C components for each stressor.

Modeling the effects of the stressor on the component's reliabilities involves estimating the changes which can occur in the failure rates of components. Also, estimates are needed of any common-cause failure probabilities associated with the occurrence of the stressor; these can be either relative or absolute assessments. For relative assessments, the effects of the potential stressors can be expressed in terms of relative changes in failure rates or failure probabilities (environmental factors) over some reference failure rates. The risk results based on such estimates will only provide relative changes in plant risk. Alternatively, if absolute values of plant risk are to be determined for a particular set of equipment, environment, and stressors, then absolute values of reliabilities or failure rates must be estimated.

4 APPROACHES FOR EVALUATING RISK-SENSITIVITY

As a conservative bounding approach for modeling the stressor's effects, the components which are affected can be assumed to be failed by the stressor. This approach will maximize the effects of the stressor, and will result in conservative assessments of risk which can be more accurately evaluated at a later time with more accurate data.

Determine the risk increase due to component failures caused by stressors

In this step, the risk impacts of the component failures are determined for those components affected by the stressors. This can be done most directly in a PRA by failing the affected components and recalculating the risk (e.g., core damage frequency) with the components failed. Sensitivity studies can be carried out by varying the increases in failure rate and common-cause failure probabilities; this will give ranges in the risk. The recalculated risk values can be used for either relative or absolute evaluations of the effects on risk from the stressors.

Risk-significant components can also be identified from evaluations carried out in this step; they are those components whose failure or whose change in reliability will significantly increase risk. Both individual I&C equipment and combinations of I&C equipment which are jointly risk-significant can be identified. Sets of jointly risk-significant I&C components will be the bases for evaluating stressors which can affect all the components in the set. Available PRA importance techniques can be used, provided they are extended to identify jointly important sets of components.

The final step in evaluating the stressor risk effects involves multiplying the likelihood of the stressor determined in Step 2 by the risk increase due to component failures as determined in Step 4, above. The risk effects of each stressor is thus the product of the likelihood times the effect.

5 ASSEMBLING DATA FOR EVALUATING RISK-SENSITIVITY OF STRESSORS

The basic information needed to evaluate the risk sensitivity of environmental stressors in NPPs is information which links the stressors to occurrences of equipment failure. This information can be used as input to appropriate plant reliability and risk models to evaluate effects on plant risk. In this chapter, we discuss the information available on specific stressors and assemble the data to be used in evaluating the risk sensitivity of stressors.

5.1 Basic Objectives and Approach

Our review of the literature shows that although there is no directly applicable information on failures of advanced digital equipment in NPP environments, there are different pieces of information on stressor effects on these equipment in various other applications. The objective, therefore, is to define approaches to adapt such information for NPP applications.

Based on our review, the available information on stressor effects can be classified into the following broad categories:

1. Failure mechanisms associated with specific stressors.
2. Failure rates of digital I&C components in different environments.
3. Changes in components' failure rates in different environments.
4. Descriptions of equipments' susceptibilities to stressors.
5. Operational experience indicating the adverse effect of specific stressors.

Diversity in the type of the available information also indicates that different approaches are necessary to best utilize all the data on stressor effects.

The simplest approach in assessing risk-significance of environmental stressors requires information on their individual effects on the equipment. Most available information, however, is on the synergistic effects of multiple stressors. The military approach to assessing environmental effects on various equipment, including digital equipment, has been to determine these effects for a set of application environment categories; the logic behind this is that environmental effects are seldom a consequence of single stressors. The synergistic effects of multiple stressors generally are the cause of many of the stressors' effects. For example, corrosion can be influenced by both the humidity and the temperature at the location of the device. Further, the effects of environmental stressors are quite dependent on the technology used. Much of the data on the performance of advanced digital equipment are not from controlled laboratory tests, as the diversity of technology and manufacturing differences would make this prohibitively expensive, but from the field where the equipment are subjected to several stressors simultaneously, and, consequently, their combined effect is reflected in performance. Such information can be used

5 ASSEMBLING DATA

to assess the overall risk impact of the stressors, but it is difficult to use directly to assess the risk-impact of individual stressors.

Information which refers to a single environmental stressor is most directly useful and can be used to evaluate individual stressors, or to modify information on the combined effects of a specific environment to account for differences in the parameters. Where there is information on the synergistic effects of various stressors, comparative analyses can identify the dominant stressor(s) which influence the equipment's performance by comparing the environments. The difference in performance then is attributed to these dominant stressor(s). Such analyses, while not precise, can be useful for order-of-magnitude comparisons of a stressor's risk effects. In the following, the information on stressor effects on digital equipment are analyzed, and adapted for risk-sensitivity evaluations using approaches which are suited to the data.

5.2 Temperature

Temperature was cited in Ref. 2 as an important stressor which accelerate the degradation and failure of digital equipment. The associated component failure mechanisms are electrical shorts and open circuits. However, these failures result from sustained operation in high temperatures, and not from a transient change in operational temperatures. No discussions on the short-term effects of temperature on digital equipment were identified in the literature, possibly because environmental qualifications require that equipment temperatures under normal and postulated abnormal or accident conditions do not exceed specified maximums. Ref. 2 gives a table on temperature-based conversion factors for equipment MTBF (mean-time-between-failures); however, these factors are estimated for a collection of discrete semiconductor devices and integrated circuits, and not separately for digital equipment. This table, reproduced as Table 5.1, shows the temperature-dependence of MTBF. A range for maximum expected temperatures considering normal, abnormal, and accident conditions in the control building in a PWR plant is between 24 and 40 degrees C (lower number for control room, higher number for cable spreading room or switch-gear room). Assuming temperature conversion factors in Table 5.1 are bounding values for change in MTBF of all equipment including digital microcircuits, the maximum change in MTBF over this range is approximately 1.1 or about 10%. Assuming a negligible time to repair the equipment (valid for most failures) compared to mean-time-to-failure, this translates into a change in the equipment's failure rate by a factor of approximately 1.1, where the failure rate is inverse of MTBF (assuming negligible mean time to repair equipment compared to the mean time to failure).

Our review of data [16] from environmental tests of digital I&C systems conducted at ORNL for temperatures of up to 160 degrees F (approximately 71 degrees C) gave no conclusive evidence of the dependence of short-term performance on temperature. There were some communications errors reported in these tests which, in one case, tended to increase statistically with temperature. However, the same pattern was not observed in similar tests. Consequently, we could not extract any data from the ORNL tests for risk sensitivity analysis.

Table 5.1 Temperature Conversion Factors (Multiply MTBF by)

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

5.3 Humidity

Humidity, as an agent in the corrosion process, was cited in Ref. 6 as the largest single risk factor in the reliability of microcircuit devices. Corrosion can degrade equipments' reliability by attacking the connector pins, exposed contact surfaces, and unprotected metallization runs which serve as conductive interconnects of metal film between elements of the integrated circuit and as bonding pads for external connections. While corrosion is an important concern for all microcircuits, it is more so for today's high-density microprocessors and other digital circuits because of their closer interconnect spacings and thinner metallic sections used to achieve the needed compactness. The failure mechanism associated with corrosion is an open circuit. While commercial plastic-encapsulated devices are more vulnerable to moisture ingress and subsequent corrosion, this process also was reported for more robust hermetically sealed microcircuits. In the presence of appropriate contaminants, humidity can significantly reduce the service life of microcircuits. Corrosion also depends on environmental temperature which affects moisture condensation, the first step in the process. Temperature can also affect moisture permeation within the device and chemical reaction rates.

Corrosion models are given in Ref. 6 to calculate the component's time to failure. These models separate the time to failure into two time elements, the time necessary for the moisture content within the package to reach a threshold level to support corrosion, and the time needed for the corrosion process to terminate in component failure. Time needed for moisture ingress to reach threshold level is generally far smaller than time for corrosion processes to cause failure. Consequently, corrosion time to failure can be approximated by the latter. The corrosion process depends on the type of circuit package, material, and environmental conditions. Correlations were developed [6], as shown in equation 5.1 below, based on analysis of test data, which provide acceleration factors for microcircuit failure times through corrosion in terms of temperature-humidity environment. Details on the corrosion model are presented in Ref. 19. The correlation is as follows:

$$k = \frac{7.6 \times 10^6}{(RH)^{-3} \exp [10444 / (T + 273)]} \quad (5.1)$$

5 ASSEMBLING DATA

where

- k : temperature-humidity environmental acceleration factor
- RH: relative humidity in percent
- T: temperature in °C

Component time-to-failure is inversely proportional to k . Using this correlation for the temperature range and humidity levels for NPP locations of interest, we generated Table 5.2 for k . The correlation factors are normalized to control room environment (24° C and 60% relative humidity) to illustrate the effects of temperature and humidity on time-to-failure through corrosion. For example, if the operating temperature increases from 24° C to 30° C at 60% relative humidity, the component's time-to-failure is shortened by a factor of 2.01. Similarly, if the humidity level changes from 60% to 100% relative humidity at 24° C, the time-to-failure is decreased by a factor of 4.63. In the calculations presented in Chapter 6, these factors are used to modify I&C failure rates in the PRA.

**Table 5.2 Factor Reduction in Digital Microcircuit Device Time-to-Failure Due to Corrosion
(Normalized to 24° C and 60% Relative Humidity)**

Temperature °C	% Relative Humidity					
	50	60	70	80	90	100
24	0.58	1.00	1.59	2.37	3.38	4.63
30	1.16	2.01	3.19	4.76	6.77	9.29
40	3.49	6.03	9.58	14.31	20.37	27.94
50	9.81	16.96	26.93	40.19	57.23	78.50

5.4 Vibration and Shock

Microprocessors and other digital microcircuit devices are structurally quite rigid and hence, not very prone to vibration-induced damage at the device level. Ref. 6 cited literature to indicate that vibration forces encountered in the field are rarely severe enough to cause fatigue and damage in individual devices. Large components in assembled systems are likely to fail much earlier.

At the device level, one concern with vibration is possible bond damage. However, Ref. 6 indicates that for military ground and airborne applications, excitation frequencies encountered in the field (from ~5Hz to ~2000Hz) are much lower than that necessary to excite wire bonds in these devices. Environments for microprocessor-based I&C systems in NPPs are not expected to include vibrations which are either higher in frequencies or in amplitudes than that encountered in various military applications, particularly since the latter include driven equipment often with components with reciprocating motion. Seismic frequencies that are of importance also lie in the low end of this frequency range. Control building locations in NPPs generally do not contain any significant sources of vibration. However, in some locations in the auxiliary building, there can be sources of vibration from mechanical equipment.

The information reviewed in this study did not yield any data directly relating vibration to the failure of digital equipment. However, the environmental factors reported in Ref. 2 for various categories of military application include the effects of vibration, particularly in some airborne applications and for equipment mounted on projectiles. These environments can be taken into account in making assumptions about the possible range of vibration effects on digital equipment in NPPs.

From a review of military application categories in Table A3 in Appendix A, we assumed that vibration for digital equipment in NPPs probably will not be worse than that for equipment installed in rotary-winged equipment (military category: ARW), such as on helicopters. A low end for vibration/shock effect can be assumed as that experienced by equipment installed in vehicles on ground (military category: GM). It also was assumed that the differences in equipment failure rates among ground fixed (GF), GM, and ARW applications can be attributed primarily to the differences in vibration/shock in these environments. A check from Ref. 2 on the failure rates of several categories of digital equipment in GM and ARW environments, presented in Table 5.3, shows that these rates vary by a factor from less than 2 (for GM) to a factor of approximately 4 (for ARW) compared to failure rates in a GF environment (assumed no vibration/shock). Therefore, a possible range of up to a factor of 4 change in failure rates over the base rate is assumed for equipment in NPP locations of interest which may be caused by vibration.

**Table 5.3 Failure Rates of Selected Digital Equipment
(Failures per Million Hours)**

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

Note: GF: Ground Fixed, GM: Ground Mobile, ARW: Airborne, Rotary winged

5.5 Radiation

Radiation can have several effects on digital I&C equipment: degradation due to accumulated dose, upsets of memory bits or flip-flops due to an ionizing radiation, and latchup of susceptible components induced by an

5 ASSEMBLING DATA

ionizing radiation. The effects of accumulated radiation are determined by the total dose exposure which is incurred by the equipment during an accident, or during its normal operational life. If this exposure is above the limit established for the equipment, then it can fail or perform abnormally. For I&C equipment located in control building areas, no significant dose exposure during normal operation is expected to occur. Also, since the control room is isolated and well controlled, PRAs do not identify any accidents which cause exposure in the control room. Accumulated dose tolerances for digital equipment, expressed by dose hardness levels (see Table A2 in Appendix A), are significantly higher than that expected in control building environments (1E+3 RAD for a plant lifetime of 40 years). For single event latchup events discussed in section 2.4, data presented in Ref. 15 on some CMOS devices in low-orbit space applications indicate that the device reliability may still be acceptable (device failure probability from latchup events approximately within 10% of random failure rates). Such an environment is characterized by highly ionizing cosmic rays, proton fluxes produced by solar flares, and trapped charged particles in radiation belts by the earth's magnetic field. Since digital I&C upgrade equipment are expected to be located in plant areas where there are no significant ionization sources, radiation does not appear to be a likely stressor through latchup events for these systems.

5.6 EMI

EMI events in digital I&C systems in NPPs have been documented in LERs. As discussed in section 2.3, in a study of LERs for 1990-1993, EMI was identified as the root cause contributing to a significant number (~19%) of system malfunctions or failures. EMI was the only stressor specifically identified. EMI-related failures of microprocessor-based systems in other industries also have been reported [11].

Of the EMI sources identified, there is a significant amount of information only for lightning-related events. Lightning is also a significant source of plant trips and ESF actuations as compared to all other sources of EMI events in NPPs [3]. Consequently, efforts were made to develop estimates of the frequency of lightning-related EMI events in NPPs to evaluate its risk-sensitivity.

In a study on surge-protecting devices in U.S. NPPs from 1980 to 1994 [12], 199 lightning-related events were reported, including loss-of-offsite power (LOOP), partial LOOP, engineered safety feature actuations or equipment failures. Twenty-nine of these events could be attributed to perturbations or failures of I&C systems resulting from electrical spike or noise generated through electromagnetic couplings, and involved both digital and analog systems. Details on these 29 events are given in Table B1 in Ref.[10]. The number of reactor years of operation during 1980-1994 for all operating U.S. nuclear plants was estimated at 1409.4 years [12].

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

$$f_{emi} = \frac{N_{emi}}{N_{RY}} \quad (5.2)$$

where

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

Then,

$$f_{emi} = \frac{29}{1409.4} = 2.1E-02 / plant-yr \quad (5.3)$$

A conditional probability, p , of I&C equipment failure of 1.0 is assumed for these events. Such failures may be detected immediately or within a short span of time following failures, or may remain undetected for some time period. A recent study [20] based on three system-years of operational data on failures in the Eagle 21 system indicate that over 70% of these failures were detected during maintenance while the rest were detected during normal operation. For estimating risk-sensitivities, we consider two possibilities in this regard: 1) early detection, i.e., failures are detected during shift checks (12 hourly), and 2) late detection, i.e., failures are detected during scheduled surveillance tests (Surveillance Test Interval or STI = 31 days, typical for safety systems, such as the ESFAS [21]).

The equipment unavailability, q , due to lightning-related EMI events can then be obtained as:

$$q = f_{emi} \times p \times \frac{Ti}{2} \quad (5.4)$$

where

f_{emi} is as defined by equation 5.2,
 p is the conditional probability of equipment failure given the event, and
 Ti is the failure detection interval

Then, the unavailabilities q , are

$$q_{12\ hours} = 2.1E-02 \times 1 \times \frac{12}{2 \times 24 \times 365} = 1.4E-05 \quad (5.5)$$

$$q_{31\ days} = 2.1E-02 \times 1 \times \frac{31}{2 \times 365} = 8.8E-04$$

5 ASSEMBLING DATA

The unavailability values estimated are the probabilities that the affected equipment will be unavailable and unable to function. The unavailabilities calculated are averages over all U.S. plants. The number of events occurring in a particular plant and, consequently, the unavailabilities, will depend on the thunderstorm activities in the region where the plant is located. To provide a perspective, in the United States, the average number of thunderstorms varies from a low of 10 per year in the northwest to as high as 100 per year in some parts of the south [11], or a factor of 10 difference in frequency between the high and the low.

Assuming a factor of 10 difference also between high and low values of equipment unavailabilities (since f_{emi} is directly proportional to the number of lightning-related EMI events) and using $q_{12 \text{ hours}}$ and $q_{31 \text{ days}}$ calculated above as the mid-value between the high and the low, the following range is obtained for equipment unavailabilities:

$$\begin{aligned} T_i = 12 \text{ hours} \quad q_{\text{high}} &= 4.4E-5, \quad q_{\text{low}} = 4.4E-06 \\ T_i = 31 \text{ days} \quad q_{\text{high}} &= 2.8E-3, \quad q_{\text{low}} = 2.8E-04 \end{aligned} \tag{5.6}$$

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

5.7 Smoke

The environmental testing of an experimental digital safety channel by the Oak Ridge National Laboratory also included exposing the system to different densities of smoke in a chamber. The tests were conducted at the Sandia National Laboratories. Ref. 22 documents details of the tests. The system's performance was monitored during smoke exposure and for a period after smoke was vented out of the chamber. Different ambient temperature and humidity conditions were maintained in the chamber during the tests. The equipment's susceptibility was tested at three different levels of smoke densities corresponding to

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

The fire scenarios were developed earlier as part of a fire-risk study [23].

The results from these tests were used to make assumptions about smoke-density thresholds for equipment malfunction and damage. The data from eight tests showed that in six involving different smoke densities, the system experienced either communication errors, network errors, or nibble errors. Communication errors were observed at all three levels of smoke. The severity of the errors generally increased with increased smoke density, and 41 percent of all errors were later classified as potentially unsafe [24]. Although some of these errors possibly can be avoided in a real system through design, for risk-sensitivity evaluations, we assumed that the digital system would be vulnerable to all three levels of smoke.

The fire frequencies were used as surrogates for frequencies of smoke occurrences in relevant areas of the plant in the absence of any available estimates on the latter. Table 5.4 shows the fire frequencies in control room area developed for SURRY [25], and used in calculating smoke risk-sensitivity (presented in section 6.6)

Table 5.4 SURRY Fire Initiating Event Frequencies in Control Room

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

Again, as in the case of EM1 events, assuming a conditional probability, p , of I&C equipment failure of 1.0 from smoke events, estimates of equipment unavailability, q , due to smoke events can be obtained as follows:

$$q = f_{smoke} \times p \times \frac{T_i}{2} \quad (5.7)$$

where

- f_{smoke} is the frequency of smoke events,
- p is the conditional probability of equipment failure given the event, and
- T_i is the failure detection interval

Using the fire event frequencies given in Table 5.4 and applying equation 5.7, Table 5.5 gives our estimates of unavailabilities of I&C equipment due to smoke in control room area for two different failure detection intervals, 12 hours (Shift Check) and 31 days (Surveillance Test Interval). These values are the probability that affected equipment will be unavailable and unable to perform its intended function.

Table 5.5 Estimated I&C Unavailabilities from Smoke Events in Control Room

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

5 ASSEMBLING DATA

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

Environmental conditions in a NPP can be categorized broadly as those inside the containment and those in other plant areas, such as the control building and the auxiliary building. Environmental conditions in the containment areas can be very harsh with high levels of temperature and radiation. However, digital I&C equipment is generally located in the other areas where the environmental conditions are not so severe. For example, for SURRY I&C equipment which is modeled in the PRA and documented in Ref. 26, only the process sensors are located within the containment; other I&C equipment are located in the control room, relay room, and the auxiliary building. All safety-related control cabinets are located in the control building. Equipment in the control room is expected to receive negligible radiation exposure. Table 5.6, edited from Ref. 27, shows environmental conditions under normal and other situations in control building areas where the I&C cabinets may be located. The abnormal condition refers to loss-of-offsite power (LOOP). The accident condition is a loss-of-coolant-accident (LOCA) coupled with a LOOP.

Table 5.6 Environmental Conditions in Selected Areas of the Example PWR

Area	Condition [†]	Temperature (°F)		Humidity (%)		Radiation (RADS*)
		Max.	Min.	Max.	Min.	
Main Control Room	Normal 1	75	70	60	30	1E+03
	Abnormal 3	75	-	-	-	1E+03
	Accident 1	75	-	60	-	1E+03
Cable Spreading Room	Normal 1	104	55	60	3	1E+03
	Abnormal 3	95	-	-	-	1E+03
	Accident 1	95	-	60	-	1E+03
Switchgear Room	Normal 1	104	55	60	3	1E+03
	Abnormal 3	104	-	-	-	1E+03
	Accident 1	104	-	60	-	1E+03

*cumulative dose over 40 years

[†] Normal 1: full power operating conditions

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

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

6 RISK-SCREENING OF ENVIRONMENTAL STRESSORS IN AN EXAMPLE PLANT

In this chapter, we discuss our study using a NUREG-1150 plant PRA to estimate the increases in the contributions of I&C equipment to core damage frequency (CDF) which could potentially occur due to the deleterious effects of environmental stressors on digital I&C equipment used at the plant. These increases are subsequently used to screen the risk-significance of the stressors. The approach developed in Chapter 4 is used to estimate the increase in I&C contributions to the CDF due to stressors.

6.1 Example Case

The SURRY Unit 1 Integrated Risk and Reliability Analysis System (IRRAS) PRA Data Base [28] is used in the following way in the evaluations:

- The PRA is used to generate a list of minimal cutsets.
- The minimal cutsets containing I&C basic events are then identified .
- Where environmental stressors and their levels are known for possible plant locations of digital I&C equipment, the likelihood of these stressors is taken to be 1 in calculating their effects on the increase in I&C contributions to the CDF.
- Where there is information on the effects of stressors on I&C failure rates in the form of environmental factors, the basic event probabilities are accordingly modified, and used to recalculate increases in I&C contributions to CDF.
- Where environmental stressors possibly could cause multiple I&C equipment failures, the probabilities of such failures are used to estimate unavailabilities for relevant I&C basic events, and the corresponding CDF contributions are calculated.
- The CDF contributions from each of the minimal cutsets containing I&C basic events are summed to obtain the total contribution from the affected equipment.
- The sum of the I&C contributions to CDF is divided by the plant's baseline CDF to obtain the relative changes in risk from I&C due to stressors.
- These relative changes form the basis for screening the environmental stressors for risk-significance.

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

Table 6.1 lists the I&C basic events modeled in the SURRY PRA. Column 2 shows the basic event identifier represented by system-component type-failure mode-component identifier. The I&C components associated with the event are listed in the third column. The actuation trains typically include process sensors, switches, logic systems, and associated relays. Column 4 shows the corresponding physical location of the I&C components to correlate with the potential effects of environmental stressors; these data were obtained from Ref. 26.

6 RISK SENSITIVITIES

Table 6. 1 I&C Basic Events Modeled in Surry PRA

No.	Basic Event	Components	Location
1	AFW-ACT-FA-PMP3A	process sensor ESF bistables relay logic network master relays slave relays	containment control room relay room relay room relay room
2	AFW-ACT-FA-PMP3B	process sensor ESF bistables relay logic network master relays slave relays	containment control room relay room relay room relay room
3	AFW-ACT-FA-VLVA	process sensor ESF bistables relay logic network master relays slave relays	containment control room relay room relay room relay room
4	AFW-ACT-FA-VLVB	process sensor ESF bistables relay logic network master relays slave relays	containment control room relay room relay room relay room
5	CLS-ACT-FA-CLS2A	pressure sensor signal comparator 3/4 relay logic control relay	containment control room relay room relay room
6	CLS-ACT-FA-CLS2B	pressure sensor signal comparator 3/4 relay logic control relay	containment control room relay room relay room
7	CPC-ICC-FA-CCPBS	temperature sensor control relay	aux. building aux. building
8	CPC-ICC-FA-SWPBS	differential pressure sensor control relay	aux. building aux. building
9	CPC-ICC-FA-TCV8B	temperature sensor control relay	aux. building aux. building

Table 6.1 I&C Basic Events Modeled in Surry PRA
(continued)

No.	Basic Event	Components	Location
10	CPC-ICC-FA-TCV8C	temperature sensor control relay	aux. building aux. building
11	RMT-ACT-FA-RMTSA	level sensor 2/4 relay matrix relay	containment relay room relay room
12	RMT-ACT-FA-RMTSB	level sensor 2/4 relay matrix relay	containment relay room relay room
13	SIS-ACT-FA-SISA	process sensors ESF bistables relay logic network master relays slave relays	containment relay room relay room control room relay room
14	SIS-ACT-FA-SISB	process sensors ESF bistables relay logic network master relays slave relays	containment relay room relay room control room relay room

where

AFW-ACT-FA-PMP3A	No actuation signal to AFW pump 3A
AFW-ACT-FA-PMP3B	No actuation signal to AFW pump 3B
AFW-ACT-FA-VLVA	No actuation signal to AOV-MS102A
AFW-ACT-FA-VLVB	No actuation signal to AOV-MS102B
CLS-ACT-FA-CLS2A	No signal from CLCS Train A
CLS-ACT-FA-CLS2B	No signal from CLCS Train B
CPC-ICC-FA-CCPBS	No actuation signal to start CPC pump 2B
CPC-ICC-FA-SWPBS	No actuation signal to start CPC pump 10B
CPC-ICC-FA-TCV8B	No actuation signal to lube oil cooling TCV8B
CPC-ICC-FA-TCV8C	No actuation signal to lube oil cooling TCV8C
RMT-ACT-FA-RMTSA	No signal from RMTS Train A
RMT-ACT-FA-RMTSB	No signal from RMTS Train B
SIS-ACT-FA-SISA	No signal from SIS Train A
SIS-ACT-FA-SISB	No signal from SIS Train B

6 RISK SENSITIVITIES

Table 6.2 shows the plant's CDF and the total I&C contributions to it for the base case. The base case CDF values are obtained using the component failure probabilities in the PRA; in neither case do they take credit for any recovery actions. Table 6.3 lists the minimal cutsets identified from the PRA which contain at least one I&C basic event and which have a minimum CDF contribution 1.0E-10 per year. These cutsets are of interest for evaluating the sensitivities of plant risk to environmental stressors. The minimal cutsets listed may correspond to different initiating events.

The I&C cutsets in Table 6.3 show the equipment combinations which are vulnerable to one or more environmental stressors, and which can impact plant risk by increasing the CDF. The CDF can increase substantially if environmental stressor(s) affect all the equipment in a particular minimal cutset (MCS). Failure of redundant trains forms the basic combination of events having large impact on CDF through stressors affecting multiple I&C equipment; these failures are the ones of particular concern. If similar hardware is used in I&C systems represented in a particular I&C MCS, the advantages of system redundancies and system diversities may be lost due to the degrading action of a single stressor. If the stressor does not affect all the basic events in a MCS, a particular I&C MCS may not need specific attention.

Table 6.2 Estimates of Core Damage Frequency (CDF)

Base Case Plant CDF (/year)	CDF Contributions from Cutsets Containing I&C Basic Events (/year)
3.6E-05	5.6E-08

6.2 Risk-Sensitivities to Temperature

I&C risk-sensitivities to temperature are estimated using the conversion factors for MTBF for different temperatures (Table 5.1). Fig. 6.1 shows the results; detailed calculations are given in Table B1, Appendix B.

The risk contributions (CDF contributions) from I&C (i.e., C or C' in equation 4.6) are expressed as a fraction of the plant's baseline CDF (i.e., C_{TOTAL}), termed as "Relative CDF Contribution." In equation 4.6, C and C_{TOTAL} are constants for a given plant; therefore, risk-sensitivity, S , is proportional to C'/C_{TOTAL} or to the "Relative CDF Contribution."

The calculated values are represented as points with the curve representing a polynomial fit to this data. The variations in relative CDF contributions are not large for the temperature range in the control building areas. For a change in temperature from 75° F (controlled temperature in control-room) to 104° F (maximum in the cable-spreading room, see Table 5.7), the increase in CDF contribution is only a factor of 1.08, or 8%. However, at an expected temperature of 120° F in the containment, this increase in CDF contributions is approximately 50%.

Table 6.3 I&C Cutsets Identified at a Frequency Truncation Level of 1.0E-10[†]

No.	CUTSET				CDF CONTRIBUTION (/yr)
1	SIS-ACT-FA-SISA	SIS-ACT-FA-SISB			2.560E-09
2	HPI-MOV-FT-1867D	SIS-ACT-FA-SISA	CPC-XHE-FO-REALN	HPI-XHE-FO-UN2S2	1.042E-10
3	HPI-MOV-FT-1867C	SIS-ACT-FA-SISB	CPC-XHE-FO-REALN	HPI-XHE-FO-UN2S2	1.042E-10
4	HPI-MOV-FT-1115D	SIS-ACT-FA-SISA	HPI-XHE-FO-UN2S2	CPC-XHE-FO-REALN	1.042E-10
5	HPI-MOV-FT-1115C	SIS-ACT-FA-SISB	HPI-XHE-FO-UN2S2	CPC-XHE-FO-REALN	1.042E-10
6	HPI-MOV-FT-1115E	SIS-ACT-FA-SISA	HPI-XHE-FO-UN2S2	CPC-XHE-FO-REALN	1.042E-10
7	HPI-MOV-FT-1115B	SIS-ACT-FA-SISB	HPI-XHE-FO-UN2S2	CPC-XHE-FO-REALN	1.042E-10
8	RMT-ACT-FA-RMTS [†]	RMT-ACT-FA-RMTSB			1.280E-09
9	LPR-MOV-FT-1862B	RMT-ACT-FA-RMTS [†]	RMT-XHE-FO-MAN-A		2.662E-10
10	LPR-MOV-FT-1862A	RMT-ACT-FA-RMTSE	RMT-XHE-FO-MAN-A		2.662E-10
11	LPI-MDP-FS-S11A	RMT-ACT-FA-RMTSE	RMT-XHE-FO-MAN-A		1.536E-10
12	LPI-MDP-FS-S11B	RMT-ACT-FA-RMTS [†]	RMT-XHE-FO-MAN-A		1.536E-10
13	LPR-MOV-FT-1860B	RMT-ACT-FA-RMTS [†]	RMT-XHE-FO-MAN-A		1.536E-10
14	LPR-MOV-FT-1860A	RMT-ACT-FA-RMTSE	RMT-XHE-FO-MAN-A		1.536E-10
15	LPI-MDP-MA-S11B	RMT-ACT-FA-RMTS [†]	RMT-XHE-FO-MAN-A		1.042E-10
16	LPI-MDP-MA-S11A	RMT-ACT-FA-RMTSE	RMT-XHE-FO-MAN-A		1.042E-10
17	LPI-MDP-FS-S11A	SIS-ACT-FA-SISB			2.400E-09
18	LPI-MDP-FS-S11B	SIS-ACT-FA-SISA			2.400E-09
19	LPI-MDP-MA-S11B	SIS-ACT-FA-SISA			1.600E-09
20	LPI-MDP-MA-S11A	SIS-ACT-FA-SISB			1.600E-09
21	SIS-ACT-FA-SISA	SIS-ACT-FA-SISB			1.280E-09
22	LPI-MOV-PG-1864B	SIS-ACT-FA-SISA			3.504E-10
23	LPI-MOV-PG-1864A	SIS-ACT-FA-SISB			3.504E-10
24	RMT-ACT-FA-RMTS [†]	RMT-ACT-FA-RMTSB			2.560E-09
25	LPR-MOV-FT-1862B	RMT-ACT-FA-RMTS [†]	RMT-XHE-FO-MANS1		5.325E-10
26	LPR-MOV-FT-1862A	RMT-ACT-FA-RMTSE	RMT-XHE-FO-MANS1		5.325E-10
27	LPI-MDP-FS-S11B	RMT-ACT-FA-RMTS [†]	RMT-XHE-FO-MANS1		3.072E-10
28	LPR-MOV-FT-1860B	RMT-ACT-FA-RMTS [†]	RMT-XHE-FO-MANS1		3.072E-10
29	LPI-MDP-FS-S11A	RMT-ACT-FA-RMTSE	RMT-XHE-FO-MANS1		3.072E-10
30	LPR-MOV-FT-1860A	RMT-ACT-FA-RMTSE	RMT-XHE-FO-MANS1		3.072E-10
31	LPI-MDP-MA-S11B	RMT-ACT-FA-RMTS [†]	RMT-XHE-FO-MANS1		2.048E-10
32	LPI-MDP-MA-S11A	RMT-ACT-FA-RMTSE	RMT-XHE-FO-MANS1		2.048E-10
33	LPI-MDP-FS-S11B	SIS-ACT-FA-SISA			4.800E-09
34	LPI-MDP-FS-S11A	SIS-ACT-FA-SISB			4.800E-09
35	LPI-MDP-MA-S11B	SIS-ACT-FA-SISA			3.200E-09
36	LPI-MDP-MA-S11A	SIS-ACT-FA-SISB			3.200E-09
37	LPI-MOV-PG-1864A	SIS-ACT-FA-SISB			7.008E-10
38	LPI-MOV-PG-1864B	SIS-ACT-FA-SISA			7.008E-10
39	LPI-CKV-FT-CV46A	SIS-ACT-FA-SISB			1.600E-10
40	LPI-CKV-FT-CV58	SIS-ACT-FA-SISB			1.600E-10
41	LPI-CKV-FT-CV46B	SIS-ACT-FA-SISA			1.600E-10
42	LPI-CKV-FT-CV50	SIS-ACT-FA-SISA			1.600E-10
43	DCP-BDC-ST-BUS1B	SIS-ACT-FA-SISA			1.440E-10
44	ACP-BAC-ST-4801J	SIS-ACT-FA-SISA			1.440E-10
45	DCP-BDC-ST-BUS1A	SIS-ACT-FA-SISB			1.440E-10
46	ACP-BAC-ST-4801H	SIS-ACT-FA-SISB			1.440E-10
47	SIS-ACT-FA-SISA	SIS-ACT-FA-SISB			2.560E-09
48	CPC-XHE-FO-REALN	HPI-MOV-FT-1115E	HPI-XHE-FO-UN2S3	SIS-ACT-FA-SISA	1.922E-10
49	CPC-XHE-FO-REALN	HPI-MOV-FT-1115D	HPI-XHE-FO-UN2S3	SIS-ACT-FA-SISA	1.922E-10
50	CPC-XHE-FO-REALN	HPI-MOV-FT-1115C	HPI-XHE-FO-UN2S3	SIS-ACT-FA-SISB	1.922E-10
51	CPC-XHE-FO-REALN	HPI-MOV-FT-1867C	HPI-XHE-FO-UN2S3	SIS-ACT-FA-SISB	1.922E-10
52	CPC-XHE-FO-REALN	HPI-MOV-FT-1867D	HPI-XHE-FO-UN2S3	SIS-ACT-FA-SISA	1.922E-10
53	CPC-XHE-FO-REALN	HPI-MOV-FT-1115B	HPI-XHE-FO-UN2S3	SIS-ACT-FA-SISB	1.922E-10
54	CPC-XHE-FO-REALN	HPI-XHE-FO-UN2S3	SIS-ACT-FA-SISA	SIS-ACT-FA-SISB	1.025E-10
55	RCS-XHE-FO-DPT7D	SIS-ACT-FA-SISA	SIS-ACT-FA-SISB		1.042E-08
56	CPC-ICC-FA-SWPBS	CPC-MDP-FR-SW10A			1.229E-09
57	CPC-ICC-FA-CCPBS	CPC-MDP-FR-CC2A			2.304E-10
58	ACP-BAC-ST-4KV1H	CPC-ICC-FA-TCV8B			1.440E-10

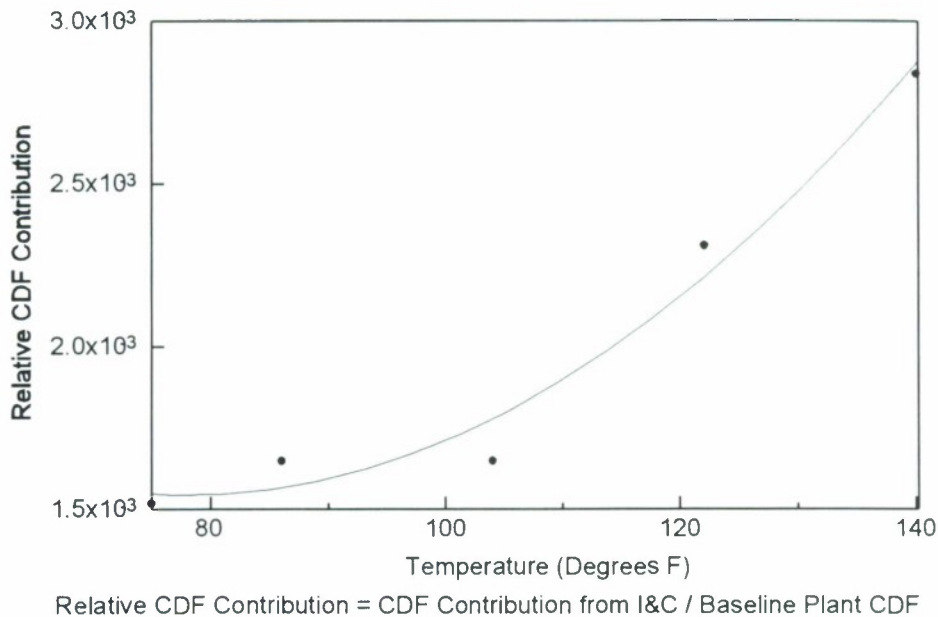
SUM OF CDF CONTRIBUTIONS
RELATIVE CDF CONTRIBUTION

5.6E-08
1.5E-03

[†] Different initiating events apply to many of the cutsets in this table. The initiating events in the cutsets are not listed.

6 RISK SENSITIVITIES

Figure 6.1 Risk-Sensitivities to Temperature

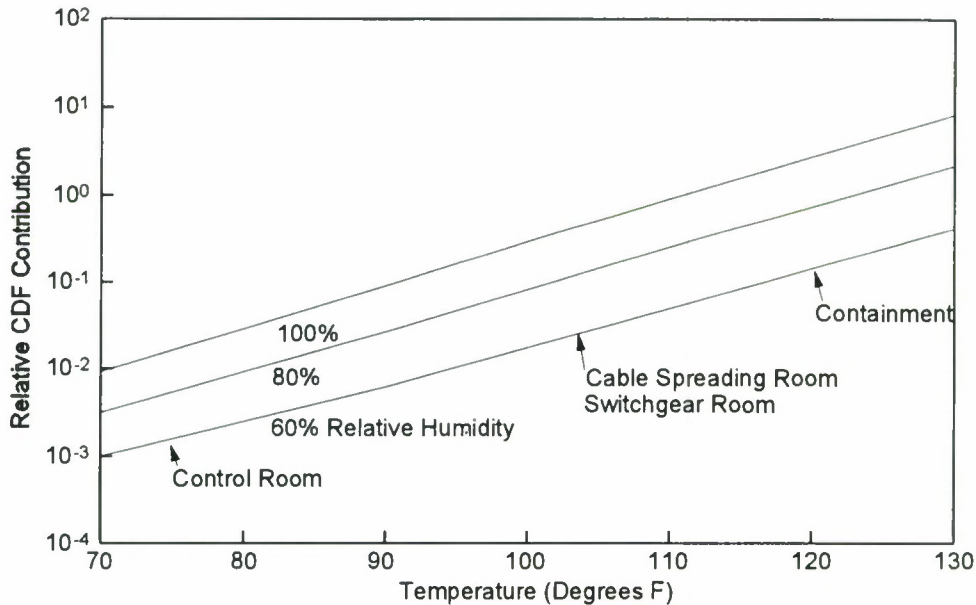


6.3 Risk-Sensitivities to Temperature-Humidity

I&C risk-sensitivities to temperature-humidity through corrosion are estimated using the environmental correlation given in section 5.3. Fig. 6.2 shows the results; detailed calculations are shown in Table B2, Appendix B.

CDF contributions from I&C again are expressed as a fraction of the plant's baseline CDF. There are significant variations (~ one order of magnitude) in relative CDF contributions when relative humidity (RH) is varied between 60% and 100%. The 60% level represents the high end of the range in RH expected in the main control room, cable-spreading room, and the switchgear room in the example plant, while the 100% level represents the maximum possible. I&C risk dependence on humidity is essentially uniform over the temperature range expected in the plant represented by these three rooms and the containment. For digital I&C equipment in the cable-spreading room/ switchgear room, the risk level is approximately one order of magnitude higher than that for equipment in the control room.

Figure 6.2 Risk-Sensitivities to Temperature-Humidity



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

6.4 Risk-Sensitivities to Vibration

I&C risk-sensitivities to vibration are estimated using the environmental factors related to vibration discussed in section 5.4. Table 6.4 shows the results; detailed calculations are given in Table B3, Appendix B. Assuming a variation of up to a factor of 4 in I&C basic-event failure rates due to vibration, the relative CDF contributions varied by a factor of about 9.

Table 6.4 Risk-Sensitivities to Vibration

Environmental Factor for Vibration	Relative CDF Contributions from I&C
1	1.5E-03
2	4.1E-03
4	1.3E-02

6 RISK SENSITIVITIES

6.5 Risk-Sensitivities to EMI from Lightning

I&C risk-sensitivities are estimated for lightning-related EMI events using the frequency of such events developed from NPP operational experience, and assuming that multiple equipment is affected by these events (section 5.6). EMI events have the potential to affect multiple equipment simultaneously, as shown in some LERs [10]. Table 6.5 shows the relative CDF contributions from I&C assuming two different periods for detection of failure from such an event for high and low estimated frequencies of lightning events and associated equipment unavailabilities. Detailed calculations are presented in Table B4, Appendix B. These events result in very large increases in relative CDF contribution over the base case if the failures are detected only at surveillance tests ($T_i = 31$ days).

Table 6.5 Risk-Sensitivities to EMI from Lightning

Failure Detection Interval (T_i)	Equipment Unavailability from Lightning EMI Events		Relative CDF Contribution from I&C
12 hours	Average	(1.4E-05)	2.9E-03
	High	(4.4E-05)	9.2E-03
	Low	(4.4E-06)	9.2E-04
31 days	Average	(8.8E-04)	1.8E-01
	High	(2.8E-03)	5.9E-01
	Low	(2.8E-04)	5.9E-02

6.6 Risk-Sensitivities to Smoke

I&C risk-sensitivities to smoke are estimated assuming it has a common effect on digital I&C equipment. As indicated in section 5.7, the frequencies of fire estimated for SURRY for control room are used as surrogates for frequencies of smoke occurrence. We assumed that all concentrations of smoke could affect digital I&C equipment. Table 6.6 shows the results of smoke on relative CDF contribution from I&C in the control room of the example plant; detailed calculations are given in Table B5, Appendix B. The high and low estimates of equipment unavailabilities correspond to 95th percentile and 5th percentile, respectively in assumed occurrence frequencies of smoke events. The relative CDF contribution for the average smoke frequency is low ($\sim 1E-04$) if failures are detected early ($T_i = 12$ hours). However, if they are detected only during surveillance tests ($T_i = 31$ days), it is approximately one order of magnitude higher than the base-case relative CDF contributions.

Table 6.6 Risk-Sensitivities to Smoke in Control Room

Failure Detection Interval (Ti)	Equipment Unavailability from Smoke Events		Relative CDF Contribution from I&C
12 hours	Average	(1.2E-06)	2.5E-04
	High	(5.1E-06)	1.1E-03
	Low	(8.2E-10)	1.7E-07
31 days	Average	(7.6E-05)	1.6E-02
	High	(3.1E-04)	6.5E-02
	Low	(5.1E-08)	1.1E-05

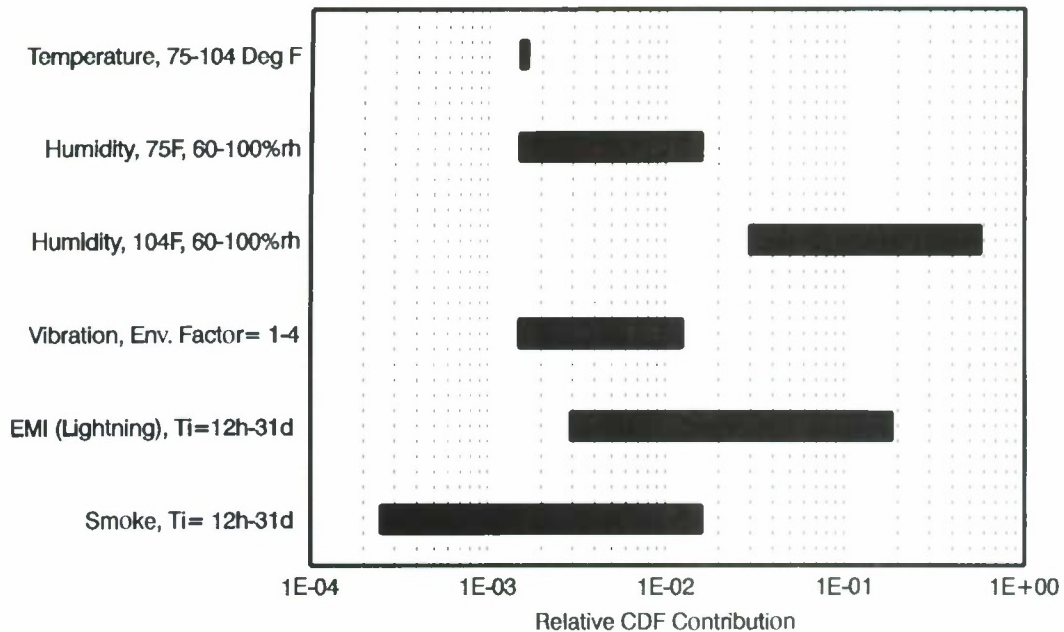
6.7 Risk-Screening of Environmental Stressors

Figure 6.3 shows the example plant's risk-sensitivities to different environmental stressors using the results from sections 6.2 through 6.6. The figure represents relative and not absolute contributions to CDF from I&C because of the assumptions made. The risk-sensitivities of environmental stressors shown in Figure 6.3 are plotted on a scale (relative CDF contribution) where risk effects from I&C failures equal the baseline total plant CDF when the x-axis value reaches 1.0. Relative CDF contributions from stressors are shown as ranges represented by a bar. These ranges for temperature, humidity, and vibration represent variations in potential risk effects from the stressors for parametric variations in stressor levels. The ranges for lightning-related EMI and smoke represent variations in potential risk effects for average estimated occurrence-frequencies and assumed periods of detection of failed I&C equipment.

The risk-sensitivities to temperature are shown for normal control-room operation (75° F maximum, no stressor effect), the cable-spreading room, and switchgear room (104° F maximum, see Table 5.6 and Figure 6.1). Risk-sensitivities to humidity through corrosion are given for two different temperatures, normal temperatures in control room (75° F maximum) and in the cable-spreading room/switchgear room (104° F maximum), for humidity levels from 60% (maximum under controlled conditions) to a maximum of 100% under uncontrolled environmental conditions (from Figure 6.2). This range in relative humidity represents situations in which air-conditioning is lost in environmentally controlled areas, such as the control room, and climatic conditions where the plant is located. Risk-sensitivities from humidity are significantly higher at the higher temperature. The results for vibration (Table 6.4) show the risk-sensitivities from a baseline, where there are no vibrations (Environmental Factor = 1), to fairly high vibrations (Environmental Factor = 4), such as would be experienced by equipment mounted on a helicopter (see section 5.4).

6 RISK SENSITIVITIES

Figure 6.3 Risk-Sensitivities of Environmental Stressors in Example Plant



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

The risk-sensitivities for lightning-related EMI events (see Table 6.5) are shown for two different periods of detection of equipment failure from these events; shift checks and surveillance-test intervals, 12 hours and 31 days, respectively. Risk-sensitivities to smoke (see Table 6.6) are also shown for the same two periods. In each case, the results show the plant risk-sensitivities for estimated average frequency of occurrences of these events.

The environmental stressors are screened for their potential for risk-significance from the results presented in Figure 6.3; this assessment is based on comparing the risk-sensitivities from environmental stressor-induced I&C failures. The base case I&C relative CDF contributions, the current contributions to CDF from I&C cutsets, is the reference value used. Here, we consider a factor of 10, or one order of magnitude change in I&C risk contributions as constituting a significant risk-sensitivity. Use of this factor allows an error factor of approximately 3 in our estimates of the environmental effects, the highest order of I&C basic-event combinations in the involved cutsets being 2. Other factors may also be used to define the risk-significance of stressors.

The base-case relative CDF contribution from I&C cutsets for the example plant is 1.5E-03 or 0.15% of CDF (see Table 6.3). A factor of 10 over this value implies that the relative CDF contribution is at least 1.5E-02 or 1.5% for the stressor to be considered as risk-significant. Hence, from the results in Figure 6.3, environmental stressors are categorized as risk-significant or risk-insignificant in Table 6.7.

Table 6.7 Risk-Screening of Environmental Stressors in Example Plant

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

* At least a factor of 10 increase in relative CDF contribution from I&C over the base-case value.

T_i - interval for detecting equipment failures from lightning and smoke.

From these results, it appears that temperature acting alone, and vibration are unlikely to be risk-significant stressors for digital I&C in a PWR. Corrosion from humidity potentially is risk-significant, more likely at higher temperatures, such as, in the cable-spreading room and the switchgear room even at 60%RH, but possibly only at very high RH levels for temperature in the control room. For EMI from lightning and smoke events, using their average occurrence rates, risk-significance depends on the interval before the equipment's failure is detected, and is significant for $T_i = 31$ days but insignificant if they are detected with $T_i = 12$ hours. This conclusion still holds for bounding estimates from EMI events from lightning, which account for uncertainties in its occurrence rates (see Table 6.5). For smoke events in the control room, table 6.6 shows that the conclusion holds for $T_i = 12$ hours, i.e., the stressor is not risk-significant even when bounding estimates account for uncertainties in occurrence rates.

6.8 Sensitivity of the Stressor Risk-Screening Results to Specific Assumptions

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

- a) equipment failures are all critical to system functions, i.e. prevent the system from performing its functions, and
- b) equipment failures are not detected until the next scheduled test, that is, the self-diagnostic capabilities of the digital systems are ignored.

6 RISK SENSITIVITIES

The assumptions give conservative results. The sensitivity of the estimated stressor risk-effects to these two assumptions are analyzed in this section; specifically, to the fraction of failure events which may be critical for the system's function, and to the probability of detecting such failures by the system's self-diagnostic features.

For redundant digital I&C systems with self-diagnostic capabilities, Ref. 29 cites data on detecting critical failures in equipment (such as in processors/memory, input, and output) by the system itself (known as diagnostic-coverage factors). The paper also lists the fractions of total failures in components which are safe from system function considerations. The diagnostic-coverage factors typically depend on the system's architecture (redundancy) and the safe failure fraction applies to independent failures of components. However, for the sensitivity analysis, we used typical values of these two parameters listed for all types of failures.

Let,

$$\begin{aligned} F_{CD} &= \text{fraction of critical failures detected by the system, and} \\ F_S &= \text{fraction of safe failures} \end{aligned}$$

Then,

$$(1 - F_S) \times (1 - F_{CD}) = \text{the fraction of critical failures that is not detected by the system and which remain unannounced until the next scheduled test.}$$

In the sensitivity analysis, the equipment unavailabilities assumed earlier are modified by this factor.

The typical value listed in Ref. 29 for F_S associated with processors/memory and input and output elements of a digital system is 0.5, i.e., half of all hardware failures are safe failures from the perspective of the system's function. For F_{CD} , the typical values listed are 0.8 for processors and memory, and 0.5 for input and output elements.

Using $F_{CD} = 0.5$, and $F_S = 0.5$ for all equipment, the unavailability associated with the stressor events are modified by $(1-0.5) \times (1-0.5)$ or 0.25. Table 6.8 shows the relative CDF contributions from I&C for each stressor and stressor level for these modified values. Detailed calculations are given in Tables B6 through B10 in Appendix B. Column 3 in Table 6.8 identifies stressors which meet our condition for risk-significance (risk-sensitivity corresponding to a relative CDF contribution from I&C $\geq 1.5E-02$). Only upper-bound relative CDF contributions from I&C are shown for EMI from lightning and smoke.

The list of risk-significant stressors at the noted parameter values remains essentially the same as in Table 6.7, except for humidity at control-room temperature of 75° F which becomes insignificant after taking into account assumptions on the fraction of critical failures and the fraction of those detected by self-diagnostic features of digital I&C systems. For EMI from lightning and smoke events, again, the intervals considered for detecting critical failures undetected by the system itself becomes the deciding factor for risk-significance. This dependence on detection intervals for failures points to the need for earlier tests of system functionality, especially those of the safety systems, following lightning-induced EMI and smoke events to lower the potential for risk.

Table 6.8 Sensitivity of Stressor Risk-Screening Results to Assumptions in Example Plant

Stressor and Level	Relative CDF Contribution from I&C	Risk-significant
Temperature, 104° F	3.0E-04	
Humidity, 100% @ 75° F	1.9E-03	
Humidity, 100% @ 104° F	4.7E-02	✓
Vibration, Env. Factor = 4	1.5E-03	
EMI from Lightning , Ti = 12 hours, upper bound	2.3E-03	
EMI from Lightning , Ti = 31 days, upper bound	1.5E-01	✓
Smoke, Control Room, Ti = 12 hours, upper bound	2.7E-04	
Smoke, Control Room, Ti = 31 days, upper bound	1.6E-02	✓

From the risk-screening results, the following conclusions are made about the stressor's risk effects involving digital I&C:

1. Temperature at the I&C cabinet locations in the example plant does not appear to be a risk-significant stressor.
2. Vibration at the levels noted also appears to have no significant risk-effects.
3. Humidity could be a significant stressor at cable-spreading room and switchgear-room temperatures; however, at control-room temperature, humidity does not appear to be potentially risk-significant except at very high levels.
4. EMI from lightning potentially can be a risk-significant stressor for digital I&C systems; however, the risk significance clearly depends on the interval before equipment failure is detected.
5. Under our assumptions, smoke also appears to have the potential to significantly increase relative risk contributions from digital I&C systems; again, such risk depends on the interval before failure is detected.

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

7 A COMPARISON OF HARDWARE UNAVAILABILITY IN A DIGITAL-VERSUS ANALOG-I&C SYSTEM

In this chapter, we compare the hardware unavailability of an existing analog I&C safety system in a nuclear power plant (NPP) with that of a microprocessor-based digital system performing the same functions. The purpose is to understand the relative reliability performance of the safety systems in NPPs when aging analog systems are upgraded with modern digital ones.

We present simplified unavailability models for the safety injection actuation system (SIAS) in a pressurized-water reactor (PWR), assuming its analog and digital implementation, and then we estimate and compare the system's hardware unavailabilities. The effect of hardware redundancies on the unavailability of the digital system are evaluated. Failure data for digital equipment from different operational conditions and environments are used to show the expected variations in system unavailabilities. The SIAS was chosen for these comparisons because of its high contribution to core-damage frequency (CDF) on failure among I&C cutsets, as shown in Table 6.3 for the example NPP.

7.1 System Description

In the example plant, SURRY, which is a Westinghouse designed PWR, the SIAS is part of the emergency safety features actuation system (ESFAS), that is designed to automatically initiate the high- and low-pressure injection systems and the motor-driven auxiliary feedwater (AFW) pumps whenever there is an indication that primary coolant makeup is needed. The SIAS has two independent trains that are used to actuate this system.

The ESFAS monitors selected parameters in the plant and determines if the safety setpoints for those parameters are exceeded, and then generates appropriate actuation signals including safety-injection actuation. Figure 7.1 shows a simplified block diagram for one train of the ESFAS in SURRY. Three or four sensors normally monitor each parameter used to actuate the ESFAS. Following the necessary signal conditioning (signal conversion, amplification, scaling, compensation), the parameters are compared against the setpoints using a comparator circuit (bistable). The monitored parameter signals are connected to a logic system. For parameters exceeding the setpoint, the corresponding comparators generate partial trip-signals that are sent to the redundant trains of the logic system and are combined there. When the trip logic is satisfied, an actuation signal communicated through master-and slave-relays initiates the relevant actuators for the safety systems. While the two logic trains are redundant, the final devices they actuate are not the same; each master-relay controls several slave-relays each of which, in turn, controls several actuators.

Table 7.1 lists the safety injection actuation parameters and the coincidence logic typically used in 4-loop Westinghouse PWRs. The containment's pressure is detected by 3 detector channels. Separate trips are provided so that for increasing pressure in the containment, different safeguards are sequenced into operation. Containment high-1 pressure at about 10% of the containment's design pressure will initiate safety injection on satisfying 2-out-of-3 logic. Low steamline pressure occurs when a steam break accident causes a rapid decrease in steamline pressure. A low steamline pressure when sensed by 2-out-of-3 steam-pressure detectors in any one of the steamlines will actuate safety injection. The pressurizer low-pressure safety injection is actuated when either a steam break accident or a large LOCA (loss-of-coolant-accident) lowers pressure in the pressurizer, and the decrease is sensed by 2-out-of-4 of the pressure detectors.

7 A COMPARISON OF SYSTEM UNAVAILABILITY

Figure 7.1 Simplified Block Diagram of One Train of ESFAS in SURRY

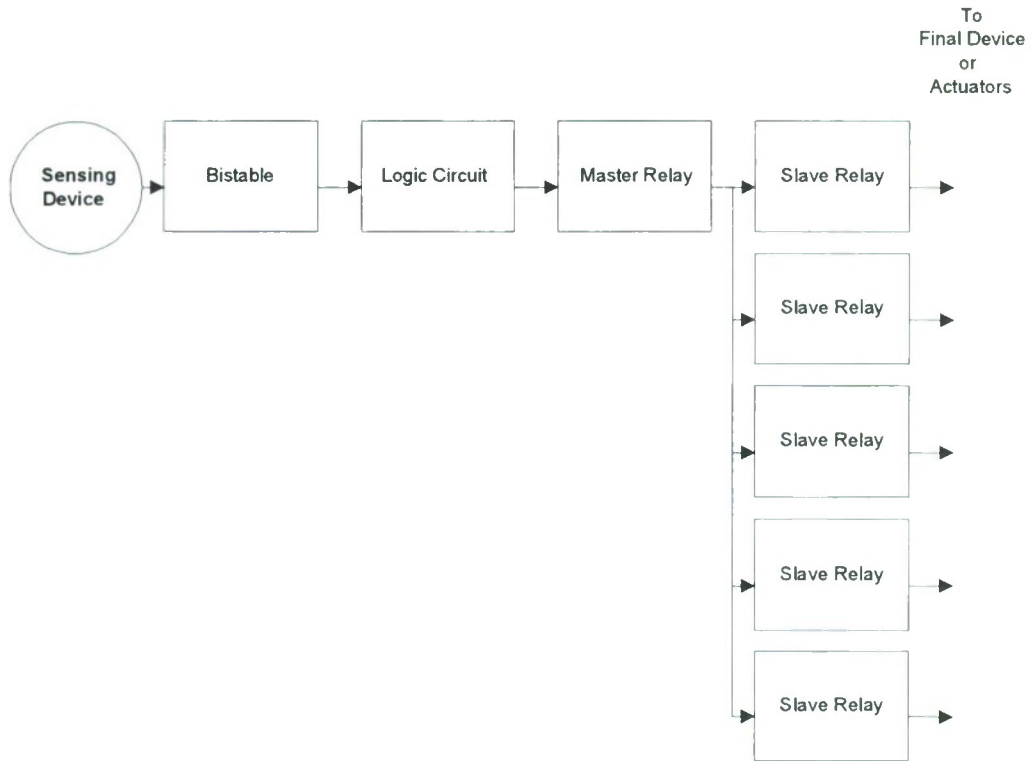


Table 7.1 Safety Injection Actuation Initiating Parameters and Logic

Parameter	Number of Instrument Channels	Number of Channels to Trip
Containment Pressure -Hi-1	3	2
Low Steamline Pressure	12 (3/steamline)	2 in any one steamline
Pressurizer Low Pressure	4	2

7.2 Safety Injection Actuation System Models

In this section, we describe the logic models developed for quantifying system unavailability, and for comparing the analog safety injection actuation system (SIAS) and its digital replacement. Subsection 7.2.1 defines the SIAS boundary and the assumptions made in modeling. Analog and digital SIAS logic models are discussed in subsections 7.2.2 and 7.2.3, respectively.

7.2.1 System Definition for Modeling

The ESFAS, of which SIAS is a part, is the actuation system that includes all I&C components starting from the sensors and sensor channels and terminating in an output relay (slave relays) associated with the actuators (such as pumps, valves), as shown in Figure 7.1. However, sensors and slave relays are excluded from our model for SIAS as they are expected to remain the same in digital upgrades. Therefore, the system is modeled in both analog and digital from the point where measured values of the plant parameters enter the signal-processing elements of the system, to the point where an actuation signal is available for the actuators or actuator-control units.

The level of modeling detail is guided by the following considerations:

- a. the availability of data to support the models, and
- b. one that clearly compares system unavailabilities of analog and digital systems, based on major components and their functional and reliability characteristics without introducing unnecessary complexities.

For example, the redundant power supplies, which are important hardware elements of both systems, are not modeled since it can be argued that the number of power supplies and their redundancies will be the same or similar in each. The technology used in the power supplies, and their reliability behavior, also is expected to be the same. Therefore, including these elements would have increased the modeling complexity without giving any significant benefit.

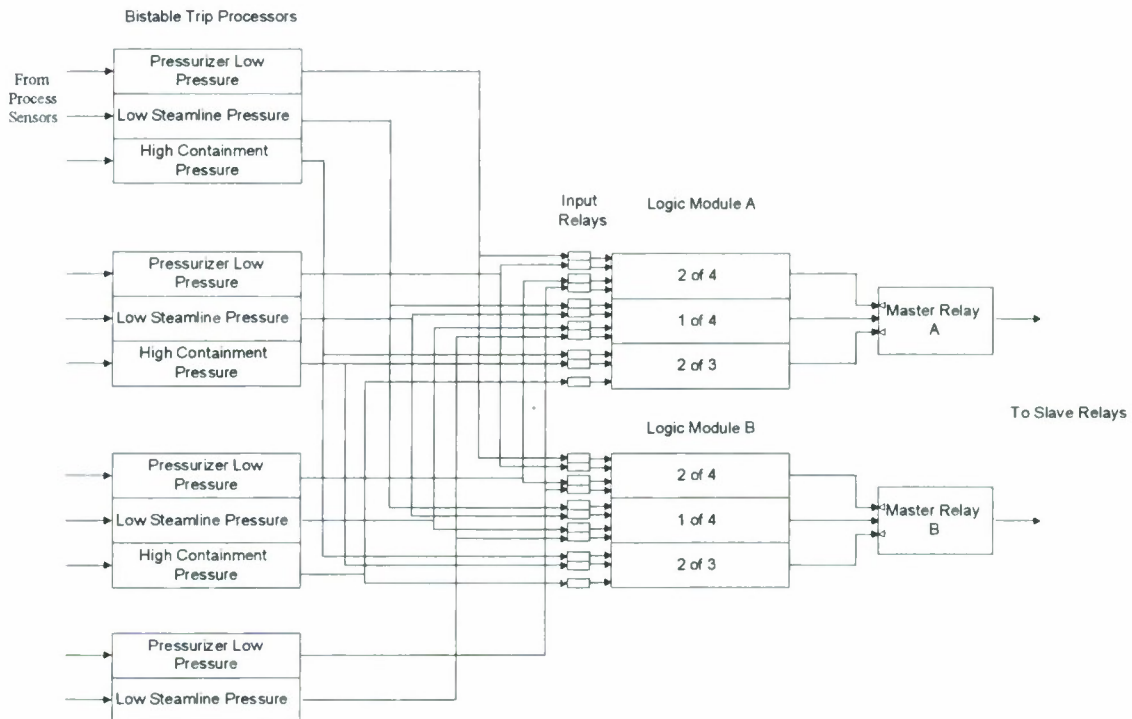
7.2.2 Analog SIAS

Figure 7.2 shows the analog SIAS modeled in this study, indicating the signal flowpaths through the system. The following major subsystems and components are modeled:

- bistable trip processors
- input relays
- logic modules
- master relays

7 A COMPARISON OF SYSTEM UNAVAILABILITY

Figure 7.2 Block Diagram of Analog SIAS Used in Evaluations of System Unavailability



The four blocks on the left hand side represent the four independent parameter channel sets. High containment pressure is represented in only 3 of 4 of these blocks since there are only 3 independent instrument channels for this parameter (see Table 7.1). Also for low steamline pressure, the three channels on each steamline (see Table 7.1) have been combined into a single channel to reduce the modeling effort. Consequently, only four independent channels are shown in the diagram for low steamline pressure, one for each steamline.

Each channel within a channel set is served by an independent bistable trip-processor. The typical one in current plants is a solid-state device and includes signal conditioning, setpoint, and comparator circuits. The comparator compares the conditioned plant-parameter signal from a sensor to the setpoint, and turns the output on or off if the parameter exceeds the setpoint.

7 A COMPARISON OF SYSTEM UNAVAILABILITY

The output signal from each bistable trip processor is transmitted to the logic modules via two input relays, one for each module. The relays energize on trip output from the comparator.

The logic modules in current plants consist of either relay logic or solid-state logic, commonly known as solid-state protection systems (SSPS). The relay logic consists of relays in a series-parallel arrangement which produces an output when the required number of relays in the logic module is closed or open activated by output signal from the bistable trip processors. In the SSPS, the same function is carried out by solid-state circuits.

For safety injection actuation, there is one master relay associated with each logic module which is activated by the output of the corresponding module.

7.2.3 Digital SIAS

Figure 7.3 shows the basic digital SIAS modeled, based on a review of upgrades currently offered by the vendors (such as Eagle 21) and digital I&C designs proposed for advanced reactors (such as AP600, ABWR, and System 80+). Reference 3 discusses advanced reactor protection and safety I&C. Advanced reactor I&C designs use four-train (division) system with differences in system architectures. Many other architectures are possible with variations in hardware redundancies and arrangement for data processing. The base model used in this study (shown in Figure 7.3) maintains the two logic train structure of SIAS in existing plants. Subsection 7.4 examines limited variations in hardware redundancies and system architecture and their effect on system unavailability. Signal flowpaths through the system are indicated. The following major subsystems and components are modeled:

- protection modules
- logic modules
- output load drivers

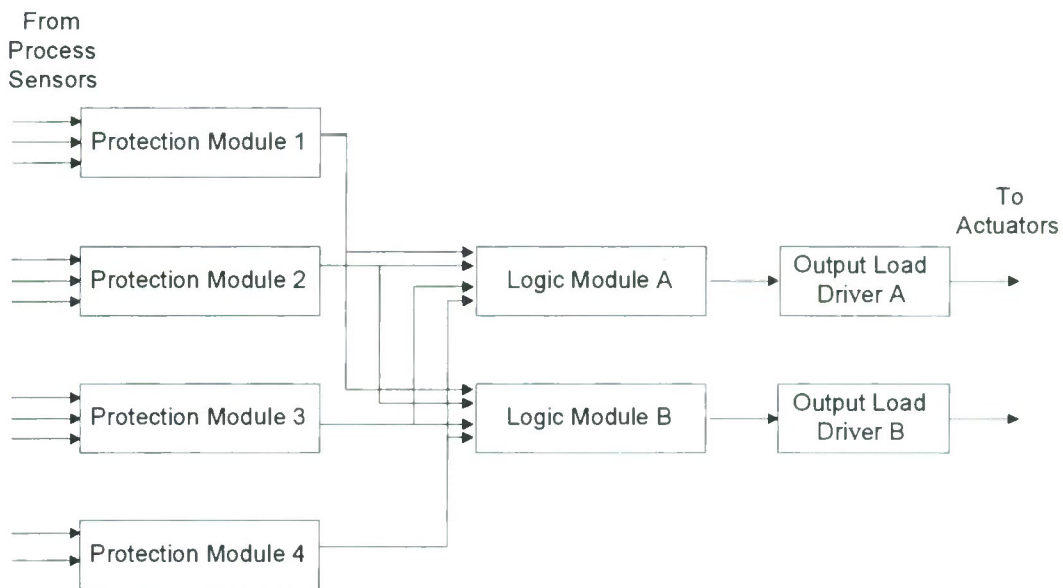
The digital upgrade is assumed to be implemented by replacing the bistable trip processors and associated relays for each channel set in Figure 7.2 by a single, microprocessor-based, hardware element, termed a "protection module" in Figure 7.3. All parameter input for a channel set is processed (signal conditioning, analog-to-digital conversion, multiplexing) by this module consisting of dual-redundant microprocessors and memory units, and input-output interfaces. This module generates the necessary partial-trip signals for the SIAS.

The output of these units are channeled to the microprocessor-based logic modules A and B, assumed to consist also of dual-redundant microprocessors and memory units, and input-output interfaces which replace analog relay-based or SSPS logic module functions in Figure 7.2. The trip-voting logic is carried out in this module.

The digitized output of the logic modules are forwarded to the solid-state output load drivers and which, in turn, generates appropriate electrical signals for the actuators hooked to each train.

7 A COMPARISON OF SYSTEM UNAVAILABILITY

Figure 7.3 Block Diagram of Digital SIAS Used in Evaluations of System Unavailability



7.2.4 SIAS Logic Models

The SIAS fault-trees for analog and digital systems are developed primarily at the functional units level, as shown in Figures 7.2 and 7.3. For analog systems, this is also the level at which data is available (from individual plant examinations or IPEs) to support the models. For the digital system, however, data is available at the component level for the protection and logic modules (such as processor, memory, input-output boards); therefore, for these units, fault-trees are developed from the component level. The following assumptions are made in developing SIAS logic models for analog- and digital-hardware- based systems:

1. System fault-trees are developed for hardware failures of SIAS to provide an actuation signal automatically on demand.
2. Wiring and cables are assumed to be available; their failure rates are not modeled because they are generally much smaller than those of other components.
3. Hardware failures include both random failures (independent failures) and failures from common-cause events (dependent failures) of redundant system elements. Common-cause failures are applied at the functional unit levels (Figures 7.2 and 7.3).
4. Test and maintenance unavailabilities are not modeled.

The SIAS fault-trees are developed in three parts:

- failure to provide input to logic modules
- failure of trip logic
- failure of output actuation signals

Figures C.1 and C.2 in Appendix C show the fault-trees developed for the top event 'No SI Actuation Signal' for the analog and digital SIAS depicted in Figures 7.2 and 7.3, respectively.

7.3 SIAS Hardware-Failure Data

Information on hardware failure for the SIAS was collected from several sources; these included NPP experience-based data reported in individual plant examinations (IPEs) and in the literature, experience from other industries, and estimates based on military data. The environmental effects are contained within the data reported, and are not available separately for the data sets we used in the analysis.

Table 7.2 shows hardware failure probabilities for the analog system components; all of them are based on failure on demand and obtained from Ref. 30. The generic data was also used in other IPEs. The mean probabilities are given, with the 5th and 95th percentile values; these percentiles provide lower and upper bounding values for estimates of failure probability, respectively. The common-cause factors (β -factors) for identical components shown are applied to the random hardware-failure probabilities to obtain common-cause failure probabilities in fault-tree quantifications.

Table 7.2 Failure Data for Analog SIAS Components

Device/Module	Failure Probability			Common-Cause Factor
	Mean	5th Percentile	95th Percentile	β
Bistable	3.89E-7	5.98E-8	9.16E-7	0.07
Logic Module	8.52E-5	2.43E-6	2.44E-4	0.001
Relay	2.41E-4	1.41E-5	6.40E-4	0.07

Table 7.3 lists data for digital-system components. The failure probabilities are estimated from failure rates assuming detection intervals of 12 hours (shift checks) and 31 days (surveillance tests). Data source 1 is Ref. (8), based on Combustion Engineering (CE) operating experience with digital control systems in its PWRs. The failure probabilities are estimated from slightly over 1 million hours of system operations and represent failures not detected by self-diagnostics in the system. The data are adjusted for critical failures, assuming a critical failure fraction of 0.5; this value is the fraction of failures not detected by the system itself and which are critical for system function. This fraction is cited as a typical value for processors, memory, and input/output in Ref. 29. Data from source 2

7 A COMPARISON OF SYSTEM UNAVAILABILITY

are based on experience from offshore platform applications for equipment located in ventilated, indoor areas [14], and are adjusted for critical failures for input/output modules. Data from source 3 are based on theoretical estimates from military data (MIL-HDBK-217D) on digital devices for an industrial process- control system reported in Ref. 14. However, it is not clear whether the data in sources 2 and 3 are based on failures undetected by systems or include all failures. The failure probability for the output load driver (Data Source 4) is estimated, assuming this is essentially a transistor device with failure rate as reported in Ref. 2 (a Field-Effect Transistor, or FET device). The output load drivers provide the SIAS with power interface with the actuators. Data on common-cause failures for the digital system are not available. In Section 7.4, a sensitivity approach is taken for common-cause failures in digital SIAS.

Table 7.3 shows that there are significant differences among the data sources in the estimated failure probabilities for processors and memory units. The off-shore platform data (Source #2) and estimates from military data for an industrial application (Source #3) are fairly consistent. For input-output modules, however, Sources 1 (NPP applications) and 3 (industrial application) are consistent, while the failure probabilities in off-shore platform applications are one to two orders of magnitude lower. These differences possibly arise from a variety of factors, such as differences in hardware quality, operating environment, duty cycling, the device's complexity and technology, but the precise contribution of each is not known. However, for a comparative study such as this one, the data on different applications give a measure of variability in the expected system unavailabilities.

Table 7.3 Failure Data for Digital SIAS Components

Device/ Module	Failure Probability							
	Data Source 1 [†]		Data Source 2 [†]		Data Source 3 [†]		Data Source 4 [†]	
	Ti=31	Ti=12	Ti=31	Ti=12	Ti=31	Ti=12	Ti=31	Ti=12
Processor	8.6E-4	1.4E-5	1.9E-2	3.1E-4	1.4E-2	2.3E-4	-	-
Memory	8.6E-4	1.4E-5	1.9E-2	3.1E-4	1.4E-2	2.3E-4	-	-
Input	2.2E-3	3.6E-5	4.7E-5	7.5E-7	3.7E-3 4.7E-3*	5.9E-5 7.5E-5*	-	-
Output	2.2E-3	3.6E-5	4.6E-4	7.4E-6	1.7E-3 6.4E-3*	2.7E-5 1.0E-4*	-	-
Output Load Driver	-	-	-	-	-	-	1.6E-4	2.5E-6

*Analog Input and Output Cards

- [†] Data Sources
- 1: NPP I&C Application (Ref. 8)
 - 2: Offshore Platform Application - Indoor, Ventilated Area (Ref. 14, Table 5)
 - 3: Estimate for Industrial Application Based on Military Data (Ref. 14, Table 6)
 - 4: Environmentally Controlled Area - Military Data (Ref 2, Table A10-2)

7.4 SIAS Fault-Tree Quantification

The fault-trees in Figures C.1 and C.2 are quantified using standard fault-tree analysis methods. In calculating system unavailabilities, the 'OR' events are summed while the relevant unavailabilities are multiplied for the 'AND' events.

System Unavailability

For the analog SIAS, common-cause failures are assumed for the following component groups following IPE analysis[30]:

- Bistables
- Input Relays
- Logic Modules
- Master Relays

Common-cause failures of bistables and input relays are assumed to fail all parameter input to logic modules.

For the digital SIAS, common-cause failures are assumed for the following component groups:

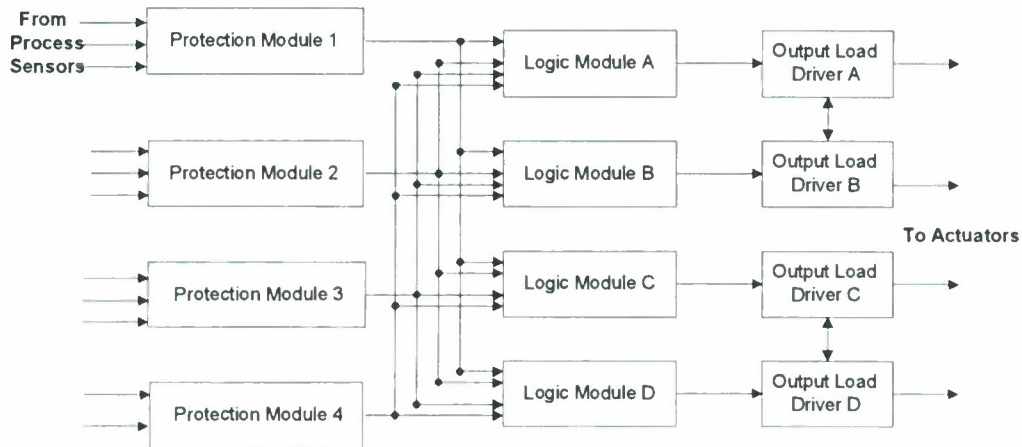
- Protection Modules
- Logic Modules
- Output Load Drivers

Some variation is considered in hardware aspects of the digital SIAS for analyzing the sensitivity of system unavailability to system redundancy. The base-case model is a two-logic train system with dual redundant processors and memory at each of the protection and logic modules. A four-train actuation logic is also considered, Figure 7.4, again with two redundant processors and memory units at each of the protection and logic modules. The number of input parameter channels, however, remain the same as before. In the four-train system, two redundant output load drivers provide a SI-actuation signal to each set of actuators (such as pumps, valves) in a 1-out-of-2 arrangement. The SI is actuated when any one of the two output load drivers associated with the particular set of actuators generate a signal. The common-cause component groups assumed are the same as those for the two-train system. Fault-trees for the four-train system are shown in Figure C.3, Appendix C.

We take a conservative, β -factor approach in treating all common-cause failures, i.e., it is assumed that if a common-cause can affect two identical components, it can affect higher multiplicities of the same components with the same probability. The assumption provides an upper bound for estimates of common-cause unavailability for component redundancies higher than two. It also is assumed that the common-cause contribution to the component failure probabilities are adequately described by the respective β -factors applied to the components' independent failure probabilities on demand.

7 A COMPARISON OF SYSTEM UNAVAILABILITY

Figure 7.4 Block Diagram of the Four-Train Digital SIAS



7.5 System Unavailability Results

Table 7.4 shows the analog SIAS unavailabilities from fault-tree quantification for mean values as well as for low (5th percentile) and high (95th percentile) values of component failure probabilities. System unavailabilities are dominated by common-cause failures, particularly the CCF of master relays because of their higher failure probabilities. The high and low values bound analog SIAS unavailability, and are compared with digital system unavailabilities. The same CCFs, shown in Table 7.2, are used to calculate system unavailability in all cases presented in Table 7.4; there is a factor of 46 difference between the low and the high system unavailabilities.

Table 7.4 Analog SIAS Unavailabilities

Component Failure Probability	System Unavailability
Mean	3.7 E-5
Low	2.1 E-6
High	9.7 E-5

In addition to unavailability evaluations for digital SIAS based on one source of data for NPP applications, fault-tree quantifications are performed in which data on component's failure probability from different applications (as discussed in Section 7.3) are used to provide a range for the expected system unavailability. Sensitivity studies are also carried out to assess the effects of failure-detection interval, hardware redundancy, and common-cause factors.

7 A COMPARISON OF SYSTEM UNAVAILABILITY

Tables 7.5 through 7.7 show the results for digital SIAS unavailability and their sensitivities. Table 7.5 shows system unavailability using component failure data in different applications for two failure detection periods (T_i). The unavailabilities are for the two-train digital SIAS (Figure 7.3) with dual-redundant processors at protection and logic modules. The base-case (Case 1) refers to data from Source 1 (Table 7.3). Cases 2 and 3 refer to data from Sources 2 and 3, respectively (Table 7.3). The failure probability for the output load driver is from Source 4 in Table 7.3 and is used in all cases. A β -factor of 0.1 is used for all common-cause events in all cases for the results in Tables 7.5 and 7.6. The choice of this CCF is rather arbitrary; however, it can be considered as conservative in view of I&C hardware CCFs commonly used in NPP systems analyses, and is considerably higher than the CCFs used in evaluating analog SIAS unavailability (Table 7.4). Table 7.7 shows the sensitivity of the results to the choice of CCFs.

For the 2-train system, digital SIAS unavailability, for the 2-train system, is higher for $T_i = 31$ days in all cases compared to existing analog-system unavailability (Table 7.4). However, for $T_i = 12$ hours, data sources 1 and 3 yield considerably lower system unavailability than the mean unavailability for the analog system, while for source 2, digital system unavailability is lower than the lower bound of unavailability for the analog system. The unavailability for the digital SIAS is driven primarily by the higher unavailability of the logic modules and the related common-cause contributions. This can be attributed to the system's architecture assumed for Cases 1 through 3 which does not consider redundant input/output elements for logic modules, although fully redundant processor and memory units are assumed. Table 7.6 shows the impact of redundancy in these hardware elements on the unavailability of the system.

Table 7.5 Digital SIAS Unavailability for Different Application Data and Failure Detection Intervals (2-Train System)

Case #	Data Source	Application Environment	System Unavailability	
			$T_i = 31$ days	$T_i = 12$ hours
1 (Base Case)	1	NPP	5.4E-4	8.3E-6
2	2	Offshore Platform	2.4E-4	1.2E-6
3	3	Industrial (based on military data)	7.4E-4	9.9E-6

The differences in system unavailability due to the differences in component failure-probability in different environments are approximately a factor of 3 from the low to the high for $T_i = 31$ days, and a factor of approximately 8 for $T_i = 12$ hours. The base-case (NPP environment) unavailabilities in Table 7.5 lie between those for failure probabilities in the other two environments (the lowest for offshore platform, and the highest for the assumed industrial environment based on military data).

Table 7.6 shows the sensitivity of digital SIAS unavailability to assumed system architectures. The base-case system unavailability for $T_i = 31$ days is compared to one assuming a 4-train system (Figure 7.4), and to a 2-train system with fully redundant input/output elements at the logic modules. Hardware failure-probabilities from

7 A COMPARISON OF SYSTEM UNAVAILABILITY

Source 1 (Table 7.3) is used in all quantifications of system unavailability in Table 7.6. There is very little improvement (<4%) in system unavailability by switching from a 2- (Case 1) to a 4-train logic (Case 4).

The small decrease in unavailability in switching to a 4-train system comes from random-failure contributions. The common-cause contributions are not affected for the 4-train system compared to the base-case because the β -factor common-cause model used does not give credit for hardware redundancies higher than two. This points to the need for developing CCFs from operational data for digital systems in NPPs to more accurately represent their effects on system unavailability. Case 5 shows significant improvements in unavailability (approximately a factor of 30 over the base case) when the input/output elements in the logic module are made redundant. Also, system unavailability is much lower than the mean unavailability for the analog system (see Table 7.4) despite of the choice of the longer failure-detection interval of $T_i = 31$ days.

**Table 7.6 Sensitivity of Digital SIAS Unavailability to System Architecture
($T_i = 31$ days)**

Case #	Logic Trains	Hardware Redundancy	System Unavailability
1 (Base Case)	2	Dual redundant processor and memory units at protection and logic modules	5.4E-4
4	4	Same as above	5.1E-4
5	2	Same as above, plus dual redundant output elements within each logic module	1.9E-5

Table 7.7 shows the sensitivity of the digital SIAS unavailability to the common-cause factors. Case 5 ($\beta=0.1$) unavailability is compared to estimates of system unavailability for $\beta=0.2$ (Case 6) and $\beta=0.01$ (Case 7), i.e., a factor of 2 higher, and a factor of 10 lower, than the common-cause factor assumed for Case 5. Data from Source 1 (as indicated in Table 7.3) is used in all evaluations for $T_i = 31$ days. Variations in the results are approximately proportional to the common-cause factors due to the dominance of their contributions to the system's unavailability. For Case 6 ($\beta=0.2$), digital SIAS unavailability (4.2E-5) is still comparable to the mean system unavailability for the analog SIAS (3.7E-5). For Case 7 ($\beta=0.01$), digital SIAS unavailability is lower than the low (5th percentile) system unavailability estimated for the analog SIAS.

Table 7.7 Sensitivity of Digital SIAS Unavailability to Common-Cause Factors

Case #	β -factor	System Unavailability
5	0.1	1.9E-5
6	0.2	4.2E-5
7	0.01	1.7E-6

8 SUMMARY AND CONCLUSIONS

This report describes our study on risk-screening of environmental stressors which can affect digital I&C systems in a nuclear power plant, and our comparison of the hardware unavailability of such a system with that of its analog counterpart.

An approach for risk-screening of environmental stressors is presented, based on their risk-sensitivities, using bounding evaluations where data are sparse. Risk-sensitivities are changes in plant risk caused by the stressor's effect on digital I&C failures. Bounding approaches use conservative values to screen out stressors not significant to plant risk. The study included reviewing and collecting data on the effects of stressors on digital I&C failures, and developing approaches to use this data in estimating the stressor's risk-sensitivities. The data and methods are applied to screen environmental stressors for risk-significance in an example plant, using its specific PRA.

The risk-sensitivities are quantified by estimating the effects of stressors on I&C failures and by determining the consequent increase in plant risk in terms of CDF. The effects of stressors on digital I&C are introduced in the PRA, either by modifying the failure rates of the equipment and incorporating the likelihood factors for stressor effects to occur, or by estimating equipment unavailabilities based on frequencies of occurrence of the stressors. The PRA then is used to recalculate the change in CDF. The risk increase due to specific I&C failures is determined by the importance of the equipment as modeled in the PRA.

The literature is reviewed, including military documents, operational events records from nuclear power plants, and journal publications, to identify information on the effects of environmental stressors on digital equipment. We found that information is sparse, particularly on the reliability of digital equipment. Further, there are uncertainties in estimates of the effects on reliability due to possible variations in parameters associated with the application of stressors, such as their intensities, duration, and also the diversity of the equipment. Therefore, these data can only be used to broadly compare risks from different stressors based on estimated ranges of, or bounds on, potential effects.

For the failure modes of digital I&C systems, our review identified several incidents of their spurious operation in NPPs. However, these events generally led to more conservative plant configurations through inadvertent operations of safety systems. None caused the system to fail to perform its essential safety functions. In only one event, identified in Ref. 8, a software deficiency in a digital I&C-based protection system caused the system to fail to set a trip output. Nevertheless, the trip was accomplished through a redundant output. In some instances, stressors affected multiple redundant equipment. Such failures are an important concern from risk considerations because of the possibility of loss of redundancy in safety systems through common-cause effects.

Risk-screening of environmental stressors in the example plant included temperature, humidity, vibration, EMI from lightning, and smoke. Risk from other sources of EMI could not be evaluated for lack of data. The following assumptions are made in estimating the risk-sensitivities of stressors:

- i. treating the requirements for qualifying I&C equipment as the same in all plant locations, which translates to the same susceptibility of equipment to environmental stressors at all locations;
- ii. treating the effects of stressors as the same on all I&C equipment primarily because of the lack of detail in I&C models in the PRA, and partly because of the lack of information on the detailed effects of stressors on different equipment and technologies;

8 SUMMARY AND CONCLUSIONS

- iii assuming a likelihood of 1.0 for temperature, humidity, and vibration since these stressors are plausible from present information; and
- iv assuming a failure probability of 1.0 for I&C equipment for potential common-cause type events, such as EMI and smoke, to bound the stressors' effects.

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

Evaluations of stressor risk-sensitivities used existing I&C models in the PRA, and only one plant is used in the screening analysis. Nevertheless, the risk-screening application demonstrates the usefulness of our approach in identifying environmental stressors which have the potent to be risk-significant.

We also compare the hardware unavailability of an existing analog safety I&C system in a NPP with that of an assumed digital upgrade. The unavailability study compares hardware performance in digital versus analog systems as well as the dependence of the digital system's unavailability on different parameters. The results indicate that, with proper system redundancies and surveillance intervals, advanced digital systems should be able to meet or better the hardware availability of current analog systems. We also compare the unavailability of the digital system using experience on equipment failure rates in NPPs, offshore platforms, and estimates of failure probabilities in an assumed industrial environment, based on military data. These comparative failure data provide a measure of variability in the expected system unavailability. The limited study shows that system unavailability may be more sensitive to the architecture of the digital system than to the environmental and operational variations involved.

From this study, detailed modeling and information requirements can be specified for improving assessments of risk effects of stressors in a NPP using digital I&C. Such risk depends not only on the physical effects of the stressors on the digital I&C equipment and their likelihoods, but also on the specific equipment that is affected, its failure modes, and risk-importance. Consequently, to more accurately estimate the risk contributions of digital I&C systems in NPPs, including the effects of stressors, the following will be required:

1. extending current I&C models in the PRA to reflect the characteristics of digital systems.
2. obtaining reliability data on digital I&C components to support these models.
3. getting additional information to resolve uncertainties in assumptions in risk-screening of stressors.
4. using plant-specific information to resolve plant-specific issues.

Extending current I&C models in the PRA is important as the architecture of digital systems is quite different from that of their analog counterparts. Developing detailed reliability models will allow us to identify specific vulnerabilities of these digital systems, through an analysis of component and system failure-modes, which may be

8 SUMMARY AND CONCLUSIONS

important for plant risk. These models should include hardware, software, and human-machine interface-related failures. Detailed digital I&C models in the PRA will allow quantification of absolute risks from implementing digital systems and also comparisons of these risks to those from existing analog systems. Risk-significant I&C components also can be identified from these models, and data gathering, evaluations of stressors, and qualification efforts can be more efficiently focused on them.

Reliability data on digital I&C components are identified from military documents and from NPP operational experience. What is now needed are engineering evaluations to adapt this data for NPPs for normal operations and off-normal conditions, to support detailed digital I&C reliability models in the PRA. An important element of this effort should be developing common-cause failure data for digital systems in NPPs.

Resolution of the uncertainties in assumptions in risk-screening of stressors will reduce unnecessary conservatism in these evaluations. From these initial results, efforts can be focussed on those assumptions which have the most impact on estimates of stressor risk-sensitivities, and experiments designed to reduce uncertainties in them. Expert opinion also can be helpful in supplementing historical data.

Plant-specific variations are expected in implementing digital I&C systems. Variations in the choice of equipment, its complexity, layout of the system, plant-specific locations and levels of stressors in those locations may influence the overall risk impacts of the stressors, as well as their relative impacts on plant risk. Such information must be incorporated in risk evaluations to address specific concerns with implementing digital I&C systems.

REFERENCES

1. NRC Information Notice No. 94-20: "Common-Cause Failures Due to Inadequate Design Control and Dedication," U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C., 20555, March 17, 1994.
2. "The Rome Laboratory Reliability Engineer's Toolkit," Systems Reliability Division, Rome Laboratory, Griffiss Air Force Base, NY, April 1993.
3. NUREG/CR-5904, "Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors," March 1994.
4. "Reliability Prediction of Electronic Equipment," MIL-HDBK-217F, December 1991.
5. "NASA Parts Application Handbook," MIL-HDBK-978-B, March 1988.
6. "Reliability Analysis/Assessment of Advanced Technologies," RADC-TR-90-72, Rome Air Development Center, Griffiss Air Force Base, NY, May 1990.
7. "Computer-Based Digital System Failures," Technical Review Report, AEOD/T94-03, Reactor Analysis Branch, Safety Programs Division, Office of Analysis and Evaluation of Operational Data, U.S. Nuclear Regulatory Commission, July 1994.
8. Brown, Edgar M., "System Operating Experience at ABB CE Plants," Nuclear Plant Journal, May-June 1995, pp. 24-29.
9. "NPRDS Reporting Guidelines Manual," Institute of Nuclear Power Operations, 89-001, Rev.3, April 1991.
10. Hassan, M. and Vesely, W.E., "Risk-Based Prioritization of Environmental Stressors Which Can Affect Advanced Digital I&C Equipment in Nuclear Power Plants," BNL Technical Report L-1908, T6, March 1996.
11. Clark, O.M. and Gavender, R.E., "Lightning Protection for Microprocessor Based Electronic Systems," Proc. of 36th Annual Petroleum & Chemical Industry, pp 197-203, Industrial Applications Society, IEEE, New York, NY, 1989.
12. NUREG/CR-6340, "Aging Assessment of Surge Protective Devices in Nuclear Power Plants," January 1996.
13. Mowrer, F.W. and Pecht, M.G., "Exploratory Research on Nonthermal Damage to Electronics from Fires and Fire-Suppression Agents," Proc. Ann. Reliability & Maintainability Symp., pp 1-5, IEEE Reliability Society, 1995.
14. Paula, H.M. and Roberts, M.W., "Operational Failure Experience of Fault-Tolerant Digital Control Systems," Reliability Engineering and System Safety, Vol. 39, No. 3, p. 273-290, Elsevier Applied Science, Essex, England, 1993.

REFERENCES

15. Willing, W.E. and Goldstein, N.P., "Combining Single-Event Latchup and Reliability Requirements for Space Vehicles," Proc. Ann. Reliability & Maintainability Symp., pp 445-449, IEEE Reliability Society, 1995.
16. Korsah, K., Tanaka, T.J. and Wilson, T.L., "Environmental Testing of an Experimental Digital Safety System," ORNL/TM-13122, September 1995.
17. Heyck, H., "Development of a Digital Reactor Control and Safety System," IAEA-Tecdoc-790, Reliability of Computerized Safety Systems at Nuclear Power Plants, Report of a Technical Committee Meeting, IAEA, Vienna, Austria, 1993.
18. ISA-S84.01-1996 (Standard), "Application of Safety Instrumented Systems for the Process Industries," Instrument Society of America, Research Triangle Park, North Carolina, February 1996.
19. Pecht, M. and Ko, W.C., "A Corrosive Rate Equation for Microelectronic Metallization," The International Journal for Hybrid Microelectronics, Vol. 13, No. 2, pp. 41-51, June 1990.
20. NUREG/CR-6293, "Verification and Validation Guidelines for High Integrity Systems," Vol.2, March 1995.
21. NUREG-1431, "Standard Technical Specifications - Westinghouse Plants," Vol.2, September 1992.
22. Tanaka, T.J., Nowlen, S.P. and Anderson, D.J., "Circuit Building of Components by Smoke," NUREG/CR-6476 Appendix E, Sandia National Laboratories, October 1996.
23. Tanaka, T.J., Nowlen, S.P. and Anderson, D.J., "Circuit Building of Components by Smoke," NUREG/CR-6476 Appendix A, Sandia National Laboratories, October 1996.
24. NUREG/CR-6479, "Technical Basis for Environmental Qualification of Microprocessor-Based Safety-Related Equipment in Nuclear Power Plants," Oak Ridge National Laboratory, January 1998.
25. NUREG/CR-4550, "Analysis of Core Damage Frequency, SURRY Unit 1, External Events," Vol.3, Rev.1, Part 3, December 1990.
26. SURRY Power Station Units 1&2, Updated Final Safety Analysis Report, July 1982.
27. Seabrook Station, Final Safety Analysis Report, Volume 8, May 1991.
28. Fowler R.D., et al., SURRY Unit 1 IRRAS Version 5.0 PRA Data Base, Idaho National Engineering Laboratory, April 28, 1993.
29. Stavrianidis, P., "Reliability and Uncertainty Analysis of Hardware Failures of a Programmable Electronic System," Reliability Engineering and System Safety, Vol. 39, No. 3, p. 309-324, Elsevier Applied Science, Essex, England, 1993.
30. "Individual Plant Examination," Report for Seabrook Station, New Hampshire Yankee, March 1991.

APPENDIX A

Effects of Environmental Stressors on I&C Devices and Systems

In this appendix, selected information is presented on the effects of environmental stressors on I&C devices and systems identified from the literature. Tables A1 through A4, and figure A1 were obtained from military documents.

APPENDIX A

Table A.1: Failure Modes and Mechanisms of Parts
 (Reproduced from, "The Rome Laboratory Reliability Engineer's Toolkit")

Type	Failure Mechanisms	%	Failure Modes	Accelerating Factors
Microcircuits				
Digital	Oxide Defect	9	Short/Stuck High	Electric Field, Temp.
	Electromigration	6	Open/Stuck Low	Power Temp.
	Overstress	18	Short then Open	Power
	Contamination	16	Short/Stuck High	Vibration, Shock, Moisture, Temp.
	Mechanical	17	Stuck Low	Shock, Vibration
	Elec. Parameters	33	Degraded	Temp., Power
Memory	Oxide Defect	17	Short/Stuck High	Electric Field, Temp.
	Overstress	22	Short then Open or Stuck Low	Power, Temp.
	Contamination	25	Short/Stuck High	Vibration, Shock, Moisture, Temp.
	Mechanical	9	Stuck Low	Shock, Vibration
	Elec. Parameters	26	Degraded	Temp., Power
Linear	Overstress	21	Short then Open or Stuck Low	Power, Temp.
	Contamination	12	Short/Stuck High	Vibration, Shock
	Mechanical	2	Stuck Low	Shock, Vibration
	Elec. Parameters	48	Degraded	Temp., Power
	Unknown	16	Stuck High or Low	
Hybrid	Overstress	17	Short then Open	Power, Temp.
	Contamination	8	Short	Vibration, Shock
	Mechanical	13	Open	Shock, Vibration
	Elec. Parameters	20	Degraded	Temp., Power
	Metallization	10	Open	Temp., Power
	Substrate Fracture	8	Open	Vibration
	Miscellaneous	23	Open	

**Table A.2: Comparison of Radiation Susceptibility for Microcircuits of Different Technologies
(From Ref. 5)**

Technology	Total Dose Hardness Level Rads (Si) (Note 1)	Relative Susceptibility To: (Note 2)	
		Soft Error	Latch-Up
<u>DIGITAL</u>			
NMOS	$5 \times 10^2 - 10^4$	High	Immune
CMOS/Bulk (unhardened)	$10^3 - 10^5$	Moderate to High	Moderate
CMOS/Bulk (hardened)	$2 \times 10^3 - 10^6$	Low	Low
CMOS/SOS	$10^3 - 10^5$	Very Low	Immune
TTL, Low Power TTL	$10^5 - 10^7$	Low to High	Low
Schottky TTL, Low Power Schottky TTL	$10^5 - 10^7$	Low to High	None to Low
Advanced Low Power Schottky TTL	$2 \times 10^4 - 10^6$	Moderate	Low
PL	$2 \times 10^4 - 10^6$	Moderate	None to Low
ECL	$\geq 5 \times 10^6$	Low	None to Low
<u>LINEAR</u>			
CMOS (unhardened)	$10^3 - 10^5$	- No Data Available -	
CMOS (hardened)	$3 \times 10^3 - 10^6$	- No Data Available -	
Bipolar, BI-FET	$6 \times 10^3 - 10^7$	- No Data Available -	

Notes:

1. These figures define process averages. However, some devices may not meet these levels while others may exceed them. For example, some Schottky TTL RAM's fail much below the low limit listed in the Table while most other devices with this technology fall within the range shown.
2. The single event susceptibility "ratings" listed here are relative to each other. However, a "moderate" error rate in a specific application may be unacceptably high if the application is critical. Also, circuit organization and/or use of error detection and correction can considerably "harden" soft parts in some applications.

APPENDIX A

**Table A.3: Military Environmental Category and Description
(From Ref. 4)**

Environment	Symbol	Equivalent MIL-HDBK-217E Notice 1 Symbol	Description
Ground, Benign	G _B	G _B G _{MS}	Nonmobile, temperature and humidity controlled environments readily accessible to maintenance; includes laboratory instruments and test equipment, medical electronic equipment, business and scientific computer complexes, and missiles and support equipment in ground silos.
Ground, Fixed	G _F	G _F	Moderately controlled environments such as installation in permanent racks with adequate cooling air and possible installation in unheated buildings, includes permanent installation of air traffic control radar and communications facilities.
Ground, Mobile	G _M	G _M M _P	Equipment installed on wheeled or tracked vehicles and equipment manually transported; includes tactical missile ground support equipment, mobile communications, handfield communications equipment, laser designations and range finders.
Naval, Sheltered	N _S	N _S N _{SB}	Includes sheltered or below deck conditions on surface ships and equipment installed in submarines.
Naval, Unsheltered	N _U	N _U N _{UU} N _H	Unprotected surface shipborne equipment exposed to weather conditions and equipment immersed in salt water, includes sonar equipment and equipment installed on hydrofoil vessels.

Table A.3: Military Environmental Category and Description (contd.)

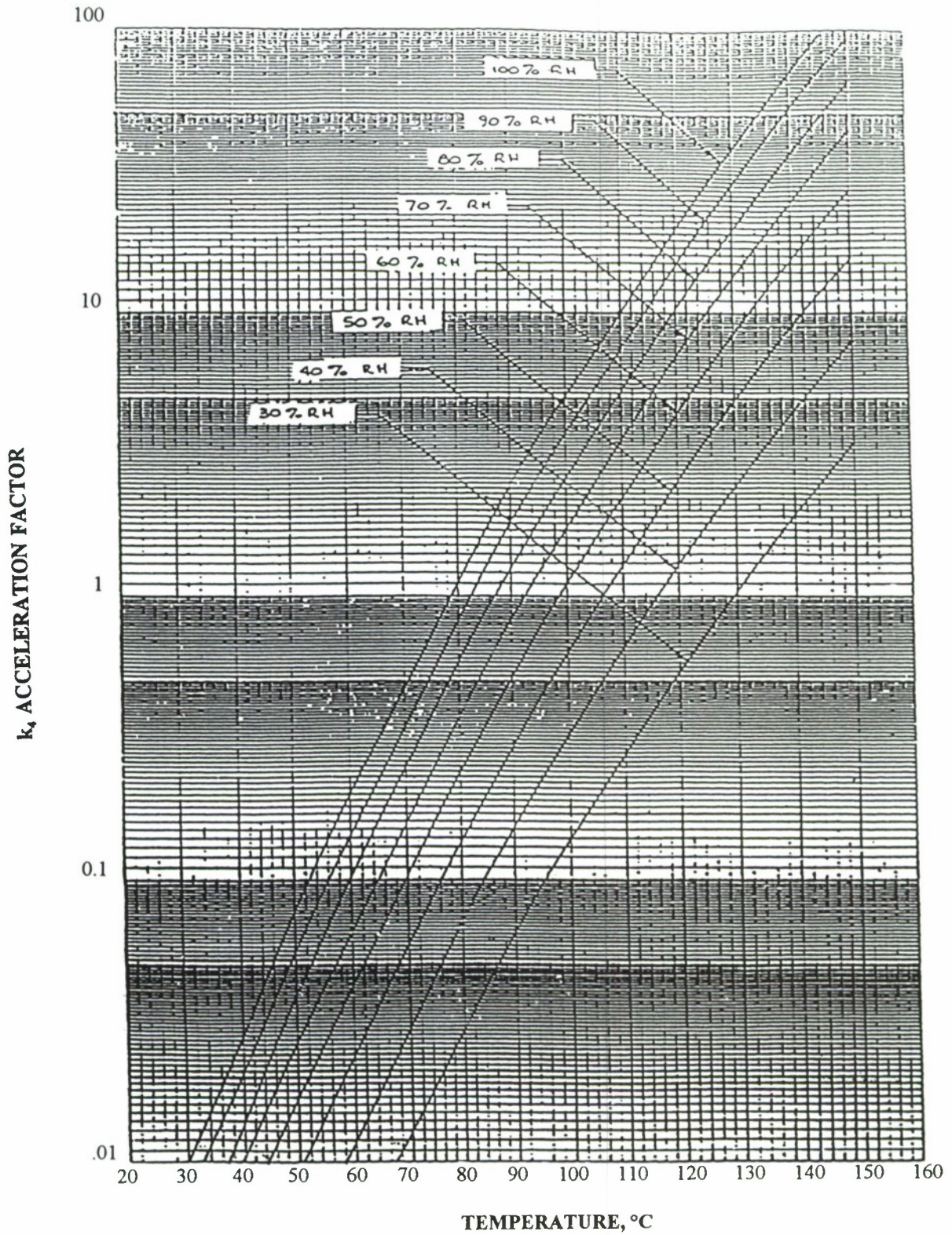
Environment	Symbol	Equivalent MIL-HDBK-217E Notice 1 Symbol	Description
Airborne, Inhabited, Cargo	A _{IC}	A _{IC} A _{IT} A _{IB}	Typical conditions in cargo compartments which can be occupied by an aircrew. Environment extremes of pressure, temperature, shock, and vibration are minimal. Examples include long mission aircraft such as the C130, C5, B52, and C11. This category also applies to inhabited areas in lower performance smaller aircraft such as the T38.
Airborne, Inhabited, Fighter	A _{IF}	A _{IF} A _{IA}	Same as A _{IC} but installed on high performance aircraft such as fighters and interceptors. Examples include the F15, F16, F111, F/A 18 and A10 aircraft.
Airborne, Uninhabited, Cargo	A _{UC}	A _{UC} A _{UT} A _{UB}	Environmentally uncontrolled areas which cannot be inhabited by an aircrew during flight. Environmental extremes of pressure, temperature and shock may be severe. Examples include uninhabited areas of long mission aircraft such as the C130, C5, B52, and C141. This category also applies to uninhabited area of lower performance smaller aircraft such as the T38.
Airborne, Uninhabited, Fighter	A _{UF}	A _{UF} A _{UA}	Same as A _{UC} but installed on high performance aircraft such as fighters and interceptors. Examples include the F15, F16, F111 and A10 aircraft.
Airborne, Rotary Wing	A _{RW}	A _{RW}	Equipment installed on helicopters. Applies to both internally and externally mounted equipment such as laser designators, fire control systems, and communications equipment.
Space, Flight	S _F	S _F	Earth orbital. Approaches benign ground conditions. Vehicle neither under powered flight nor in atmospheric reentry, includes satellites and shuttles.
Missile, Flight	M _F	M _{FF} M _{FA}	Conditions related to powered flight of air breathing missiles, cruise missiles, and missiles in unpowered free flight.
Missile, Launch	M _L	M _L U _{SL}	Severe conditions related to missile launch (air, ground and sea), space vehicle boost into orbit, and vehicle re-entry and landing by parachute. Also applies to solid rocket motor propulsion powered flight, and torpedo and missile launch from submarines.
Cannon, Launch	C _L	C _L	Extremely severe conditions related to cannon launching of 155 mm and 5 inch guided projectiles. Conditions apply to the projectile from launch to target impact.

APPENDIX A

**Table A.4: Potential Electrical Failure Mechanisms for Advanced Technologies
(From Ref. 6)**

Mechanism	Failure Mode	Accelerating Conditions
Time Dependent Dielectric Breakdown	Gate shorts, interlayer shorts in interconnection system	Voltage, increased temperature
Electromigration	Interlayer or intralayer shorts in interconnection system, and open circuits	Current, increased temperature
Hot Carriers	Threshold shifts, g_m shifts	Source/drain voltage, decreased temperature
Mobile Ions	Threshold shifts	Gate/source voltage, decreased temperature
Surface State Movement	Leakage	Radiation, current
Latent ESD Damage	Gate shorts, protection network shorts	Voltage, current
Corrosion	Opens in interconnections	Humidity, increased temperature
Unequal Metal Diffusion Rates	Contact resistance change	Current, increased temperature

Figure A.1 Temperature-Humidity Environment Acceleration Factor
(From Ref. 6)



APPENDIX B

Calculations of Environmental Stressor Risk-Sensitivity

In this appendix, details are presented of the risk-sensitivity calculations for temperature, humidity, vibration, EMI from lightning, and smoke as environmental stressors. We show the CDF contributions corresponding to each minimal cutset, associated with I&C basic events. Estimated environmental factors (which modify I&C basic event failure rates to include the stressors' effects) and the stressors' likelihoods are indicated in each case. The total CDF contributions from minimal cutsets associated with I&C basic events are calculated. The relative CDF contributions is the ratio of total CDF contribution calculated earlier to the baseline plant CDF calculated using the PRA.

Table 82 Temperature-Humidity Effects on CDF Contributions
 d:\I&C-96\NUREG\TAB-B-2.wk3

REL. HUMIDITY (%) TEMP (F)	CDF CONTRIBUTIONS FROM I&C			
	60	70	80	90
75	5.55E-08	1.06E-07	1.95E-07	3.44E-07
90	2.27E-07	4.85E-07	9.71E-07	1.83E-06
110	1.78E-06	4.21E-06	9.01E-06	1.78E-05
130	1.48E-05	3.64E-05	8.00E-05	1.61E-04

REL. HUMIDITY (%) TEMP (F)	RELATIVE CDF CONTRIBUTIONS				
	60	70	80	90	100
75	0.0015	0.0029	0.0053	0.0094	0.016
90	0.0062	0.0133	0.0266	0.0503	0.0901
110	0.0489	0.1154	0.2471	0.4886	0.9047
130	0.4056	0.9983	2.1936	4.4094	8.2517

APPENDIX B

Table B3 Vibration Effects on CDF Contributions
d:\I&C-96\NUREG\TAB-B-3.WK3

No.	Cutset	Base Freq. (/yr)	No. of I&C Basic Events in Cutset	Cutset Freq. (/yr)	Environmental Factor
1	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	2.660E-09	2	1.02E-08	4.10E-08
2	HPI-MOV-FT-18670 SIS-ACT-FA-SISA	1.042E-10	1	2.08E-10	4.17E-10
3	HPI-MOV-FT-1867C SIS-ACT-FA-SISB	1.042E-10	1	2.08E-10	4.17E-10
4	HPI-MOV-FT-1150 SIS-ACT-FA-SISA	1.042E-10	1	2.08E-10	4.17E-10
5	HPI-MOV-FT-1115C SIS-ACT-FA-SISB	1.042E-10	1	2.08E-10	4.17E-10
6	HPI-MOV-FT-1115E SIS-ACT-FA-SISA	1.042E-10	1	2.08E-10	4.17E-10
7	HPI-MOV-FT-1115B SIS-ACT-FA-SISB	1.042E-10	1	2.08E-10	4.17E-10
8	RMT-ACT-FA-RMTS RMT-ACT-FA-RMTSB	1.280E-09	2	5.12E-09	2.06E-08
9	PR-MOV-FT-1862B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	2.662E-10	1	5.32E-10	1.06E-09
10	PR-MOV-FT-1862A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	2.662E-10	1	5.32E-10	1.06E-09
11	LP-MOP-FS-S11A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.536E-10	1	3.07E-10	6.14E-10
12	LP-MOP-FS-S11B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.536E-10	1	3.07E-10	6.14E-10
13	PR-MOV-FT-1860B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.536E-10	1	3.07E-10	6.14E-10
14	PR-MOV-FT-1860A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.536E-10	1	3.07E-10	6.14E-10
15	LP-MOP-MA-S11B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.042E-10	1	2.08E-10	4.17E-10
16	LP-MDP-MA-S11A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.042E-10	1	2.08E-10	4.17E-10
17	LP-MDP-FS-S11A SIS-ACT-FA-SISB	2.400E-09	1	4.80E-09	9.60E-09
18	LP-MOP-FS-S11B SIS-ACT-FA-SISA	2.400E-09	1	4.80E-09	9.60E-09
19	LP-MOP-MA-S11B SIS-ACT-FA-SISA	1.600E-09	1	3.20E-09	6.40E-09
20	LP-MOP-MA-S11A SIS-ACT-FA-SISB	1.600E-09	1	3.20E-09	6.40E-09
21	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.280E-09	1	2.56E-09	6.12E-09
22	PL-MOV-PG-1864B SIS-ACT-FA-SISA	3.604E-10	1	7.01E-10	1.40E-09
23	PL-MOV-PG-1864A SIS-ACT-FA-SISB	3.504E-10	1	7.01E-10	1.40E-09
24	RMT-ACT-FA-RMTS RMT-ACT-FA-RMTSB	2.560E-09	2	1.02E-08	4.10E-08
25	LPR-MOV-FT-1862B RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	5.325E-10	1	1.07E-09	2.13E-09
26	LPR-MOV-FT-1862A RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	5.325E-10	1	1.07E-09	2.13E-09
27	LP-MDP-FS-S11B RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	3.072E-10	1	6.14E-10	1.23E-09
28	LPR-MOV-FT-1860B RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	3.072E-10	1	6.14E-10	1.23E-09
29	LP-MDP-FS-S11A RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	3.072E-10	1	6.14E-10	1.23E-09
30	LPR-MOV-FT-1860A RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	3.072E-10	1	6.14E-10	1.23E-09
31	LP-MOP-MA-S11B RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	2.048E-10	1	4.10E-10	8.19E-10
32	LP-MOP-MA-S11A RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	2.048E-10	1	4.10E-10	8.19E-10
33	LP-MOP-FS-S11B SIS-ACT-FA-SISA	4.800E-09	1	9.60E-09	1.92E-08
34	LP-MOP-FS-S11A SIS-ACT-FA-SISB	4.800E-09	1	9.60E-09	1.92E-08
35	LP-MOP-MA-S11B SIS-ACT-FA-SISA	3.200E-09	1	6.40E-09	1.28E-08
36	LP-MOP-MA-S11A SIS-ACT-FA-SISB	3.200E-09	1	6.40E-09	1.28E-08
37	PL-MOV-PG-1864A SIS-ACT-FA-SISB	7.008E-10	1	1.40E-09	2.80E-09
38	PL-MOV-PG-1864B SIS-ACT-FA-SISA	7.008E-10	1	1.40E-09	2.80E-09
39	PL-CVKV-FT-CV46A SIS-ACT-FA-SISB	1.600E-10	1	3.20E-10	6.40E-10
40	PL-CVKV-FT-CV5B SIS-ACT-FA-SISB	1.600E-10	1	3.20E-10	6.40E-10
41	LP-CVKV-FT-CV46B SIS-ACT-FA-SISA	1.600E-10	1	3.20E-10	6.40E-10
42	LP-CVKV-FT-CV50 SIS-ACT-FA-SISA	1.600E-10	1	3.20E-10	6.40E-10
43	DCP-BOC-ST-BUS1B SIS-ACT-FA-SISA	1.440E-10	1	2.88E-10	6.76E-10
44	ACP-BAC-ST-4801J SIS-ACT-FA-SISA	1.440E-10	1	2.88E-10	6.76E-10
45	DCP-BOC-ST-BUS1 SIS-ACT-FA-SISB	1.440E-10	1	2.88E-10	6.76E-10
46	ACP-BAC-ST-4801H SIS-ACT-FA-SISB	1.440E-10	1	2.88E-10	6.76E-10
47	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	2.560E-09	2	1.02E-08	4.10E-08
48	CPC-XHE-FO-REALNHPH-MOV-FT-1115E HPI-XHE-FO-UN253 SIS-ACT-FA-SISA	1.922E-10	1	3.84E-10	7.69E-10
49	CPC-XHE-FO-REALNHPH-MOV-FT-1115D HPI-XHE-FO-UN253 SIS-ACT-FA-SISA	1.922E-10	1	3.84E-10	7.69E-10
50	CPC-XHE-FO-REALNHPH-MOV-FT-1115C HPI-XHE-FO-UN253 SIS-ACT-FA-SISB	1.922E-10	1	3.84E-10	7.69E-10
51	CPC-XHE-FO-REALNHPH-MOV-FT-1867C HPI-XHE-FO-UN253 SIS-ACT-FA-SISB	1.922E-10	1	3.84E-10	7.69E-10
52	CPC-XHE-FO-REALNHPH-MOV-FT-18670 HPI-XHE-FO-UN253 SIS-ACT-FA-SISA	1.922E-10	1	3.84E-10	7.69E-10
53	CPC-XHE-FO-REALNHPH-MOV-FT-1115B HPI-XHE-FO-UN253 SIS-ACT-FA-SISB	1.922E-10	1	3.84E-10	7.69E-10
54	CPC-XHE-FO-REALNHPH-XHE-FO-UN253 SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.025E-10	2	4.10E-10	1.64E-09
55	RCS-XHE-FO-DPT70SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.042E-08	2	4.17E-08	1.67E-07
56	ICC-ICC-FA-CCP8B CPC-MOP-FR-SW10A	2.229E-10	1	2.46E-09	4.92E-09
57	ICC-ICC-FA-CCP8B CPC-MOP-FR-CC2A	2.304E-10	1	4.61E-10	9.22E-10
58	ACP-BAC-ST-4KV1 CPC-ICC-FA-TCV8B	1.440E-10	1	2.88E-10	6.76E-10

COF CONTRIBUTIONS SUMTOTAL 1.60E-07 4.56E-07
 RELATIVE COF CONTRIBUTIONS 4.11E-03 1.25E-02

Table B4 Lightning-Related EMI Effects on COF Contributions
d:\16C-97\NUREG\TAB-B-4.WK3

No.	Cuteat	Base Freq. (/yr)	No. of I&C Basic Event In Cuteat	Basic Event Probability	Cuteat Freq. with I&Cs Failed (/yr)	Cuteat Freq. for Lightning EMI Events					
						Equipment Unavailability		Ti = 12 hours		Ti = 31 days	
						4.40E-05	4.40E-06	4.40E-05	4.40E-06	1.40E-05	1.40E-06
1	SIS-ACT-FA-SISA	2.580E-09	2	1.60E-03	1.00E-03	4.40E-05	4.40E-06	8.80E-04	8.80E-07	2.80E-03	2.80E-04
2	HPI-MOV-FT-1867C	1.042E-10	1	1.60E-03	6.51E-08	9.12E-13	4.40E-08	4.40E-09	8.80E-07	2.80E-06	2.80E-07
3	HPI-MOV-FT-1867C	1.042E-10	1	1.60E-03	6.51E-08	9.12E-13	2.87E-12	2.87E-13	5.73E-11	1.82E-10	1.82E-11
4	HPI-MOV-FT-1115C	1.042E-10	1	1.60E-03	6.51E-08	9.12E-13	2.87E-12	2.87E-13	5.73E-11	1.82E-10	1.82E-11
5	HPI-MOV-FT-1115C	1.042E-10	1	1.60E-03	6.51E-08	9.12E-13	2.87E-12	2.87E-13	5.73E-11	1.82E-10	1.82E-11
6	HPI-MOV-FT-1115C	1.042E-10	1	1.60E-03	6.51E-08	9.12E-13	2.87E-12	2.87E-13	5.73E-11	1.82E-10	1.82E-11
7	HPI-MOV-FT-1115C	1.042E-10	1	1.60E-03	6.51E-08	9.12E-13	2.87E-12	2.87E-13	5.73E-11	1.82E-10	1.82E-11
8	RMT-ACT-FA-RMTS	1.280E-09	2	1.60E-03	5.00E-04	7.00E-09	2.20E-08	2.20E-09	4.40E-07	1.40E-06	1.40E-07
9	PR-MOV-FT-1862A	2.602E-10	1	1.60E-03	1.66E-07	2.33E-12	7.32E-12	7.32E-13	1.46E-10	4.66E-10	4.66E-11
10	PR-MOV-FT-1862A	2.602E-10	1	1.60E-03	1.66E-07	2.33E-12	7.32E-12	7.32E-13	1.46E-10	4.66E-10	4.66E-11
11	PR-MOV-FT-1862A	1.536E-10	1	1.60E-03	9.00E-08	1.34E-12	4.22E-12	4.22E-13	8.45E-11	2.69E-10	2.69E-11
12	PR-MOV-FT-1862A	1.536E-10	1	1.60E-03	9.00E-08	1.34E-12	4.22E-12	4.22E-13	8.45E-11	2.69E-10	2.69E-11
13	PR-MOV-FT-1862A	1.536E-10	1	1.60E-03	9.00E-08	1.34E-12	4.22E-12	4.22E-13	8.45E-11	2.69E-10	2.69E-11
14	PR-MOV-FT-1862A	1.536E-10	1	1.60E-03	9.00E-08	1.34E-12	4.22E-12	4.22E-13	8.45E-11	2.69E-10	2.69E-11
15	LP-MOP-MA-S11B	1.042E-10	1	1.60E-03	6.51E-08	9.12E-13	2.87E-12	2.87E-13	5.73E-11	1.82E-10	1.82E-11
16	LP-MOP-MA-S11A	2.400E-09	1	1.60E-03	1.50E-06	2.10E-11	6.00E-11	6.00E-12	1.32E-09	4.20E-09	4.20E-10
17	LP-MOP-MA-S11B	2.400E-09	1	1.60E-03	1.50E-06	2.10E-11	6.00E-11	6.00E-12	1.32E-09	4.20E-09	4.20E-10
18	LP-MOP-MA-S11B	1.600E-09	1	1.60E-03	1.00E-06	1.40E-11	4.40E-11	4.40E-12	8.80E-10	2.80E-09	2.80E-10
19	LP-MOP-MA-S11A	1.600E-09	1	1.60E-03	1.00E-06	1.40E-11	4.40E-11	4.40E-12	8.80E-10	2.80E-09	2.80E-10
20	LP-MOP-MA-S11A	1.280E-09	1	1.60E-03	8.00E-07	1.12E-11	3.52E-11	3.52E-12	7.04E-10	2.24E-09	2.24E-10
21	SIS-ACT-FA-SISA	3.504E-10	1	1.60E-03	2.19E-07	3.07E-12	9.64E-12	9.64E-13	1.93E-10	6.13E-10	6.13E-11
22	LP-MOP-MA-S11B	3.504E-10	1	1.60E-03	2.19E-07	3.07E-12	9.64E-12	9.64E-13	1.93E-10	6.13E-10	6.13E-11
23	LP-MOP-MA-S11A	2.580E-09	2	1.60E-03	1.00E-03	1.40E-08	4.40E-08	4.40E-09	8.80E-07	2.80E-06	2.80E-07
24	RMT-ACT-FA-RMTS	5.325E-10	1	1.60E-03	3.33E-07	4.66E-12	1.46E-11	1.46E-12	2.93E-10	9.32E-10	9.32E-11
25	PR-MOV-FT-1862A	5.325E-10	1	1.60E-03	3.33E-07	4.66E-12	1.46E-11	1.46E-12	2.93E-10	9.32E-10	9.32E-11
26	PR-MOV-FT-1862A	3.072E-10	1	1.60E-03	1.92E-07	2.69E-12	8.45E-12	8.45E-13	1.69E-10	5.38E-10	5.38E-11
27	LP-MOP-MA-S11B	3.072E-10	1	1.60E-03	1.92E-07	2.69E-12	8.45E-12	8.45E-13	1.69E-10	5.38E-10	5.38E-11
28	LP-MOP-MA-S11A	3.072E-10	1	1.60E-03	1.92E-07	2.69E-12	8.45E-12	8.45E-13	1.69E-10	5.38E-10	5.38E-11
29	LP-MOP-MA-S11A	3.072E-10	1	1.60E-03	1.92E-07	2.69E-12	8.45E-12	8.45E-13	1.69E-10	5.38E-10	5.38E-11
30	PR-MOV-FT-1860A	2.048E-10	1	1.60E-03	1.28E-07	1.79E-12	5.63E-12	5.63E-13	1.13E-10	3.58E-10	3.58E-11
31	LP-MOP-MA-S11B	2.048E-10	1	1.60E-03	1.28E-07	1.79E-12	5.63E-12	5.63E-13	1.13E-10	3.58E-10	3.58E-11
32	LP-MOP-MA-S11A	4.800E-09	1	1.60E-03	3.00E-06	4.20E-11	1.32E-10	1.32E-11	2.64E-09	8.40E-09	8.40E-10
33	LP-MOP-MA-S11B	4.800E-09	1	1.60E-03	3.00E-06	4.20E-11	1.32E-10	1.32E-11	2.64E-09	8.40E-09	8.40E-10
34	LP-MOP-MA-S11A	3.200E-09	1	1.60E-03	2.00E-06	2.80E-11	8.80E-11	8.80E-12	1.76E-09	5.60E-09	5.60E-10
35	LP-MOP-MA-S11B	3.200E-09	1	1.60E-03	2.00E-06	2.80E-11	8.80E-11	8.80E-12	1.76E-09	5.60E-09	5.60E-10
36	LP-MOP-MA-S11A	7.008E-10	1	1.60E-03	4.38E-07	6.13E-12	1.93E-11	1.93E-12	3.85E-09	1.23E-09	1.23E-10
37	LP-MOP-MA-S11B	7.008E-10	1	1.60E-03	4.38E-07	6.13E-12	1.93E-11	1.93E-12	3.85E-09	1.23E-09	1.23E-10
38	LP-MOP-MA-S11A	1.600E-10	1	1.60E-03	1.00E-07	1.40E-12	4.40E-12	4.40E-13	8.80E-11	2.80E-10	2.80E-11
39	LP-MOP-MA-S11B	1.600E-10	1	1.60E-03	1.00E-07	1.40E-12	4.40E-12	4.40E-13	8.80E-11	2.80E-10	2.80E-11
40	LP-MOP-MA-S11A	1.600E-10	1	1.60E-03	1.00E-07	1.40E-12	4.40E-12	4.40E-13	8.80E-11	2.80E-10	2.80E-11
41	LP-MOP-MA-S11B	1.600E-10	1	1.60E-03	1.00E-07	1.40E-12	4.40E-12	4.40E-13	8.80E-11	2.80E-10	2.80E-11
42	LP-MOP-MA-S11A	1.440E-10	1	1.60E-03	9.00E-08	1.26E-12	3.96E-12	3.96E-13	7.92E-11	2.52E-10	2.52E-11
43	LP-MOP-MA-S11B	1.440E-10	1	1.60E-03	9.00E-08	1.26E-12	3.96E-12	3.96E-13	7.92E-11	2.52E-10	2.52E-11
44	LP-MOP-MA-S11A	1.440E-10	1	1.60E-03	9.00E-08	1.26E-12	3.96E-12	3.96E-13	7.92E-11	2.52E-10	2.52E-11
45	LP-MOP-MA-S11B	1.440E-10	1	1.60E-03	9.00E-08	1.26E-12	3.96E-12	3.96E-13	7.92E-11	2.52E-10	2.52E-11
46	LP-MOP-MA-S11A	2.580E-09	2	1.60E-03	1.00E-03	1.40E-08	4.40E-08	4.40E-09	8.80E-07	2.80E-06	2.80E-07
47	SIS-ACT-FA-SISA	1.922E-10	1	1.60E-03	1.20E-07	1.68E-12	5.29E-12	5.29E-13	1.06E-10	3.36E-10	3.36E-11
48	LP-MOP-MA-S11B	1.922E-10	1	1.60E-03	1.20E-07	1.68E-12	5.29E-12	5.29E-13	1.06E-10	3.36E-10	3.36E-11
49	LP-MOP-MA-S11A	1.922E-10	1	1.60E-03	1.20E-07	1.68E-12	5.29E-12	5.29E-13	1.06E-10	3.36E-10	3.36E-11
50	LP-MOP-MA-S11B	1.922E-10	1	1.60E-03	1.20E-07	1.68E-12	5.29E-12	5.29E-13	1.06E-10	3.36E-10	3.36E-11
51	LP-MOP-MA-S11A	1.922E-10	1	1.60E-03	1.20E-07	1.68E-12	5.29E-12	5.29E-13	1.06E-10	3.36E-10	3.36E-11
52	LP-MOP-MA-S11B	1.922E-10	1	1.60E-03	1.20E-07	1.68E-12	5.29E-12	5.29E-13	1.06E-10	3.36E-10	3.36E-11
53	LP-MOP-MA-S11A	1.032E-10	2	1.60E-03	4.00E-05	5.61E-10	1.76E-09	1.76E-10	3.52E-08	1.12E-07	1.12E-08
54	LP-MOP-MA-S11B	1.032E-10	2	1.60E-03	4.00E-05	5.61E-10	1.76E-09	1.76E-10	3.52E-08	1.12E-07	1.12E-08
55	LP-MOP-MA-S11A	1.032E-10	2	1.60E-03	4.00E-05	5.61E-10	1.76E-09	1.76E-10	3.52E-08	1.12E-07	1.12E-08
56	LP-MOP-MA-S11B	1.229E-09	1	3.20E-04	3.84E-06	5.38E-11	1.69E-10	1.69E-11	3.38E-09	1.08E-08	1.08E-09
57	LP-MOP-MA-S11A	2.304E-10	1	3.20E-04	7.20E-07	1.01E-11	3.17E-11	3.17E-12	6.34E-10	2.02E-09	2.02E-10
58	LP-MOP-MA-S11B	1.440E-10	1	1.60E-03	9.00E-08	1.26E-12	3.96E-12	3.96E-13	7.92E-11	2.52E-10	2.52E-11

COF CONTRIBUTIONS SUMTOTAL 1.069E-07 3.360E-07 3.360E-08 6.720E-06 2.138E-05 2.138E-06
 RELATIVE COF CONTRIBUTIONS 2.83E-03 9.21E-03 9.21E-04 1.84E-01 5.86E-01 5.86E-02

APPENDIX B

Table B5 Risk-Sensitivities to Smoke
d:\16C-97\NUREG21-TAB-B-5.WK3

No.	Cutset	Base Freq. (/yr)	No. of I&C Basic Event in Cutset	Basic Event Probability	Cutset Freq. w. I&Cs Failed (/yr)	Cutset Freq. for Smoke Events						
						T ₁ = 12 hours	T ₁ = 31 days					
1	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	2.560E-09	2	1.80E-03	1.00E-03	1.20E-06	8.20E-13	5.1E-06	7.80E-08	5.10E-11	3.10E-04	
2	HPI-MOV-FT-18670 SIS-ACT-FA-SISA CPC-XHE-FO-REALN HPI-XHE-FO-UN252	1.042E-10	1	1.80E-03	6.51E-08	7.82E-14	5.34E-17	3.32E-13	4.95E-12	3.32E-15	2.02E-11	
3	HPI-MOV-FT-18670 SIS-ACT-FA-SISA CPC-XHE-FO-REALN HPI-XHE-FO-UN252	1.042E-10	1	1.80E-03	6.51E-08	7.82E-14	5.34E-17	3.32E-13	4.95E-12	3.32E-15	2.02E-11	
4	HPI-MOV-FT-1115D SIS-ACT-FA-SISA HPI-XHE-FO-UN252 CPC-XHE-FO-REALN 1.042E-10	1.042E-10	1	1.80E-03	6.51E-08	7.82E-14	5.34E-17	3.32E-13	4.95E-12	3.32E-15	2.02E-11	
5	HPI-MOV-FT-1115D SIS-ACT-FA-SISA HPI-XHE-FO-UN252 CPC-XHE-FO-REALN 1.042E-10	1.042E-10	1	1.80E-03	6.51E-08	7.82E-14	5.34E-17	3.32E-13	4.95E-12	3.32E-15	2.02E-11	
6	HPI-MOV-FT-1115E SIS-ACT-FA-SISA HPI-XHE-FO-UN252 CPC-XHE-FO-REALN 1.042E-10	1.042E-10	1	1.80E-03	6.51E-08	7.82E-14	5.34E-17	3.32E-13	4.95E-12	3.32E-15	2.02E-11	
7	HPI-MOV-FT-1115E SIS-ACT-FA-SISA HPI-XHE-FO-UN252 CPC-XHE-FO-REALN 1.042E-10	1.042E-10	1	1.80E-03	6.51E-08	7.82E-14	5.34E-17	3.32E-13	4.95E-12	3.32E-15	2.02E-11	
8	RMT-ACT-FA-RMTS RMT-ACT-FA-RMTS 1.280E-09	1.280E-09	2	1.80E-03	5.00E-04	6.00E-10	4.10E-13	2.55E-09	3.80E-08	2.55E-11	1.55E-07	
9	PR-MOV-FT-18628 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	2.662E-10	1	1.80E-03	1.86E-07	2.00E-13	1.36E-16	8.49E-13	1.26E-11	8.49E-15	5.16E-11	
10	LPI-MDP-FS-S11A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	2.662E-10	1	1.80E-03	1.86E-07	2.00E-13	1.36E-16	8.49E-13	1.26E-11	8.49E-15	5.16E-11	
11	LPI-MDP-FS-S11A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.539E-10	1	1.80E-03	9.80E-08	1.15E-13	7.87E-17	4.90E-13	7.30E-12	4.90E-15	2.98E-11	
12	LPI-MDP-FS-S11B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.539E-10	1	1.80E-03	9.80E-08	1.15E-13	7.87E-17	4.90E-13	7.30E-12	4.90E-15	2.98E-11	
13	LPR-MOV-FT-18608 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.539E-10	1	1.80E-03	9.80E-08	1.15E-13	7.87E-17	4.90E-13	7.30E-12	4.90E-15	2.98E-11	
14	LPR-MOV-FT-18608 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.539E-10	1	1.80E-03	9.80E-08	1.15E-13	7.87E-17	4.90E-13	7.30E-12	4.90E-15	2.98E-11	
15	LPI-MOP-MA-S11B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.042E-10	1	1.80E-03	6.51E-08	7.82E-14	5.34E-17	3.32E-13	4.95E-12	3.32E-15	2.02E-11	
16	LPI-MOP-MA-S11A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.042E-10	1	1.80E-03	6.51E-08	7.82E-14	5.34E-17	3.32E-13	4.95E-12	3.32E-15	2.02E-11	
17	LPI-MDP-FS-S11A SIS-ACT-FA-SISB	2.400E-09	1	1.80E-03	1.50E-06	1.80E-12	1.23E-15	7.65E-12	1.14E-10	7.65E-14	4.65E-10	
18	LPI-MOP-MA-S11B SIS-ACT-FA-SISA	2.400E-09	1	1.80E-03	1.50E-06	1.80E-12	1.23E-15	7.65E-12	1.14E-10	7.65E-14	4.65E-10	
19	LPI-MOP-MA-S11A SIS-ACT-FA-SISA	1.600E-09	1	1.80E-03	1.00E-06	1.20E-12	8.20E-16	5.10E-12	7.80E-11	5.10E-14	3.10E-10	
20	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.280E-09	1	1.80E-03	8.00E-07	9.60E-13	6.56E-16	4.08E-12	6.08E-11	4.08E-14	2.48E-10	
21	LPI-MOP-PG-18648 SIS-ACT-FA-SISA	3.504E-10	1	1.80E-03	2.19E-07	2.63E-13	1.80E-16	1.12E-12	1.66E-11	1.12E-14	6.79E-11	
22	LPI-MOP-PG-18648 SIS-ACT-FA-SISB	3.504E-10	1	1.80E-03	2.19E-07	2.63E-13	1.80E-16	1.12E-12	1.66E-11	1.12E-14	6.79E-11	
23	RMT-ACT-FA-RMTS RMT-ACT-FA-RMTS 2.560E-09	2.560E-09	2	1.80E-03	3.33E-07	3.99E-13	2.73E-16	1.70E-12	7.80E-08	5.10E-11	3.10E-07	
24	LPR-MOV-FT-18628 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN51	5.325E-10	1	1.80E-03	3.33E-07	3.99E-13	2.73E-16	1.70E-12	2.53E-11	1.70E-14	1.03E-10	
25	LPR-MOV-FT-18628 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN51	5.325E-10	1	1.80E-03	3.33E-07	3.99E-13	2.73E-16	1.70E-12	2.53E-11	1.70E-14	1.03E-10	
26	LPI-MOP-FS-S11B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN51	3.072E-10	1	1.80E-03	1.92E-07	2.30E-13	1.57E-16	9.79E-13	1.46E-11	9.79E-15	5.95E-11	
27	LPI-MOP-FS-S11B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN51	3.072E-10	1	1.80E-03	1.92E-07	2.30E-13	1.57E-16	9.79E-13	1.46E-11	9.79E-15	5.95E-11	
28	LPR-MOV-FT-18608 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN51	3.072E-10	1	1.80E-03	1.92E-07	2.30E-13	1.57E-16	9.79E-13	1.46E-11	9.79E-15	5.95E-11	
29	LPI-MOP-FS-S11A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN51	3.072E-10	1	1.80E-03	1.92E-07	2.30E-13	1.57E-16	9.79E-13	1.46E-11	9.79E-15	5.95E-11	
30	LPR-MOV-FT-18608 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN51	3.072E-10	1	1.80E-03	1.92E-07	2.30E-13	1.57E-16	9.79E-13	1.46E-11	9.79E-15	5.95E-11	
31	LPI-MOP-MA-S11B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN51	2.048E-10	1	1.80E-03	1.28E-07	1.54E-13	1.08E-16	6.53E-13	9.73E-12	6.53E-15	3.97E-11	
32	LPI-MOP-MA-S11A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN51	2.048E-10	1	1.80E-03	1.28E-07	1.54E-13	1.08E-16	6.53E-13	9.73E-12	6.53E-15	3.97E-11	
33	LPI-MOP-FS-S11B SIS-ACT-FA-SISA	4.800E-09	1	1.80E-03	3.00E-06	3.60E-12	2.46E-15	1.53E-11	2.28E-10	1.53E-13	9.30E-10	
34	LPI-MOP-FS-S11A SIS-ACT-FA-SISB	4.800E-09	1	1.80E-03	3.00E-06	3.60E-12	2.46E-15	1.53E-11	2.28E-10	1.53E-13	9.30E-10	
35	LPI-MOP-MA-S11B SIS-ACT-FA-SISA	3.200E-09	1	1.80E-03	2.00E-06	2.40E-12	1.64E-15	1.02E-11	1.52E-10	1.02E-13	6.20E-10	
36	LPI-MOP-MA-S11A SIS-ACT-FA-SISB	3.200E-09	1	1.80E-03	2.00E-06	2.40E-12	1.64E-15	1.02E-11	1.52E-10	1.02E-13	6.20E-10	
37	LPI-MOP-PG-1864A SIS-ACT-FA-SISB	7.009E-10	1	1.80E-03	4.38E-07	5.29E-13	3.59E-16	2.23E-12	3.33E-11	2.23E-14	1.36E-10	
38	LPI-MOP-PG-1864B SIS-ACT-FA-SISA	7.009E-10	1	1.80E-03	4.38E-07	5.29E-13	3.59E-16	2.23E-12	3.33E-11	2.23E-14	1.36E-10	
39	LPI-MOP-FS-S11B SIS-ACT-FA-SISB	1.600E-10	1	1.80E-03	1.00E-07	1.20E-13	8.20E-17	5.10E-13	7.80E-12	5.10E-15	3.10E-11	
40	LPI-MOP-FS-S11A SIS-ACT-FA-SISB	1.600E-10	1	1.80E-03	1.00E-07	1.20E-13	8.20E-17	5.10E-13	7.80E-12	5.10E-15	3.10E-11	
41	LPI-MOP-FS-S11A SIS-ACT-FA-SISA	1.600E-10	1	1.80E-03	1.00E-07	1.20E-13	8.20E-17	5.10E-13	7.80E-12	5.10E-15	3.10E-11	
42	LPI-MOP-FS-S11A SIS-ACT-FA-SISA	1.600E-10	1	1.80E-03	1.00E-07	1.20E-13	8.20E-17	5.10E-13	7.80E-12	5.10E-15	3.10E-11	
43	DCP-80C-ST-BU518 SIS-ACT-FA-SISA	1.440E-10	1	1.80E-03	9.00E-08	1.08E-13	7.38E-17	4.59E-13	6.84E-12	4.59E-15	2.79E-11	
44	DCP-80C-ST-BU518 SIS-ACT-FA-SISA	1.440E-10	1	1.80E-03	9.00E-08	1.08E-13	7.38E-17	4.59E-13	6.84E-12	4.59E-15	2.79E-11	
45	DCP-80C-ST-BU51A SIS-ACT-FA-SISB	1.440E-10	1	1.80E-03	9.00E-08	1.08E-13	7.38E-17	4.59E-13	6.84E-12	4.59E-15	2.79E-11	
46	DCP-80C-ST-BU51A SIS-ACT-FA-SISA	1.440E-10	1	1.80E-03	9.00E-08	1.08E-13	7.38E-17	4.59E-13	6.84E-12	4.59E-15	2.79E-11	
47	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	2.560E-09	2	1.80E-03	1.00E-03	1.20E-09	8.20E-13	5.10E-09	7.80E-08	5.10E-11	3.10E-07	
48	CPC-XHE-FO-REALN HPI-MOV-FT-1115E HPI-XHE-FO-UN253 SIS-ACT-FA-SISA	1.922E-10	1	1.80E-03	1.20E-07	1.44E-13	9.89E-17	6.13E-13	9.13E-12	6.13E-15	3.72E-11	
49	CPC-XHE-FO-REALN HPI-MOV-FT-1115D HPI-XHE-FO-UN253 SIS-ACT-FA-SISA	1.922E-10	1	1.80E-03	1.20E-07	1.44E-13	9.89E-17	6.13E-13	9.13E-12	6.13E-15	3.72E-11	
50	CPC-XHE-FO-REALN HPI-MOV-FT-1115C HPI-XHE-FO-UN253 SIS-ACT-FA-SISB	1.922E-10	1	1.80E-03	1.20E-07	1.44E-13	9.89E-17	6.13E-13	9.13E-12	6.13E-15	3.72E-11	
51	CPC-XHE-FO-REALN HPI-MOV-FT-1115C HPI-XHE-FO-UN253 SIS-ACT-FA-SISA	1.922E-10	1	1.80E-03	1.20E-07	1.44E-13	9.89E-17	6.13E-13	9.13E-12	6.13E-15	3.72E-11	
52	CPC-XHE-FO-REALN HPI-MOV-FT-18670 HPI-XHE-FO-UN253 SIS-ACT-FA-SISB	1.922E-10	1	1.80E-03	1.20E-07	1.44E-13	9.89E-17	6.13E-13	9.13E-12	6.13E-15	3.72E-11	
53	CPC-XHE-FO-REALN HPI-MOV-FT-18670 HPI-XHE-FO-UN253 SIS-ACT-FA-SISA	1.922E-10	1	1.80E-03	1.20E-07	1.44E-13	9.89E-17	6.13E-13	9.13E-12	6.13E-15	3.72E-11	
54	CPC-XHE-FO-REALN HPI-MOV-FT-1115B HPI-XHE-FO-UN253 SIS-ACT-FA-SISB	1.025E-10	2	1.80E-03	4.00E-05	4.80E-11	3.28E-14	2.04E-10	3.04E-09	2.04E-12	1.24E-08	
55	CPC-XHE-FO-REALN HPI-MOV-FT-1115B HPI-XHE-FO-UN253 SIS-ACT-FA-SISA	1.025E-10	2	1.80E-03	4.00E-05	4.80E-11	3.28E-14	2.04E-10	3.04E-09	2.04E-12	1.24E-08	
56	RCS-XHE-FO-PTD7D SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.042E-08	2	3.20E-04	3.84E-06	4.61E-12	3.15E-15	1.96E-11	2.92E-10	1.96E-13	1.19E-09	
57	EPC-ICC-FA-SWPBS CPC-MOP-FR-SW10A	2.304E-10	1	3.20E-04	7.20E-07	8.64E-13	5.80E-16	3.67E-12	5.47E-11	3.67E-14	2.23E-10	
58	ACP-BAC-ST-4KVTHCPC-ICC-FA-TCVBB	1.440E-10	1	1.80E-03	9.00E-08	1.08E-13	7.38E-17	4.59E-13	6.84E-12	4.59E-15	2.79E-11	
COF CONTRIBUTIONS5 SUMTOTAL						5.552E-08	9.16E-09	6.26E-12	3.89E-08	5.80E-07	3.89E-10	2.37E-06
RELATIVE COF CONTRIBUTIONS5						1.52E-03	2.51E-04	1.72E-07	1.07E-03	1.59E-02	1.07E-05	6.49E-02

Table 68 Sensitivity to Assumptions of Temperature Effects on CDF Contributions (for change from 75 F)
 d:\L&C-97\NUREG\TA0-B-6\WK3

No.	Cutset	Base Freq.	No. of I&C Basic Events in Cutset	Environmental Factor		CDF Contributions (/yr)
				104 F	104 F	
1	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	2,560E-09	2	1.06	1.06	1,80E-10
2	HPI-MOV-FT-18670 SIS-ACT-FA-SISA CPC-XHE-FO-REALN HPI-XHE-FO-UNZS2	1,042E-10	1	1.06	1.06	2,78E-11
3	HPI-MOV-FT-18670 SIS-ACT-FA-SISB CPC-XHE-FO-REALN HPI-XHE-FO-UNZS2	1,042E-10	1	1.06	1.06	2,78E-11
4	HPI-MOV-FT-11150 SIS-ACT-FA-SISA HPI-XHE-FO-UNZS2 CPC-XHE-FO-REALN	1,042E-10	1	1.06	1.06	2,78E-11
5	HPI-MOV-FT-11150 SIS-ACT-FA-SISB HPI-XHE-FO-UNZS2 CPC-XHE-FO-REALN	1,042E-10	1	1.06	1.06	2,78E-11
6	HPI-MOV-FT-1115E SIS-ACT-FA-SISA HPI-XHE-FO-UNZS2 CPC-XHE-FO-REALN	1,042E-10	1	1.06	1.06	2,78E-11
7	HPI-MOV-FT-1115E SIS-ACT-FA-SISB HPI-XHE-FO-UNZS2 CPC-XHE-FO-REALN	1,042E-10	1	1.06	1.06	2,78E-11
8	RMT-ACT-FA-RMTS RMT-ACT-FA-RMTS6	1,280E-09	2	1.06	1.06	6,99E-11
9	PR-MOV-FT-18628 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	2,862E-10	1	1.06	1.06	7,05E-11
10	PR-MOV-FT-18628 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	2,862E-10	1	1.06	1.06	7,05E-11
11	PL-MDP-FS-S1A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1,536E-10	1	1.06	1.06	4,07E-11
12	PL-MDP-FS-S1B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1,536E-10	1	1.06	1.06	4,07E-11
13	PR-MOV-FT-18608 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1,536E-10	1	1.06	1.06	4,07E-11
14	PR-MOV-FT-18608 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1,536E-10	1	1.06	1.06	4,07E-11
15	PL-MOP-MA-S1B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1,042E-10	1	1.06	1.06	2,78E-11
16	PL-MOP-MA-S1A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1,042E-10	1	1.06	1.06	2,78E-11
17	PL-MOP-FS-S1A SIS-ACT-FA-SISB	2,400E-09	1	1.06	1.06	6,36E-10
18	PL-MOP-FS-S1B SIS-ACT-FA-SISA	2,400E-09	1	1.06	1.06	6,36E-10
19	PL-MOP-MA-S1B SIS-ACT-FA-SISA	1,600E-09	1	1.06	1.06	4,24E-10
20	PL-MOP-MA-S1A SIS-ACT-FA-SISB	1,600E-09	1	1.06	1.06	4,24E-10
21	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1,280E-09	1	1.06	1.06	3,38E-10
22	PL-MOV-PG-18648 SIS-ACT-FA-SISA	3,504E-10	1	1.06	1.06	9,29E-11
23	PL-MOV-PG-1864A SIS-ACT-FA-SISB	3,504E-10	1	1.06	1.06	9,29E-11
24	RMT-ACT-FA-RMTS RMT-ACT-FA-RMTS6	2,560E-09	2	1.06	1.06	1,80E-10
25	PR-MOV-FT-18628 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-S1	5,325E-10	1	1.06	1.06	1,41E-10
26	PR-MOV-FT-18628 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-S1	3,072E-10	1	1.06	1.06	8,14E-11
27	PL-MOP-FS-S1B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-S1	3,072E-10	1	1.06	1.06	8,14E-11
28	PR-MOV-FT-18608 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-S1	3,072E-10	1	1.06	1.06	8,14E-11
29	PL-MOP-FS-S1A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-S1	3,072E-10	1	1.06	1.06	8,14E-11
30	PR-MOV-FT-18608 RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-S1	3,072E-10	1	1.06	1.06	8,14E-11
31	PL-MOP-MA-S1B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-S1	2,046E-10	1	1.06	1.06	5,43E-11
32	PL-MOP-MA-S1A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-S1	2,046E-10	1	1.06	1.06	5,43E-11
33	PL-MOP-FS-S1B SIS-ACT-FA-SISA	4,800E-09	1	1.06	1.06	1,27E-09
34	PL-MOP-FS-S1A SIS-ACT-FA-SISA	4,800E-09	1	1.06	1.06	1,27E-09
35	PL-MOP-MA-S1B SIS-ACT-FA-SISA	3,200E-09	1	1.06	1.06	8,48E-10
36	PL-MOP-MA-S1A SIS-ACT-FA-SISB	3,200E-09	1	1.06	1.06	8,48E-10
37	PL-MOV-PG-1864A SIS-ACT-FA-SISB	7,006E-10	1	1.06	1.06	1,88E-10
38	PL-MOV-PG-1864B SIS-ACT-FA-SISA	7,006E-10	1	1.06	1.06	1,88E-10
39	PL-KV-FT-CV46A SIS-ACT-FA-SISB	1,600E-10	1	1.06	1.06	4,24E-11
40	PL-KV-FT-CV58 SIS-ACT-FA-SISA	1,600E-10	1	1.06	1.06	4,24E-11
41	PL-KV-FT-CV46B SIS-ACT-FA-SISA	1,600E-10	1	1.06	1.06	4,24E-11
42	PL-KV-FT-CV50 SIS-ACT-FA-SISA	1,600E-10	1	1.06	1.06	4,24E-11
43	DCP-BOC-ST-6051B SIS-ACT-FA-SISA	1,440E-10	1	1.06	1.06	3,82E-11
44	ACP-BAC-ST-4801J SIS-ACT-FA-SISA	1,440E-10	1	1.06	1.06	3,82E-11
45	DCP-BOC-ST-6051A SIS-ACT-FA-SISB	1,440E-10	1	1.06	1.06	3,82E-11
46	ACP-BAC-ST-4801H SIS-ACT-FA-SISB	1,440E-10	1	1.06	1.06	3,82E-11
47	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	2,560E-09	2	1.06	1.06	1,80E-10
48	CPC-XHE-FO-REALN HPI-MOV-FT-1115E HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISA	1,922E-10	1	1.06	1.06	5,09E-11
49	CPC-XHE-FO-REALN HPI-MOV-FT-1115D HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISA	1,922E-10	1	1.06	1.06	5,09E-11
50	CPC-XHE-FO-REALN HPI-MOV-FT-1115C HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISB	1,922E-10	1	1.06	1.06	5,09E-11
51	CPC-XHE-FO-REALN HPI-MOV-FT-18670 HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISB	1,922E-10	1	1.06	1.06	5,09E-11
52	CPC-XHE-FO-REALN HPI-MOV-FT-18670 HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISA	1,922E-10	1	1.06	1.06	5,09E-11
53	CPC-XHE-FO-REALN HPI-MOV-FT-1115E HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISB	1,922E-10	1	1.06	1.06	5,09E-11
54	CPC-XHE-FO-REALN HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1,025E-10	2	1.06	1.06	7,20E-12
55	RCS-XHE-FO-D7D SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1,042E-08	2	1.06	1.06	7,32E-10
56	CPC-ICC-FA-SWP8S CPC-MOP-RR-SW10A	1,229E-09	1	1.06	1.06	3,26E-10
57	CPC-ICC-FA-CCP8S CPC-MOP-RR-CC2A	2,304E-10	1	1.06	1.06	6,11E-11
58	ACP-BAC-ST-4KV1H CPC-ICC-FA-1CV6B	1,440E-10	1	1.06	1.06	3,82E-11

COF CONTRIBUTIONS SUMTOTAL 5.552E-08 1.09E-08

RELATIVE COF CONTRIBUTIONS 1.52E-03 2.99E-04

APPENDIX B

Table B7 Sensitivity to Assumption of Temperature-Humidity Effects on CDF Contributions
 d:\&C-97\NUREG2\TAB-B-7.wk3

REL. HUMIDITY (%) TEMP (F)	CDF CONTRIBUTIONS FROM I&C				
	60	70	80	90	100
75	1.02E-08	1.74E-08	2.82E-08	4.52E-08	6.91E-08
90	3.19E-08	5.83E-08	1.03E-07	1.74E-07	2.87E-07
110	1.70E-07	3.56E-07	7.02E-07	1.31E-06	2.33E-06

REL. HUMIDITY (%) TEMP (F)	RELATIVE CDF CONTRIBUTIONS				
	60	70	80	90	100
75	2.80E-04	4.76E-04	7.73E-04	1.24E-03	1.89E-03
90	8.73E-04	1.60E-03	2.81E-03	4.77E-03	7.87E-03
110	4.67E-03	9.77E-03	1.93E-02	3.60E-02	6.40E-02

Table B8 Sensitivity to Assumption of Vibration Effects on CDF Contributions
d11&C-97NUNREG21AB-B-8.WK3

No.	Cutset	Base Frag. (/yr)	No. of Basic Events in Cutset	Cutset Freq. (/yr)	
				Environmental Factor 2	4
1	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	2.680E-09	2	6.40E-10	2.58E-09
2	HPI-MOV-FT-1887D SIS-ACT-FA-SISA CPC-XHE-FO-REALHPI-XHE-FO-UN2S2	1.042E-10	1	5.21E-11	1.04E-10
3	HPI-MOV-FT-1887C SIS-ACT-FA-SISB CPC-XHE-FO-REALHPI-XHE-FO-UN2S2	1.042E-10	1	5.21E-11	1.04E-10
4	HPI-MOV-FT-1155D SIS-ACT-FA-SISA HPI-XHE-FO-REALHPI-XHE-FO-UN2S2 CPC-XHE-FO-REAL	1.042E-10	1	5.21E-11	1.04E-10
5	HPI-MOV-FT-1155C SIS-ACT-FA-SISB HPI-XHE-FO-REALHPI-XHE-FO-UN2S2 CPC-XHE-FO-REAL	1.042E-10	1	5.21E-11	1.04E-10
6	HPI-MOV-FT-1155E SIS-ACT-FA-SISA HPI-XHE-FO-REALHPI-XHE-FO-UN2S2 CPC-XHE-FO-REAL	1.042E-10	1	5.21E-11	1.04E-10
7	HPI-MOV-FT-1155B SIS-ACT-FA-SISB HPI-XHE-FO-REALHPI-XHE-FO-UN2S2 CPC-XHE-FO-REAL	1.042E-10	1	5.21E-11	1.04E-10
8	RMT-ACT-FA-RMTS RMT-ACT-FA-RMTS	1.280E-09	2	3.20E-10	1.28E-09
9	LPR-MOV-FT-1862B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	2.862E-10	1	1.33E-10	2.86E-10
10	LPR-MOV-FT-1862A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	2.882E-10	1	1.33E-10	2.86E-10
11	LPI-MDP-FS-SI1A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.536E-10	1	7.68E-11	1.54E-10
12	LPI-MDP-FS-SI1B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.536E-10	1	7.68E-11	1.54E-10
13	LPR-MOV-FT-1860B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.638E-10	1	7.68E-11	1.54E-10
14	LPR-MOV-FT-1860A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.638E-10	1	7.68E-11	1.54E-10
15	LPI-MDP-MA-SI1B RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.042E-10	1	5.21E-11	1.04E-10
16	LPI-MDP-MA-SI1A RMT-ACT-FA-RMTS RMT-XHE-FO-MAN-A	1.042E-10	1	5.21E-11	1.04E-10
17	LPI-MDP-FS-SI1A SIS-ACT-FA-SISB	2.400E-09	1	1.20E-09	2.40E-09
18	LPI-MDP-FS-SI1B SIS-ACT-FA-SISA	2.400E-09	1	1.20E-09	2.40E-09
19	LPI-MDP-MA-SI1A SIS-ACT-FA-SISA	1.800E-09	1	8.00E-10	1.80E-09
20	LPI-MDP-MA-SI1B SIS-ACT-FA-SISB	1.800E-09	1	8.00E-10	1.80E-09
21	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.280E-09	1	8.40E-10	1.28E-09
22	LPI-MOV-PG-1864A SIS-ACT-FA-SISA	3.504E-10	1	1.76E-10	3.50E-10
23	LPI-MOV-PG-1864B SIS-ACT-FA-SISB	3.504E-10	1	1.76E-10	3.50E-10
24	RMT-ACT-FA-RMTS RMT-ACT-FA-RMTS	2.580E-09	2	6.40E-10	2.58E-09
25	LPR-MOV-FT-1882B RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	5.325E-10	1	2.66E-10	5.33E-10
26	LPR-MOV-FT-1882A RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	5.325E-10	1	2.66E-10	5.33E-10
27	LPI-MDP-FS-SI1B RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	3.072E-10	1	1.54E-10	3.07E-10
28	LPR-MOV-FT-1860B RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	3.072E-10	1	1.54E-10	3.07E-10
29	LPI-MDP-FS-SI1A RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	3.072E-10	1	1.54E-10	3.07E-10
30	LPR-MOV-FT-1860A RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	3.072E-10	1	1.54E-10	3.07E-10
31	LPI-MDP-MA-SI1B RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	2.048E-10	1	1.02E-10	2.05E-10
32	LPI-MDP-MA-SI1A RMT-ACT-FA-RMTS RMT-XHE-FO-MANS1	2.048E-10	1	1.02E-10	2.05E-10
33	LPI-MDP-FS-SI1B SIS-ACT-FA-SISA	4.800E-09	1	2.40E-09	4.80E-09
34	LPI-MDP-FS-SI1A SIS-ACT-FA-SISB	4.800E-09	1	2.40E-09	4.80E-09
35	LPI-MDP-MA-SI1B SIS-ACT-FA-SISA	3.200E-09	1	1.60E-09	3.20E-09
36	LPI-MDP-MA-SI1A SIS-ACT-FA-SISB	3.200E-09	1	1.60E-09	3.20E-09
37	LPI-MOV-PG-1864A SIS-ACT-FA-SISA	7.008E-10	1	3.50E-10	7.01E-10
38	LPI-MOV-PG-1864B SIS-ACT-FA-SISB	7.008E-10	1	3.50E-10	7.01E-10
39	LPI-CKV-FT-CV46A SIS-ACT-FA-SISA	1.600E-10	1	8.00E-11	1.60E-10
40	LPI-CKV-FT-CV58 SIS-ACT-FA-SISB	1.600E-10	1	8.00E-11	1.60E-10
41	LPI-CKV-FT-CV46B SIS-ACT-FA-SISA	1.600E-10	1	8.00E-11	1.60E-10
42	LPI-CKV-FT-CV50 SIS-ACT-FA-SISB	1.600E-10	1	8.00E-11	1.60E-10
43	DCP-BDC-ST-8US1B SIS-ACT-FA-SISA	1.440E-10	1	7.20E-11	1.44E-10
44	ACP-BAC-ST-4801J SIS-ACT-FA-SISA	1.440E-10	1	7.20E-11	1.44E-10
45	DCP-BDC-ST-8US1A SIS-ACT-FA-SISB	1.440E-10	1	7.20E-11	1.44E-10
46	ACP-BAC-ST-4801H SIS-ACT-FA-SISA	2.660E-09	2	6.40E-10	2.66E-09
47	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.822E-10	1	8.61E-11	1.92E-10
48	CPC-XHE-FO-REALHPI-MOV-FT-1116E HPI-XHE-FO-UN2S3 SIS-ACT-FA-SISA	1.822E-10	1	9.61E-11	1.92E-10
49	CPC-XHE-FO-REALHPI-MOV-FT-1115D HPI-XHE-FO-UN2S3 SIS-ACT-FA-SISA	1.822E-10	1	9.61E-11	1.92E-10
50	CPC-XHE-FO-REALHPI-MOV-FT-1116C HPI-XHE-FO-UN2S3 SIS-ACT-FA-SISB	1.822E-10	1	9.61E-11	1.92E-10
51	CPC-XHE-FO-REALHPI-MOV-FT-1887C HPI-XHE-FO-UN2S3 SIS-ACT-FA-SISB	1.822E-10	1	9.61E-11	1.92E-10
52	CPC-XHE-FO-REALHPI-MOV-FT-1887D HPI-XHE-FO-UN2S3 SIS-ACT-FA-SISA	1.822E-10	1	9.61E-11	1.92E-10
53	CPC-XHE-FO-REALHPI-MOV-FT-1116B HPI-XHE-FO-UN2S3 SIS-ACT-FA-SISB	1.822E-10	1	9.61E-11	1.92E-10
54	CPC-XHE-FO-REALHPI-XHE-FO-UN2S3 SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.028E-10	2	2.58E-11	1.03E-10
55	RCS-XHE-FO-DPT7D SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.229E-08	2	2.61E-09	1.04E-08
56	ICP-ICC-FA-CCP8B CPC-MDP-FR-SW10A	2.304E-10	1	1.15E-10	2.30E-10
57	ICP-ICC-FA-CCP8A CPC-MDP-FR-CC2A	2.304E-10	1	1.15E-10	2.30E-10
58	ACP-BAC-ST-4KV1 CPC-ICC-FA-1CV8B	1.440E-10	1	7.20E-11	1.44E-10
CDF CONTRIBUTIONS SUMTOTAL				2.29E-08	6.65E-08
RELATIVE CDF CONTRIBUTIONS				1.52E-03	1.62E-03

APPENDIX B

Table B9 Sensitivity to Assumptions of Lightning-Related EMI Effects on COF Contributions

No.	Cutset	Base Freq. (yr)	No. of I&C Basic Event In Cutset	Basic Event Probability	Current Freq. with I&Cs Failed (yr)	Current Freq. for Lightning EMI Events	
						Tr = 12 hours	Tr = 31 days
1	SIS-ACT-FA-SISA	2.50E-09	2	1.00E-03	1.00E-03	3.50E-06	1.10E-08
2	HPI-MOV-FT-18670	1.042E-10	1	1.00E-03	6.51E-08	1.10E-09	1.10E-08
3	HPI-MOV-FT-18670	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
4	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
5	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
6	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
7	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
8	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
9	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
10	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
11	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
12	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
13	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
14	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
15	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
16	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
17	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
18	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
19	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
20	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
21	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
22	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
23	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
24	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
25	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
26	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
27	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
28	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
29	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
30	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
31	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
32	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
33	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
34	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
35	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
36	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
37	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
38	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
39	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
40	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
41	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
42	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
43	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
44	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
45	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
46	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
47	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
48	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
49	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
50	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
51	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
52	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
53	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
54	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
55	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
56	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
57	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14
58	HPI-MOV-FT-11150	1.042E-10	1	1.00E-03	6.51E-08	2.28E-13	7.16E-14

COF CONTRIBUTIONS SUMTOTAL 2.673E-08 8.400E-08 8.400E-09 1.680E-06 5.348E-06 5.348E-07

RELATIVE COF CONTRIBUTIONS 7.39E-04 2.30E-03 2.30E-04 4.61E-02 1.47E-01 1.47E-02

Table B10 Sensitivity to Assumptions of Smoke Events on COF Contributions
d:\1\C-97\NUREG2TAB-B-10.WK3

No	Cutset	Base Freq. (1/yr)	No. of I&C Basic Event in Cutset	Basic Event Probability	Cutset Freq. w. I&C Failed (1/yr)	Cutset Freq. for Smoke Events	
						T ₁ = 12 hours	T ₂ = 31 days
1	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	2.560E-09	2	1.60E-03	3.00E-07	2.05E-10	1.90E-05
2	HPI-MOV-FT-1867D SIS-ACT-FA-SISA CPC-XHE-FO-REALM HPI-XHE-FO-UNZS2	1.042E-10	1	1.60E-03	3.00E-14	2.05E-13	1.90E-08
3	HPI-MOV-FT-1867C SIS-ACT-FA-SISB CPC-XHE-FO-REALM HPI-XHE-FO-UNZS2	1.042E-10	1	1.60E-03	1.95E-14	1.34E-17	8.30E-11
4	HPI-MOV-FT-1115D SIS-ACT-FA-SISA HPI-XHE-FO-REALM HPI-XHE-FO-UNZS2 CPC-XHE-FO-REALM	1.042E-10	1	1.60E-03	1.95E-14	1.34E-17	8.30E-11
5	HPI-MOV-FT-1115E SIS-ACT-FA-SISB HPI-XHE-FO-REALM HPI-XHE-FO-UNZS2 CPC-XHE-FO-REALM	1.042E-10	1	1.60E-03	1.95E-14	1.34E-17	8.30E-11
6	HPI-MOV-FT-1115F SIS-ACT-FA-SISA HPI-XHE-FO-REALM HPI-XHE-FO-UNZS2 CPC-XHE-FO-REALM	1.042E-10	1	1.60E-03	1.95E-14	1.34E-17	8.30E-11
7	HPI-MOV-FT-1115B SIS-ACT-FA-SISB HPI-XHE-FO-REALM HPI-XHE-FO-UNZS2 CPC-XHE-FO-REALM	1.042E-10	2	1.60E-03	1.95E-14	1.34E-17	8.30E-11
8	RMT-ACT-FA-RMSTS RMT-ACT-FA-RMSTS RMT-XHE-FO-MAN-A	1.280E-09	2	1.60E-03	5.00E-04	1.02E-13	9.50E-09
9	LPR-MOV-FT-1862B RMT-ACT-FA-RMSTS RMT-XHE-FO-MAN-A	2.692E-10	1	1.60E-03	1.06E-07	4.99E-14	3.16E-12
10	LPR-MOV-FT-1862A RMT-ACT-FA-RMSTS RMT-XHE-FO-MAN-A	2.692E-10	1	1.60E-03	1.06E-07	4.99E-14	3.16E-12
11	LPMOP-FS-S1A RMT-ACT-FA-RMSTS RMT-XHE-FO-MAN-A	1.536E-10	1	1.60E-03	9.60E-08	1.97E-17	1.22E-13
12	LPMOP-FS-S1B RMT-ACT-FA-RMSTS RMT-XHE-FO-MAN-A	1.536E-10	1	1.60E-03	9.60E-08	1.97E-17	1.22E-13
13	LPR-MOV-FT-1860B RMT-ACT-FA-RMSTS RMT-XHE-FO-MAN-A	1.536E-10	1	1.60E-03	9.60E-08	1.97E-17	1.22E-13
14	LPR-MOV-FT-1860A RMT-ACT-FA-RMSTS RMT-XHE-FO-MAN-A	1.536E-10	1	1.60E-03	9.60E-08	1.97E-17	1.22E-13
15	LPMOP-FS-S1A RMT-ACT-FA-RMSTS RMT-XHE-FO-MAN-A	1.042E-10	1	1.60E-03	6.91E-08	1.95E-14	1.34E-17
16	LPMOP-FS-S1B RMT-ACT-FA-RMSTS RMT-XHE-FO-MAN-A	1.042E-10	1	1.60E-03	6.91E-08	1.95E-14	1.34E-17
17	LPMOP-FS-S1A SIS-ACT-FA-SISB	2.400E-09	1	1.60E-03	1.50E-06	4.50E-13	3.08E-10
18	LPMOP-FS-S1B SIS-ACT-FA-SISB	2.400E-09	1	1.60E-03	1.50E-06	4.50E-13	3.08E-10
19	LPMOP-FS-S1A SIS-ACT-FA-SISB	1.600E-09	1	1.60E-03	3.00E-13	2.05E-10	1.28E-11
20	LPMOP-FS-S1B SIS-ACT-FA-SISB	1.600E-09	1	1.60E-03	3.00E-13	2.05E-10	1.28E-11
21	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.280E-09	1	1.60E-03	8.00E-07	2.40E-13	1.02E-11
22	LPMOP-FG-1864B SIS-ACT-FA-SISA	3.504E-10	1	1.60E-03	2.19E-07	6.57E-14	4.49E-17
23	LPMOP-FG-1864A SIS-ACT-FA-SISB	3.504E-10	1	1.60E-03	2.19E-07	6.57E-14	4.49E-17
24	RMT-ACT-FA-RMSTS RMT-ACT-FA-RMSTS RMT-XHE-FO-MANS1	2.560E-09	2	1.60E-03	3.00E-10	2.05E-13	1.27E-09
25	LPR-MOV-FT-1862B RMT-ACT-FA-RMSTS RMT-XHE-FO-MANS1	5.325E-10	1	1.60E-03	3.33E-07	9.98E-14	6.82E-17
26	LPR-MOV-FT-1862A RMT-ACT-FA-RMSTS RMT-XHE-FO-MANS1	5.325E-10	1	1.60E-03	3.33E-07	9.98E-14	6.82E-17
27	LPMOP-FS-S1B RMT-ACT-FA-RMSTS RMT-XHE-FO-MANS1	3.072E-10	1	1.60E-03	1.92E-07	5.76E-14	3.94E-17
28	LPR-MOV-FT-1860B RMT-ACT-FA-RMSTS RMT-XHE-FO-MANS1	3.072E-10	1	1.60E-03	1.92E-07	5.76E-14	3.94E-17
29	LPR-MOV-FT-1860A RMT-ACT-FA-RMSTS RMT-XHE-FO-MANS1	3.072E-10	1	1.60E-03	1.92E-07	5.76E-14	3.94E-17
30	LPMOP-FS-S1A RMT-ACT-FA-RMSTS RMT-XHE-FO-MANS1	3.072E-10	1	1.60E-03	1.92E-07	5.76E-14	3.94E-17
31	LPMOP-FS-S1B RMT-ACT-FA-RMSTS RMT-XHE-FO-MANS1	2.048E-10	1	1.60E-03	1.28E-07	3.84E-14	2.62E-17
32	LPMOP-FS-S1A RMT-ACT-FA-RMSTS RMT-XHE-FO-MANS1	2.048E-10	1	1.60E-03	1.28E-07	3.84E-14	2.62E-17
33	LPMOP-FS-S1B SIS-ACT-FA-SISA	4.800E-09	1	1.60E-03	3.00E-06	9.00E-13	6.15E-10
34	LPMOP-FS-S1A SIS-ACT-FA-SISA	4.800E-09	1	1.60E-03	3.00E-06	9.00E-13	6.15E-10
35	LPMOP-FS-S1B SIS-ACT-FA-SISA	3.200E-09	1	1.60E-03	2.00E-06	6.00E-13	4.10E-10
36	LPMOP-FS-S1A SIS-ACT-FA-SISA	3.200E-09	1	1.60E-03	2.00E-06	6.00E-13	4.10E-10
37	LPMOP-FG-1864A SIS-ACT-FA-SISB	7.008E-10	1	1.60E-03	4.38E-07	1.31E-13	8.98E-17
38	LPMOP-FG-1864B SIS-ACT-FA-SISA	7.008E-10	1	1.60E-03	4.38E-07	1.31E-13	8.98E-17
39	LPR-MOV-FT-1115E SIS-ACT-FA-SISB	1.600E-10	1	1.60E-03	1.00E-07	3.00E-14	2.05E-17
40	LPR-MOV-FT-1115F SIS-ACT-FA-SISB	1.600E-10	1	1.60E-03	1.00E-07	3.00E-14	2.05E-17
41	LPR-MOV-FT-1115B SIS-ACT-FA-SISA	1.600E-10	1	1.60E-03	1.00E-07	3.00E-14	2.05E-17
42	LPR-MOV-FT-1115D SIS-ACT-FA-SISA	1.600E-10	1	1.60E-03	1.00E-07	3.00E-14	2.05E-17
43	DCP-80C-ST-BUS18 SIS-ACT-FA-SISA	1.440E-10	1	1.60E-03	9.00E-08	2.70E-14	1.89E-17
44	DCP-80C-ST-4801J SIS-ACT-FA-SISA	1.440E-10	1	1.60E-03	9.00E-08	2.70E-14	1.89E-17
45	DCP-80C-ST-BUS1A SIS-ACT-FA-SISA	1.440E-10	1	1.60E-03	9.00E-08	2.70E-14	1.89E-17
46	DCP-80C-ST-4801H SIS-ACT-FA-SISB	1.440E-10	1	1.60E-03	9.00E-08	2.70E-14	1.89E-17
47	SIS-ACT-FA-SISA SIS-ACT-FA-SISB	2.560E-09	2	1.60E-03	3.00E-10	2.05E-13	1.27E-09
48	CPC-XHE-FO-REALM HPI-MOV-FT-1115E HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISA	1.922E-10	1	1.60E-03	1.20E-07	3.60E-14	2.40E-17
49	CPC-XHE-FO-REALM HPI-MOV-FT-1115F HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISA	1.922E-10	1	1.60E-03	1.20E-07	3.60E-14	2.40E-17
50	CPC-XHE-FO-REALM HPI-MOV-FT-1115C HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISB	1.922E-10	1	1.60E-03	1.20E-07	3.60E-14	2.40E-17
51	CPC-XHE-FO-REALM HPI-MOV-FT-1867C HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISB	1.922E-10	1	1.60E-03	1.20E-07	3.60E-14	2.40E-17
52	CPC-XHE-FO-REALM HPI-MOV-FT-1867D HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISB	1.922E-10	1	1.60E-03	1.20E-07	3.60E-14	2.40E-17
53	CPC-XHE-FO-REALM HPI-MOV-FT-1115B HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISB	1.922E-10	1	1.60E-03	1.20E-07	3.60E-14	2.40E-17
54	CPC-XHE-FO-REALM HPI-MOV-FT-1115D HPI-XHE-FO-UNZS3 SIS-ACT-FA-SISB	1.922E-10	2	1.60E-03	4.00E-05	1.20E-11	8.21E-15
55	RCS-XHE-FO-DPT70 SIS-ACT-FA-SISA SIS-ACT-FA-SISB	1.025E-10	2	1.60E-03	4.00E-05	1.20E-11	8.21E-15
56	DCP-ICC-FA-SWP8S CPC-MOP-FR-SW10A	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
57	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2A	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
58	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2B	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
59	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2C	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
60	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2D	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
61	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2E	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
62	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2F	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
63	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2G	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
64	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2H	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
65	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2I	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
66	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2J	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
67	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2K	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
68	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2L	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
69	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2M	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
70	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2N	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
71	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2O	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
72	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2P	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
73	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2Q	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
74	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2R	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
75	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2S	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
76	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2T	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
77	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2U	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
78	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2V	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
79	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2W	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
80	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2X	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
81	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2Y	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
82	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2Z	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
83	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AA	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
84	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AB	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
85	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AC	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
86	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AD	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
87	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AE	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
88	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AF	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
89	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AG	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
90	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AH	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
91	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AI	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
92	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AJ	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
93	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AK	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
94	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AL	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
95	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AM	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
96	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AN	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
97	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AO	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
98	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AP	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
99	DCP-ICC-FA-SWP8S CPC-MOP-FR-CG2AQ	1.229E-09	1	3.20E-04	3.84E-06	1.15E-12	7.87E-16
100	DCP-ICC-FA-SWP						

APPENDIX C

Fault-Tree Diagrams

In this appendix, we present the fault-tree diagrams developed for quantifying system unavailability. Figure C.1 presents the analog SIAS fault-trees. Figure C.2 and C.3 represent the digital SIAS fault-trees for 2-train and 4-train systems, respectively.

Figure C.1 Analog SIAS Fault-Tree

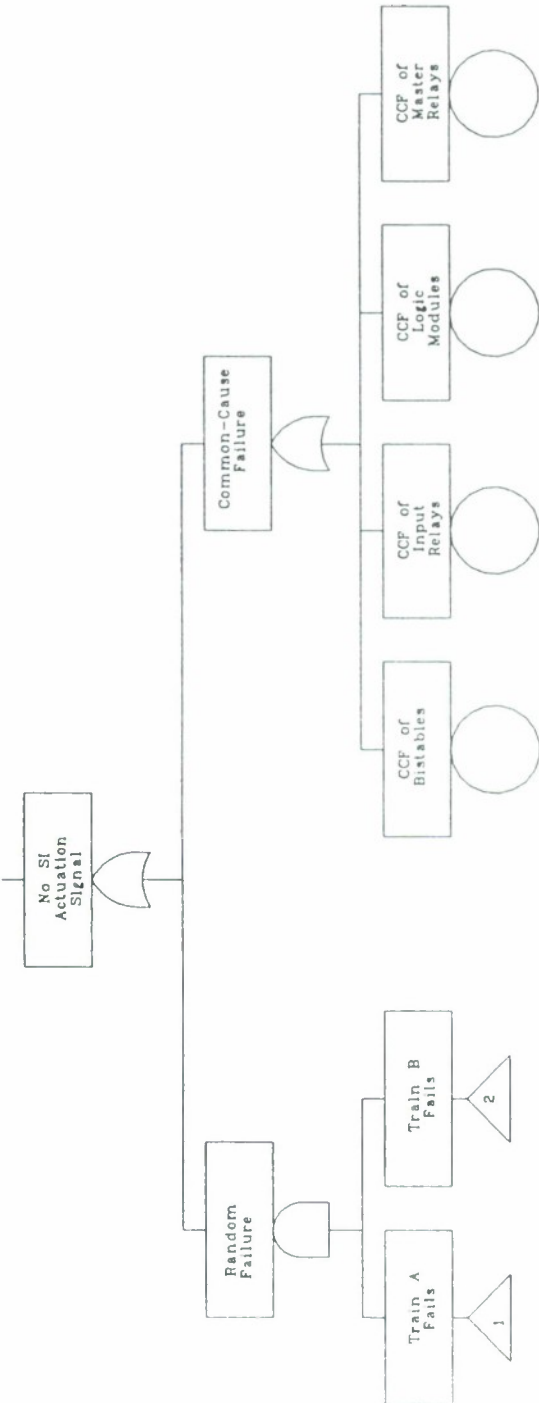


Figure C.1 Analog SIAS Fault-Tree (continued)

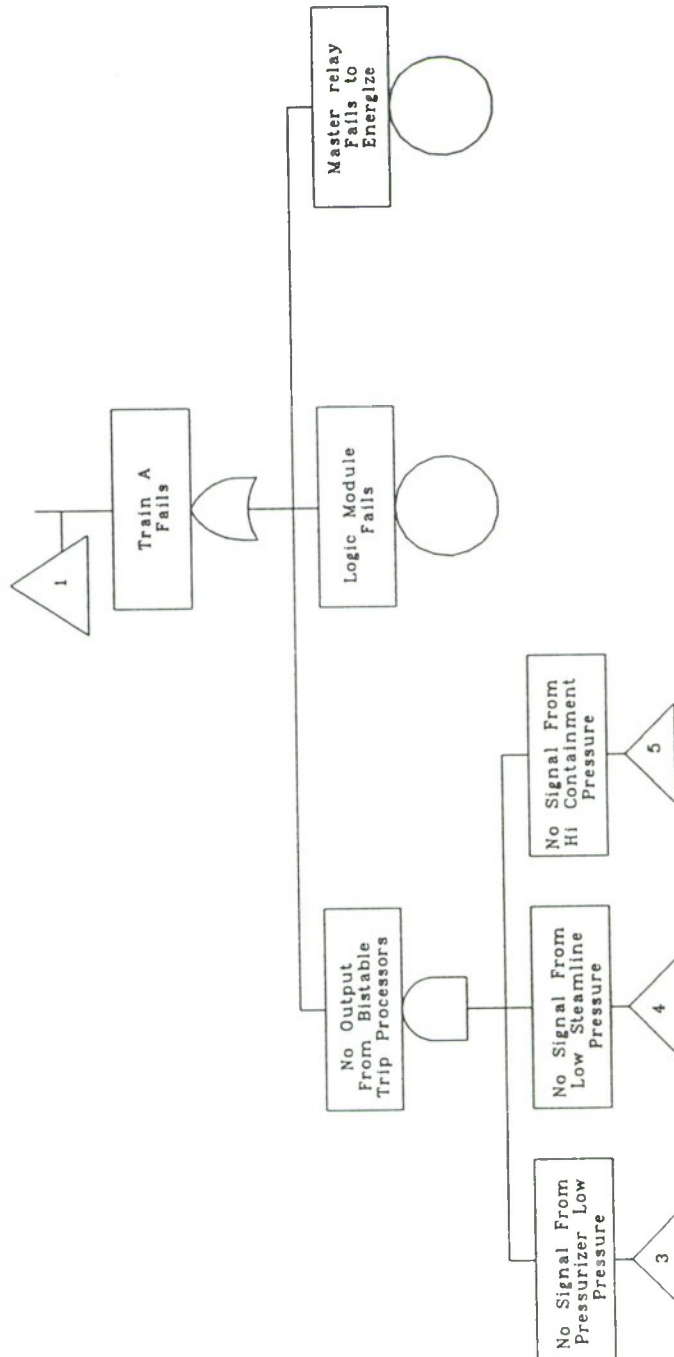


Figure C.1 Analog SIAS Fault-Tree (continued)

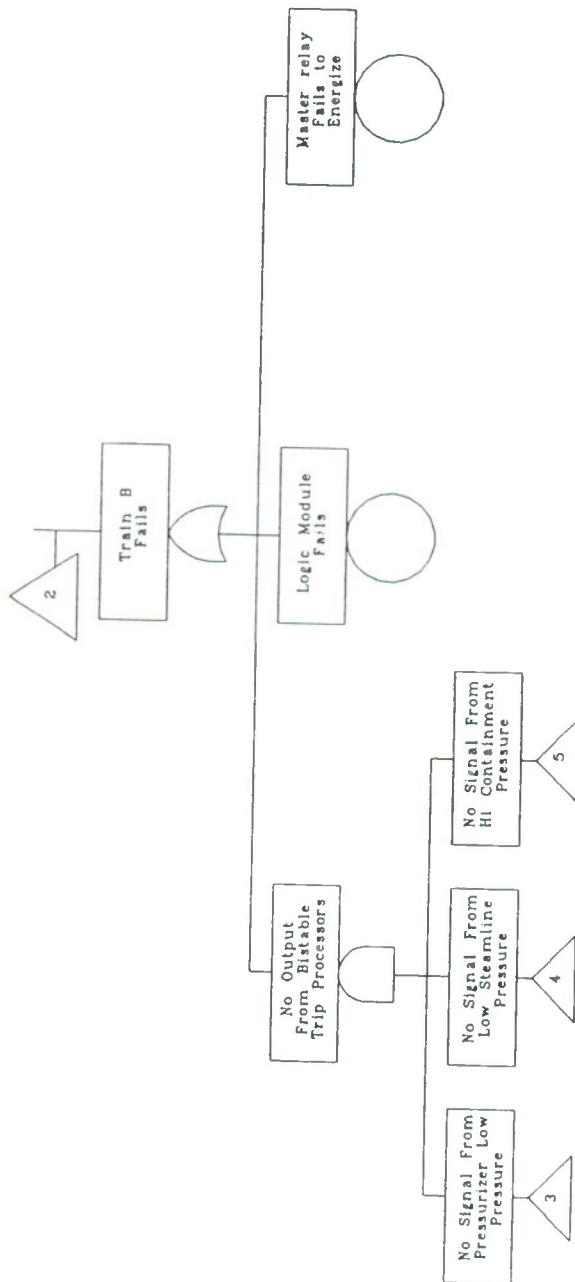
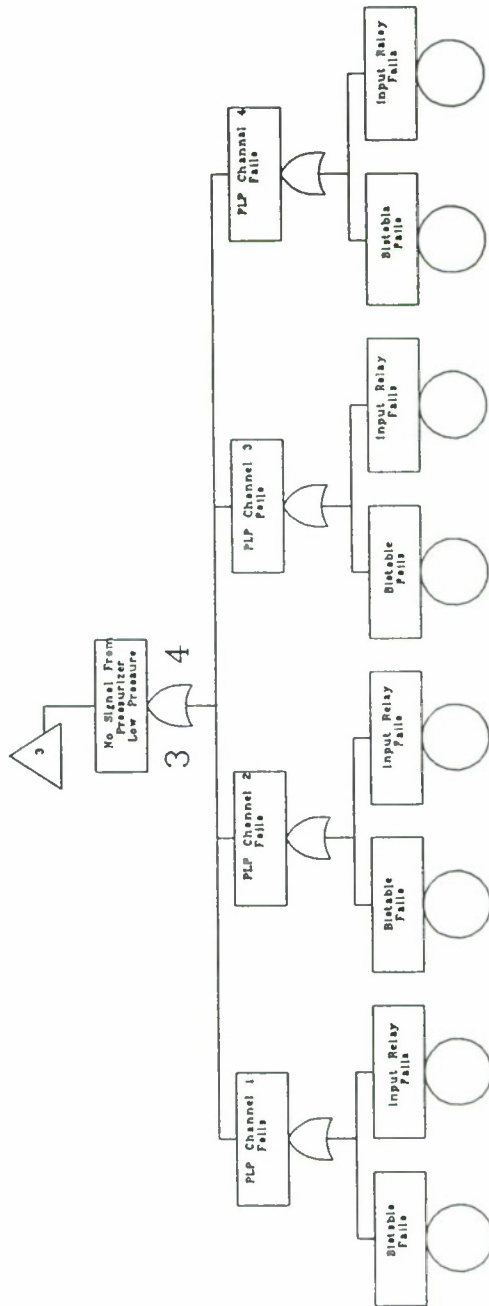


Figure C.1 Analog SIAS Fault-Tree (continued)



APPENDIX C

Figure C.1 Analog SIAS Fault-Tree (continued)

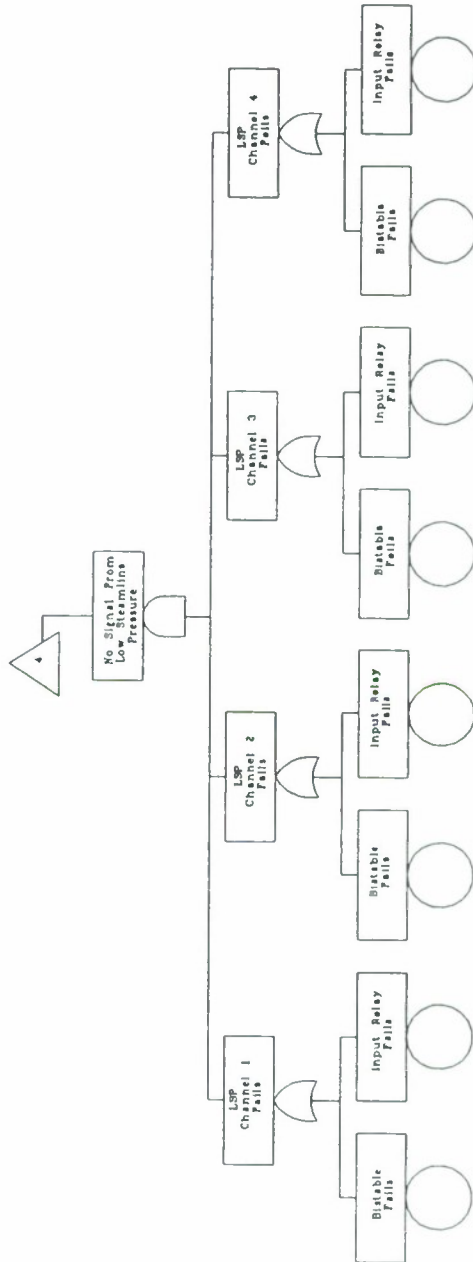


Figure C.1 Analog SIAS Fault-Tree (continued)

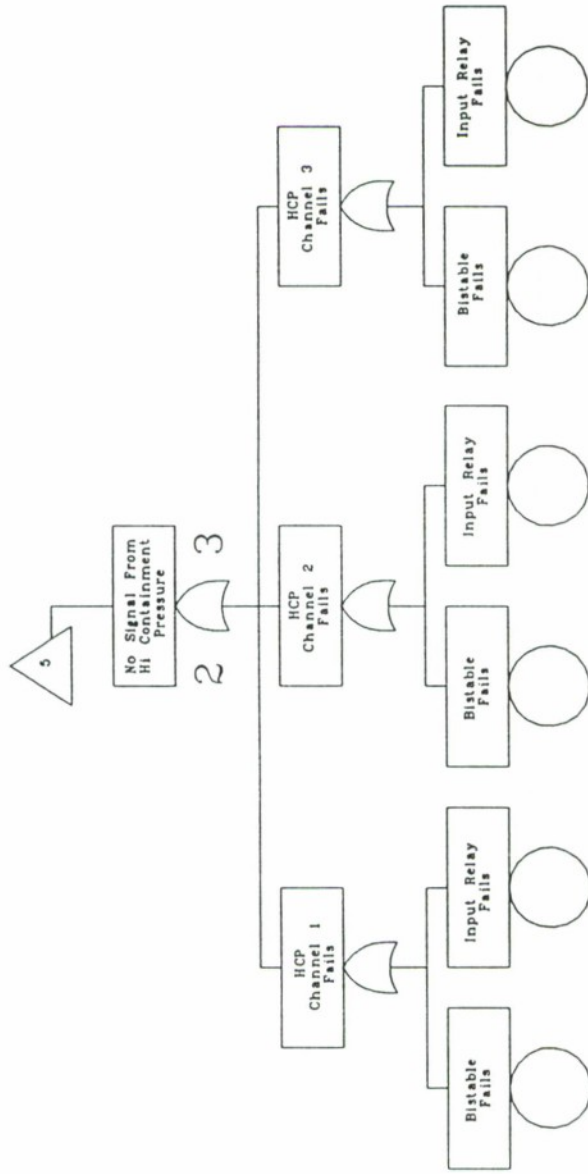


Figure C.2 Digital SIAS Fault-Tree

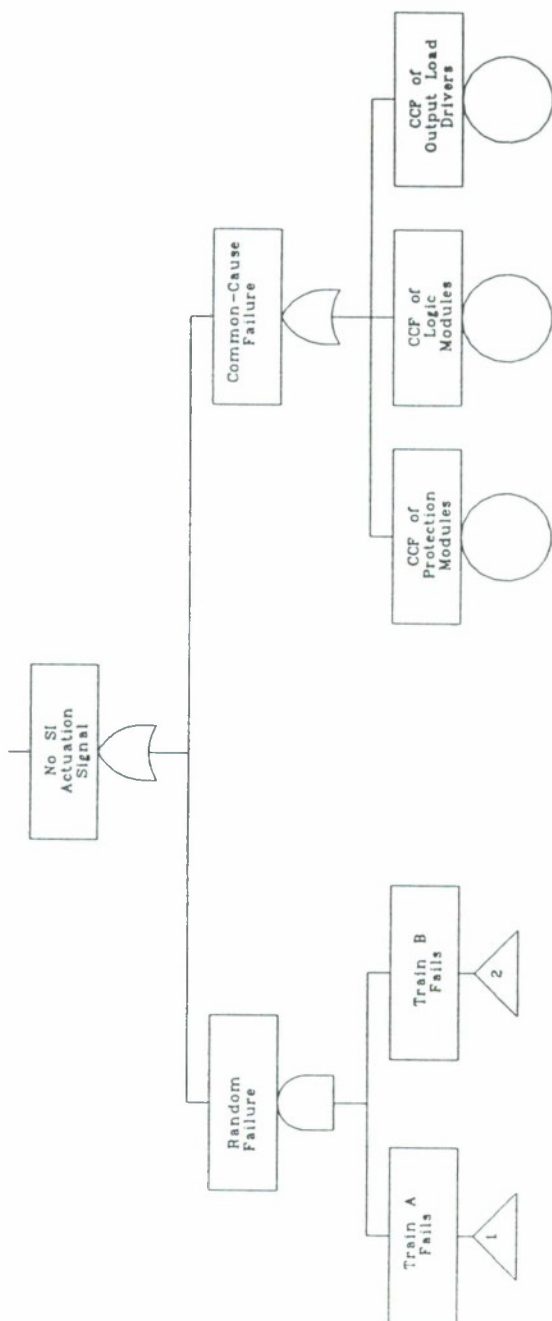
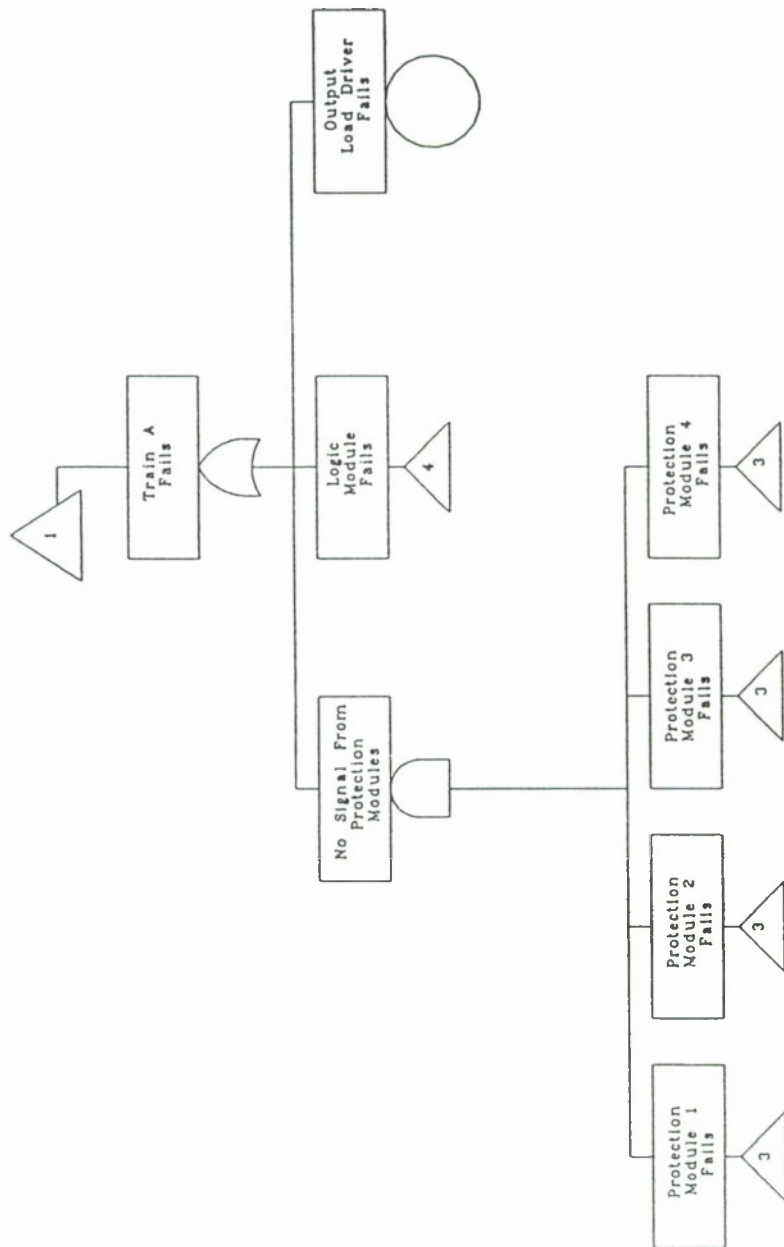
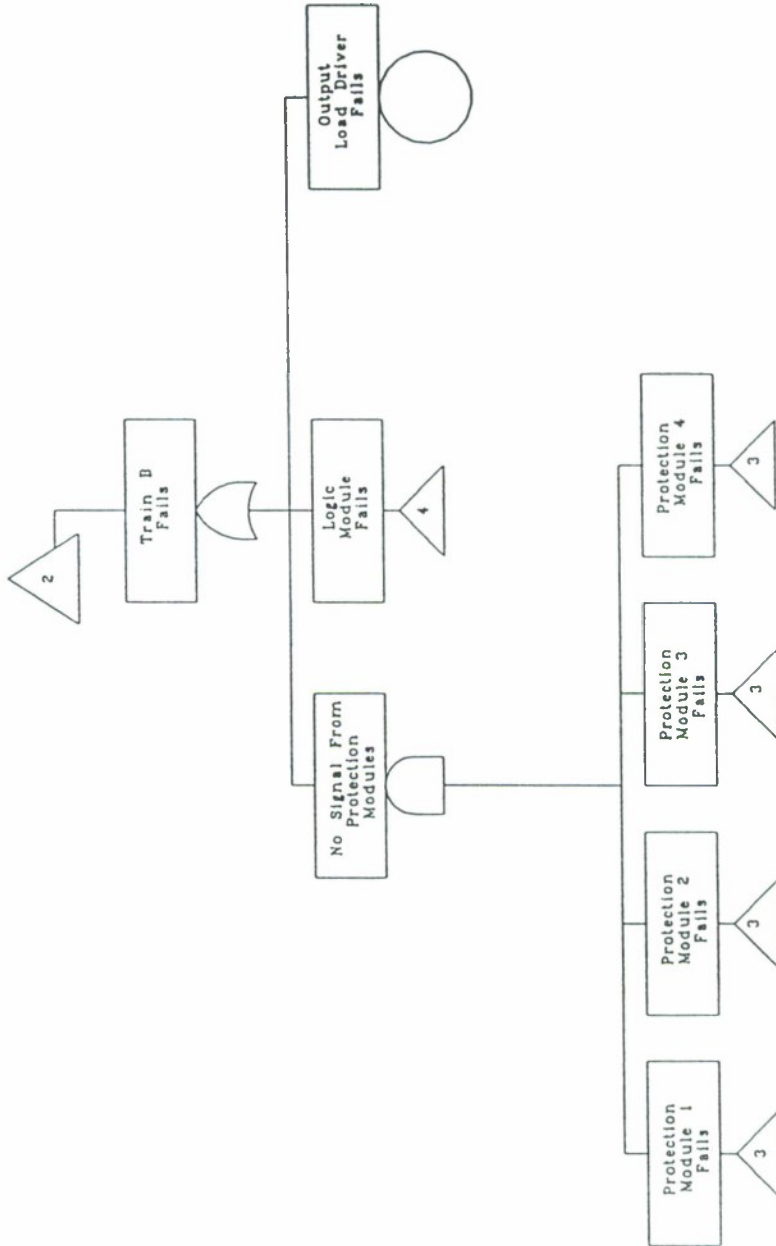


Figure C.2 Digital SIAS Fault-Tree (continued)



* Transfer 3 refers to identical but different equipment in each case
 in Transfer 4 refers to identical but different equipment for Trains A and B

Figure C.2 Digital SIAS Fault-Tree (continued)



* Transfer 3 refers to identical but different equipment in each case
 Transfer 4 refers to identical but different equipment for Trains A and B

Figure C.2 Digital SIAS Fault-Tree (continued)

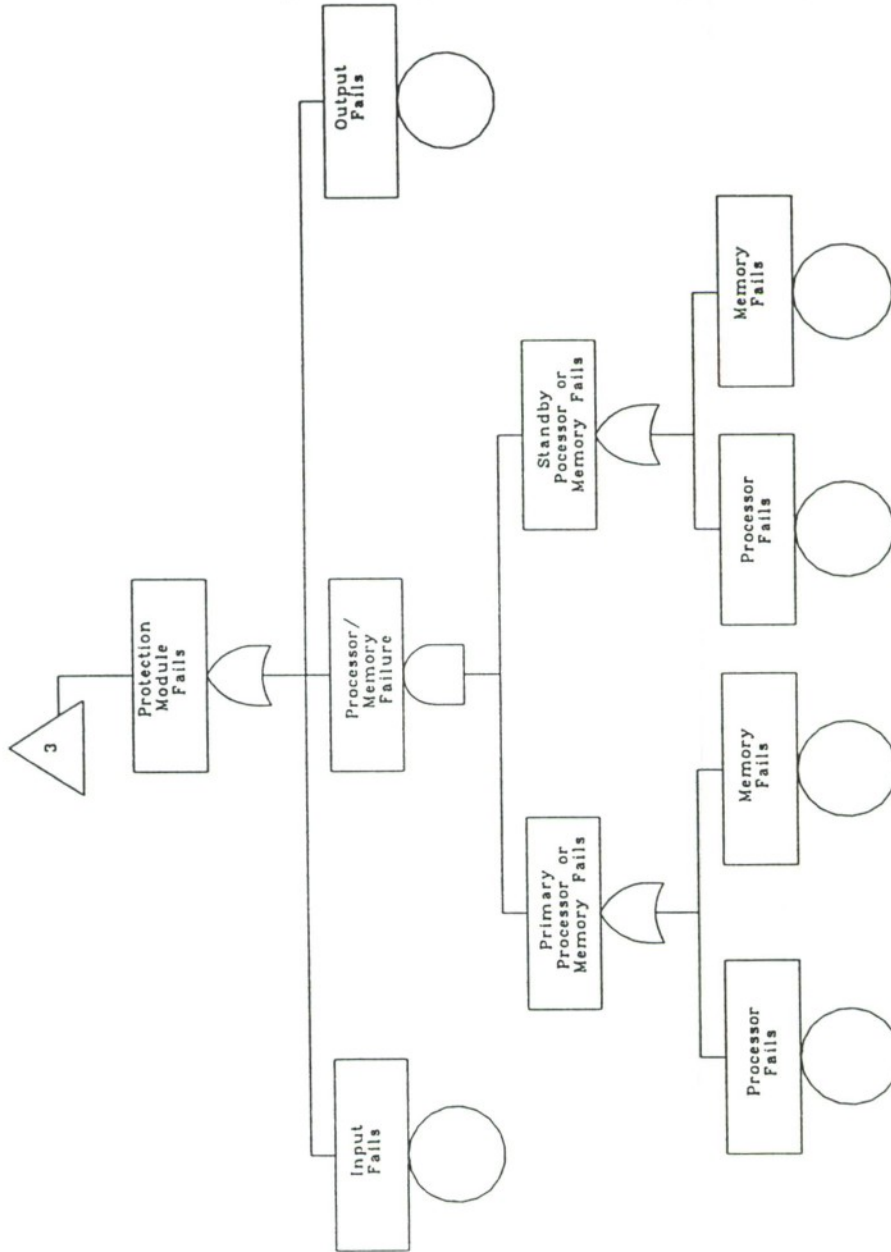


Figure C.2 Digital SIAS Fault-Tree (continued)

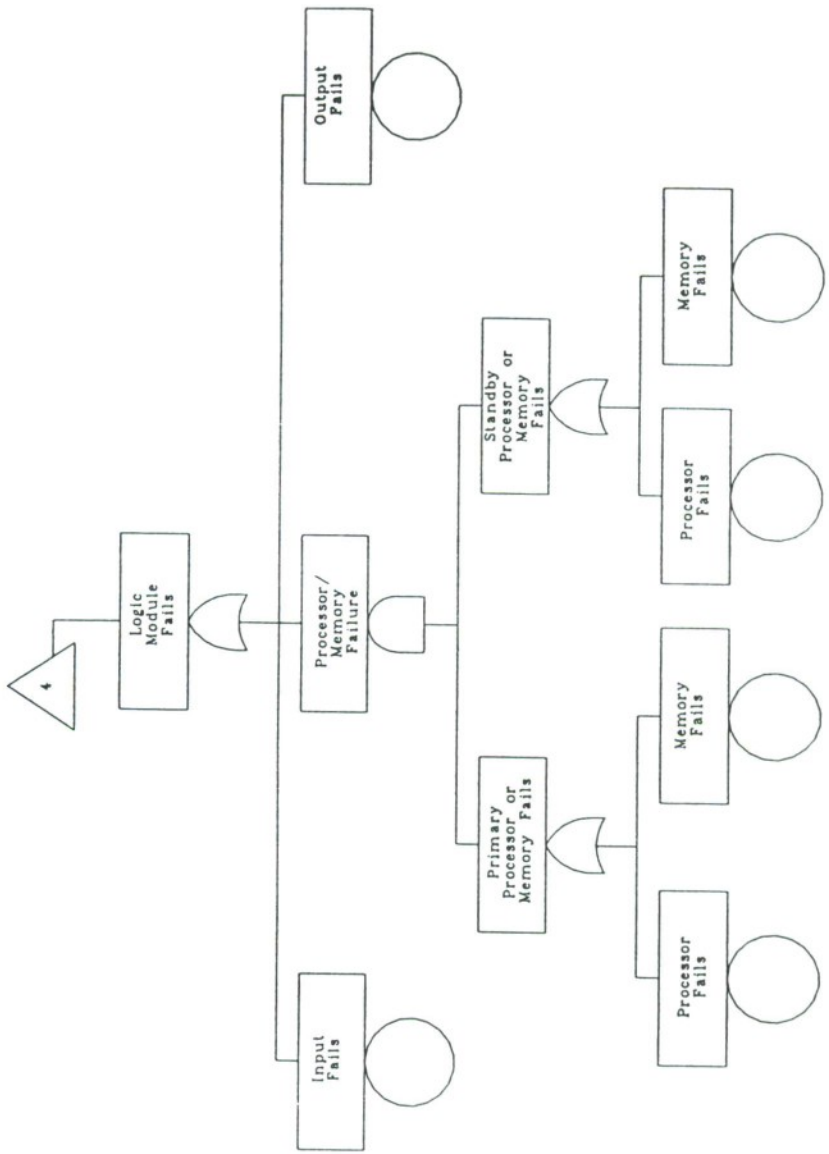


Figure C.3 Four-Train Digital SIAS Fault-Tree

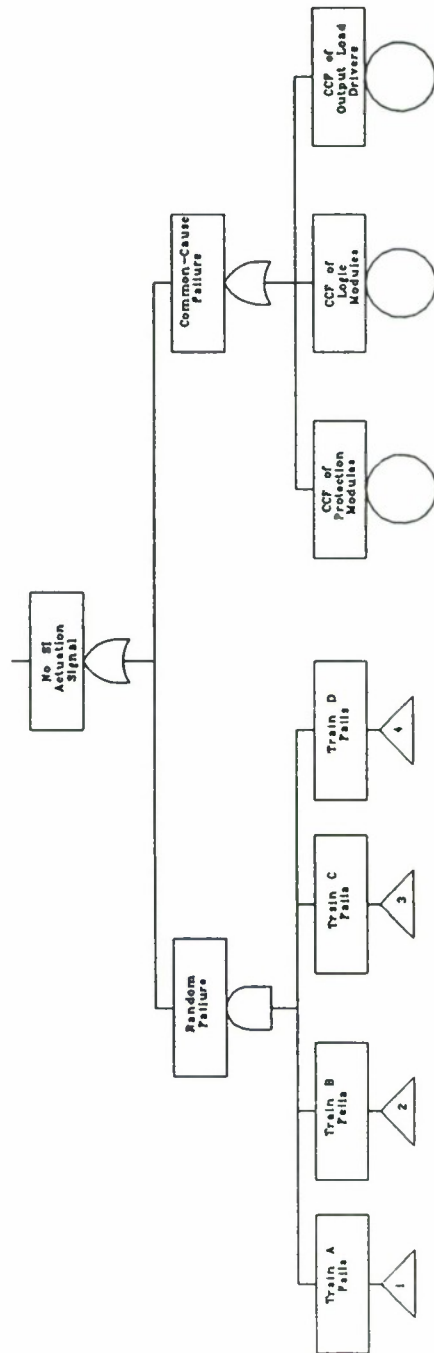
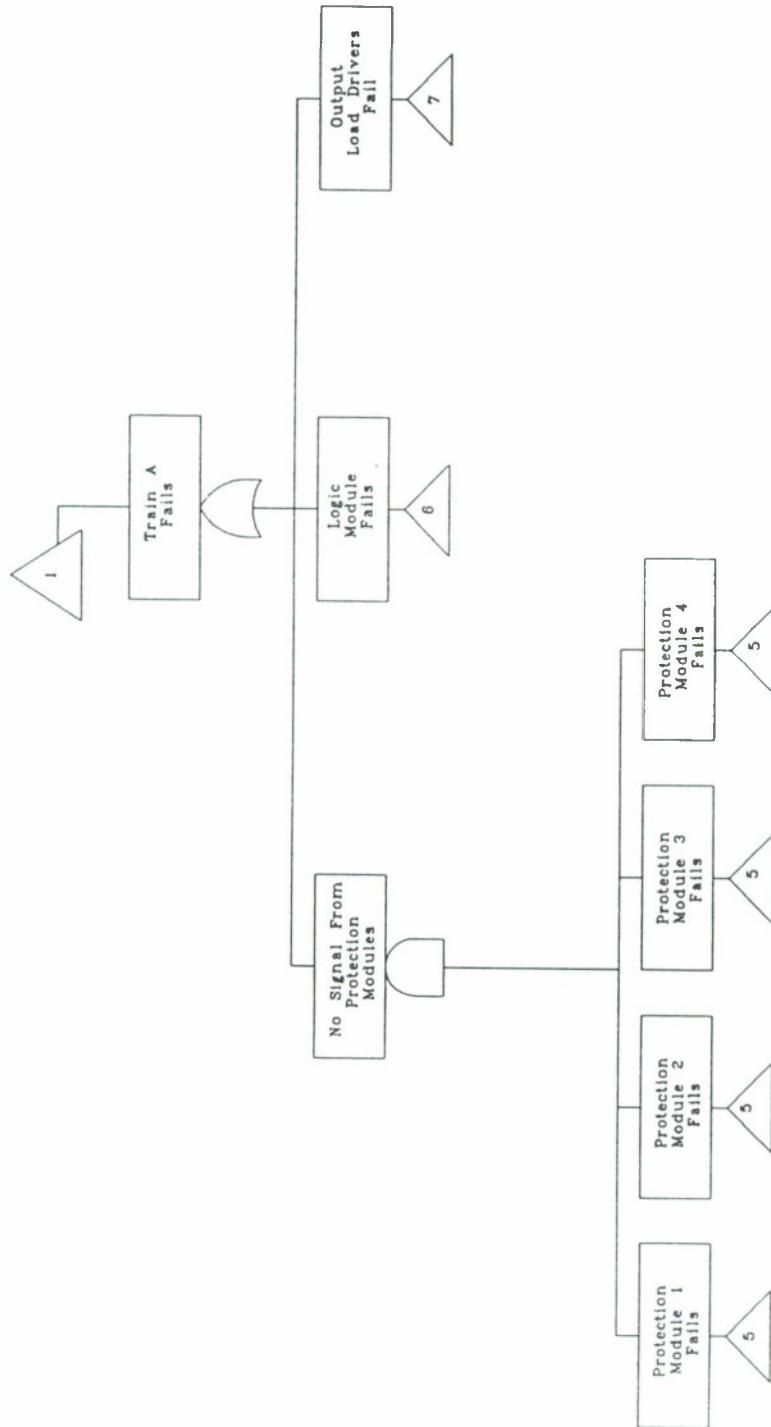
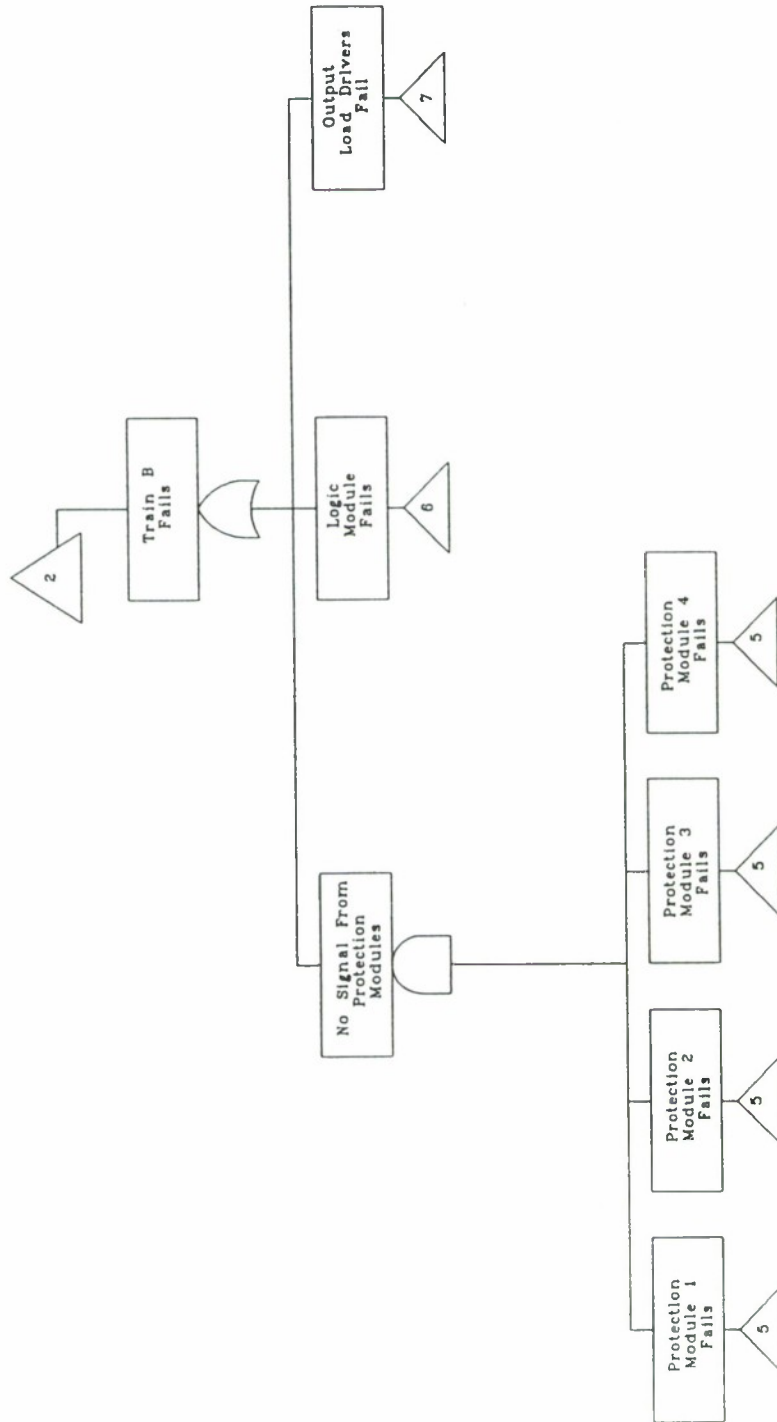


Figure C.3 Four-Train Digital SIAS Fault-Tree (continued)



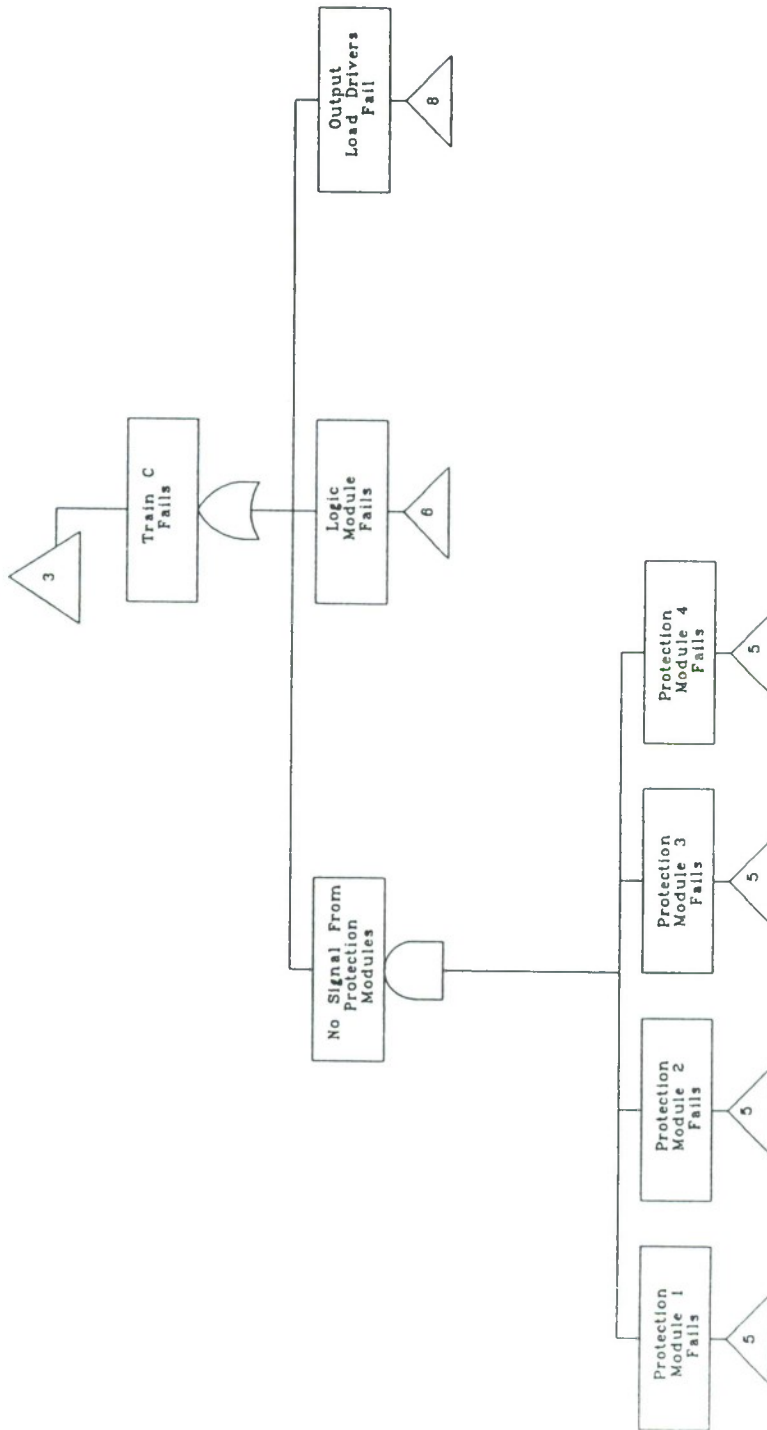
Transfer 5 refers to identical but different equipment in each case
 Transfer 6 refers to identical but different equipment for Trains A,B, C, and D

Figure C.3 Four-Train Digital SIAS Fault-Tree (continued)



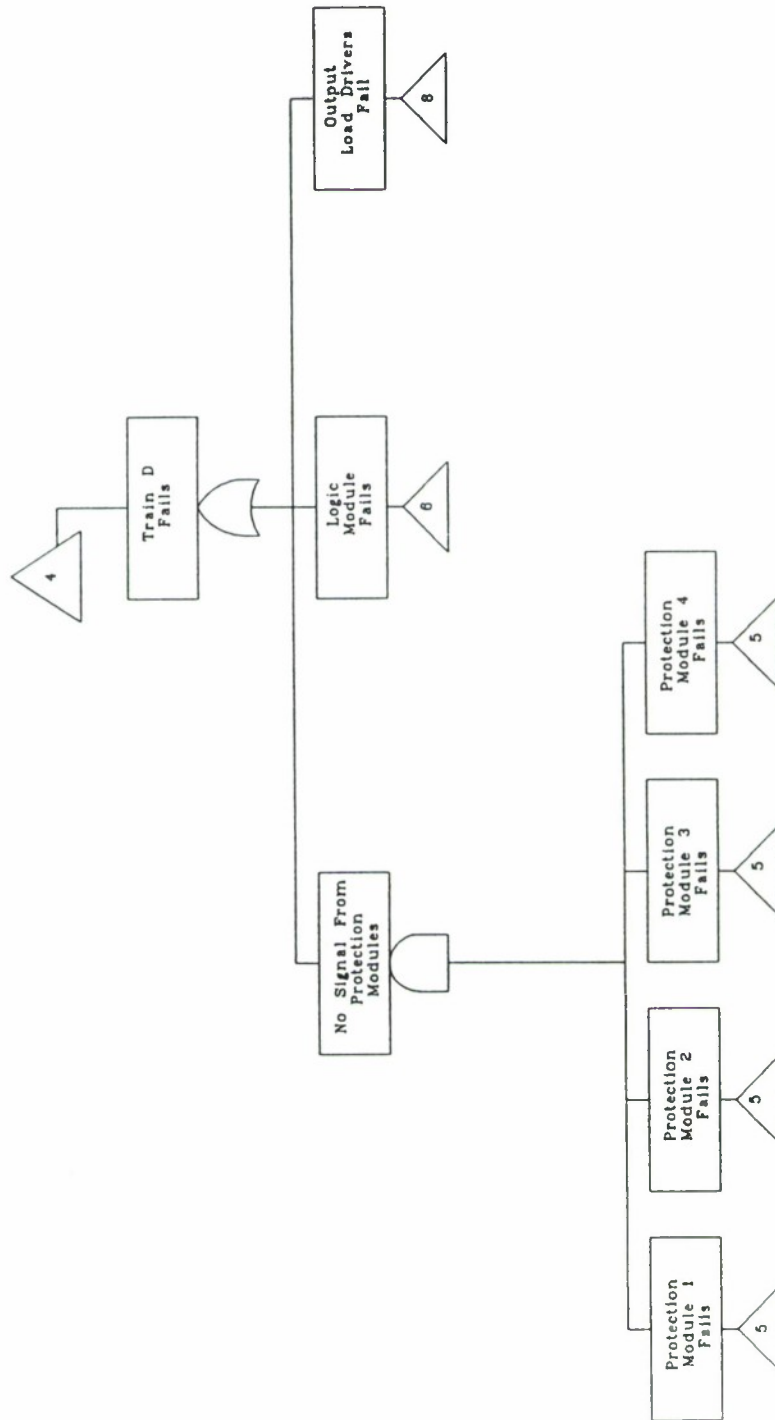
* Transfer 5 refers to identical but different equipment in each case
 Transfer 6 refers to identical but different equipment for Trains A,B, C, and D

Figure C.3 Four-Train Digital SIAS Fault-Tree (continued)



* Transfer 5 refers to identical but different equipment in each case
 * Transfer 6 refers to identical but different equipment for Trains A,B, C, and D

Figure C.3 Four-Train Digital SIAS Fault-Tree (continued)



* Transfer 5 refers to identical but different equipment in each case
 Transfer 6 refers to identical but different equipment for Trains A,B, C, and D

Figure C.3 Four-Train Digital SIAS Fault-Tree (continued)

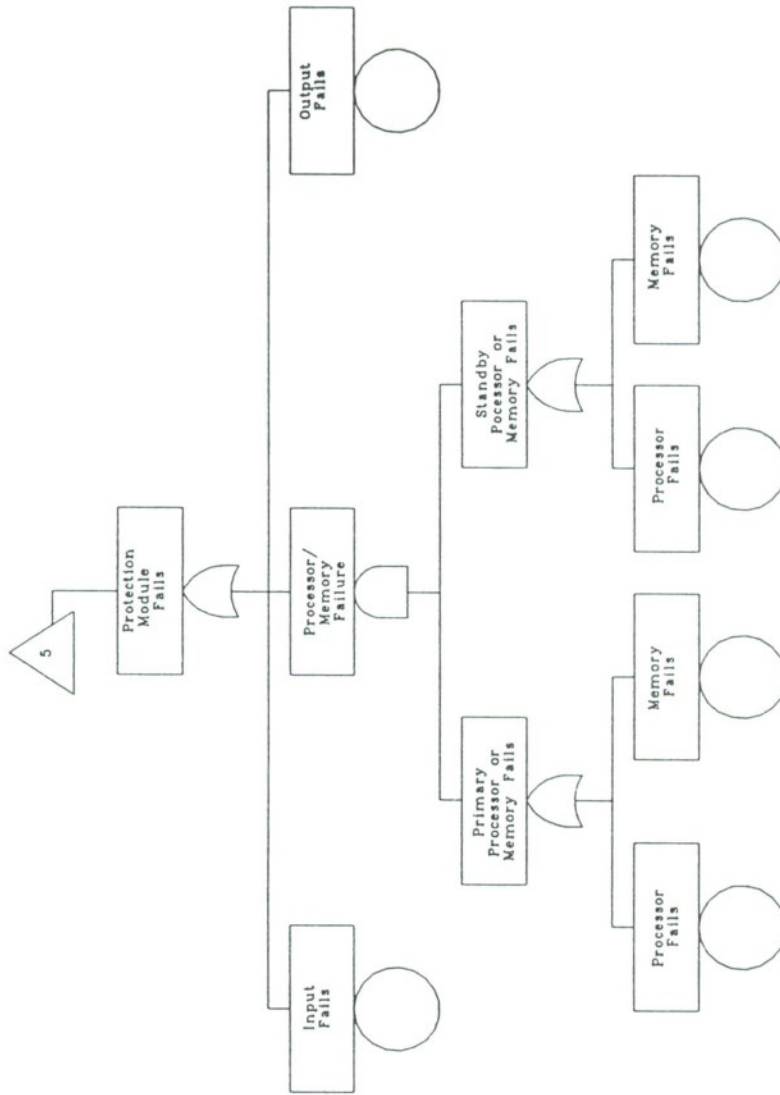


Figure C.3 Four-Train Digital SIAS Fault-Tree (continued)

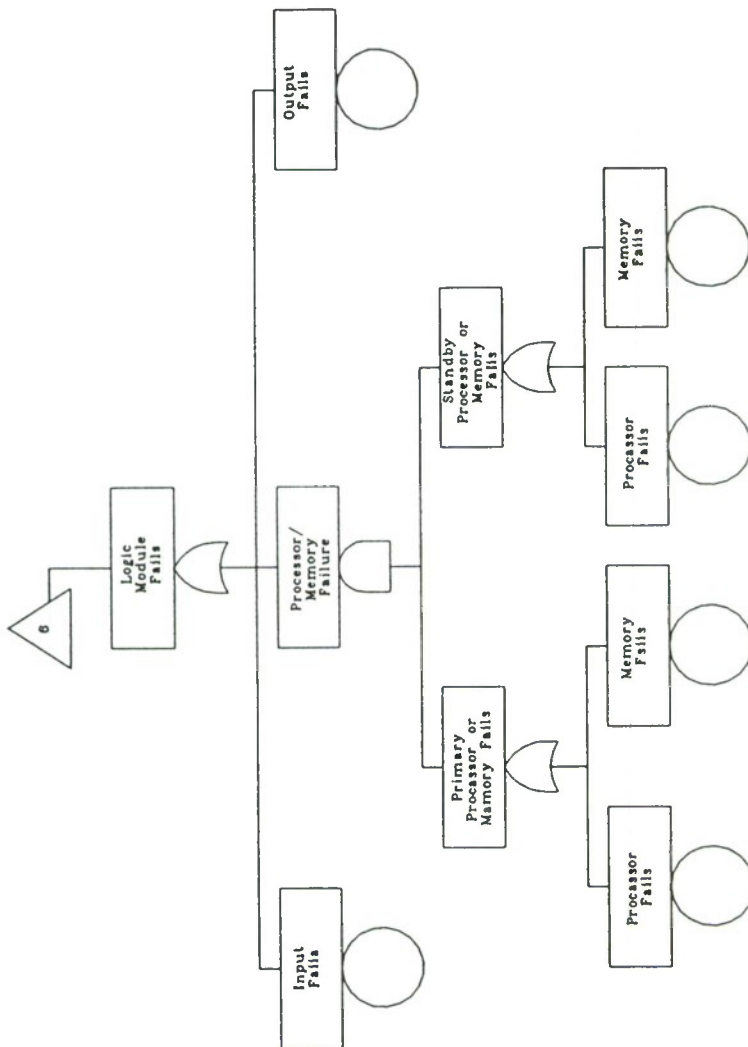
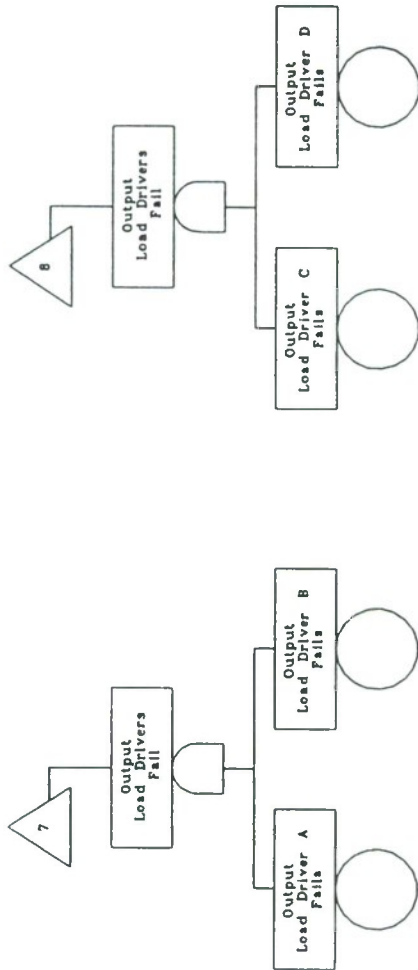


Figure C.3 Four-Train Digital SIAS Fault-Tree (continued)



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-6579
BNL-NUREG-52536

2. TITLE AND SUBTITLE

Digital I&C Systems in Nuclear Power Plants

Risk-Screening of Environmental Stressors and a Comparison
of Hardware Unavailability With an Existing Analog System

3. DATE REPORT PUBLISHED

MONTH	YEAR
January	1998

4. FIN OR GRANT NUMBER

W6542

5. AUTHOR(S)

M. Hassan, Brookhaven National Laboratory
W.E. Vesely, Science Applications International Corporation

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.)*

Brookhaven National Laboratory
Upton, NY 11973-5000

Science Applications International Corporation
655 Metro Place South, Suite 745
Dublin, OH 43017

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.E. Antonescu, NRC Project Manager

11. ABSTRACT *(200 words or less)*

In this report, we present a screening study to identify environmental stressors for digital instrumentation and control (I&C) systems in a nuclear power plant (NPP) which can be potentially risk-significant, and compare the hardware unavailability of such a system with that of its existing analog counterpart. The stressors evaluated are temperature, humidity, vibration, radiation, electro-magnetic interference (EMI), and smoke. The results of risk-screening for an example plant, subject to some bounding assumptions and based on relative changes in plant risk (core damage frequency impacts of the stressors), indicate that humidity, EMI from lightning, and smoke can be potentially risk-significant. Risk from other sources of EMI could not be evaluated for a lack of data. Risk from temperature appears to be insignificant as that from the assumed levels of vibrations. A comparison of the hardware unavailability of the existing analog Safety Injection Actuation System (SIAS) in the example plant with that of an assumed digital upgrade of the system indicates that system unavailability may be more sensitive to the level of redundancy in elements of the digital system than to the environmental and operational variations involved. The findings of this study can be used to focus activities relating to the regulatory basis for digital I&C upgrades in NPPs, including identification of dominant stressors, data-gathering, equipment qualification, and requirements to limit the effects of environmental stressors.

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

Digital Upgrades
Instrumentation and Control
Digital Systems
Nuclear Power Plants
Digital Instrumentation and Control
Risk Assessments
Probabilistic Risk Analysis

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)

unclassified

(This Report)

unclassified

15. NUMBER OF PAGES

16. PRICE