NUREG/CR-5904
ORNL/TM-12164

Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors

Prepared by
K. Korsah, R. L. Clark, R. T. Wood

Oak Ridge National Laboratory

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

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

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

2. The Superintendent of Documents, U.S. Government Printing Office, Mail Stop SSOP, Washington, DC 20402-9328

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

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 GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grant publications, 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, 7920 Norfolk Avenue, Bethesda, Maryland, 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.

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, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability of 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.

NUREG/CR-5904
ORNL/TM-12164

Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors

Manuscript Completed: March 1994
Date Published: April 1994

Prepared by
K. Korsah, R. L. Clark, R. T. Wood

Oak Ridge National Laboratory
Managed by Martin Marietta Energy Systems, Inc.

Oak Ridge National Laboratory
Oak Ridge, TN 37831-6050

Prepared for
Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC FIN L1798
Under Contract No. DE-AC05-84OR21400

Abstract

A study f significant "new" technologies proposed for use in safety-related instrumentation and controls (I&C) systems of advanced light-water reactors (ALWRs) was performed as part of the Qualification of Advanced Instrumentation and Control Systems project conducted for the Office of Nuclear Regulatory Research of the U.S. Nuclear Regulatory Commission. Templates showing digital protection systems of some ALWR designs and the effect of expected environmental stressors on system components were developed to illustrate functional and qualification issues.

The study also identified optical fiber systems as technologies that are relatively new to the nuclear power plant environment and examined the failure modes and age-related degradation mechanisms associated with fiber-optic cables and components. The data were then used to propose a methodology for identifying circumstances in which accelerated aging should be used in an equipment qualification program for "new" I&C technologies.

Other findings and conclusions from the study are as follows:

1. The type of transmitters, sensing lines, and cabling, up to the multiplexing and sampling components, are likely to be the same for ALWRs as for existing light-water reactors (LWRs). Environmental conditions (temperature, humidity, radiation, etc.) for the instrumentation are also likely to be very similar. However, a study of the Licensee Event Report database over a 10-year period (1982–1991) shows that the fraction of electromagnetic interference/radio-frequency interference (EMI/RFI)-related protection system events is significant compared to traditionally recognized environmental stressors such as elevated temperature. The problem is likely to be even more significant for ALWR safety systems because of the increased use of microprocessor-based technology and software. Thus, it appears that while safety systems in ALWRs will have to be qualified to the same environment as current LWRs, EMI/RFI emissions and susceptibility criteria and guidelines specific to the nuclear power plant environment should be considered. Specific EMI/RFI requirements are addressed in a companion document, NUREG/CR-5941, *Electromagnetic and Radio-Frequency Interference in Safety-Critical I&C Systems*.

2. The protection systems of ALWRs employ a voting scheme (2-out-of-4) similar to present-day (analog) implementations. The essential difference, however, is that the voting will be performed in software rather than in hardware and will in some cases involve software data communication among the channels. This cross-communication could be a source of problems and should receive close scrutiny. Failure modes in which a processor waits indefinitely for information from another channel, or where erroneous data are communicated to the other channels without being noticed, are of concern and will require consideration in appropriate standards and regulatory guides. Processors performing communication functions may be required to be different from processors performing protection system functions.

3. In existing plants, physical separation and fire protection requirements, rather than environmental qualification of the Class 1E equipment per se, are generally relied upon to mitigate the consequences of a fire. This approach also appears to have been followed for the next generation of nuclear power plants.

Contents

Page

List of Figures

List of Tables

Summary

Issues of obsolescence and lack of infrastructural support in (analog) spare parts, coupled with the potential benefits of digital systems, are driving the nuclear industry to retrofit analog instrumentation and control (I&C) systems with digital and microprocessor-based systems. This trend is expected to become even more evident in advanced light-water reactors (ALWRs), which will make extensive use of microprocessor-based technology, including fiber-optic transmission and multiplexing techniques. While these technologies have several advantages and, in fact, have been in widespread use in the nonnuclear industry for several years, their application to safety-related systems in nuclear power plants raises key issues relating to the systems' environmental qualification and functional reliability. For example, does the new hardware introduce new degradation mechanisms that could adversely impact the safety of the plant? Do the systems introduce the possibility of new and different malfunction scenarios or increase the probability of common-mode failures that could reduce the reliability of the safety system? Are current qualification methodologies adequate for the "new" technologies to be introduced in the next generation of nuclear power plants? What should be the acceptance criteria for safety-related digital I&C systems?

To bound the problem of new I&C system functionality and qualification, we focused our study on *protection systems* proposed for use in ALWRs. Specifically, both functional and environmental qualification issues for ALWR protection system I&C were addressed by developing an environmental, functional, and aging data template for a protection division of each proposed ALWR design. By using information provided by manufacturers, environmental conditions and stressors to which I&C equipment in reactor protection divisions may be subjected were identified. The resulting data were then compared to a similar template for an instrument string typically found in an analog protection division of a present-day nuclear power plant. We also identified fiber-optic transmission systems as technologies that are relatively new to the nuclear power plant environment and examined the failure modes and age-related degradation mechanisms of fiber-optic components and systems. The information gathered on fiber-optic systems as well as on digital protection systems was used to propose a methodology for identifying when accelerated aging should be used in a qualification program for safety-related I&C equipment not covered under 10 CFR 50.49.

One reason for the exercise of caution in the introduction of software into safety-critical systems is the potential for common-cause failure due to the software. Our study, however, approaches the functionality problem from a *systems* point of view (software verification and validation issues are not a part of this study). System malfunction scenarios are postulated to illustrate the fact that, when dealing with the performance of the overall *integrated* system, the real issues are *functionality* and *fault tolerance*, not hardware vs software.

ACKNOWLEDGEMENTS

Several people have made significant contributions to this study. In particular, the authors wish to thank NRC Aging and Components Section chief, J. P. Vora, and the NRC Program Manager, Christina Antonescu, for their help in initiating, planning, and implementing this study.

Site visits were made to several reactor manufacturers, nuclear utilities, and non-nuclear process industries during this study. In addition, subsequent contacts and fruitful discussions were maintained with personnel at some of the plants. Assisting organizations include Westinghouse, General Electric, Duke Power, OLIN Corporation, ABB Combustion Engineering, and the Foxboro Company. Without their cooperation, this study would not have been possible, and their contributions are gratefully acknowledged.

The authors also wish to thank R. A. Kisner, R. C. Kryter, D. N. Fry, N. E. Clapp, Jr., and R. E. Battle of Oak Ridge National Laboratory for their excellent technical contributions, editorial reviews, and helpful suggestions.

Finally, the authors wish to thank Kathy McIntyre, Joyce Huffstetler, Linda Sparks, Janice Asher, and the staff of the Technical Support Center for their help in preparing the manuscript.

Acronyms

ABB/CE	ASEA-Brown Boveri/Combustion Engineering
ABWR	advanced boiling water reactor
A/D	analog-to-digital
ALWR	advanced light-water reactor
ANSI	American National Standards Institute
APD	avalanche photodetector
ARI	alternate rod injection
ATWS	anticipated transient without scram
B&W	Babcock and Wilcox
BPU	bypass unit
BTP	bistable trip processor
BWR	boiling water reactor
CEA	control element assembly
CEDMCS	control element drive mechanisms control system
CMOS	complementary metal-oxide semiconductor
CP	coincidence processor
CPC	core protection calculator
CRC	cyclic redundancy check
CS	communications subsystem
DBA	design basis accident
DBE	design basis event
DLD	dark line defect
DNBR	departure from nucleate boiling ratio
DTBS	dynamic trip bus subsystem
DTM	digital trip module
EEPROM	electrically erasable, programmable, read-only memory
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EMS	Essential Multiplexing System
EPRI	Electric Power Research Institute
EPROM	erasable, programmable, read-only memory
ESD	electrostatic discharge
ESF	engineered safety feature
ESFAC	engineered safety feature actuation cabinets
ESFAS	engineered safety feature actuation system
FDDI	fiber distributed data interface
GTS	global trip subsystem
HELB	high-energy line break
HVAC	heating, ventilation, and air-conditioning
I&C	instrumentation and control
IEEE	Institute of Electrical and Electronics Engineers
I/O	input/output
IPC	integrated protection cabinet
ITP	interface and test processor
LED	light-emitting diode
LER	Licensee Event Report
LWR	light-water reactor
NPAR	Nuclear Plant Aging Research (program)
NPE	Nuclear Power Experience

NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
OLU	output logic unit
PIN	positive-intrinsic-negative
PPS	plant protection system
PWR	pressurized water reactor
RAM	random access memory
RFI	radio-frequency interference
RMU	remote multiplexing unit
RPS	reactor protection system
RTIL	reactor trip initiation logic
RTS	reactor trip system or subsystem
SAMA	Scientific Apparatus Manufacturers Association
SBWR	simplified boiling water reactor
SLCS	standby liquid control system
SSC	systems, structures, and components
SSE	safe shutdown earthquake
SSLC	Safety System Logic and Control
TLU	trip logic unit
UVTA	undervoltage trip attachment
V&V	verification and validation

Definition of Terms

During this study, it was found that many terms are used somewhat inconsistently in the literature. We have therefore included a definition of terms as used in this document. Where applicable, the source of the definitions is also included:

Accelerated aging.[a] Artificial aging in which the simulation of natural aging approximates, in a short time, the aging effects of longer term service conditions.

Age conditioning. See **preconditioning.**

Age-related degradation.[a] Aging effects that could impair the ability of a system, structure, or component (SSC) to function within acceptance criteria.

Aging[a] (noun). General process in which characteristics of an SSC gradually change with time or use.

Artificial aging.[a] Simulation of natural aging effects on SSCs by application of stressors representing plant preservice and service conditions but perhaps different in intensity, duration, and manner of application.

Channel.[b] An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined.

Common-cause failure.[a] Two or more failures due to a single cause.

Common-mode failure.[a] Two or more failures in the same manner or mode due to a single cause.

Detectable failures.[b] Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication.

Division.[b] The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components. In this document, a division refers to a group of components and modules that functionally makes up one redundant set of a reactor trip system.

Fail Safe.[c] Pertaining to a system or component that automatically places itself in a safe operating mode in the event of a failure.

Fault tolerance.[c] The ability of a system or component to continue normal operation despite the presence of hardware or software faults.

Functionality. The working relationships among the modules in a safety system.

Gray (Gy). The international standard unit for dose. 1 Gy = 100 rad.

Harsh environment.[d] An environment expected as the result of the postulated service conditions appropriate for the design basis and postdesign basis accidents of the station. [A design basis accident is the subset of design basis events (DBEs) that require safety function performance.] Harsh environments are the result of a loss-of-cooling accident (LOCA)/high-energy line break (HELB) inside containment and post-LOCA or HELB outside containment.

Instrument string. The arrangement of components and modules to generate a trip signal from a single process variable such as coolant hot leg temperature. (Synonymous with **instrument channel**).

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

Partial trip. A protective action signal generated from a single process variable, such as coolant hot leg temperature. This is analogous to "channel trip" as implied in the definition of *channel* in reference *b*. However, "partial trip" (also used in some Westinghouse literature) has been used in some cases to describe microprocessor-based trip systems since "a channel loses its identity where single protective action signals are combined."[b]

Preconditioning.[a] Simulation of natural aging effects in an SSC by the application of any combination of artificial and natural aging. Synonymous with **age conditioning**.

Qualified life.[a] Period for which an SSC has been demonstrated, through testing, analysis, or experience, to be capable of functioning within acceptance criteria during specified operating conditions while retaining the ability to perform its safety functions in a design basis accident or earthquake.

Random failure.[c] Any failure whose cause or mechanism, or both, makes its time of occurrence unpredictable.

Safety system.[b] Those systems (the reactor trip system, an engineered safety feature, or both, including all their auxiliary supporting features and other auxiliary features) which provide a safety function. Synonymous with **safety-critical system.**

Safety-critical system. (Synonymous with **safety system**).

Service conditions.[d] Environmental, loading, power, and signal conditions expected as a result of normal operating requirements, expected extremes (abnormal) in operating requirements, and postulated conditions appropriate for the DBEs of the station.

Service life.[a] Actual period from initial operation to retirement of an SSC.

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

Synergistic effects.[a] Portion of changes in characteristics of an SSC produced solely by the interaction of stressors acting simultaneously, as distinguished from changes produced by superposition from each stressor acting independently.

[a] *Nuclear Power Plant Common Aging Terminology*, EPRI TR-100844, Electric Power Research Institute, November 1992.

[b] IEEE Standard 603-1980, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*.

[c] IEEE Standard 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*.

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

[e] IEEE Standard 100-1988, *Standard Dictionary of Electrical and Electronic Terms*.

1 Introduction

1.1 Background

Advanced light-water reactors (ALWRs), such as the Westinghouse *AP600*, the General Electric *simplified boiling water reactor* (SBWR), and the ASEA-Brown Boveri/Combustion Engineering, Incorporated (ABB/CE), *System* 80^+, will make extensive use of digital controls, microprocessors, multiplexing, and fiber-optic signal transmission. While the application of advanced technology in the nuclear environment is generally encouraged by the U.S. Nuclear Regulatory Commission (NRC),[1] the introduction of such *new* technology, either as retrofits in existing nuclear power plants or in the next generation of light-water reactors (LWRs), will require development of acceptance criteria and new or revised qualification standards and guidelines. Accordingly, NRC initiated the research program, Qualification of Advanced Instrumentation and Control Systems, to develop an understanding of the technical issues involved in qualifying advanced instrumentation and control (I&C) systems proposed for use in ALWR designs.

The anticipated change from completely analog systems to analog/digital to fully digital, computer-based I&C systems can be expected to yield significant benefits, including a potential for improvements in the safe and reliable operation of nuclear power plants, reduced stress on I&C components from frequent maintenance and testing cycles (because of the self-testing/diagnostic capabilities of microprocessor-based systems), and a potential for reduction in system costs and cabling (due to sharing of data transmission lines via multiplexing). However, the introduction of digital technology in safety-related systems of nuclear power plants also raises issues relating to the systems' *environmental* and *functional* reliability. One issue is the continuing trend toward higher clock frequencies, faster operating speeds, and lower logic-level voltages. The faster logic families have shown a greater susceptibility to upsets and malfunctions because of the effects of electromagnetic interference/radio-frequency interference (EMI/RFI). This raises the question of how much reliance can be placed on a digital, microprocessor-based protection system. Also, does the new hardware introduce new age-related degradation mechanisms that could adversely impact the long-term properties and performance as well as the safety of the plant? Do microprocessor-based systems introduce the possibility of new and different malfunction scenarios or increase the probability of common-mode failures that could reduce the reliability of the safety system? Are current qualification methodologies adequate for the "new" technologies to be introduced in the next generation of nuclear power plants? What should be the acceptance criteria for safety-related digital I&C systems?

The reliability of microprocessor-based systems strongly depends on the quality of the accompanying software verification and validation (V&V) program. For example, a software programming error common to all the channels in a safety system can defeat the hardware redundancy designed into the system. In this study, however, the approach taken has been to study the *integrated system* from a *hardware* perspective. Software V&V is outside the scope of this I&C qualification research program.

The desired end product of the advanced I&C qualification research program is to develop a qualification methodology for new I&C systems proposed for nuclear power plant environments. This is depicted in Figure 1.1. Notice from the figure that knowledge gained in this program will serve as input, together with other programs dealing with software reliability issues, to the development of a technical basis for acceptance criteria for new I&C technologies in nuclear power plants.

The major source of information for this study came from completed Nuclear Plant Aging Research (NPAR) program studies on present-day nuclear power plant instrumentation and protection systems and from discussions with selected reactor and instrument manufacturers concerning safety channel instrumentation and system configurations. The information acquired from industry representatives forms the basis for ascertaining the extent to which advanced technology will be used in proposed safety system designs for ALWRs. By comparing advanced safety systems with traditional analog designs, some new concerns presented by the introduction of digital technology into nuclear applications have been identified. Also, an ALWR evaluation template has been developed by assembling a configuration of an instrument string in a protection channel for an ALWR and then comparing the impact of environmental stressors on that string with their effect on an equivalent string in a

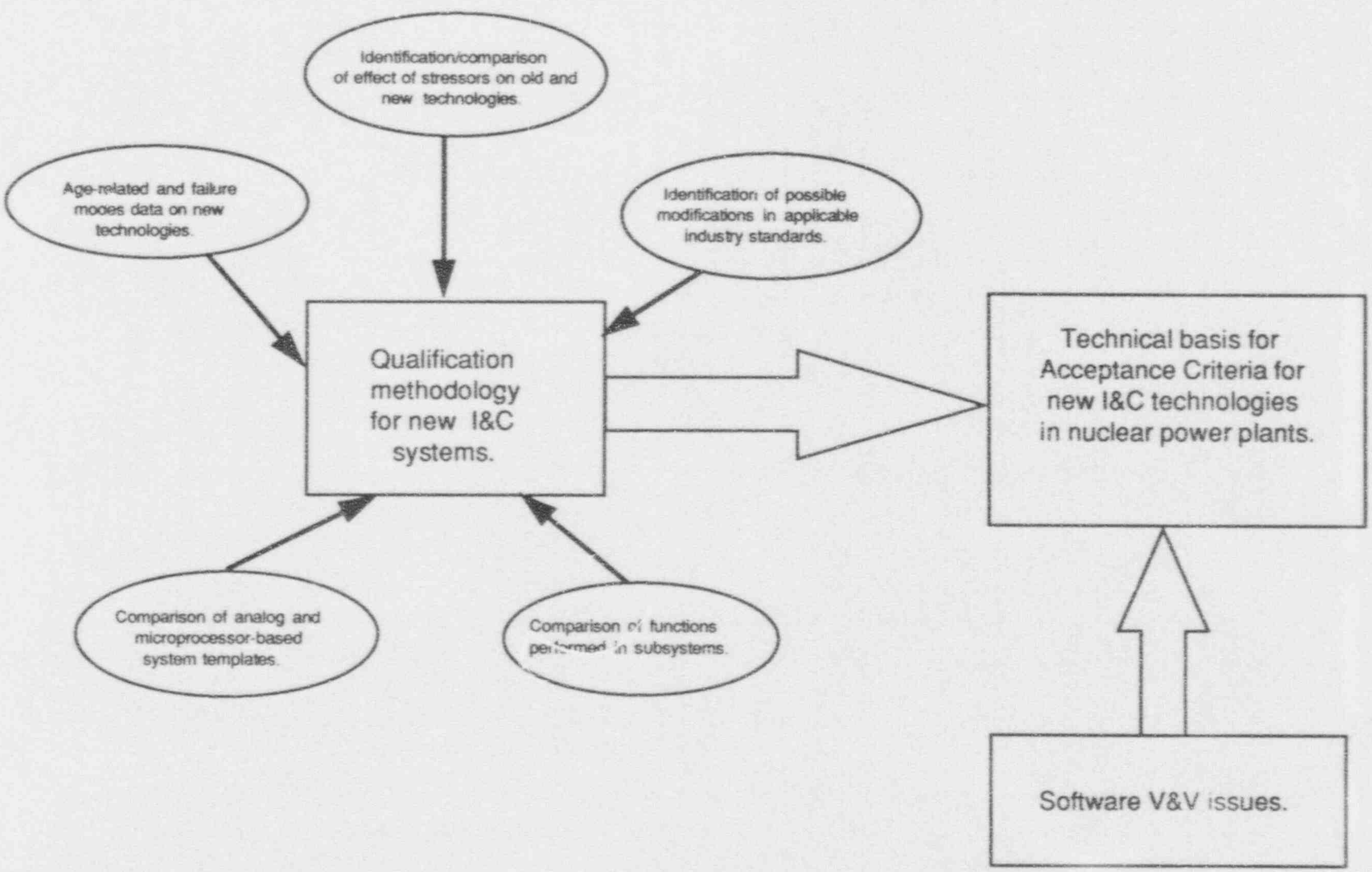

Identification/comparison of effect of stressors on old and new technologies.
Age-related and failure mooes data on new technologies.
Identification of possible modifications in applicable industry standards.
Qualification methodology for new I&C systems.
Technical basis for Acceptance Criteria for new I&C technologies in nuclear power plants.
Comparison of analog and microprocessor-based system templates.
Comparison of functions performed in subsystems.
Software V&V issues.

Figure 1.1 Developing acceptance criteria for application of "new" I&C technologies to safety-critical systems in nuclear power plants

present-day LWR. Functional issues considered in the templates include distribution of function, calibration, and testing capabilities and failure prediction based on environmental monitoring.

1.2 Project Objective

The objective of this study is to identify functional and environmental qualification issues that arise from the application of innovative "advanced" technologies to the nuclear power plant environment. Particular emphasis has been placed on identifying vulnerabilities and environmental effects that could be experienced by microprocessor-based reactor trip systems, optical fibers, and multiplexers.

1.3 Scope of Study

A simplified block diagram of a reactor protection system (RPS), showing the boundaries of the present study, is shown in Figure 1.2. The RPS includes the reactor trip system (RTS), the reactor switchgear, and the engineered safety feature actuation system (ESFAS). Our study of functional issues was limited to the RTS. Qualification issues cover identified technologies that are comparatively new to the nuclear power plant environment.

1.4 Research Approach

The research approach used in this study was to first survey three reactor manufacturers (Westinghouse, General Electric, and ABB/CE), and one of the major instrument manufacturers in the nuclear industry (Foxboro) to identify new features, characteristics, and specifications for advanced instrumentation that may be incorporated in ALWR designs. Other visits to both nuclear and nonnuclear process industries were also conducted to ascertain industry experience with regard to the reliability and functionality of modern I&C systems in industrial environments. A study of current practices with regard to I&C upgrades at nuclear power plants was conducted with a view to identifying issues for the functional evaluation and qualification of computer-based safety systems for ALWRs. Finally, information from the open literature and database sources such as Licensee Event Reports (LERs) were analyzed and integrated with an analog safety instrument string template, developed under the NPAR program, to develop technical bases for some of the qualification issues discussed in this report.

2 Functionality and Qualification of Protection Systems for Current Light-Water Reactors

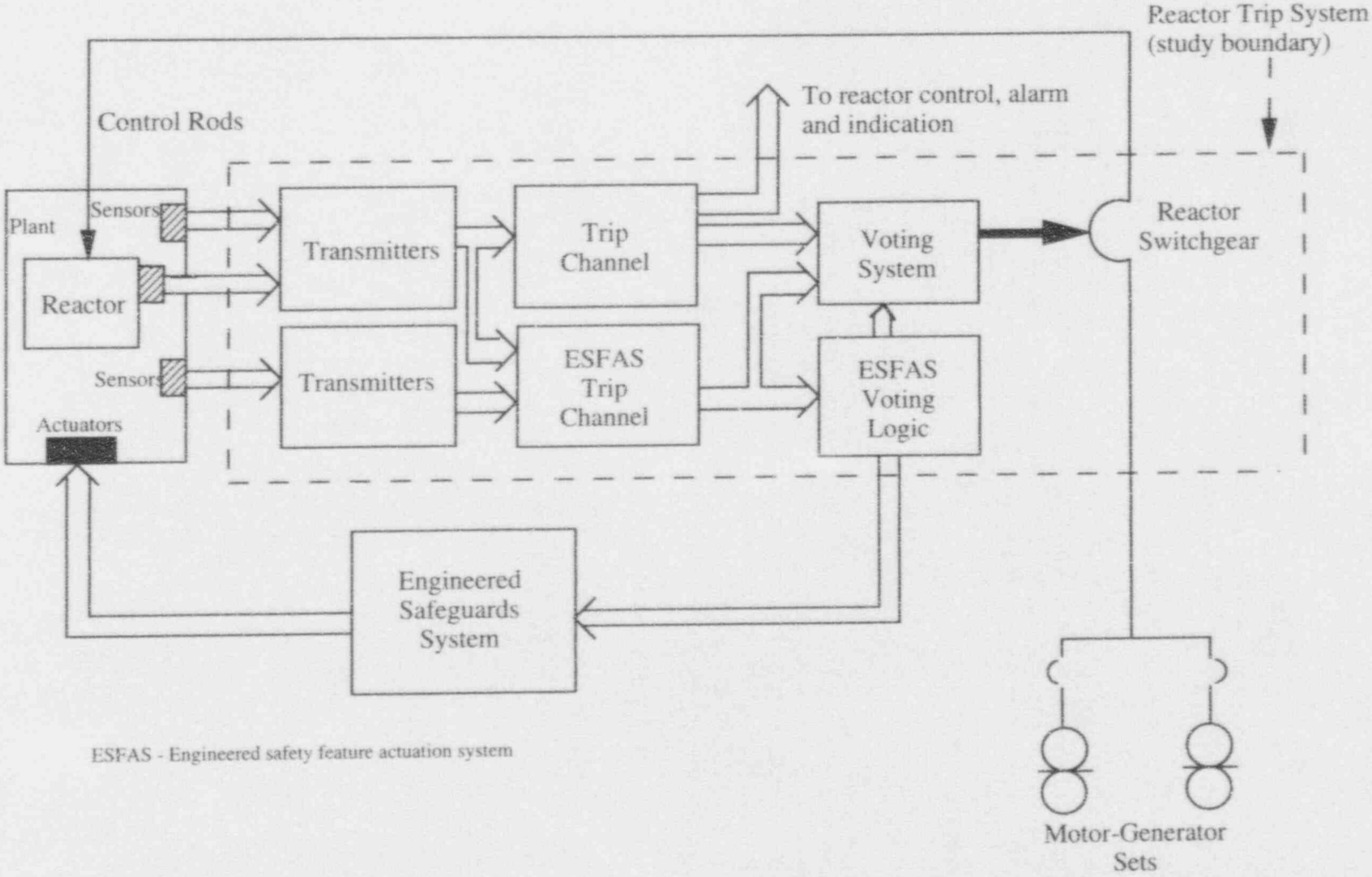
2.1 Introduction

In this chapter, the functionality and qualification methodologies for present-day nuclear power plants are discussed briefly. This discussion is intended to form the basis for addressing similar issues with regard to the introduction of "new" technologies in safety systems of nuclear power plants.

Three basic questions are addressed in the following sections:

1. What is the functional configuration of present-day reactor trip systems?
2. What are the predominant stressors that may lead to failures in present-day protection system I&C?
3. What are the limitations in current qualification methodologies for I&C systems?

The first question is an attempt to form a basis for addressing functional issues for the I&C portions of reactor protection systems proposed for ALWRs. The second and third questions are intended to form the basis for developing a methodology for qualifying new I&C systems in nuclear power plants.



ESFAS - Engineered safety feature actuation system

Figure 1.2 Simplified block diagram of a reactor protection system, showing the boundary selected for this study

2.2 Functional Configuration of Analog Trip Systems

The basic function of the RPS is to initiate a reactor scram and activate engineered safety features, if and when needed. Normally, the reactor trip function is achieved by monitoring several process variables relevant to maintaining the integrity of the fuel and the reactor coolant system pressure boundary. Each monitored signal passes through signal-conditioning circuitry (e.g., current-to-voltage conversion, scaling, etc.) to a comparator (bistable), where the signal is compared to its preestablished trip set point. If the process variable exceeds its set point, the bistable changes state and deenergizes its output to generate a parameter trip signal. Typically, four sets of neutron flux and selected process signals are monitored by four physically separate and redundant channels. Some form of redundant voting scheme, based on the partial trip information provided by each protection system channel, is typically used to generate the final reactor trip signal that shuts down the reactor.

Three generic analog trip system configurations, representative of the majority of shutdown systems used in the United States, are discussed briefly in this section.

2.2.1 Reactor Trip System I

This type of shutdown system is typical of pressurized water reactors (PWRs) designed by Westinghouse. In this configuration, the solid-state or relay trip signal for each of the monitored variables in each analog protection channel is supplied to each of two voting logic systems (trains A and B), as shown in Figure 2.1. Each train utilizes a 2-out-of-4 logic scheme such that the coincidence of any two partial trip signals will initiate a reactor scram signal to open the reactor trip breakers (i.e., create a de-energized condition). The reactor trip breakers are arranged in series with the power supply to the control rod drive system so that a reactor trip signal from any of the logic trains will initiate a scram.

Westinghouse designs typically allow the sharing of some transmitter signals for control as well as protection purposes. When this is the case, the control signal is separated from the protection signal by a suitable isolation device. The design philosophy of combining identical trip signals from the analog protection channels in each of the two logic trains ensures that coincidence from identical variables, referred to as *local coincidence* logic, will initiate a reactor scram. For example, if two or more reactor coolant system pressure trip signals, derived from the analog protection channels, occur in either logic train, a reactor scram will occu.. However, trip coincidence of different variables from two different channels (e.g., high flux on one channel and high temperature on another channel) will not cause a reactor scram. The design philosophy of initiating a reactor scram by combining trip signals from different variables from two or more different protection channels using an "OR" gate is referred to as *general coincidence*. Both local coincidence and general coincidence logic are used by reactor manufacturers.

The voting system or logic train may be based on relays, as in older reactors, or on solid-state circuitry, as in some of the newer or modified PWRs. Relay-based logic trains for a four-loop plant typically contain over 700 relays with ~4000 contacts connected in various matrices and are housed in 14 2-1/2-ft-wide by 2-1/2-ft-deep cabinets. In contrast, a system based on solid-state technology eliminates the majority of the 4000 contacts, typically resulting in the reduction of the number of cabinets required to 6.

In addition to performing the voting functions for reactor trip in hardware, the logic trains are also responsible for determining if conditions exist for initiating engineered safety feature (ESF) actuation signals. These safety features are provided to limit core damage and the amount of off-site dose to the public in the event of an accident. If an ESF actuation is required, each train will send a signal to actuate (e.g., start, open, close) the appropriate engineered safeguards system. Such safety systems are typically redundant, just as the logic trains are redundant.

Permissive signals are provided by the logic trains to allow automatic or manually initiated interlocks and bypasses.

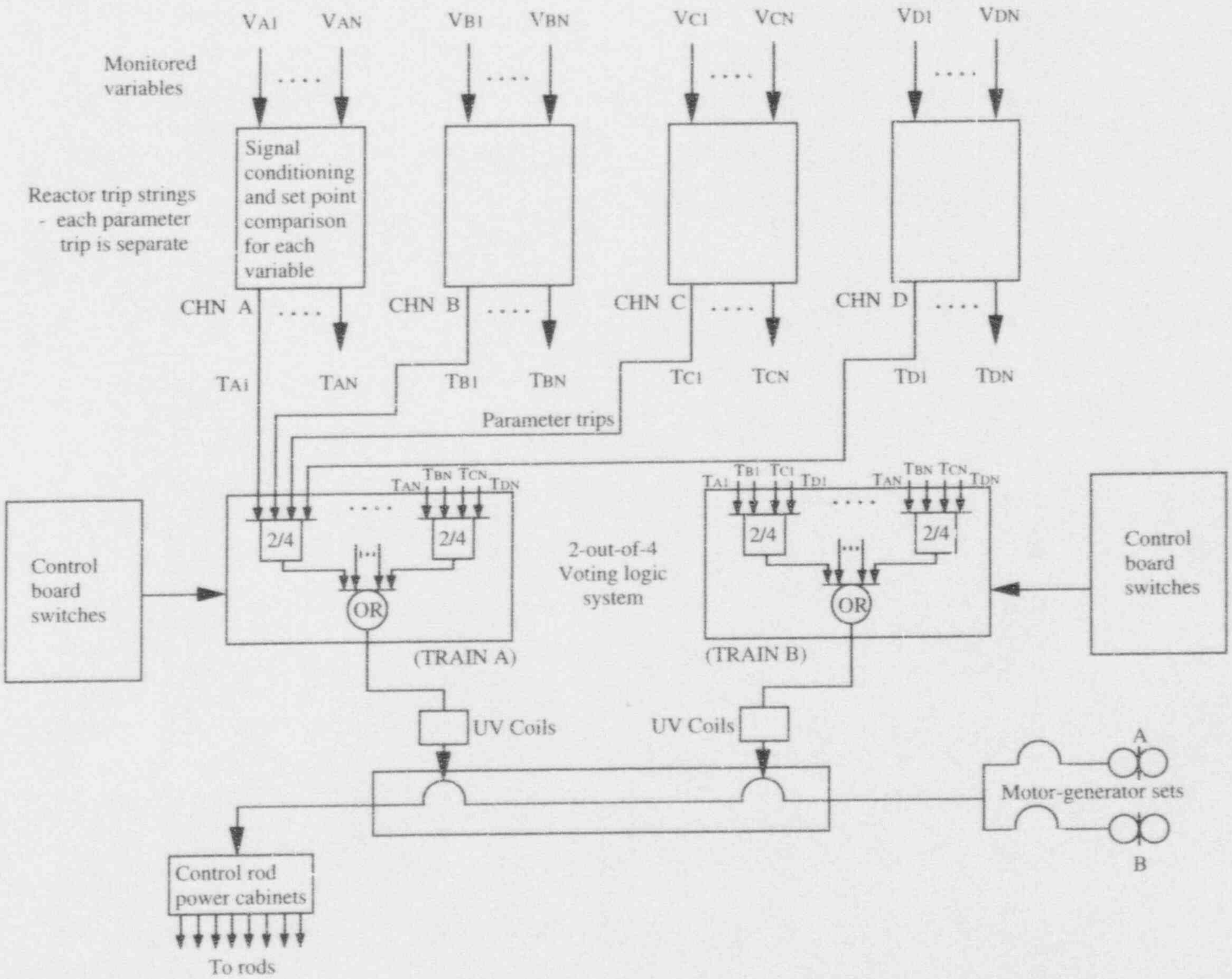


Figure 2.1 Simplified block diagram of a PWR reactor trip system (Westinghouse design)

2.2.2 Reactor Trip System II

Another configuration used in PWR protection system designs in the United States is shown in Figure 2.2. This is typical of Babcock and Wilcox (B&W) plants. As in system I, there are four separate trip channels: A, B, C, and D. However, general coincidence is used in each trip channel such that any of the nuclear (neutron) and nonnuclear (pressure, temperature, etc.) process variables that exceeds its trip set point causes a channel trip. (This means that the trip relay contacts from the monitored parameters in a channel are all connected in series.) Each trip channel output is connected to four trip modules. Each trip module initiates a reactor trip whenever any two of the four reactor trip channels signal a trip. The trip combinations that will initiate a reactor trip in *each* trip module are: $T_A.T_B$, $T_A.T_C$, $T_A.T_D$, $T_B.T_C$, $T_B.T_D$, and $T_C.T_D$. The outputs of the trip modules are connected to scram breakers that control both ac and dc power supplies to the safety rod groups, as shown. Note that the output from trip modules A and B actuate the two ac scram breakers, while the output from modules C and D actuate the dc scram breakers. The trip module output combinations that will result in a full reactor trip are A and B, A and D, B and C, or C and D.

Each of the protection system channels receives power from a Class 1E source, and each of the trip channels utilizes physically separate sensor taps, sensing lines, and sensor rack locations. Also, cables for each trip channel are routed separately to meet redundancy and independence requirements for the RPS.

2.2.3 Reactor Trip System III

Figure 2.3 shows a simplified protection system commonly used in boiling water reactors (BWRs) in the United States. As with B&W plants, general coincidence logic is used in each trip channel such that if any nuclear or nonnuclear process variable exceeds its trip set point, a channel trip signal is initiated. The four trip channels--channels A through D--are configured as two independent trip systems I and II. Trip system I consists of trip channels A and C, and trip system II consists of trip channels B and D. The protection system logic is *one-out-of-two-taken-twice*. That is, the reactor will scram only when there is a trip condition from any one of the trip channels in system I, *in conjunction with* a trip from either one of the trip channels in system II.

Unlike PWRs where control rods drop into the reactor under scram conditions, the control rods in a BWR are pushed into the reactor core from the bottom. The scram action is achieved as follows:

Associated with each rod is a scram pilot solenoid valve and two scram valves. Each scram pilot valve has two solenoids. One solenoid is energized from trip system I, and the other is energized from trip system II. The scram pilot solenoid valve controls the air supply to the scram valves for each control rod. Under normal reactor operating conditions, both solenoids for each scram pilot valve are energized, and air pressure holds the scram inlet and scram outlet valves closed. The scram valves control supply and discharge paths for control drive water. If a trip condition occurs in both trip systems I *and* II, both solenoids become de-energized, and the ports of the scram pilot valve shift so as to block the air pressure supply. At the same time, the trapped air pressure keeping the scram inlet and outlet valves closed is vented off, allowing the springs in the scram valves to open the valves. This allows water from the scram accumulator to act on the control rod drive piston, scramming the rod. The displaced water from each rod piston movement is vented into a scram discharge volume.

As with the other protection system designs, several manual scram bypasses, available on control panels in the control room, are provided to accommodate varying protection system requirements that are dependent on operating conditions.

To meet redundancy and independence requirements for the RPS, physically separate sensor taps, sensing lines, and sensor rack locations are used. Cables for each protection system channel are routed separately to four protection system cabinets in the control room.

Each of the protection system channels receives power from a Class 1E uninterruptible power system. These power sources, together with the two motor-generator sets, are usually located in areas where they can be serviced during reactor operation.

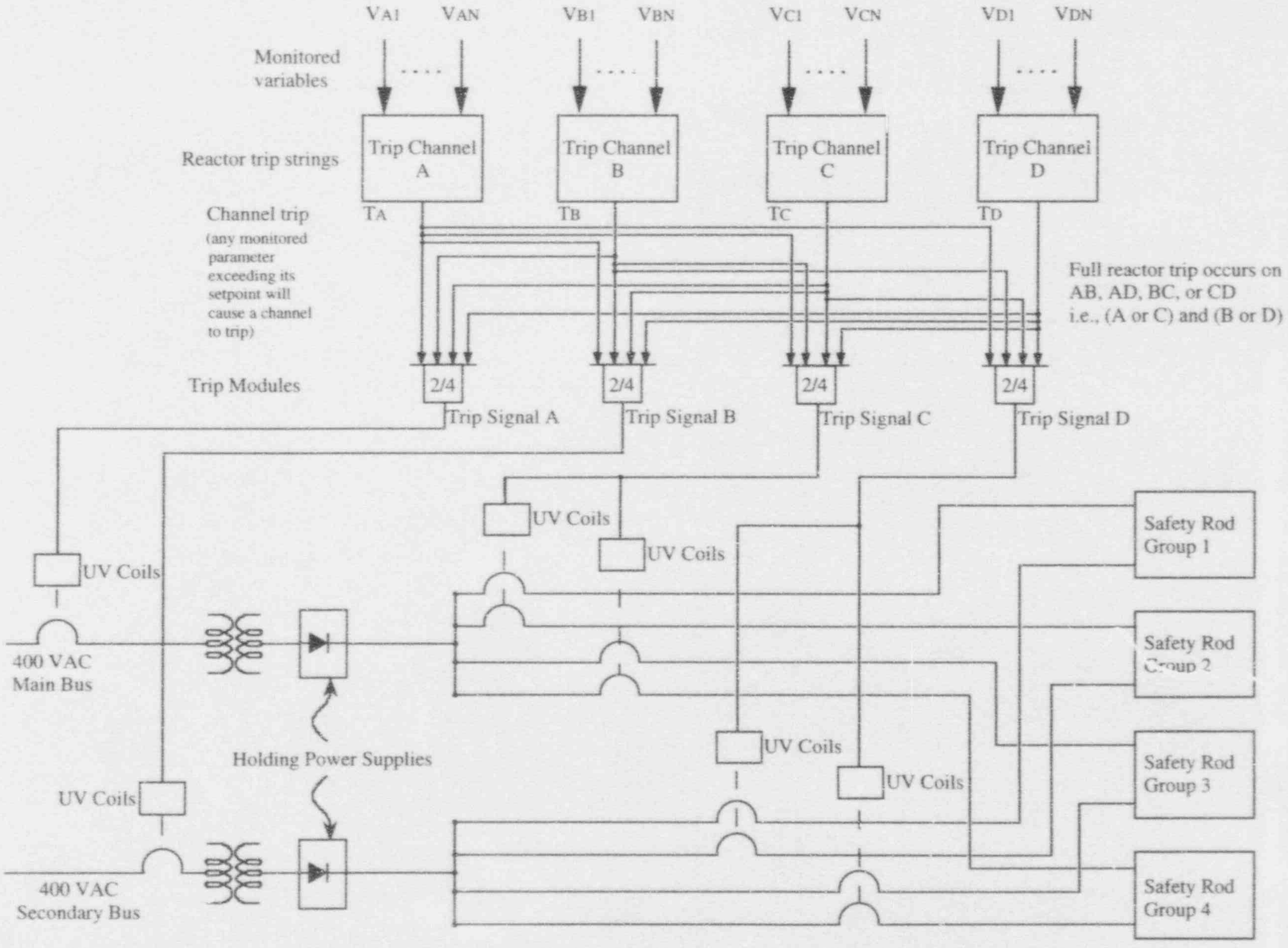


Figure 2.2 Simplified block diagram of a PWR reactor trip system (B&W design)

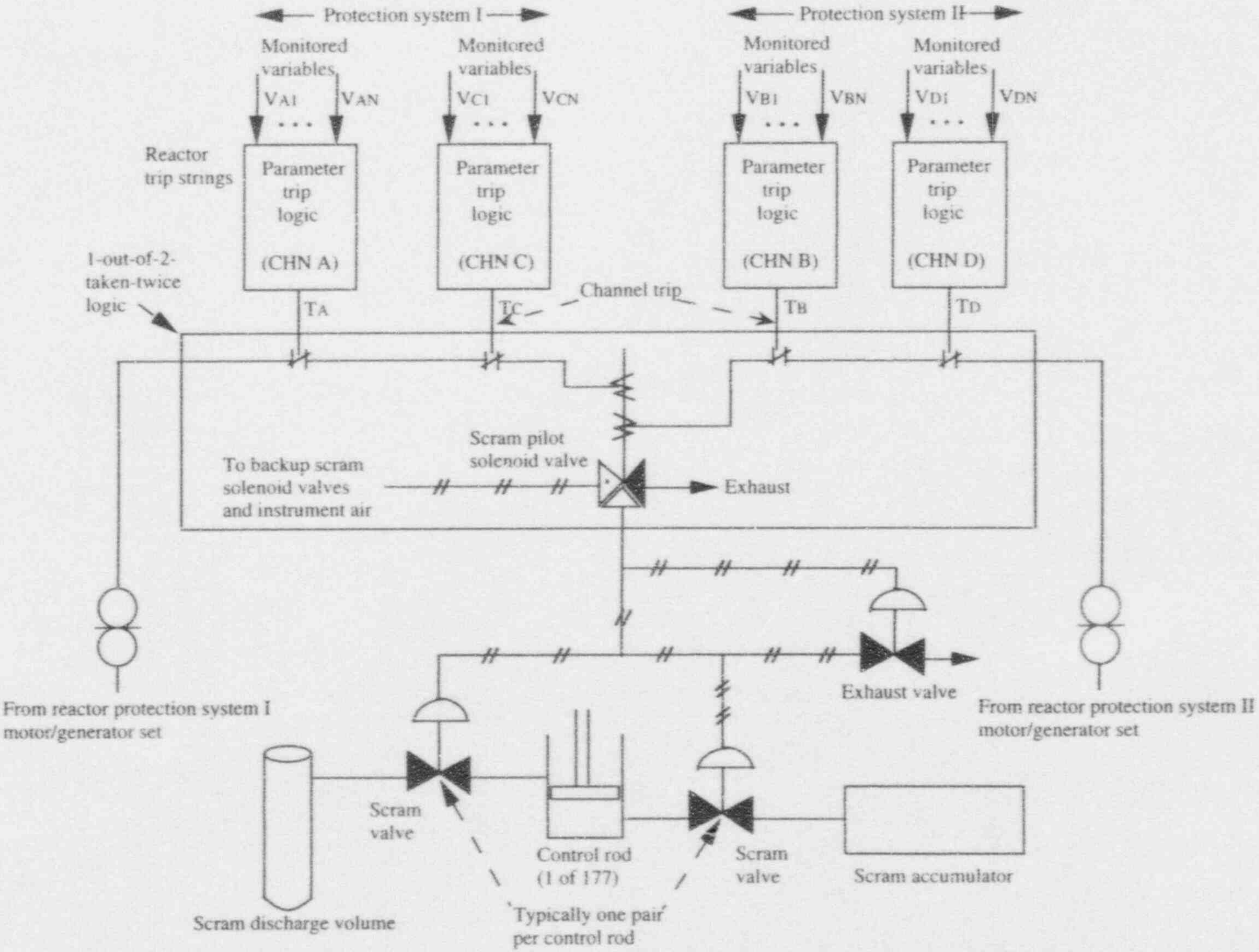

Protection system I
Protection system II
Monitored variables
VA1
VAN
Monitored variables
VC1
VCN
Monitored variables
VB1
VBN
Monitored variables
VD1
VDN
Reactor trip strings
Parameter trip logic (CHN A)
Parameter trip logic (CHN C)
Parameter trip logic (CHN B)
Parameter trip logic (CHN D)
1-out-of-2-taken-twice logic
TA
TC
Channel trip
TB
TD
Scram pilot solenoid valve
To backup scram solenoid valves and instrument air
Exhaust
Exhaust valve
From reactor protection system I motor/generator set
From reactor protection system II motor/generator set
Scram valve
Control rod (1 of 177)
Scram valve
Scram accumulator
Scram discharge volume
Typically one pair per control rod

Figure 2.3 Simplified block diagram of a BWR reactor trip system (General Electric design)

As with other protection systems, surveillance testing is performed periodically on the RPS. This includes sensor functional testing, sensor calibration, and trip response time measurements with simulated inputs to individual trip units and sensors. Sensor (transmitter) readings are usually verified by comparing the readings from other channels of the same variable.

In addition to the basic RTSs, PWRs typically have equipment (complete from sensor output to final actuation device) separate from the RTS that is used to automatically initiate emergency feedwater and a turbine trip under conditions indicative of an *anticipated transient without scram*, or ATWS.[2] For BWRs, the following systems are typically provided as a backup to the basic reactor trip already described:

- an alternate rod injection (ARI) system that is diverse from sensor output to the final actuation device;
- a standby liquid control system (SLCS) capable of injecting boron solution into the pressure vessel for reactor shutdown; and
- equipment capable of tripping the reactor coolant circulating pumps automatically under conditions indicative of an ATWS.

The following facts and conclusions may be drawn from this overview on trip systems found in existing LWRs:

- Electrical and physical separation is maintained in the trip channels up to, but not including, the voting scheme implementation. However, voters are redundant, with separation and isolation typically provided between voters.
- The voting is performed in hardware, using relays or solid-state logic devices.
- Both local and general coincidence schemes are used in protection system implementations.
- Backup trip and emergency feedwater actuation systems are provided to mitigate against conditions indicative of an ATWS.
- Both the nuclear industry and regulatory bodies generally accept the *analog* hardware implementations of protection systems in existing LWRs because considerable experience has been accumulated over the years with regard to these systems. In addition, the operation and failure modes of analog systems are well understood. It is therefore reasonable to use the present analog trip systems as a basis for evaluating trip systems proposed for ALWRs, as well as equivalent systems designed to be used as retrofits in existing LWRs.

2.3 Investigation of Environmentally Related Failures in Safety Systems

We investigated the frequency of reactor trips and ESF actuations that were attributable to environmentally related faults in I&C systems. The motivation for this study was to qualitatively estimate the effectiveness of current qualification procedures in reducing the frequency of protection system I&C failures caused by environmental stressors.

Several databases exist from which various aspects of nuclear plant data may be obtained.[3-5] The most widely used of these databases are the *Nuclear Plant Reliability Data System* (NPRDS), the *Licensee Event Reports* (LER), and the *Nuclear Power Experience* (NPE) databases. The LER database at the Nuclear Safety Information Center in Oak Ridge, Tennessee, was examined to determine the causes of malfunctions in protection systems in existing LWRs. A search of the LER database over a 10-year period (1982–1991) yielded a total of 1065 reportable events. Some of the events were related to faults that occurred in safety-related systems, whether or not they resulted in a reactor trip or ESF actuation. Others were not necessarily faults but were reported for various reasons such as technical specification violations, etc. Out of the 1065 reportable events, the following was used as the selection criterion for further analysis:

Did the fault in the safety-related system result in a channel trip, a full reactor trip, or ESF actuation?

A total of 216 of the LER events that met this criterion occurred in PWRs, while 294 events occurred in BWRs. Table 2.1 shows the causes of the LER events by reactor type. The category listed as "other" includes events for which the cause(s) were not clearly stated or could not be inferred or events that could not be categorized as environmentally related. The latter included causes such as a "failed amplifier," "faulty summator in the signal condition circuitry," etc. Table 2.2 provides information similar to Table 2.1, but with the number of faults in a given category given as a percentage of the number of selected events of the same reactor type. That is, the first column shows the number of LER events falling into each category, computed as a percentage of the total number of PWR events that met the selection criterion. The second column shows similar data for BWRs. The third column lists the number of faults in each category as a percentage of the total number of selected events (PWR *and* BWR).

Table 2.1 Causes of reactor trips and ESF actuations, reported as number of events over the 10-year period 1982-1991

	Reactor type		
Cause of problem	PWR	BWR	Total
Temperature	7	5	12
Humidity/moisture	10	13	23
Corrosion	3	8	11
EMI/RFI, ESD*	22	21	43
Lightning	6	4	10
Maintenance error	50	51	101
Other	118	192	310
Total	216	294	510

*EMI/RFI, ESD–electromagnetic interference/radio-frequency interference, electrostatic discharge.

Table 2.2 Causes of reactor trips and ESF actuations, reported as percentages of selected events. The events cover the same time span as those of Table 2.1.

Cause of problem	PWR	BWR	(PWR + BWR)
Temperature	3.3	1.7	2.4
Humidity	4.6	4.4	4.5
Corrosion	1.4	2.7	2.2
EMI/RFI, ESD*	10.2	7.2	8.4
Lightning	2.8	1.4	2.0
Maintenance error	23.1	17.3	19.8
Other	54.6	65.3	60.7
Total	100.0	100.0	100.0

*EMI/RFI, ESD–electromagnetic interference/radio-frequency interference, electrostatic discharge.

The LER events were selected without regard to operating power. That is, the reactor might already have been in cold shutdown when the trip or ESF actuation occurred. The assumption made here was that if the reactor had been operating when the problem occurred, there is no reason to believe that the results would have been different.

It is possible that a small fraction of the faults listed as "other" were actually environmentally related, although it was impossible to ascertain this from the documentation related to the LER event. For example, a failure might be reported to have been due to a "failed undervoltage output driver card," but there generally would be no indication that this might have been due to high ambient temperature or other environmental parameter.

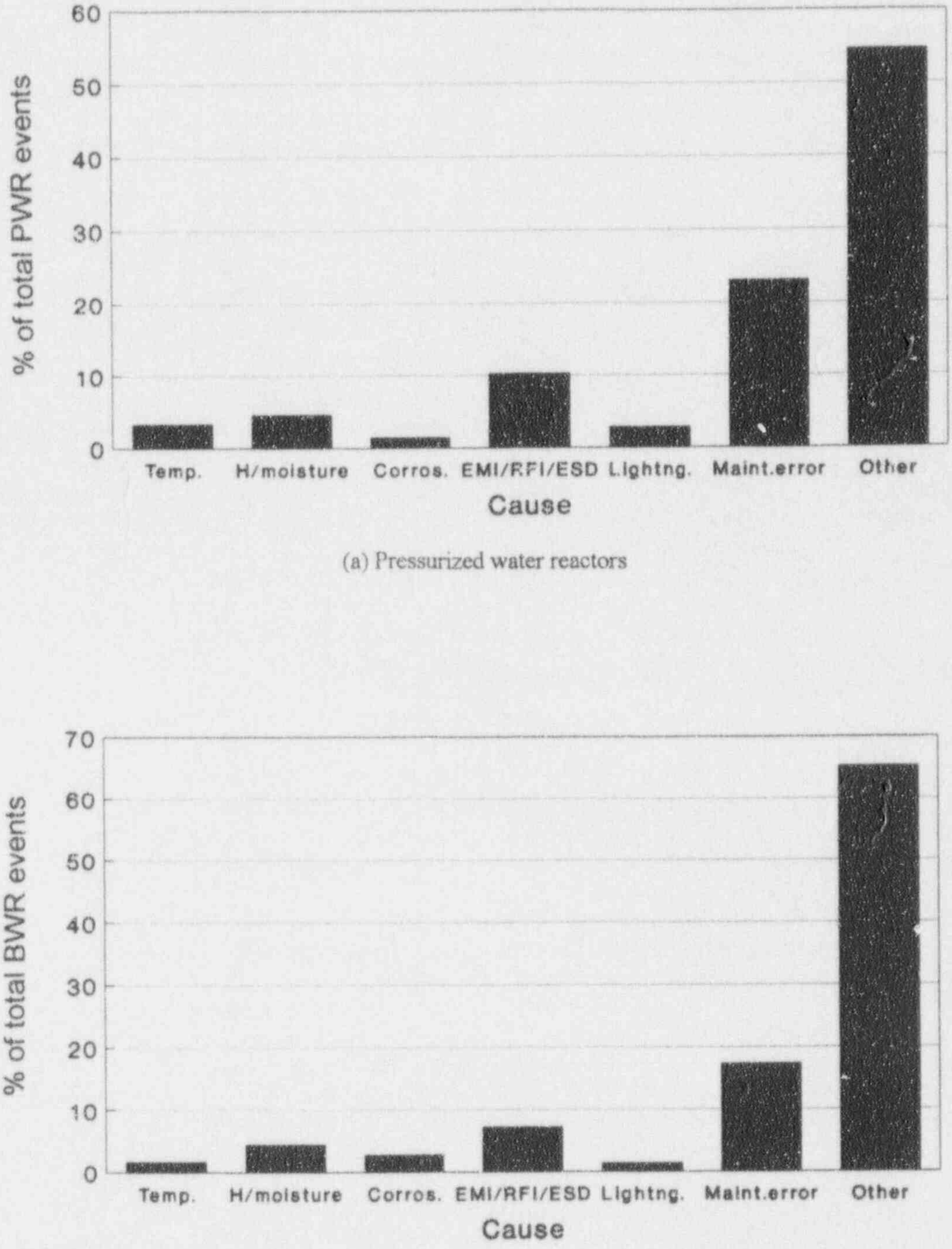
The "maintenance error" category includes errors that were not directly attributable to the operator or technician. An example is inadequate written procedures for a test sequence whose application causes a trip or ESF actuation.

Trips or ESF actuations that were listed under the "EMI/RFI" category included transient noise spike(s), the source of which could not be ascertained from the LER event; trips that were attributed to the use of portable radios in the vicinity of transmitters; EMI/RFI-induced noise spikes in protection channel or safety-related circuits; or electrostatic discharge (ESD) induced in safety-related circuits. This breakdown of EMI/RFI-related trips or ESF actuations is given in Table 2.3. The numbers in parentheses indicate the number of EMI/RFI-related events in that category as a percentage of the total EMI/RFI-related events. Thus, 41% of all EMI/RFI-related half/full scrams or ESF actuations in PWRs were attributed to safety-related circuits that failed directly as a result of EMI/RFI noise spikes. In BWRs, the figure was 66.7%. This category (category III) includes EMI/RFI-induced faults that were attributed to the use of portable radios in the vicinity of cabinets, noise due to a floating lead, etc. Note that category II also involves EMI/RFI-related faults attributed to the use of portable radios. However, category II relates only to faults that were induced in *transmitters*, whereas the category III faults occurred in circuits and systems other than transmitters. Figure 2.4 shows the plotted data from the second and third columns of Table 2.2.

Table 2.3 EMI/RFI-related causes of trips and ESF actuations

Category No.	Specific EMI/RFI-related problem	PWR	BWR
		No. of events (% of EMI events)	No. of events (% of EMI events)
I	Transient noise spike(s) of unknown source	5 (22.7%)	2 (9.5%)
II	Use of portable radios resulting in false reading of transmitters	7 (31.8%)	5 (23.8%)
III	EMI/RFI-induced noise spikes in safety channel circuits	9 (41.0%)	14 (66.7%)
IV	Electrostatic discharge in safety channel circuits	1 (4.5%)	0 (0%)

While this study has some limitations because the root cause of many of the system malfunctions is not documented in the LER database, useful conclusions can nevertheless be drawn. The first is that the fraction of EMI/RFI-related protection system events is significant compared to traditionally recognized environmental stressors such as elevated temperature. Another conclusion is that the use of automatic testing and surveillance techniques, as well as advanced diagnostics techniques that will enable the prediction of impending malfunctions in circuits, could significantly reduce maintenance errors as well as increase the reliability of safety systems and should be encouraged and/or researched.



(a) Pressurized water reactors

(b) Boiling water reactors

Fig. 2.4 Causes of protection channel trip and ESF actuations in commercial nuclear power plants. (a) Pressurized water reactors. (b) Boiling water reactors.

2.4 Equipment Qualification of Present-Day Class 1E Electrical Systems

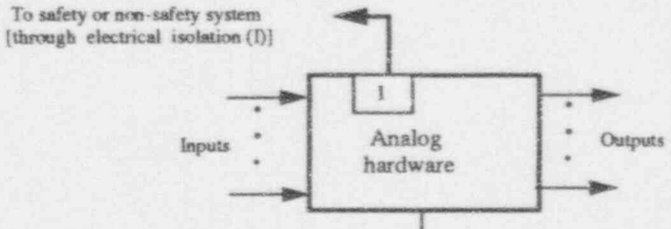
The study in Sect. 2.3 indicates that environmental stressors contribute much less to partial or full reactor trips or ESF actuations than maintenance error. Although stressors do accelerate the aging of equipment, no firm conclusions on the efficacy of current qualification methodologies can be drawn from the study because no attempt was made to identify age-related failures. Qualifying equipmen. for application in a Class 1E environment gives added assurance that it will function as intended during a design basis event (DBE). The DBE may occur after the equipment has undergone a certain amount of *deterioration* (aging) while in service. Hence, accelerated aging of equipment to simulate the condition of its greatest vulnerability to an accident is a fundamental concept in a qualification methodology. In a prior study focusing on reactor protection systems,[6] assessments were made of the relative number of occurrences of aging-related failures vs other failures. In that study a quantity, aging fraction, was defined for a particular piece of equipment as

Aging fraction = (failures due to aging)/(total failures).

It was found that different types of I&C equipment had similar aging fractions ranging between 0.2 and 0.4. While this study was performed using the NPRDS database, another study using the LER database produced similar results,[7] despite differences in judgments in both studies regarding what constitutes aging effects. It appears from these two studies that aging is a significant contributing factor to I&C equipment failures.

Current standards for qualifying safety-related systems are embodied in IEEE Standard 323-1974 (endorsed by NRC Regulatory Guide 1.89), "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and IEEE Standard 344-1987 (as endorsed by Regulatory Guide 1.100), "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations." While environmental qualification may be accomplished by either type testing, operating experience, or analysis,[8] the primary means is by type testing. The type test sequence as stipulated in IEEE 323-1974 is summarized in Figure 2.5. An important part of the qualification procedure is the thermal aging process. The Arrhenius equation[9] is the physical model used in accelerated aging. However, one of the major problem areas is the adequacy of the model in simulating actual equipment aging. This is especially true of electronic systems, where the different components making up a subsystem have different activation energies and different degradation mechanisms. Another problem is that of synergism, where the effect of *simultaneous* application of radiation and temperature may be different from the *sequential* application typically employed. Figure 2.6 depicts the qualification procedure used by a Class 1E equipment manufacturer selected at random to study industry conformity with present standards. As illustrated in Figure 2.6, thermal aging is performed before radiation aging, where both are applicable. (Note that the horizontal arrows in the figure depict where functional testing is performed.) Evidence to date shows that, with regard to cables at least, the order of application of the stressors may be significant.[10]

A third observation with regard to present-day methodologies is that EMI/RFI qualification is not generally considered as part of environmental qualification. Although reactor manufacturers do conduct EMI/RFI tests on safety system equipment, such tests are generally for the purpose of demonstrating physical independence of Class 1E and nón-Class 1E circuitry. In general, EMI testing is addressed only on an individual equipment basis, as necessary. However, the unpredictable behavior of protection system software under the influence of EMI may require that EMI/RFI susceptibility tests be performed as part of an environmental qualification procedure. NRC Regulatory Guide 1.89 defines qualification as "verification of design limited to demonstrating that the electric equipment is capable of performing its safety function under significant *environmental stresses* resulting from design basis accidents in order to avoid common-cause failures." Electromagnetic interference is an *environmental stressor.*[11] It may cause spurious equipment operation, resulting in overcycling of components and systems, damage to components that protect against electrical noise and transients, and progressive degradation to specific components such as insulation. Thus, while detailed procedures for testing a system's susceptibility to EMI need not be explicitly defined in IEEE Standard 323, the latter could specify that EMI/F qualification be met in accordance with appropriate (IEEE) standards that deal with such criteria.


To safety or non-safety system
[through electrical isolation (I)]
I
Analog
hardware
Inputs
Outputs

QUALIFICATION PROCESS BY TYPE TEST	COMMENTS
	Diagram represents a generalized safety instrumentation and control system consisting of analog and electromechanical components. Interfaces to other safety systems or non-safety systems typically employ electrical isolation.
Environmental qualification test sequence	The test sequence described here (IEEE Std 323-1974) represents the most severe sequence. IEEE 323 allows a different sequence to be used if it can be justified as the most severe for the item being tested. (NOTE: Although the NRC has not specifically endorsed IEEE Std 323-1983, the type test sequence in the two versions are essentially the same.)
Operate equipment under normal conditions	The functional performance of the equipment is tested under normal operating conditions.
Operate equipment to the extremes of all performance and electrical characteristics	This does not include design basis event and post design basis event conditions. Functional testing is again performed at this point.
Subject equipment through a thermal aging process.	Functional testing is performed after the aging process. The aging process may include the design basis radiation unless the required radiation level can be shown to produce less effect than that which would cause loss of the equipment's Class 1E function. Supplement to Section 6.3.3 of IEEE 323-1974 - "Aging" - is provided in Regulatory Guide 1.89.
Subject equipment to non-seismic and seismic vibration conditions.	IEEE Std 323-1974 references IEEE Std 344-1971 for seismic qualification. However, the 1987 version of this standard is endorsed by Regulatory Guide 1.100, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants."
Expose equipment to simulated design basis event	Test for functionality of those portions required to operate while exposed to the design basis event. IEEE Std 323-1974 allows radiation to be excluded if it was incorporated in the aging process.
Expose equipment to simulated post accident conditions	Test for functionality of those portions required to operate following the simulated design basis event.

Figure 2.5 Equipment qualification procedure by type test for present-day (analog) safety system

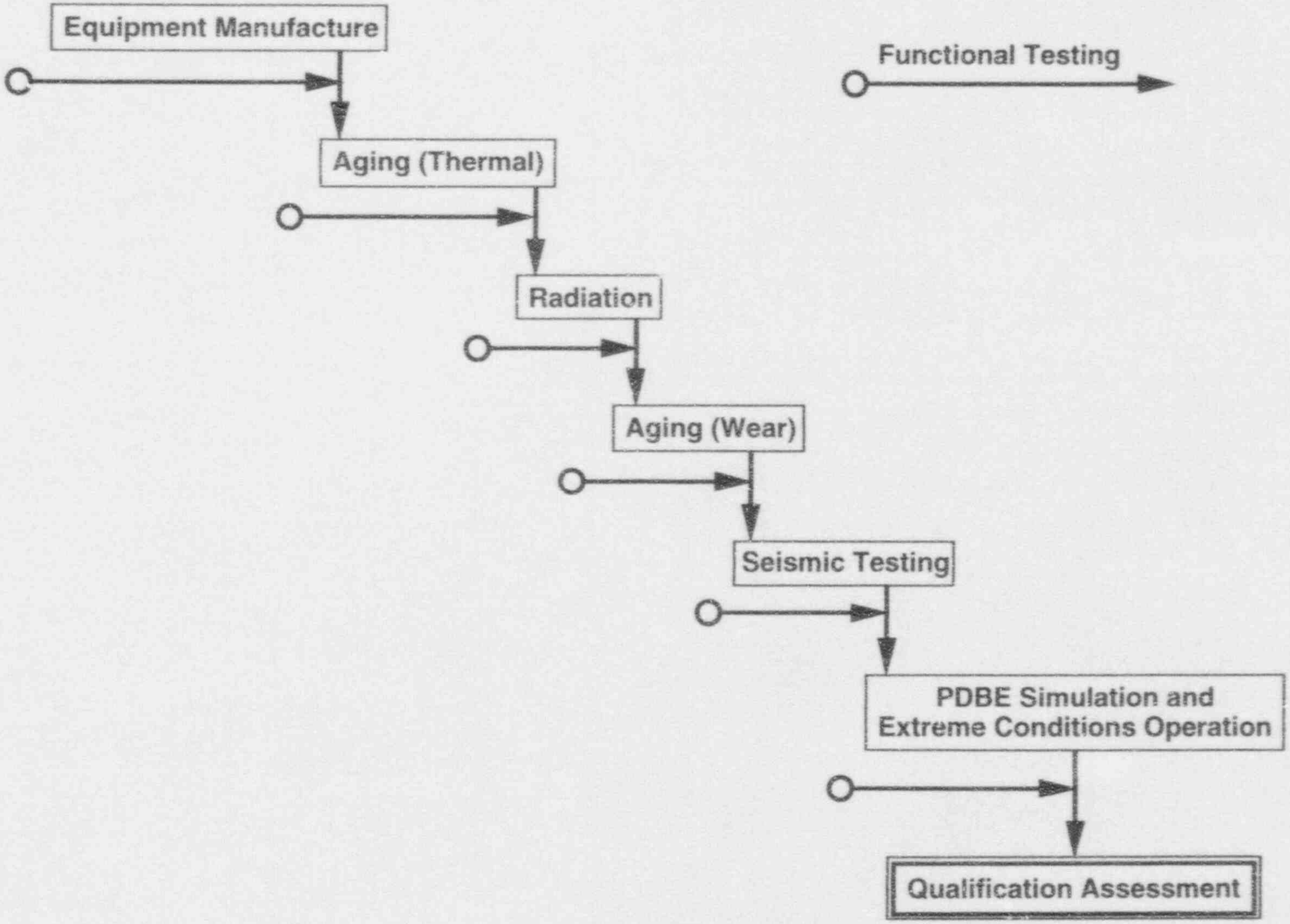


Figure 2.6 Equipment qualification process employed by a selected Class 1E electrical equipment manufacturer

2.5 Environmental and Aging Data Template for a Typical Analog Instrument String

Important aspects of the I&C qualification program include identification of the materials and the normal and abnormal stressors and environments to which safety-related I&C systems of ALWRs may be subjected. Most electromechanical equipment degrades with time, especially in the presence of environmental cycles of temperature, pressure, humidity, radiation, vibration, or chemical spray. Thus, it is necessary to establish a qualified life span, especially for Class 1E equipment, during which system operation within specifications can be reasonably assured. In this section, we describe an environmental and aging data template for an instrument string typically found in an (analog) protection channel in a present-day nuclear power plant. This will be used as a basis for developing a similar template for ALWRs.

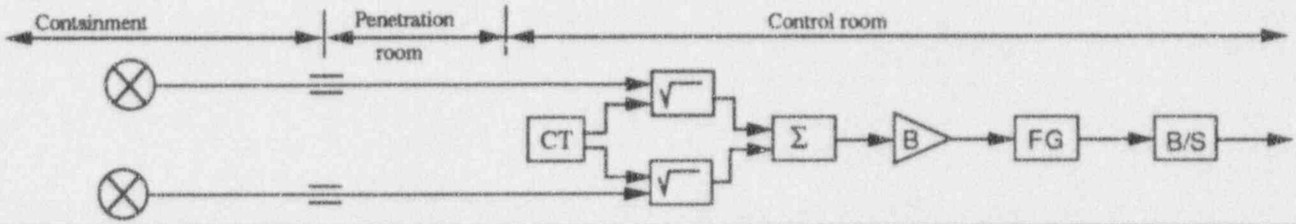
Traditionally, discrete analog technology has been used in implementing reactor protection systems, including instrument strings in the protection channels of most existing LWRs. A typical instrument string (e.g., reactor coolant flow) is shown in Figure 2.7. The figure presents data on environmental conditions typically found at the location of major components in the string, as well as stressors that contribute to component degradation. This diagram draws on information from Reference 12. In the figure, neutron flux and reactor coolant flow are continuously monitored by a power-imbalance-flow bistable. Total coolant flow is measured by monitoring the flow in each of the plant's coolant loops using differential pressure transmitters that generate an output current proportional to the differential pressure produced across an orifice introduced in the coolant loop. Electronic circuitry is used to develop a signal proportional to the square root of this differential pressure signal, giving a measure of the flow in that loop. Other analog circuitry is used to compute the sum of the signals from both loops to obtain the total flow. Typically, the channel is designed to trip on the basis of a power-to-flow relationship. In this example, a power/ imbalance/flow ($\phi/\Delta\phi/F$) relationship is used.[12] Although not all LWR types use a power/imbalance/flow relationship as one of the reactor trip parameters, the environmental conditions shown in the figure, as well as the stressors to which system components are subject, are nevertheless fairly typical of all LWR types. Also, the channel components–namely transmitters, cables, connectors, and electronic components–are typical of other reactor protection system channels. The design, material composition, and aging mechanisms in different types of transmitters used in nuclear power plants are well documented elsewhere.[12,13] The analog circuits in transmitters are subject to malfunction or damage due to noise spikes, voltage surges, lightning, EMI/RFI, and high temperatures. Steps usually taken to minimize the effect of these parameters include the use of appropriate isolation devices, shielding, grounding, and heat sinks.

The environmental conditions and stressors to which the flow channel components are exposed are discussed is some detail below, with respect to Figure 2.7.

2.5.1 Radiation

For obvious reasons, radiation levels are higher inside reactor containment than outside. Many locations in the reactor building of a typical PWR receive a total dose of about 5 × 10^4 rad over a 20-year period, with an upper limit dose of about 3 × 10^5 rad.[14] The total dose level in PWR control rooms is typically lower than 4 × 10^2 rad over the 40-year plant life. Since channel electronics for protection systems in LWRs are typically in racks and cabinets situated in control room environments, it may be safe to assume that protection system electronics in current commercial nuclear power plants will not receive a 40-year dose of more than 4 × 10^2 rad, typically considered a "mild environment."

Presently, most transmitters for use within containment have a qualified life of 10 to 40 years, depending on transmitter type, materials of construction, and other factors. For example, the strain gauge transmitter has a qualified life of 40 years, while the differential capacitance transmitter is qualified for 20 years. Seals and gaskets for transmitters may have a much lower qualified life (e.g., 4 years).[12]



	Flow transmitter	Reactor building cable	Reactor building penetration	Penetration room cable	Calibration/ test module	Square root extractor	Summing circuit	Buffer amplifier	Function generator	Power/flow comparator bistable
Functions performed in software	None									
Radiation	~ 4 x 10^4 rad over 20 years				<4 x 10^2 rad over 40 year plant life					
Ambient temperature	Average temperature in containment:~ 120°F. Average transmitter operating limits: -40° to 240° F		60 to 130° F		~ 60 to 80° F in control room.					
EMI/RFI	Nuclear qualified transmitters typically operate normally around sources of radio frequency from ~30 to 500 MHz and field intensity of 20 V/m.				EMI/RFI susceptibility tests are generally addressed on an individual equipment basis as necessary, such as demonstrating physical independence of Class 1E and non-Class 1E circuitry .					
Interfaces	Reactor coolant piping, junction boxes, seals, 110 Vac and 120 Vdc power supp'ies, inverters, interlocks, and bypass modules.									
Signal type	Pressure to current transduction (4- to 20- mA current loop.				±10 Vdc					
Stressors	Temperature, radiation, moisture, maintenance and installation handling, environmental cycles.				Maintenance/testing cycles, elevated temperatures inside cabinet housing the electronic modules/components, electromagnetic interference.					
Materials	CABLE MATERIALS: *Reactor building instruments:* **Conductor:** 16 AWG copper conductor **Insulation:** Cross linked polyethylene* **Sheath:** Neoprene* **Outer Jacket:** Galvanized steel				Several types of transmitters are used. The following is representative: MATERIALS IN CAPACITANCE TYPE PRESSURE TRANSDUCERS:[a] **Housing:** Aluminum with epoxy polyester paint or 316 stainless steel. **Fill fluid:** Silicon oil. **Isolation diaphragm:** 316 stainless steel. **Housing seal:** Ethylene propylene.* **Electronic components:** Seals and insulating materials used on electronic components.* **Circuit boards:** Epoxy glass laminate.*			Seals and insulating materials used on electronic components, encapsulating materials for electronic components, and solder joints are all subject to aging degradation.		

[a] Materials subject to aging degradation are representative of other transmitter types.

*Materials subject to aging degradation.

Figure 2.7 Environmental and aging data template for coolant flow string in an analog protection channel. (Adapted from L. Meyer, *Nuclear Plant Aging Research on Reactor Protection Systems*, NUREG/CR-4740, Idaho National Engineering Laboratory, January 1988.)

2.5.2 Environment Temperature

Environmental temperatures inside containment average about 120°F, with maximum temperatures approaching 150°F. Operating limits for nuclear qualified transmitters lie between −40°F and 240°F. These data were estimated from examination of the technical specifications for a number of nuclear qualified transmitters. Temperatures in penetration rooms or cable spreading rooms may range from 60°F to 130°F, while control room temperatures are typically between 50°F and 80°F. Thus, while transmitters and cables are subjected to relatively high temperatures, protection system cabinets during normal operation experience much lower temperatures as well as radiation levels.

2.5.3 EMI/RFI

We examined the EMI/RFI specifications for a number of nuclear qualified transmitters. The transmitters were found to be guaranteed by the manufacturers to operate normally in the vicinity of sources of radio-frequency energy ranging from ~30 MHz to 500 MHz, at a field intensity of 20 V/m. In many cases, information on the standards used for EMI/RFI tests on transmitters could not be obtained. For one manufacturer, however, testing standards used to evaluate transmitters were ascertained to include the following:

Electromagnetic interference–IEC 801-3, Mil Standard 461C
Electromagnetic susceptibility–SAMA PMG 33.1

In addition, standards developed in-house were used. We can only assume that the use of the above standards, in addition to internal standards, is fairly typical of other transmitter manufacturers. To the authors' knowledge, no specific guidelines are presently available that set EMI/RFI limits and criteria for nuclear power plants. Work in this area is in progress at the time of writing this document.[15,16]

2.5.4 Interfaces

Interfaces include the high- and low-pressure taps and the piping arrangement used to connect the differential pressure (ΔP) transmitter to the process. Valves and test points are usually provided in the piping for calibration purposes. The ΔP transmitters (together with other transmitters measuring other variables) are typically located in the penetration room. In addition to the piping penetrations, there also are instrument cable penetrations that carry the 4- to 20-mA transmitter signals to the reactor protection system instrumentation. Penetrations are pressurized so that a detected decrease in pressure will signal a deterioration of the seals. Penetrations are typically qualified for 40 years plus 1 year post-DBE. Electrical cables are also qualified for 40 years.

2.5.5 Stressors

Stressors applied to transmitters include elevated temperature, vibration, radiation, moisture, power transients, chemical spray, maintenance handling, and environmental cycling. Elevated temperature, vibration, and radiation can affect the electronic components inside the transmitter housing and the environmental seals over a period of time. If the transmitter termination seals fail before or during a design basis accident (DBA), this will result in contamination of the transmitter electronics by steam and/or chemical spray and probable failure of the transmitter. Normal environmental humidity conditions do not pose a problem for nuclear qualified transmitters because they are sealed for DBA environmental steam conditions. However, the environmental seals may harden or crack under high-radiation and/or -temperature conditions, thereby allowing moisture to seep into the system under damp conditions.

Examination of the LER database from 1976 to 1981 by Meyer[12] showed that 63% of all faults in the RTS were discovered by testing, 34% were discovered during normal operations, and 3% were discovered by other means. This strongly indicates that periodic testing is very important to the maintenance of overall protection system reliability. However, manual testing is rather slow and tedious, suggesting that automated, on-line testing methods could contribute significantly to nuclear power plant operations. On-line surveillance and diagnostic methods are indeed among the salient features of microprocessor-based protection systems proposed for both retrofits and the next generation of nuclear power plants.

2.6 Concluding Remarks

In this chapter the configuration and voting logic of RTSs for current nuclear power plants in the United States were briefly reviewed in order to establish a basis for evaluating equivalent systems for retrofits and ALWRs. The frequencies of reactor trip and ESF actuations attributed to environmentally related faults in I&C systems were studied to estimate the severity of EMI/RFI and other environmental related problems in present-day nuclear power plants. The stressors to which protection channels are subject were also discussed. Finally, some of the limitations in present qualification methodologies were presented. The following conclusions may be drawn:

A. *Two-out-of-four* or *one-out-of-two-taken-twice* voting schemes are widely used and accepted in the nuclear industry. Thus, RTS configurations that use a different design philosophy may need to be more carefully evaluated.

B. While there are some limitations with current qualification methodologies, qualification standards and procedures appear to be effective. This conclusion is supported by the relatively low frequency of environmentally related causes of channel trips and ESF actuations compared to other causes, such as maintenance error.

C. The fraction of EMI/RFI-related protection system events is significant compared to traditionally recognized environmental stressors such as elevated temperature. The situation could be more aggravated with the widespread use of microprocessors in safety systems, where the increasing level of integration at the chip level tends to decrease the noise immunity of the digital devices. Thus, qualification methods in this area appear to require strengthening.

D. Automatic testing and surveillance techniques may significantly reduce the present relatively high incidence of protection system events due to maintenance errors. Also, advanced diagnostic techniques that will enable the prediction of impending malfunctions in circuits can significantly increase the reliability of safety systems and should be encouraged and/or researched.

3 Qualification and Functional Issues for "New" I&C Technologies in Commercial Light-Water Reactors

3.1 Introduction

The issue of obsolescence is a major motivating factor in current efforts directed toward the modernization of I&C systems in commercial nuclear power plants. Of the ~110 power plants now in operation, over 50% are 15 years old or greater, with some being over 25 years old. Many of the I&C systems in these plants use equipment and technology no longer supported by suppliers. Equipment suppliers are driven in large measure by the needs of the nonnuclear process industry, which is the largest customer for I&C equipment. The process industry has been much more prone to embrace digital technology than the nuclear industry, and this trend, coupled with a lack of new reactor orders for the last several years, has reduced the incentive for some suppliers to the nuclear power industry to remain suppliers of exact replacement equipment. For example, it has been estimated that 70% of the original equipment suppliers for older nuclear plants are no longer in business.[17] In addition to these compelling market forces driving utilities to consider the use of digital retrofits in safety-related systems, digital systems themselves have some inherent and desirable advantages compared to analog systems. One the most important of these is the potential for extensive self-testing and diagnostics capabilities, allowing continuous assessment and assurance of system operability. Another is the potential for on-line surveillance, reducing not only the need for frequent operator surveillance, but also the avoidance of premature aging of I&C systems.

However, the introduction of digital technology in safety-related systems of nuclear power plants also raises key issues relating to the systems' *environmental* and *functional* reliability. For example, do the new systems introduce additional system degradation mechanisms that could impact the reliability of the I&C system and the safety of the plant? Do the systems introduce the possibility of a different type of malfunction or increase the probability of common-mode failures that could reduce the reliability of the safety system? Do EMI/RFI effects pose a significant reliability problem? The intent of this study, therefore, is to identify, as far as practical given the available information, issues involved in the qualification and evaluation of "advanced" I&C systems proposed for ALWRs. This includes the identification of potential degradation mechanisms of equipment proposed for use in safety-related systems of ALWRs.

We approached the problem by first reviewing RTS designs proposed for ALWRs. For each trip system studied, an evaluation template was then developed by identifying subsystem functions and the impact of designated stressors on components in one channel compared to equivalent components in a trip channel of an existing LWR.

3.2 Reactor Trip Systems Proposed for ALWRs

This section briefly discusses reactor trip designs proposed for use in three ALWRs. Information in this section was obtained from discussions with reactor manufacturers.

3.2.1 Overview of Protection System Configuration for the AP600

The AP600 is Westinghouse Corporation's ALWR design. Protection system functions are implemented in four integrated protection cabinets (IPCs). The protection system consists of four physically and electrically independent divisions. A division includes all plant sensors for all process instruments that are used for protection functions plus the associated control electronics. The functions performed in a division (apart from the sensors/transmitters) are all implemented as *subsystems* within an IPC. A simplified block diagram of an IPC is shown in Figure 3.1. Each subsystem is typically a separate card chassis in the IPC. The functions of a subsystem are implemented on boards mounted in the card chassis. Independence between subsystems is maintained by using

- separate input/output (I/O) circuitry (for each subsystem) to maintain independence at the subsystem interfaces;

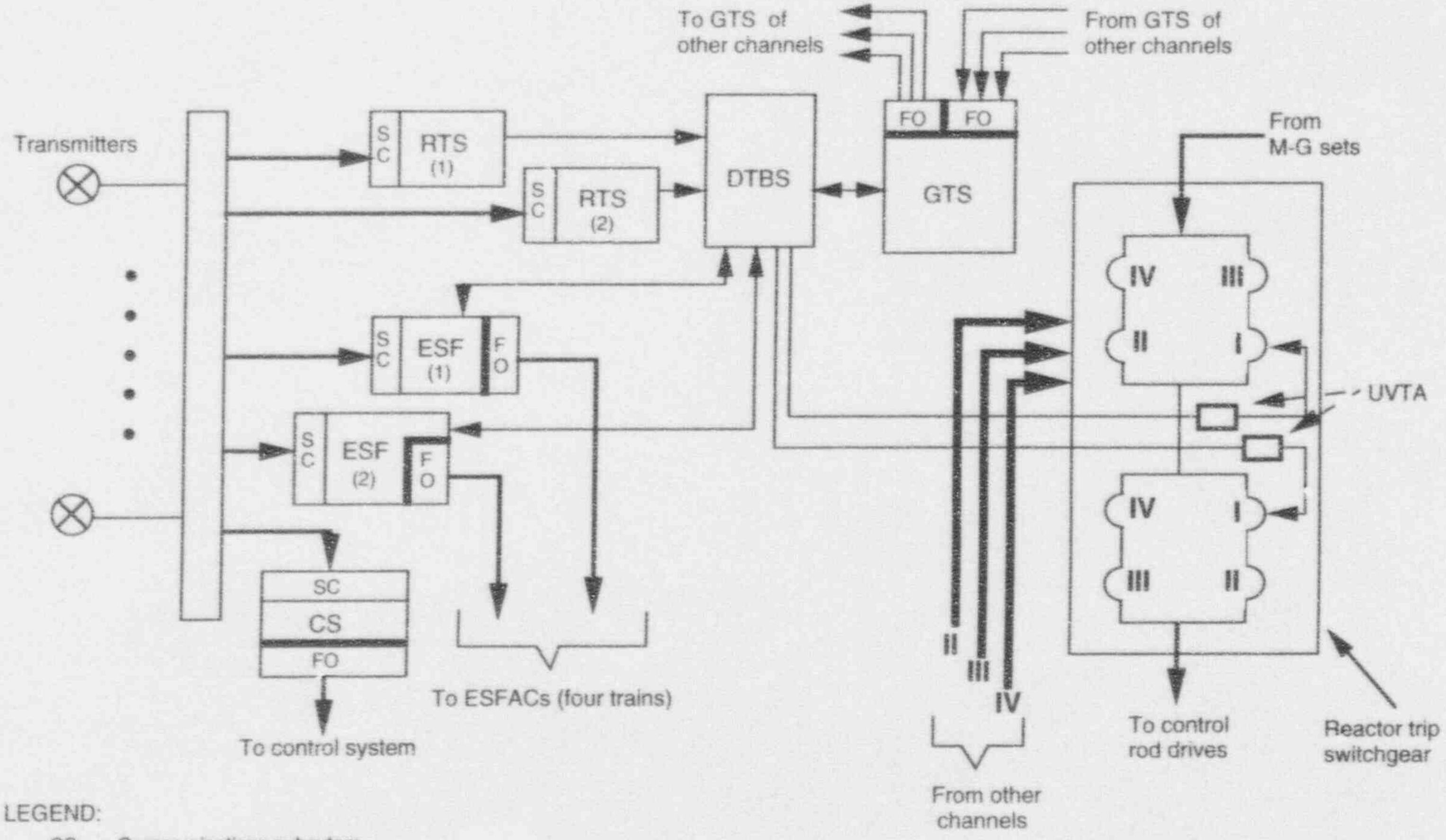
- separate dc power supplies with output protection to prevent interaction between subsystems upon failure of a subsystem; and

- optical coupling or resistor buffering between subsystems.

Inputs to subsystems receiving sensor signals have signal conditioning circuitry consisting of passive filter networks that provide RFI filtering, surge withstand capability, and signal amplification/translation designed to translate the input signals to a standard level compatible to the analog-to-digital (A/D) converters in the subsystems.

A 12-bit A/D converter, with multiplexed inputs and working under microprocessor-based control, is used to digitize inputs in a subsystem. A built-in automatic calibration feature is used to enhance the accuracy of the analog inputs. Each subsystem's A/D converter periodically reads high and low reference voltages, which are then used to calculate compensation terms for bias and gain errors. Correction terms are unique to each analog input signal. Cognizant Westinghouse personnel indicated that this procedure should reduce gain and offset errors to the accuracy level of the precision reference voltages.

The analog variables monitored for reactor trip functions are processed into digital format by the reactor trip subsystem (RTS). The subsystem provides a partial trip signal to the dynamic trip bus subsystem (DTBS) whenever *each* protection division parameter exceeds its set limit. The function of the DTBS is to open the reactor trip switchgear in its own protection division as required by the monitored parameters. It receives data from the global trip subsystem (GTS) to determine the desired state of the switchgear.



LEGEND:

CS - Communications subsytem
DTBS - Dynamic trip bus subsystem
ESF - Engineered safety feature subsystem
FO - Isolation/fiber optic data links
GTS - Global trp subsystem
RTS - Reactor trip subsystem
SC - Signal conditioning circuitry
UVTA - Undervoltage trip attachment

Figure 3.1 Simplified reactor trip system (one division) for the AP600

The partial trip and bypass information sent to the GTS is multiplexed over serial data links to the other three GTSs in the other divisions. At the same time, the GTS of the division under consideration receives similar partial trip (and partial trip bypass) information from the other divisions.

A protection division generates a reactor trip to open the circuit breakers in its division under the following conditions:

1. Any two-out-of-four unbypassed partial trips. This two-out-of-four voting is performed on each set of four identical protection system parameters.

2. If one protection channel has been bypassed, the voting is performed on each of the two-out-of-three unbypassed partial trips. [Failures within a protection division is communicated to the other three divisions as a global (i.e., protection division) bypass. When a global bypass is indicated, each of the other protection divisions considers each process variable within that ("bad") division to be in a bypass state.] Cognizant Westinghouse personnel indicated that failure of the communication hardware or the data link used for the data transmission produces identical results.

In addition, each IPC allows a technician to place each individual partial trip function in manual trip, manual bypass, or normal mode. This provision should allow a particular transmitter/sensor or associated input circuitry to be manually placed in a bypassed state, rather than incapacitate an entire protection division. Under partial bypass conditions, a full reactor trip will be generated when any of the following conditions are true:

1. Two-out-of-four partial bypasses in coincidence with one-out-of-two of the remaining unbypassed partial trips.
2. Three-out-of-four partial bypasses.

When the condition(s) necessary for a division trip is met, the signal from the DTBS, which normally energizes the undervoltage trip attachment (UVTA) on each of the two trip breakers for that division, is lost. The loss of signal causes the UVTAs to be de-energized, which, in turn, causes the reactor trip breakers to be opened. The RTS consists of eight circuit breakers configured as shown in Figure 3.1.

Westinghouse's solution to the problem of possible loss of functional diversity due to multiplexing several trip parameters is to divide the trip parameters into two groups within each IPC, with each group monitored by a separate RTS. Independence of the functionally diverse trips is maintained in the reactor trip groups from the input circuitry through to the DTBS. It should be noted that while each RTS measures a different set of process variables, a process variable may be taken to reactor trip group 1 subsystem, engineered safety feature group 1 subsystem, and the communication subsystem in the IPC. This is performed through suitable isolation and is done because all three systems--shutdown, engineered safety feature actuation, and control--may need the same process variable to function. An example is pressurizer pressure signal, which is taken to RTS group 2 subsystem [for core limit (departure from nucleate boiling) calculation], ESF group 2 subsystem (for safety injection), and the communication subsystem (for control purposes).

Each subsystem performs on-line diagnostics on its own hardware. The health of the subsystem is communicated to the communications subsystem (CS) within the IPC. This information is available to external systems through optical data links. Other status information available to external systems is cabinet temperature, cabinet entry status (i.e., whether open or closed), dc power supply voltages, and subsystem diagnostic status. The function of the CS also is to process signals meant for control purposes on analog input boards separate from protection signals, enabling filter time constants optimized for control functions to be used if desired.

Other subsystems shown in Figure 3.1 are the ESF group 1 subsystem and ESF group 2 subsystem. Parameters monitored by ESF group 1 are different from those measured by ESF group 2. As is the case with the RTSs, this provides functional diversity and improves the system's reliability with regard to accident protection. The primary functions of the subsystems are to calculate partial bistable actuations, combine the automatic actuation with the manual actuation and manual bypass data, and transmit the data to the engineered safety feature actuation cabinets

(ESFACs). Note that the ESFACs are separate cabinets and are not part of the IPC. However, the ESF group 1 and group 2 subsystems are part of the IPC.

The IPCs are typically installed in fire protected rooms, separate from the control room. (Maximum allowable *ambient* temperature is reported to be 120°F. This suggests that the maximum allowable temperature *inside* an IPC is higher). The reactor trip, ESF, and communication subsystems have battery backups. Battery power to the subsystems to support necessary functions will be maintained for a maximum of 3 days without attendance.

In the AP600, all essential software programs (including set points) reside in erasable, programmable, read-only memory (EPROM) or electrically erasable, programmable, read-only memory (EEPROM). Thus, set point changes are only possible at the cabinet site with specialized equipment.

3.2.2 Overview of Protection System Configuration for the System 80$^+$

The System 80$^+$ is ABB Combustion Engineering's ALWR design. The protection system is part of their integrated plant I&C called the *Nuplex 80$^+$* advanced control complex. The RTS is implemented in four physically and electrically separate plant protection system (PPS) cabinets. A simplified block diagram is shown in Figure 3.2. Each RTS division consists of five subsystems: a bistable trip processor (BTP), a core protection calculator (CPC), coincidence processor (CP), reactor trip initiation logic (RTIL), and an automatic tester subsystem for the automatic testing of the plant protection system logic. Process measurements that serve as trip variables have one process channel each in each protection division, with the exception of the control element assembly (CEA) position, which has two position measurement channels in each protection division. Some of the analog variables monitored for reactor trip functions serve as inputs to the BTP. Others are used as inputs to the CPC, where calculation of departure from nucleate boiling ratio (DNBR) and local power density are performed.

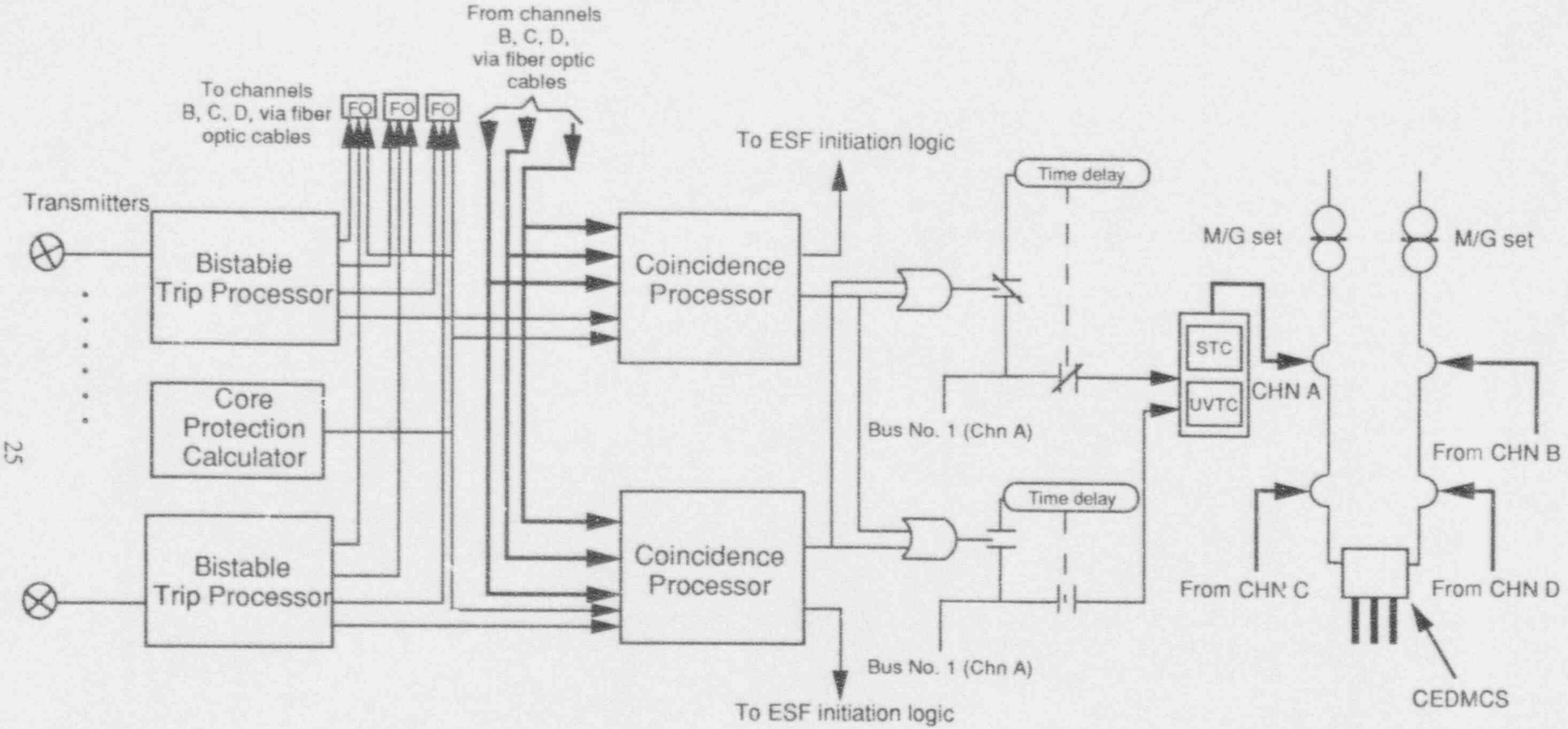
The BTP subsystem initiates a channel trip signal to the CP in that channel when the digitized value of the measured variable exceeds its set point. The trip signal(s) is sent simultaneously to the other divisions over fiber-optic data links. Each CP subsystem also receives channel trip inputs from the CPC in its respective division, as well as bypass signals. Using local coincidence logic, a CP subsystem evaluates whether to generate a division trip initiation signal to the switchgear system, based on the state of the four *like* trip signals and their respective bypasses. Two-out-of-four logic is used, but this is converted to two-out-of-three logic for parameters that have been bypassed. The system is designed such that only one channel for any one parameter may be bypassed at any one time. Bypass status outputs are also available for display at the local and remote operators' modules.

The CP outputs are connected to *initiation logic* consisting of OR circuits and time delay circuits. The time delay circuit functions as a noise filter by allowing the trip signal to pass through to the initiation relay in the appropriate PPS division only if the trip signal maintains a continuous presence for a minimum amount of time. The initiation relays are connected to the undervoltage and shunt trip elements and act to trip the appropriate circuit breakers in the reactor switchgear system. Two motor-generator sets are connected through the circuit breaker arrangement to the control rod groups, or the control element drive mechanisms control system (CEDMCS). Complete removal of power from the CEDMCS is possible only if a minimum of two breakers in opposite legs of the circuit are opened. The loss of either motor-generator set does not cause a release of the control rod assemblies.

Each PPS cabinet receives ac power from a separate vital instrument bus, while the control logic for each switchgear circuit breaker receives dc power from a separate battery system.

A measure of functional diversity is provided in the System 80$^+$ protection system design by dividing the trip parameters into two groups within each PPS cabinet, with each group monitored by a separate BTP.

Automatic as well as manual testing is provided for the complete reactor protection system. Automatic testing is performed passively, that is, without the injection of active test signals to the protection system. Each of the four protection divisions has an interface and test processor (ITP), which reads relevant protection system data for subsequent analysis and determination of the health of the system. The tests include division-to-division



LEGEND:

CEDMCS - Control element drive mechanism control system.
CHN - Channel.
M/G - Motor/Generator.
STC - Shunt trip circuit.
UVTC - Undervoltage trip circuit.

Figure 3.2 Simplified reactor trip system (one division) for the System 80+

comparison of input signals for the detection of signal discrepancies, thereby assuring correct sensor/transmitter operation and/or the accuracy of A/D conversion(s). Other tests include status consistency checks and set point checks.

In accordance with 10 CFR 50.62, the System 80$^+$ protection system includes an *alternate protection system* that is separate and diverse from the plant protection system. The alternate protection system includes an alternate RTS, which initiates a reactor trip when pressurizer pressure exceeds a predetermined value, and an alternate feedwater actuation signal, which initiates emergency feedwater when steam generator water level decreases below a predetermined value.

3.2.3 Overview of Trip System Configuration for the ABWR and the SBWR

The advanced boiling water reactor (ABWR) and the simplified boiling water reactor (SBWR) are ALWR concepts proposed by General Electric. As far as the reactor protection system is concerned, the two reactor types are almost identical. Some of the differences relate to the number of process variables monitored for trip functions and the scope of the Essential Multiplexing System (EMS). [The EMS provides data highways for sensor inputs to the logic units and for the logic output to the appropriate actuators (e.g., pumps, valves, motors, etc.)]. The EMS for both reactor types is similar in system design philosophy, but it has a smaller scope in the SBWR. For example, in both the ABWR and the SBWR, most sensor signals are multiplexed. However, while ESF output trips are also multiplexed in the ABWR, all output trips in the SBWR are hardwired.

In both cases, instruments used to measure appropriate RPS signals from the reactor vessel are mounted on instrument racks in the four quadrants of the reactor building. Sensors for RPS signals from equipment in the turbine building are mounted locally. The ABWR protection system is briefly described below.

The reactor trip functions together with several other safety-related functions are implemented in four electrically and geographically separate divisions. This four-division system is called the Safety System Logic and Control (SSLC). A simplified block diagram of the reactor trip system for one division is shown in Figure 3.3.

Reactor trip process variables [both analog and discrete (e.g., ON/OFF state of switches)] are acquired by a remote multiplexing unit (RMU), which then converts the signals into a digital format suitable for multiplexing. This "digital format" of the input signal includes not only the magnitude or status information of the input signal, but also signal identification, error checking, and synchronizing data bits. Signal conditioning as well as automatic calibration of the associated A/D converter are also performed in the RMU. The data are converted into an optical signal and sent as serial, time multiplexed data stream unto a dual redundant FDDI (fiber distributed data interface) network.

The process data are acquired off the network by a digital trip module (DTM) within the SSLC. The DTM performs the trip logic calculations by comparing the individual monitored variables for that division with set point values and, for each variable, sends a separate "trip" or "no trip" signal to the trip logic unit (TLU) in that division, as well as to each TLU of the other three divisions. Communication with the other three divisional TLUs is via fiber-optic serial data links. Both the DTM and TLU are implemented in separate microprocessors. The software in these processors is RPS-unique; that is, the software does not perform any other safety-related logic functions.

The TLU performs two-out-of-four voting on each set of four *like* trip conditions to determine whether a scram signal should be generated for that division. The module also receives bypass inputs from the bypass unit (BPU) and manual inputs from switches within the same division. [The manual switches enable the reactor operator(s) to modify the trip logic as appropriate during maintenance or testing, and the bypass units perform appropriate interlock logic for sensor bypasses and division TLU bypasses.] The trip information is sent to the output logic unit (OLU), as shown in Figure 3.3. The OLU sends a scram signal to trip actuators--isolated load drivers and relays for automatic scram and air header dump initiation--associated with that division. The load drivers are solid state devices whose output is connected between the 120-Vac power source and the scram solenoids for the hydraulic control unit such that a trip signal at the input will cause a de-energization of the scram solenoids. The

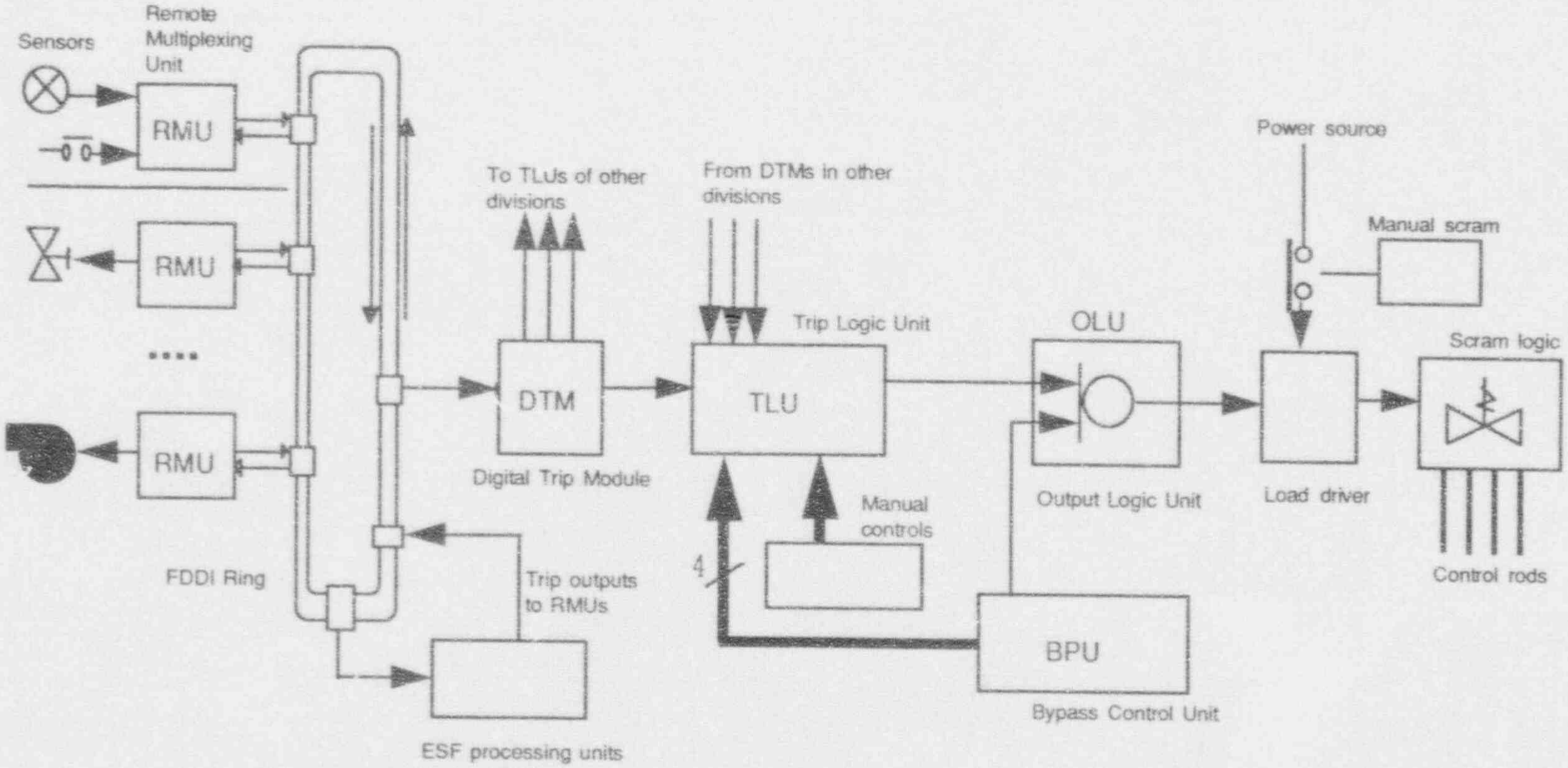


Figure 3.3 Simplified reactor trip system (one division) for the ABWR

load drivers in all four divisions are interconnected in a two-out-of-four arrangement such that a reactor scram occurs when load drivers associated with any two or more divisions receive trip signals.

Essentially, each module in the RTS is a general purpose computer module with self-testing capability. Tests include continuous error checking of all transmitted and received data on the serial data links of each SSLC controller (e.g., checksum and cyclic redundancy checking techniques). In addition to the self-diagnostics capability, which allows problem identification to the card level, surveillance testing of the RPS (e.g., sensor calibration, trip channel actuation, etc.) can be performed periodically during plant operation.

The protection systems of ALWRs employ a voting scheme (two-out-of-four) similar to present-day (analog) implementations. The essential difference, however, is that the voting will be performed in software rather than in hardware and will in some cases involve software data communication between the divisions. The possibility of a processor waiting indefinitely for information from another division, or erroneous data being communicated to the other divisions without being "noticed," may be the failure modes that are significantly different from present-day trip systems.

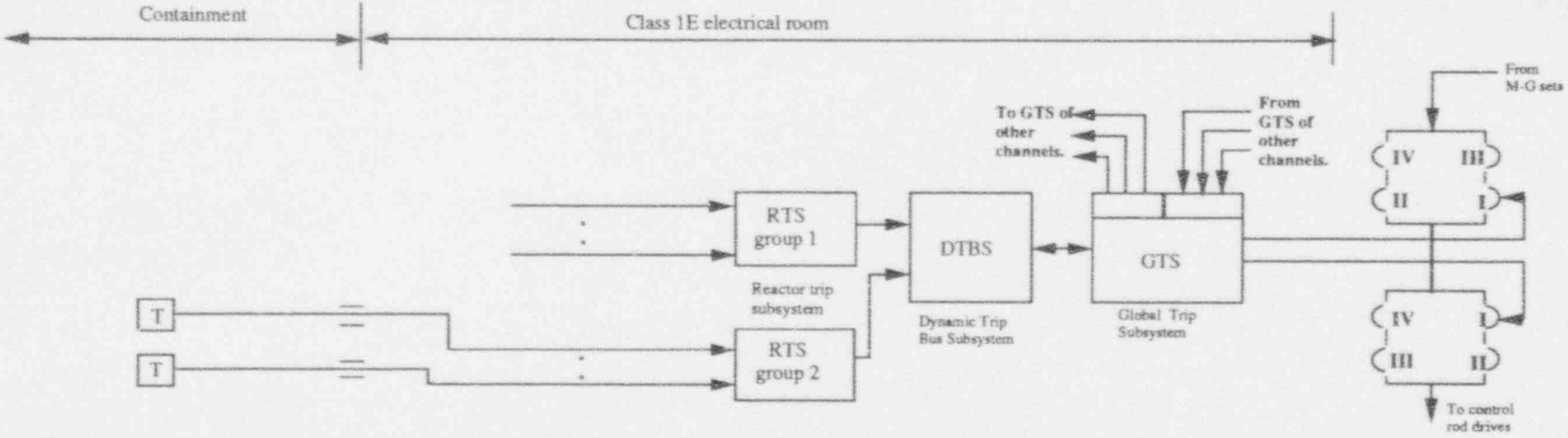
The ABWR design in which multiplexed protection system process variables are sent to the SSLC cabinets over an FDDI network probably constitutes the most significant design difference among the trip systems studied. Here again, transmission of corrupted data to the SSLC, or complete loss of signal due to either an RMU or the fiber media, may constitute failure modes that may be significantly different from present-day, hardwired systems. However, the token ring access method used by the FDDI network should make the ring deterministic and predictable. The choice of optical fiber eliminates the network's potential susceptibility to radiated noise from high-voltage conductors, high-frequency motor control drives, and transient pulses created by switching devices. This no: withstanding, the optical transmitting and receiving components will still be "weak links," and their susceptibility to EMI/RFI needs to be addressed.

3.3 Impact of Environmental Stressors on Protection System Components of ALWRs

In microprocessor-based protection systems, many of the functions previously performed by discrete analog components are performed in software. As shown in the previous section, the monitored trip parameters for each channel will in some cases be hardwired to multiplexers local to protection system cabinets for subsequent local signal conversion and processing. Others will be connected to remote multiplexers for subsequent transmission of the digitized data over data highways to the protection system cabinets. While the actual process variables to be used in proposed ALWRs are not an objective in this study, the flow channel in Figure 2.6 has been used as a basis to develop an environmental and aging data template for a protection channel in an ALWR. Note that the diagram in Figure 2.6 refers to identifiable analog components in the "path" of a (flow) process variable monitored for a protection system function. In microprocessor-based systems, however, this identification of individual components through trip bistable circuitry is no longer meaningful after the multiplexer(s), since a single microprocessor may now perform multiple functions. Thus, Figures 3.4 to 3.6 show environmental, functional, and aging data templates for *protection channels* fo: the AP600 by Westinghouse, the System 80$^+$ by ABB Combustion Engineering, and the ABWR by General Electric. The following discussion relates to Figures 3.4 to 3.6. Channel components in ALWRs are identified. In addition, environmental conditions and aging stressors to which major components in ALWR protection channels are subjected are compared to environmental conditions and stressors in present-day nuclear power plants.

3.3.1 Transmitters

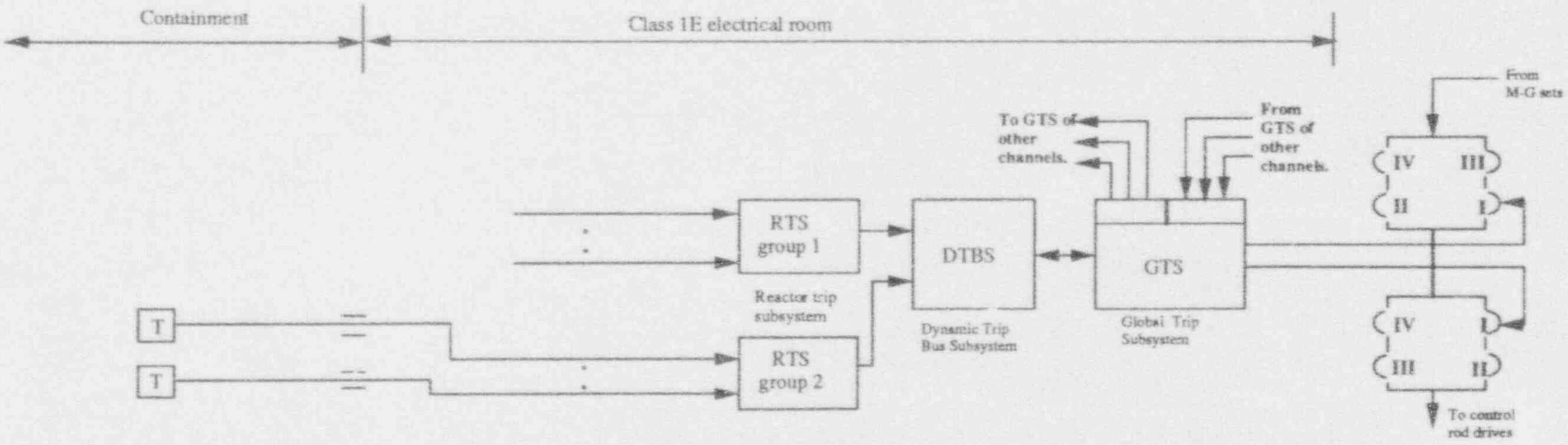
Discussions with ALWR system designers indicate that conventional analog transmitters will be used in ALWR designs and that environmental conditions in containment (e.g., temperature, humidity, and radiation) are not likely to be significantly different from those in existing nuclear plants. This observation may also apply to EMI and RFI sources to which instrumentation within containment may be subjected. Under normal plant operating conditions, transmitters are subject to aging stressors from temperature, moisture, radiation, and vibration, with temperature being the dominant stressor in most cases.[12] However, transmitters also may be subjected to aging stressors from testing and maintenance practices, the monitored process, and power supply variations. Humidity



	Transmitters	Class 1E electrical penetration rooms and cables (Transmitters are hardwired to integrated protection cabinet)	Microprocessor-based boards performing trip functions	Switchgear
Functions performed in software	None		Multiplexer scanning, sample-and-hold functions, digital data acqusition Digital signal conditioning and filtering, calibration and scaling Channel trip calculations	None
Radiation	~ 4 × 10^4 rad over 20 years	<4 × 10^2 rad over 40- year plant life*		
Ambient temperature	Average temperature* in containment: ~120° F Average transmitter operating limits: -40° to 240° F	~65-75°F ambient in Class 1E electrical room Design limits for instrumentation: Normal operating limits: 41 to 104° F, 5 to 95% relative humidity Abnormal operating limits: 40 to 120° F, 5 to 95% relative humidity (non-condensing)**		
EMI/RFI	Operate normally around sources of radio frequency from ~30 MHz to 500 MHz and field intensity of 20 V/m	Protection system is reported to operate normally around sources of radio frequency from 20 MHz to 500 MHz and field intensity of 10 V/m. These data were obtained from interviews with ALWR manufacturers. Test verification sources were not available.		
Interfaces	sensing lines, piping, junction boxes, seals	AC & DC power supplies, interlocks, and bypass modules		
Stressors	Temperature, radiation, moisture, vibration, maintenance & installation handling, environmental cycles	Maintenance/testing cycles, elevated temperatures inside cabinet, electromagnetic interference. Smoke can adversely affect electronic equipment far removed from the source of the smoke or fire.		

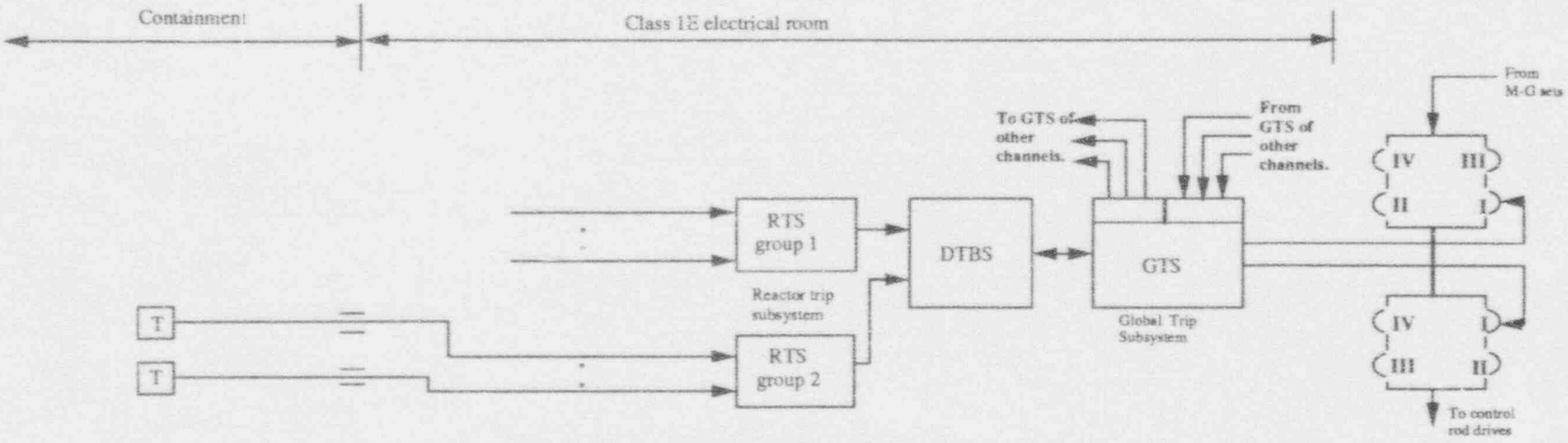
* Estimated. ** Abnormal conditions are expected to exist for a time period of less than or equal to 12 hours.

Figure 3.4 Environmental, functional, and aging data template for the AP600



	Transmitters	Class 1E electrical penetration rooms and cables (Transmitters are hardwired to integrated protection cabinet)	Microprocessor-based boards performing trip functions	Switchgear
Protection against the environment	Nuclear qualified transmitters and cables		Room is reported to have smoke detectors. 8 to 10 temperature monitors provided in each cabinet. Two Class 1E electrical rooms served by a separate HVAC system via a common ductwork (i.e., two HVAC systems for all four integrated protection cabinets). In case of fire, each HVAC system can be manually placed in a purge mode to remove smoke to the plant vent.	Nuclear qualified components
Signal type	Pressure to current transduction. 4 to 20 mA current loop derived from power supply in protection cabinet.		Current to voltage conversion, then conversion to logic level. Digital bit patterns in 5 volt logic.	High voltage/current level translation
Electronics implementation technology	Discrete silicon semiconductors		N-channel metal oxide semiconductor (NMOS) and complementary metal oxide semiconductor (CMOS) circuitry implemented in Large Scale Integration (LSI) and Very Large Scale Integration (VLSI) chips	Solid state circuitry, electromechanical components.
Communication	Point-to-point analog signals		RS-232 datalinks (19.2 kilobits/s) are used for most internal communications. RS-422A datalinks (64 kbits/s) used in some cases. Parallel I/O is performed using IEEE Std. 796 bus cards when appropriate Interchannel communication is performed via fiber optic datalinks	Point-to-point analog signals
Human interfaces	Periodic maintenance and calibration performed on transmitters		Automatic tester subsystem can be used to functionally test a safety channel, from input to output. This must be manually enabled through a keyswitch. Parallel interfaces are provided to connect to an external printer. Human-machine interface to manual testing functions is via a personal computer. Specific tests can be selected from on-screen menus	Automatic testing can be performed to trip actuation. Manual testing may also be performed.

Figure 3.4 (continued)

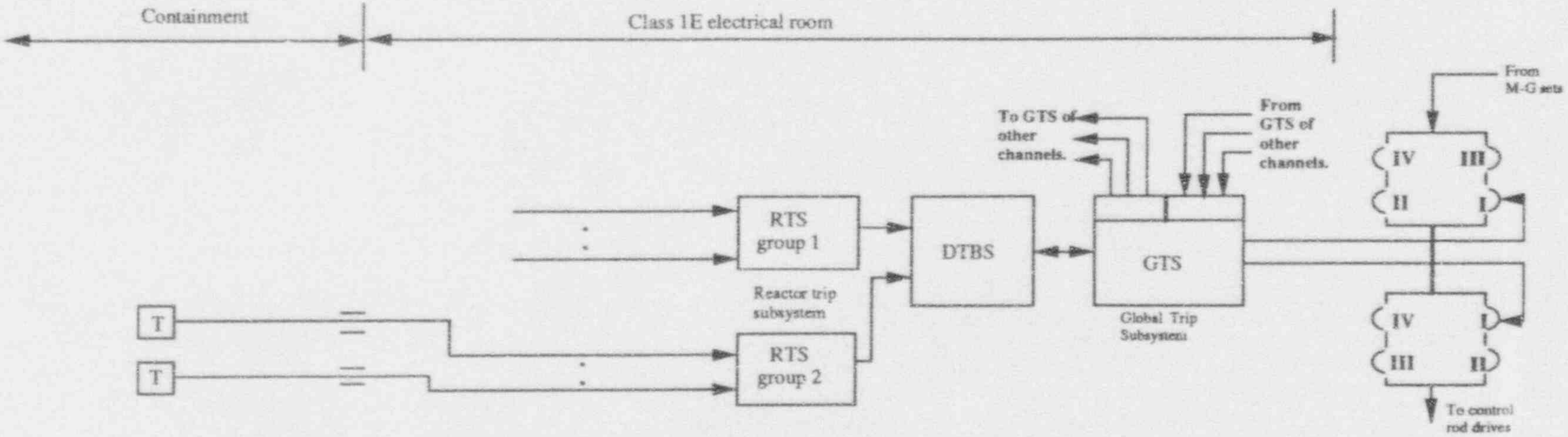


	Transmitters	Class 1E electrical penetration rooms and cables (Transmitters are hardwired to integrated protection cabinet)	Microprocessor-based boards performing trip functions	Switchgear
Materials	Transmitters will be similar to those found in present-day power plants. MATERIALS IN PRESSURE TRANSMITTERS USING RESONANT WIRE TECNOLOGY[a] : Housing: Copper aluminum alloy with epoxy paint, or cast austenitic stainless steel. Process wetted parts: Cobalt-nickel-chrome alloy, 316 stainless steel. Fill fluid: Silicone oil. Isolation diaphragm: Cobalt-nickel-chrome alloy. Housing seal: Ethylene propylene*. Electronic components: Seals and insulating materials used on electronic components*. Circuit boards: Epoxy glass laminate*. MATERIALS SUBJECT TO AGING DEGRADATION IN CABLES: Insulation (cross linked polyethylene). Sheath (Neoprene). Outer jacket (Galvanized steel).		Optical fiber datalinks will be used in the interfaces between protection, control, and engineered safety feature actuations. Will also be used in the interfaces between subsystems. Silica core fibers will be used. Data on optical fiber type used here could not be ascertained. Choice of fiber type and coating are important factors that can affect fiber performance in power plant environments. Seals and insulating materials used on electronic components, encapsulating materials for electronic components, and solder joints are all subject to aging degradation.	

[a] Materials subject to aging degradation are representative of other transmitter types.

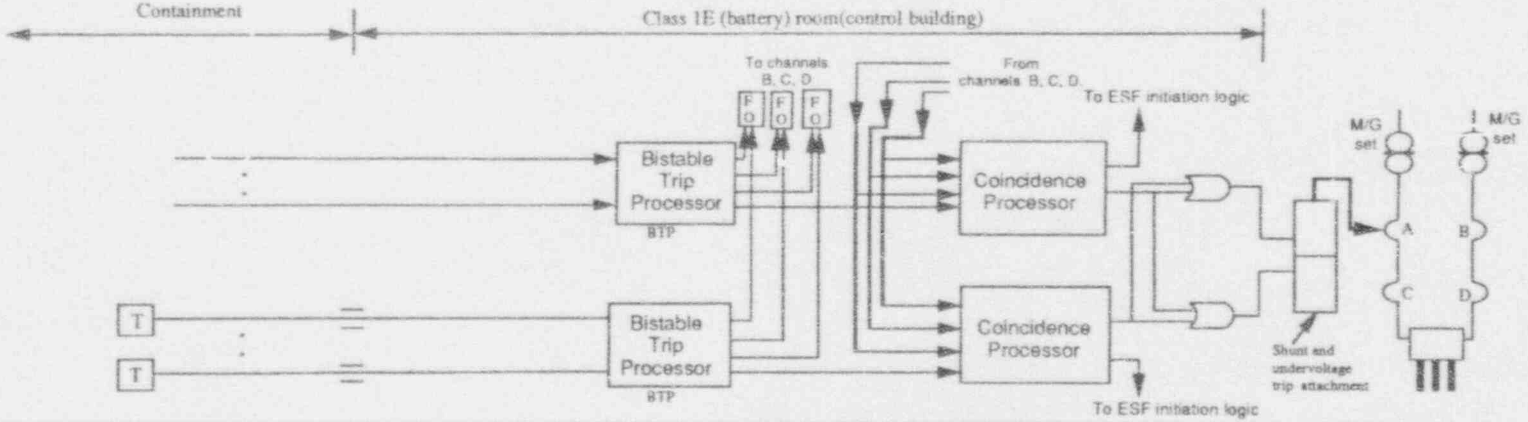
*Materials subject to aging degradation.

Figure 3.4 (continued)



	Transmitters	Class 1E electrical penetration rooms and cables (Transmitters are hardwired to integrated protection cabinet)	Microprocessor-based boards performing trip functions	Switchgear
Channel independence	Transmitters are not shared among channels. Those shared in one channel for protection and control employ electrical isolation. System uses separate, independent processors to perform trip functions, communication functions, and surveillance testing functions.			Two circuit breakers associated with each channel. Breaker cells have steel barriers to completely encapsulate a breaker to provide physical separation between breakers in different divisions.
Diversity	Two sets of variables are monitored (in the same channel), using two separate processors. Hardware diversity is not used to the extent that different microprocessor hardware is used in different channels. Software diversity is not used.			
Control of access	Each key to a protection system cabinet is different. Open protection system cabinet is indicated in the control room. All protection system "software" is in firmware. Administrative controls will reportedly be in place to ensure supervised access to the protection cabinets.			
Capability for test and calibration	Automatic tester subsystem is used to automatically test protection channel while the latter is bypassed. Test involves injecting simulated inputs and monitoring the outputs to verify results. Tester subsystem also monitors failure and diagnostic information from the protection subsystems in that channel during normal operation. The level of software V&V for the tester subsystem is reportedly equivalent to the protection system software.			

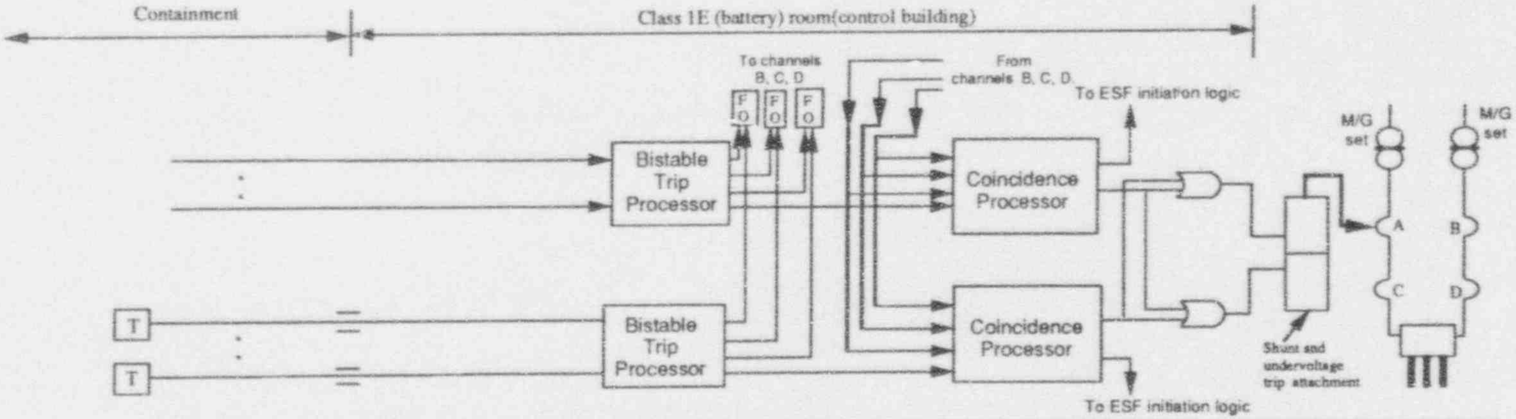
Figure 3.4 (continued)



	Transmitters	Penetration room and cables. (Transmitters are hardwired to plant protection system cabinet).	Bistable trip processors generate trips based on the digitized input value exceeding a digitized setpoint	Processors evaluate the local coincidence logic based on the state of the four *like* trip signals and respective bypasses.	Switchgear
Functions performed in software	None		Multiplexer scanning, sample-and-hold functions, digital data acquisition Channel trip calculations. Process signals provided to the BTP through conventional (analog) signal conditioning equipment.		None
Radiatio.ı	$< 3 \times 10^6$ rads gamma (60 yr total dose).	Total integrated dose over 60 yr: $<= 10^3$ rads gamma.			
Ambient temperature	60° - 110°F Average transmitter operating limits: -40° to 240°F	~77°F ambient in battery room. Design limits for instrumentation: (Not Available)			
EMI/RFI	Operate normally around sources of radio frequency from ~30 MHz to 500 MHz and field intensity of 20 V/m	Mil Standard 462 is used for EMI testing. Particular tests used are CS01, CS02, CS06, RS03, and RS04.			
Interfaces	sensing lines, piping, junction boxes, seals	AC & DC power supplies, interlocks, and bypass modules			
Stressors	Temperature, radiation, moisture, vibration, maintenance & installation handling, environmental cycles	Maintenance/testing cycles, elevated temperatures inside cabinet, electromagnetic interference. Smoke can adversely affect electronic equipment far removed from the source of the smoke or fire.			

F.O.: Isolation via optical fiber.

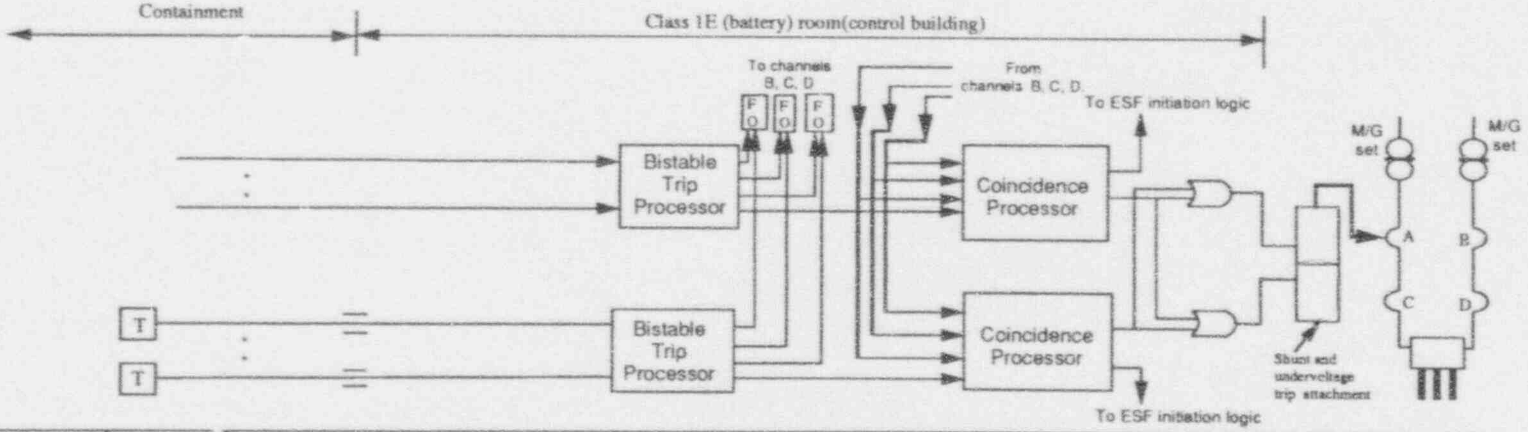
Figure 3.5 Environmental, functional, and aging data template for the System 80+



	Transmitters	Penetration room and cables. (Transmitters are hardwired to plant protection system cabinet).	Microprocessor-based boards performing trip functions	Switchgear
Protection against the environment	Nuclear qualified transmitters and cables		Each equipment room in which the PPS is located will have smoke and temperature sensing as part of the HVAC design. Ventilation systems are division specific so that fire or smoke in an area containing a safety related division of equipment cannot migrate through the ventilation ducts to an area containing the redundant division of safety related equipment.	Nuclear qualified components
Signal type	Process to current transduction. 4 to 20 mA current loop derived from power supply in protection cabinet.		Current to voltage conversion, then conversion to logic level. Digital bit patterns in 5 volt logic.	High voltage/current level translation
Electronics implementation technology	Discrete silicon semi-conductors	NA	N-channel metal oxide semiconductor (NMOS) and complementary metal oxide semiconductor (CMOS) circuitry implemented in Large Scale Integration (LSI) and Very Large Scale Integration (VLSI) chips	Solid state circuitry, electromechanical components.
Communication	Point-to-point analog signals		Communication between bistable processors in one channel and the local coincidence processors in the other three PPS channels is via proprietary, fiber optic datalinks. Communication between testing processors (one in each channel) will be by fiber optic ethernet datalinks.	Point-to-point analog signals
Human interfaces	Periodic maintenance and calibration performed on transmitters		Manufacturer indicates that *automatic test network (ATN)* capable of performing tests during reactor operation is provided. Operation of the ATN may be verified locally at the PPS cabinet by requesting test results data. Testing by the ATN reportedly does not involve any active test signals. Instead, all PPS data are read into *Interface and Test Processors* (ITPs). The data are then analyzed to determine if the protection system is operating properly.	Devices that are not in the PPS, such as the reactor switchgear, are tested manually.

PPS - Plant Protection System.
NA - Not applicable.
F.O.: Isolation via optical fiber.

Figure 3.5 (continued)



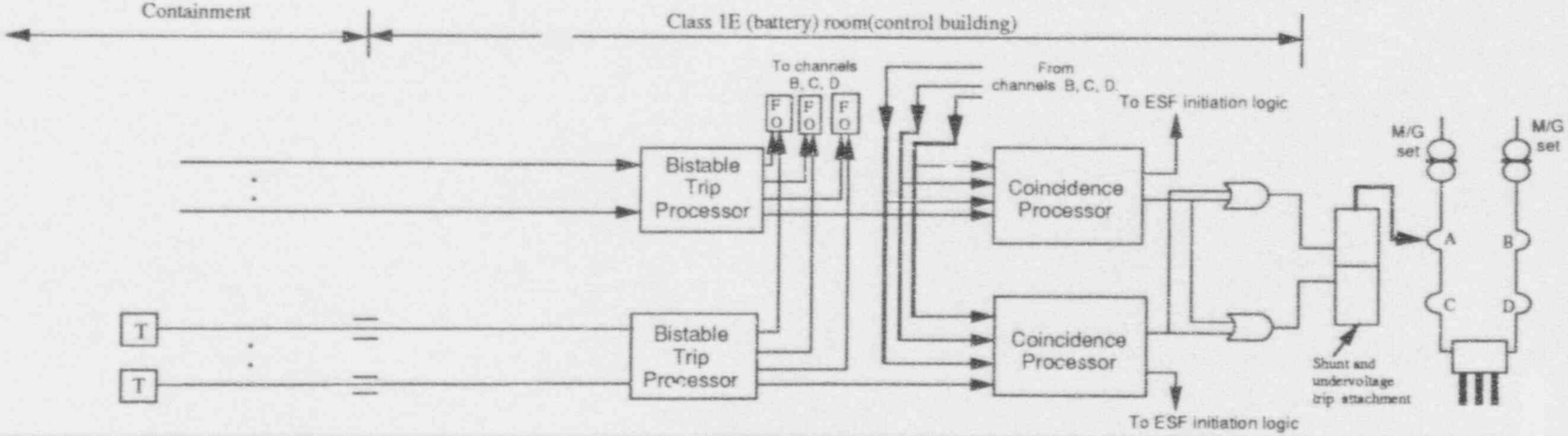
	Transmitters	Penetration room and cables. (Transmitters are hardwired to plant protection system cabinet).	Microprocessor-based boards performing trip functions	Switchgear
Materials	Transmitters will be identical to those found in present-day power plants. MATERIALS IN CAPACITANCE TYPE PRESSURE TRANSDUCERS:[a] Housing: Aluminum with epoxy polyester paint or 316 stainless steel. Fill fluid: Silicon oil. Isolation diaphragm: 316 stainless steel. Housing seal: Ethylene propylene.* Electronic components: Seals and insulating materials used on electronic components.* Circuit boards: Epoxy glass laminate.*		Optical fibers will be used for interchannel communication. The following specifications are typical of type(s) to be used: FIBER MATERIAL: NA SECONDARY BUFFER: Polyester elastometer. STRENGTH MEMBER: Aramid yarn. OUTER JACKET: Flame retardant chlorinated polyethylene. FLAMMABILITY: Tested to IEEE 383-1974 OPERATING LIMITS: -20° C to 80° C (operating) 5 to 100% (relative humidity).	
	MATERIALS SUBJECT TO AGING DEGRADATION IN CABLES: Insulation (cross linked polyethylene). Sheath (Neoprene). Outer jacket (Galvanized steel).		Seals and insulating materials used on electronic components, encapsulating materials for electronic components, and solder joints are all subject to aging degradation.	

[a] Materials subject to aging degradation are representative of other transmitter types.

*Materials subject to aging degradation.

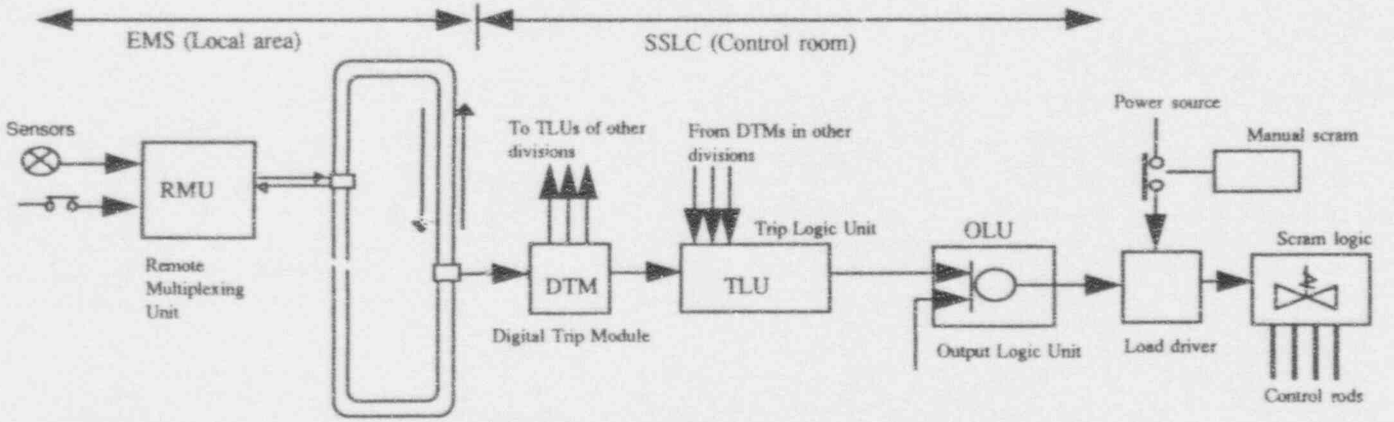
NA - Not available.

Figure 3.5 (continued)



	Transmitters	Penetration room and cables. (Transmitters are hardwired to plant protection system cabinet).	Microprocessor-based boards performing trip functions	Switchgear
Channel independence	Protection system sensors are generally separate from control system sensors. Where control and protection systems have identical sensor input requirements, redundant Class 1E sensors that are used independently by each channel of the protection system may in cases also be used by the control system. In such cases fiber optic interfaces are used to ensure electrical independence. Separate processors are used for performing trip functions and communication functions.			Switchgear breakers are located in the electrical equipment rooms which are geographically separated from each other.
Diversity	Two sets of trip variables are monitored (in the same channel), using two separate bistable processors. Hardware diversity is not used to the extent that different processor hardware is used in different protection channels. Diversity of software within the plant protection system is not used. A defense-in-depth approach is used to protect against common mode software errors.			
Control of access	Each protective system cabinet is located within one of the four locked electrical equipment rooms. Each cabinet is also locked to prevent unauthorized entry. An open cabinet door is automatically indicated to the operator.			
Capability for test and calibration	Automatic Test Network (ATN) is used to monitor/test major portions of the RPS, from sensor input through the protective system to the trip circuit breakers. Analog-to-Digital conversion accuracy is checked by making a channel-to-channel comparison of input signals to detect any signal discrepancies. Monitoring tasks performed by the ATN are reported to be passive in nature: no active test signals are applied to the protection system. Electromechanical devices, as well as devices not within the PPS cabinets, are tested manually.			

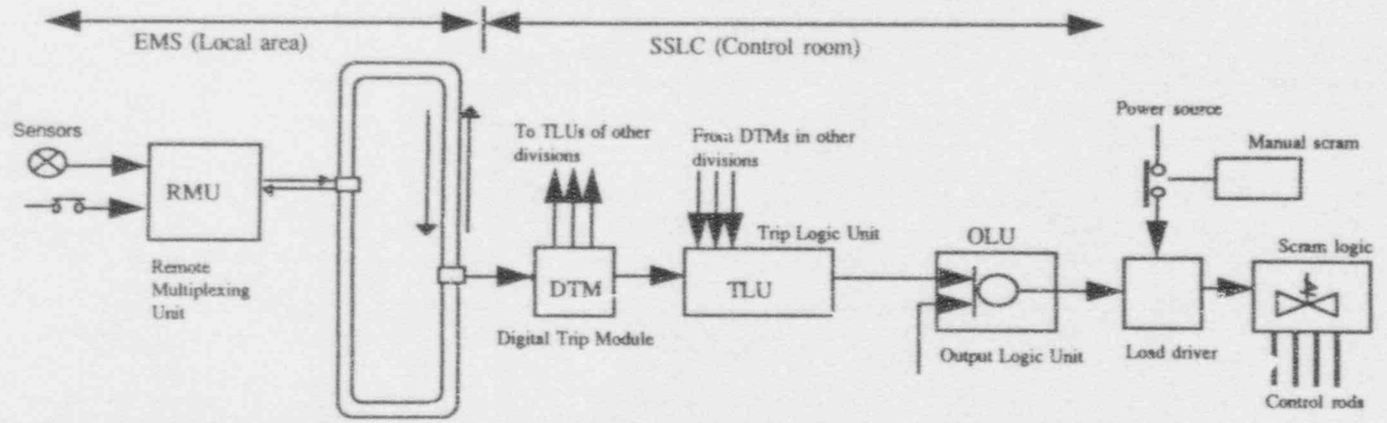
Figure 3.5 (continued)



	Shared sensors	Electrical penetrations and cables. Transmitters are hardwired to RMU.	FDDI ring.	Microprocessor-based subsystems performing trip functions.	Solid state logic
Functions performed in software	Signal conditioning, signal identification, error checking, data synchronization.			Set point comparisons, voting, communication functions.	None
Radiation	< 3 x 10^6 rad gamma (60 yr total dose).		Total integrated dose over 60 yr: <= 10^3 rads gamma.		
Ambient temperature	Max. temp. in IRR[a] 104°F. Avg. transmitter operating limits: -40 to 240°F.[b]		Ambient temperature typical of reactor building clean area with electronic equipment: 65° to 85°F.		
EMI/RFI	Nuclear qualified transmitters typically operate normally around sources of radio frequencies from ~ 30 to 500MHz and field intensity of 20 V/m.		Information on EMI/RFI test limits and acceptance criteria for SSLC not available.		
Interfaces	Sensing lines, piping, junction boxes, AC & DC power supplies, interlocks, and bypass modules; optical fiber communication interfaces, Class 1E isolation devices.				
Stressors	Temperature, radiation, moisture, vibration, maintenance & installation handling, environmental cycles	Maintenance and installation handling		Maintenance/testing cycles, elevated temperature inside cabinet,, EMI/RFI; smoke can adversely affect electronic equipment far removed from the source ot the smoke or fire.	

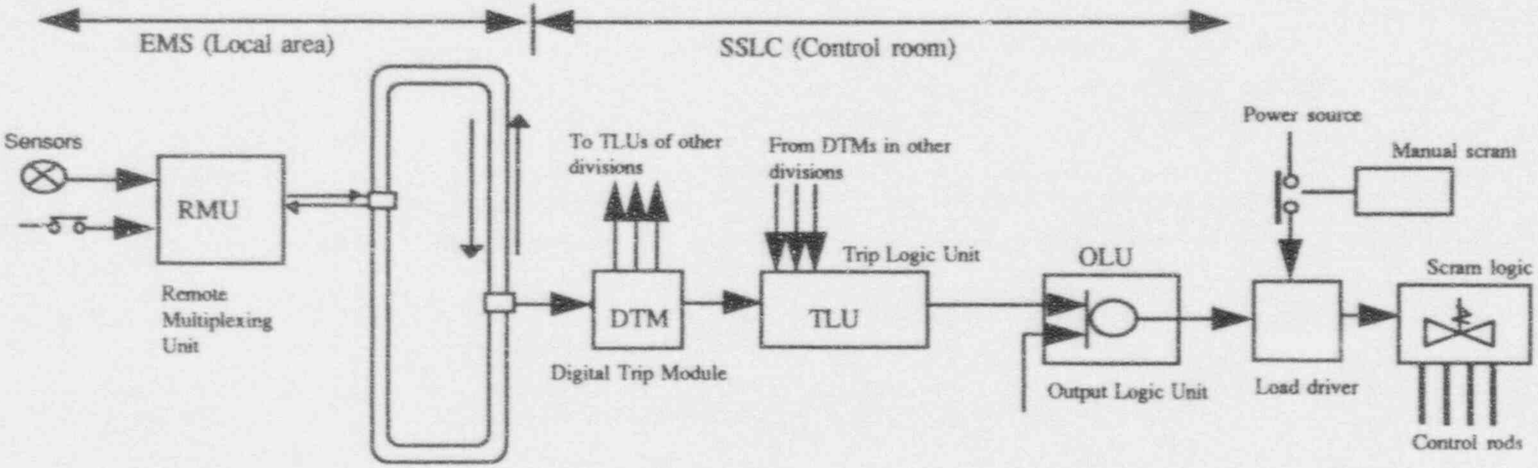
[a] IRR = Instrument rack room.
[b] Operation close to these limits will not be with normal accuracy.

Figure 3.6 Environmental, functional, and aging data template for the ABWR



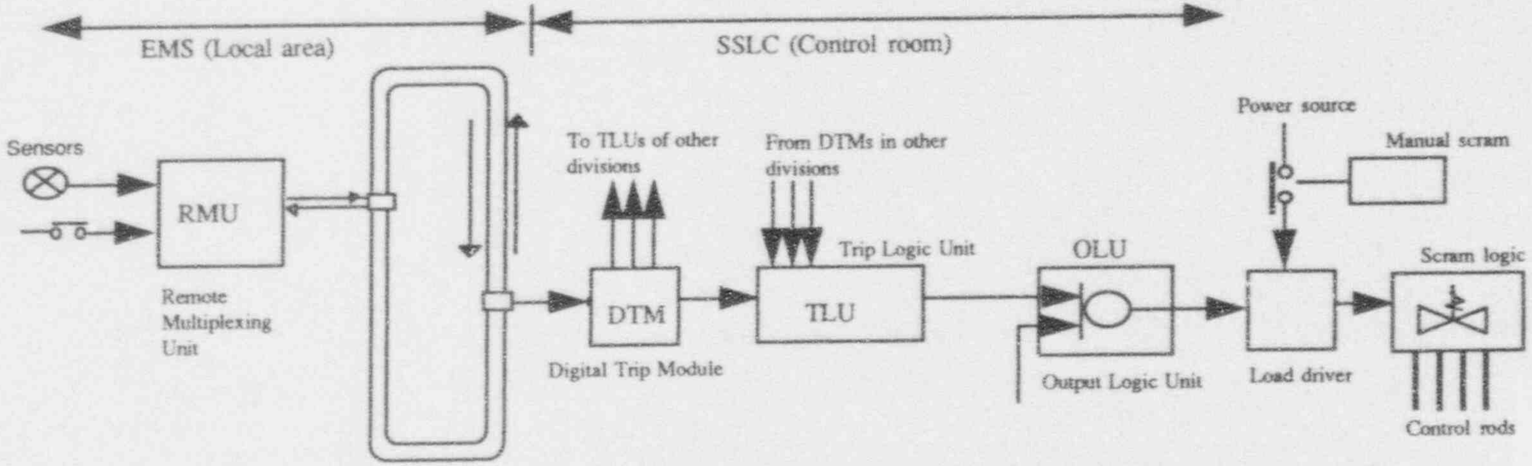
	Shared sensors	Electrical penetrations and cables. Transmitters are hardwired to RMU.	FDDI ring.	Microprocessor-based subsystems performing trip functions.	Solid state logic	
Protection against the environment	Nuclear qualified transmitters and cables are used. Portions of the HVAC system that penetrate through the safety envelope are Class 1E. Duct penetrations through the safety envelope include redundant, Class 1E powered isolation dampers to maintain integrity of the safety envelope during accidents.			Clean area ventilation system maintains air pressures higher than atmospheric to minimize infiltration of outside air. Redundant smoke exhaust fans operate only when needed for smoke removal from affected areas.		Nuclear-qualified components.
Signal type	Current/ON-OFF state - to - voltage conversion. Digital bit pattern in 5V logic. Electrical-to-optical conversion.		Optical signals.	Optical-to-electrical conversion. Digital bit patterns in 5V logic.		High voltage/current level translation.
Electronics implementation technology	Discrete silicon semiconducters.			NMOS and CMOS circuitry implemented in LSI and VLSI chips		Solid state circuitry; electromechanical components.
Communication	Point-point signals.	Multiplexed signals.		Communication among SSLCs in other divisions is via optical serial datalinks		Point-to-point analog signals.
Human interfaces	Periodic maintenance and calibration performed on transmitters	Multiplexing and network diagnostic information not available.		Capability for periodic maintenance is provided.		

Figure 3.6 (continued)



Shared sensors	Electrical penetrations and cables. Transmitters are hardwired to RMU.	FDDI ring.	Microprocessor-based subsystems performing trip functions.	Solid state logic
Materials	TYPICAL TRANSMITTER COMPONENTS SUBJECT TO DEGRADATION: **Housing seal:** ethylene propylene. **Electronics:** Seals and insulating materials used on electronic components. **Circuit boards:** epoxy glass laminate. MATERIALS SUBJECT TO AGING DEGRADATION IN CABLES: Insulation [e.g., cross linked polyethylene (XLPE)]. Sheath (e.g., neoprene)		MATERIAL SUBJECT TO AGING DEGRADATION IN OPTICAL FIBER CABLES **cable jacket materials:** polyethylene, polyurethane, thermoplastic elastometer (TPE).	

Figure 3.6 (continued)



Shared sensors	Electrical penetrations and cables. Transmitters are hardwired to RMU.	FDDI ring.	Microprocessor-based subsystems performing trip functions.	Solid state logic	
Channel independence	Channel independence is maintained from reactor protection system sensors through trip logic equipment. Sensor wiring associated with one division will not be routed with, or in close proximity to, any wiring or cabling associated with a redundant division. Trip channel data sent from one division to other divisions is performed through Class 1E isolation devices. Three-four fire barriers, isolation devices, and physical separation used to achieve independence between Class 1E equipment, devices, and cables.				Circuitry from the actuation devices to the solenoids of the scram pilot valves of the HCUs will be run in grounded steel conduits. Separate steel conduits will be provided for each of four scram groups.
Control of access	Each key to a protection system cabinet is different. Open protection system cabinet is indicated in the control room. All protection system "software" are in firmware. Administrative controls will be in place to ensure supervised access to the protection cabinets.				
Capability for test and calibration	RMU modules have a self-check feature that will detect malfunctions and alarm in control room.		Essentially, each card in the SSLC is a microcontroller module with self testing capability. The self tests include checksum and cyclic redundancy checks on all transmitted and received data to and from each microcontroller card. Periodic, operator-initiated, automatic surveillance testing can also be perfomed using a dedicated diagnostic instrument.		

Figure 3.6 (continued)

levels under normal plant conditions should not pose a problem for nuclear qualified transmitters since such transmitters are sealed for DBAs such as main steam line breaks.

Presently, most transmitters for use within containment have a qualified life of 10 to 40 years, depending on type, materials of construction, and other factors. For example, strain gauge transmitters typically have a qualified life of 40 years, while a differential capacitance transmitter may be qualified for only 10 years. Seals and gaskets for transmitters typically have a much lower qualified life (e.g., 4 years).[12,13] The performance and lifetime of transmitters are expected to be the same for ALWRs as for conventional reactors.

Since I&C systems for the next generation of nuclear power plants are still evolving, it is possible that some form of "smart" transmitter technology could still be used in future plants. A significant factor that precludes the use of present-day smart transmitters in containment environments is the susceptibility of their complementary metal-oxide semiconductor (CMOS) electronics to damage at modest radiation levels. CMOS technology is used because the power consumption requirements of standard two-wire instrument loops (Figure 3.7) limit the total current to a range of 4 to 20 mA. In a smart transmitter, microprocessor-based electronics replace the analog electronics (marked as *electronic card*) found in conventional transmitters. This means that the total power consumption of the transmitter electronics (including microprocessor, memory, etc.) must have a total internal current load of a little less than 4 mA to be able to regulate the loop current down to this value. At present, CMOS is one of the few electronic technologies having power requirements low enough to make this possible.

Integral dose levels inside PWR containment over 20 years may be on the order of 5×10^4 rad or more, and under such radiation conditions, commercial CMOS circuitry is susceptible to damage/degradation. Some tests show that such transmitters fail at a total gamma dose of between 2.5×10^3 and 1×10^4 rad.[14] Some tests also indicate that dose *rate* may be a more serious factor than integral dose. This suggests that a burst of radiation over a short period due to an accident condition may render affected smart transmitters useless.

Despite the present limitations, work is progressing on the development of several technologies with low power capabilities, such as CMOS silicon-on-insulator, that can withstand a total radiation dose of several tens of megarads (Si).[18-20] Use of these technologies will enable the advantages of smart transmitters to be exploited for the nuclear power plant containment environment. These advantages include (1) capability for remote calibration, (2) capability for remote verification of calibration, (3) capability for remote range changes, (4) automatic diagnostics, and (5) little cost difference between smart and conventional transmitters.

Apart from improvements in transmitter electronics, new pressure sensing technologies are also being evaluated to improve pressure sensor performance.[21] Present-day pressure transmitters are subject to certain failure modes that are unacceptable, especially in safety-related systems of nuclear power plants. An example is the loss of oil from an oil-filled transmitter.[22] This type of failure significantly increases the transmitter's response time and may also limit its dynamic range. These effects, however, are not usually observable during steady-state operation. Technologies that are currently being investigated for the development of improved transmitters include fiber-optic, mechanical tuning fork resonance frequency, and quartz pressure sensor technologies.[22]

From the review of proposed transmitters for ALWRs and trends in transmitter technology, it is the opinion of the authors that no significant changes need be made in qualification guidelines with regard to transmitters proposed for ALWRs.

3.3.2 Cables and Fiber-Optic Data Links

As with transmitters, cable types and connections within ALWR containments are not likely to be markedly different from those used in present-day reactors. Stressors that are known to promote cable degradation include temperature, radiation, and moisture. Cable materials experience ambient temperature and radiation for long periods of time. Under accident conditions, however, they may be subjected to much higher radiation and temperature transients, and this is taken into consideration in their design and qualification. Electrical cables are normally qualified for 40 years, and their performance and lifetime can be expected to be the same in ALWRs as in conventional reactors.

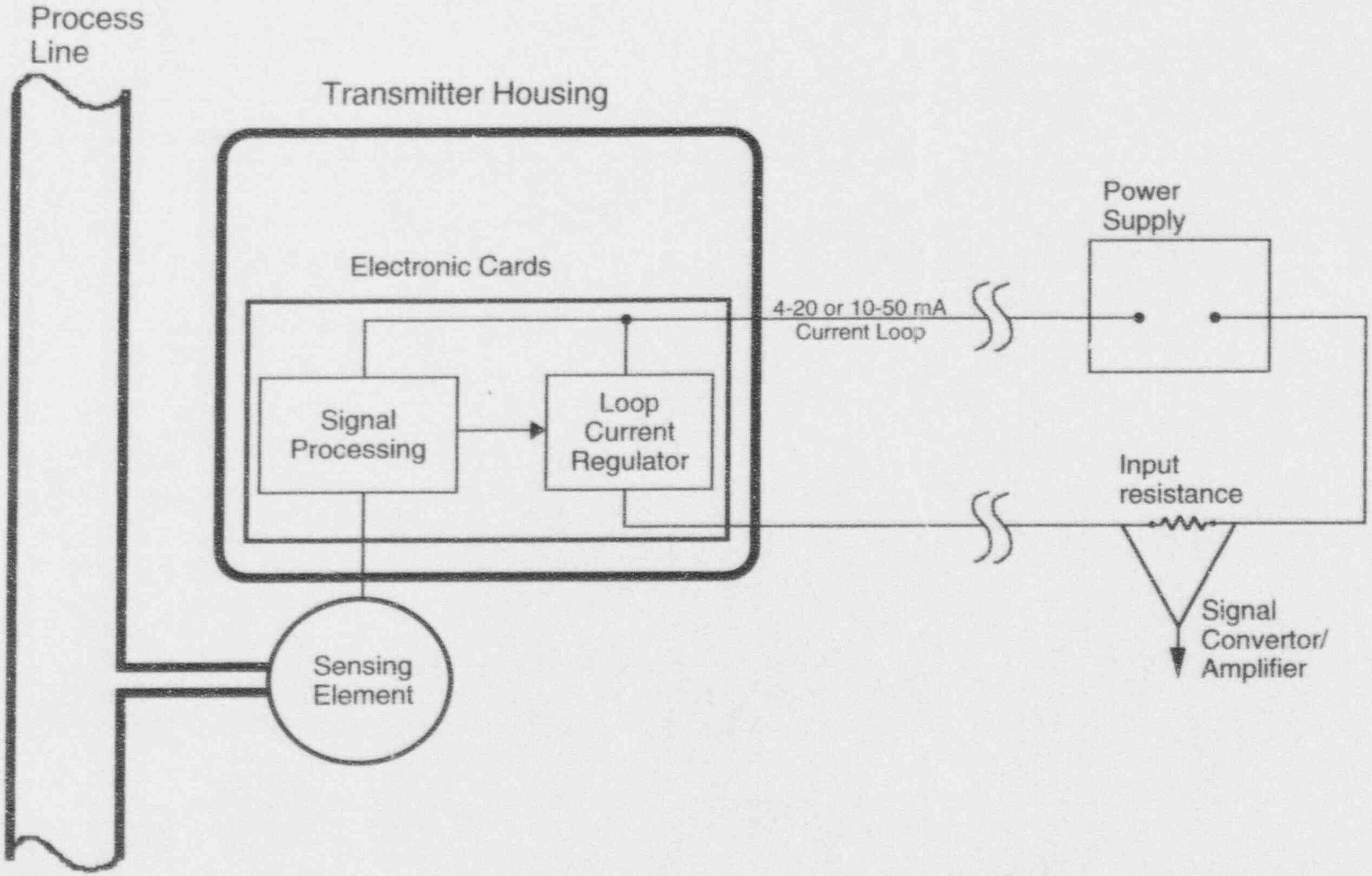


Figure 3.7 Standard two-wire transmitter loop

As far as the protection channels of ALWRs are concerned, optical fiber data links will be used for interchannel communication and, in some cases, between subsystems within a channel. Fiber-optic cables also will be heavily employed in the (distributed) control system and in the interface between the trip system and ESF systems. Protection system cabinets are typically located in an area with lower radiation levels than containment. Temperature and humidity levels are also less harsh. However, since ALWRs are subject to design changes and requirements, it is conceivable that eventually fiber-optic cables may be used in environments that are less benign than have so far been ascertained. In any case, it is important that long-term mechanical and optical degradation mechanisms in optical fibers be considered. Several environmental variables, or their synergistic effects, can result in aging and increased failure rates for certain fiber-optic cables. These include high relative humidity, high temperatures, high pH,[23] excessive installation strains, inadequate cable designs, inappropriate choice of fiber coatings,[24] low initial fiber strength, and residual cable installation stresses.[25] In addition, little work has been done on the *long term* radiation effects on optical fiber, fiber connections, optical sources, and detectors.

We attempted to probe further the qualification of optical fibers and systems for nuclear power plant applications by examining the failure modes and degradation mechanisms of optical fiber cables and transmission components. The objective of this review is twofold: (1) to qualitatively assess how environmental stressors in nuclear power plants are likely to affect the performance of fiber-optic cables at their proposed locations and (2) to use the resulting knowledge as a basis for developing a qualification methodology for "new" technologies in nuclear power plants.

Optical Fiber Communication Systems

An optical fiber transmission system consists of three major subsystems:

1. E-to-O conversion of electrical signals to optical signals, typically by means of a light-emitting diode (LED) or a semiconductor laser diode. The emitter is typically embedded in and driven by the *transmitter* or *transceiver* electronics. The performance of the emitter will impact the entire system; in particular, a marked decrease in emitter output power will result in an unacceptably high bit error rate.

2. Light transmission via fiber-optic cables, which typically consist of glass or plastic fibers having suitable cladding material, a buffer layer (either acrylic or polyamide) a strength member (such as Kevlar or steel), and an outer jacket. A dielectric cable is formed when the strength member is made of a dielectric material (e.g., Kevlar or fiberglass) *and* both the fiber and strength member are enveloped in a dielectric sheath or outer jacket. Nondielectric cables have a metallic strength member; they are typically used in areas of extreme adverse conditions. Unlike a nondielectric cable, a dielectric cable is virtually immune to EMI.

3. O-to-E conversion of the optical signals to electrical signals, typically by means of a PIN (positive-intrinsic-negative) photodetector or an avalanche photodetector (APD). As with the emitter, the detector is typically housed with additional circuitry in a single package as a *receiver* or with an emitter and supporting electronics in one package as a *transceiver*.

A number of advantages associated with the use of optical fiber transmission, such as the immunity of the fibers to EMI/RFI, have been significant motivating factors in their application to the nuclear power plant environment. However, the transmitter and receiver components are quite sensitive to EMI. Also, the cable itself, as well as the transmitter and receiver, is subject to age-related degradation and failure modes that are different from those of conventional copper transmission systems. The most significant of these failure mechanisms are listed in Tables 3.1 to 3.3 and are discussed in the following sections.

Table 3.1 Failure mechanisms of optical sources

Possible components	Mode of failure	Cause	Prevention methods
Light-emitting diodes (LEDs): (InGaAsP/InP; AlGaAs/GaAs; AlGaAs/Si)	Dark line defects; dark spot defects	Nonradiative recombination caused by impurities and crystal lattice defects in the material.	1. Choice of material. 2. Fabrication and wire bonding methods. 3. Quality control.
Solid-state laser devices: (AlGaAs/GaAs; InGaAsP/InP)	Dark spot defects	Contact degradation causes an increase in thermal resistance in heat sink/laser device interface. Resulting temperature rise causes an increase in leakage current in active region of device. Increase in leakage current contributes to nonradiative recombination.	Fabrication methods: application of a passivation layer helps reduce surface contamination and in-migration of atoms from contact deterioration (dark spot defects).
	Laser wearout	1. Increase in leakage current due to increase in ambient operating temperature results in a decrease in laser power at a given bias level. Threshold current must be increased to sustain same power level.	Decrease operating temperature and current density. Improve contact material compatibility.
		2. Photo-oxidation on facets due to extended high-threshold currents. Reduces reflectivity. Occurs most frequently when device is operated in high humidity/moist environments.	Fabrication techniques: typically, a thin coating of silicon dioxide (SiO_2), aluminum oxide (Al_2O_3), or silicon nitride (Si_3N_4) is applied.
		3. Lattice defects in material result in the formation of dark line defects over a large surface area of active device. Eventually causes optical output power to decrease.	1. Choice of material: (select one with low lattice defects). 2. Quality control: (helps in testing for quality materials).

Table 3.2 Failure mechanisms of optical fibers and connectors

Subsystem	Possible components	Mode of failure	Cause	Prevention methods
Fiber-optic cable	**Fiber material:** silica or plastic. **Secondary buffer:** polyester elastometer. **Strength member:** polymer (Kevlar), steel, or carbon fiber. **Outer jacket:** plastic sheath, flame retardant chlorinated polyethylene.	Signal attenuation in fiber.	Hydrogen migration into fiber due to: 1. diffusion into interstitial sites in the silica molecular structure and 2. chemical reaction of hydrogen with the glass constituents to form OH groups.	Design cables with materials that do not generate hydrogen.*
			Formation of microcracks due to: 1. bending radius of the cable; 2. cable handling during installation; and 3. differences in the thermal expansion coefficients of coating materials and fiber.	Bending and handling radius must be specified and inspected during installations. Use coating materials that can prevent/reduce shrinking, cracking, or swelling. Good cable handling practices.
			Optical losses due to ionization in the fiber from: 1. gamma radiation and 2. neutron radiation. Fiber may become temporarily opaque or may be permanently discolored.	Design to be radiation-hardened.†
		Fiber fracture	Stress corrosion or fatigue due to microcracks.	Residual tension should be less than 33% of the rated proof-tested tensile strength.
Connectors		Signal attenuation or complete signal loss.	Insertion loss due to angular misalignment, core misalignment, end separation, reflections, and preparation quality.	Various connector design techniques are used to reduce mating losses. In applying index-matching fluid, care should be taken to avoid dust and dirt.
			Aging of index-matching fluid due to: 1. changes in viscosity due to temperature stresses and 2. maintenance handling (mating/unmating over time).	

*The hydrogen may be generated from degradation of polymers in the cable. It can also be generated by galvanic action between two dissimilar metals or by the action of sea water on cable sheaths. However, these sources are negligible in control room environments in power plants.

†In noncontainment environments, optical loss due to radiation damage is negligible. Pure silica-core fibers are much more radiation resistant than plastic fibers or phosphorus-doped fibers.

Table 3.3 Failure mechanisms of optical receivers

Possible components	Mode of failure	Cause	Prevention methods
Technology: 1. PIN (positive-intrinsic-negative) photodetector 2. Avalanche photodetector (APD) **Material:** *PIN*: silicon, InGaAs, germanium *APD*: silicon, germanium	Increase in dark current (reverse current in the absence of incident radiation).	1. Thermally generated charge carriers (PIN photodiodes).	**System design technique:** 1. Choose detector with inherently low dark current. 2. Operate device at low environmental temperature.
		2. Thermal deterioration of the metal contacts (APD).	**Fabrication technique:** Thin layer of In or InGaAs grown onto active region.
	Possible electrical short circuits when device is operated above a relative humidity of 85%.	Electrochemical oxidation.	Use hermetically sealed devices if they are going to be operated in such environments.

Optical Sources

Of the two most frequently used optical sources mentioned above, LEDs have the advantages of low cost, high reliability, and good linearity; while laser diodes offer high output power level, conversion efficiency, bit-rate-modulation capability, and good mode stability of the emitted light.[26] However, the cost and reliability of laser diodes have improved over the last few years. Both component types are subject to either catastrophic failure (where the cessation of output power is abrupt and final) or gradual degradation over time. Gradual degradation usually results in a decrease in output power, which may be readjusted back to the desired level by increasing the current from the drive electronics. However, such compensation is effective only up to a point because the increased drive current can overheat the device, leading to catastrophic failure.

LEDs are subject to two degradation modes: rapid degradation due to formation of dark line defects (DLDs) and dark spot defects (DSDs) and slow degradation, in which the output power *decreases* as temperature or time *increases*. DLDs and DSDs are caused by impurities and crystal lattice defects in the material, which give rise to nonradiative recombination in the active region of the device. Slow degradation, which will occur even if there are no DLDs or DSDs, is considered to be a result of diffusion of impurities into the active region from the surrounding material and/or the in-migration of metal atoms from the contact materials once contact deterioration has started.[27]

Semiconductor laser diode degradation is a function of a number of parameters, including humidity, temperature, manufacturing techniques, and optical power density. The degradation typically manifests itself as an increase in *threshold current* (the minimum current necessary for the lasing action to be sustained). The root cause may be contact degradation, which causes an increase in the thermal resistance of the contact between the heat sink and the laser device. This, in turn, causes the junction temperature of the device to increase, resulting in an increase in threshold current. Another mechanism is facet oxidation, that is, staining of facets due to photo-oxidation. This degradation mechanism is accelerated when the device is operated in an environment with a high moisture or oxygen content.

With regard to radiation, tests performed with gamma rays[28] on InGaAsP LEDs operating at 1300 nm showed no significant degradation of parameters up to a total dose of 10^5 Gy. The output power decreased by 5% with an irradiation dose of 10^6 Gy, and it was estimated that the output power would decrease to 50% of its initial value at a total dose of 2×10^7 Gy. A study of the effect of neutron irradiation on LEDs[26,29] fabricated from strained-layer superlattice structures in the GaAs/GaAsP configuration showed no significant light output degradation at neutron fluences below 3×10^{14} n/cm^2.

Optical Fibers and Connectors

Gradual failure in optical fibers usually manifests itself as an increase in attenuation in the fiber. However, excessive strain on the fiber can also result in fiber breakage, resulting in catastrophic failure. Chemical impurities introduced during the fiber drawing process constitute a major source of changes to optical and physical properties. Factors that affect signal attenuation include hydrogen migration caused by diffusion into interstitial sites in the fiber molecular structure, chemical reaction of hydrogen with the glass constituents to form OH groups, formation of microcracks due to bending stresses, and optical losses due to the formation of color centers in the fiber core. (Color centers are formed primarily by the trapping of radiolytic electrons and holes at defect sites in the fiber when it is exposed to ionizing radiation.)

Pure silica-core fibers show the least radiation-induced damage in both mixed neutron/gamma and gamma-only environments. Some tests have shown that such fibers exhibit no performance change following doses of as much as 3800 Gy.[30] On the other hand, some fibers fluoresce enough under irradiation to obscure signals of very low strength. Pure silica-core fibers appear to be the most suitable for use in nuclear power plants.

Environmental variables such as high temperature and humidity can result in aging and increased failure rates for certain fiber-optic cables. In such harsh environments (e.g., inside containment, certain areas outside containment, and during accidents), the fiber coating material is of primary importance to performance. In the presence of high temperature and humidity, some degree of hydrolytic degradation in fiber coating will occur. If the coating is not designed to take this into account, its properties may degrade severely, and the coating may discolor or lose its adhesion to the glass.[31] In addition, significant strength reduction can also occur.[1] For example, an abnormally high incidence of fiber breakage with a newly installed cable in a telephone company was traced to deterioration of the strength and coating of the fiber due to exposure of the outer cable layer to temperatures as high as 80°C. The reel of cable in question had been stored outside for about 4 years with the protective thermal wrap removed.[32]

To examine the effects of a multivendor environment on the strength of aged fiber, Bonanno et al. tested several kilometers of commercial-quality uncoated optical fibers in both bending and tension.[32] Fibers from five different suppliers were tested[2] before and after aging in water at temperatures of 20, 60, and 80°C for periods as long as 270 days. Fibers were also aged in air under the following cyclic temperature conditions for periods up to 172 h: 10 h at −60°C, 2 h ramping to 85°C, 10 h at 85°C, and 2 h ramping down to −60°C. For the samples aged in water, there was almost no reduction in strength for those fibers maintained at 20°C. The largest strength reduction was observed for the 80°C exposures. For these fibers, median strengths fell below the 2-GPa (6-lb) handling limit for two fibers and minimum strengths fell below 2 GPa for four fibers. No strength reduction was observed for the samples cycled between −60°C and +85°C. Since the thermal cycling tests involved low humidity, these results confirmed the observation that interactions between water molecules and fused silica are responsible for the observed strength reductions.[32]

Splices and connectors can also introduce significant losses in an optical transmission system. Typically, splices are used to permanently join sections of optical cables together, while connectors are used at the end equipment,

[1] The strength of optical fibers approaches 10^6 psi. This is equivalent to about 20 lb tension when measured in short lengths, compared with the 16-lb tensile strength of 24-gauge copper wire.

[2] All fibers tested consisted of a 125-μm diam, silica-based glass coated with a dual-layer, uv-cured acrylate to an overall diameter of 250 μm. Three different coating formulations were represented by the fibers from the five suppliers.

where frequent mating and unmating are anticipated. The most frequent failure mechanisms in splices include bad cleaves, fiber breakage, fiber end-face separation due to improper assembly, dirt, and vibration.[33,34] A significant contributor to failure in connectors may be particles of dirt that enter the connector when it is disconnected.

Optical Receivers

The predominant failure mode in photodetectors is an increase in dark current (i.e., the current flow in the absence of light) due to elevated ambient temperature and possible electrical shorts due to electrochemical oxidation. A tenfold increase in dark current from the initial value is usually used as an end-of-life indicator. A PIN photodiode operating at about 800 nm has a lower dark current relative to an APD. However, the situation is reversed at 1300 nm, where the PIN has a higher dark current.

Electrochemical oxidation can cause electrical shorts in photodetectors at relative humidities up to 85%. Above this level, tests have shown that the lifetime of photodetectors decreases rapidly with increasing relative humidity.[35] With regard to radiation, optical receivers are sensitive to ionizing radiation as well as to optical radiation. The same physical processes that make the detector sensitive to radiation are also responsible for the detector's responsitivity to ionizing radiation. However, ionizing (gamma) radiation interaction is a bulk effect, meaning that charge carriers (electron-hole pairs) are generated throughout the bulk of the semiconductor material. On the other hand, photons generate carriers only in the small, active region. Therefore, the contribution of ionizing radiation to total photodiode current can be reduced by the following measures:

1. reducing the volume of the optically nonactive region and

2. reducing the volume of the active region while maintaining a high optical response (i.e., by using a material with a large absorption coefficient at the wavelength of the optical radiation).

Research data[26,29,36] show that double heterostructure AlGaAs/GaAs devices are far superior to silicon radiation-hardened photodiodes. In one study,[8] GaAs devices were able to operate reliably with dose rates up to 10^6 Gy/s, which is several orders of magnitude above the tolerance of silicon PIN photodiodes. Data on neutron irradiation effects on photodiodes show that the leakage current increases by about a factor of 10 in AlGaAs/GaAs photodiodes and a factor of 10^3 in silicon PIN photodiodes after exposure to a neutron fluence of 7×10^{14} n/cm^2. Degradation of optical responsitivity at this level of neutron fluence is negligible for AlGaAs/GaAs photodiodes, whereas silicon devices may experience a reduction in responsitivity of as much as 60% from preirradiation conditions.

Quite a number of age-related degradation and potential failure mechanisms are associated with fiber-optic transmission components. While some of the potential failures can be prevented or reduced by good engineering design and fabrication methods, some degradation will still occur and will be exacerbated by environmental stressors such as temperature, humidity, and radiation. Thus the environments in which the transmission subsystems will be used are significant. The more critical Class 1E applications of optical fibers in proposed ALWRs appear to be as data links between protection system divisions or as a communication network (FDDI) over which multiplexed data are carried to protection or engineering safety system processing units. ALWR protection system cabinets will typically be located in a control room environment, where radiation, temperature, and humidity levels are much more benign than in containment. For example, average temperature in containment may be 120°F, while an estimated average value for the control room is 65–70°F. Integral gamma dose levels in a PWR containment over a 60-year period may be on the order of 3×10^4 Gy, while the integral gamma dose levels in the control room over the same period are estimated to be less than 10 Gy.[37] Available data suggest that system degradation under these radiation conditions may be negligible. Therefore, it appears that given good design choices and installation procedures, fiber-optic components are likely to perform reliably in their proposed operating environments. However, information on long-term field performance is inadequate, and lifetime predictions for photonic devices vary widely. In addition, standardized tests are not always used, making it more difficult for test data to be more closely correlated.

For application in Class 1E systems, it is necessary to ensure that the fiber subsystems are qualified for the environment in which they are designed to operate. Typically, the optical subsystem manufacturer performs extensive burn-in and *stress screening tests on a number of samples to qualify the components initially. Assuming this to be true, the qualification of a Class 1E* ***system*** *can be accomplished by type testing in accordance with IEEE 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." However, given the limitations in current qualification methodologies (e.g., uncertainties in the Arrhenius equation), it appears that new standards or methodologies are required for evaluating "new" I&C technologies for application in Class 1E systems. One such methodology is proposed in Sect. 3.5.*

3.3.3 Trip System Electronic Hardware

Instrument and protection system cabinets normally have been placed in areas classified as "mild," and discussions with Westinghouse, General Electric, and ABB/CE suggest that this will be the case also for their respective protection system cabinets. A mild environment is defined as "*an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences.*"[38] For protection system cabinets, this assumes that environmental parameters such as temperature will remain well within operational limits at all times. However, elevated temperatures can exist undetected in inadequately cooled instrument cabinets, which will result in accelerated component aging and failure. Because this may not be easily identifiable, a pattern of component failures may have to be tracked over time before the cause can be identified as internal cabinet temperatures or elevated ambient temperatures.[11]

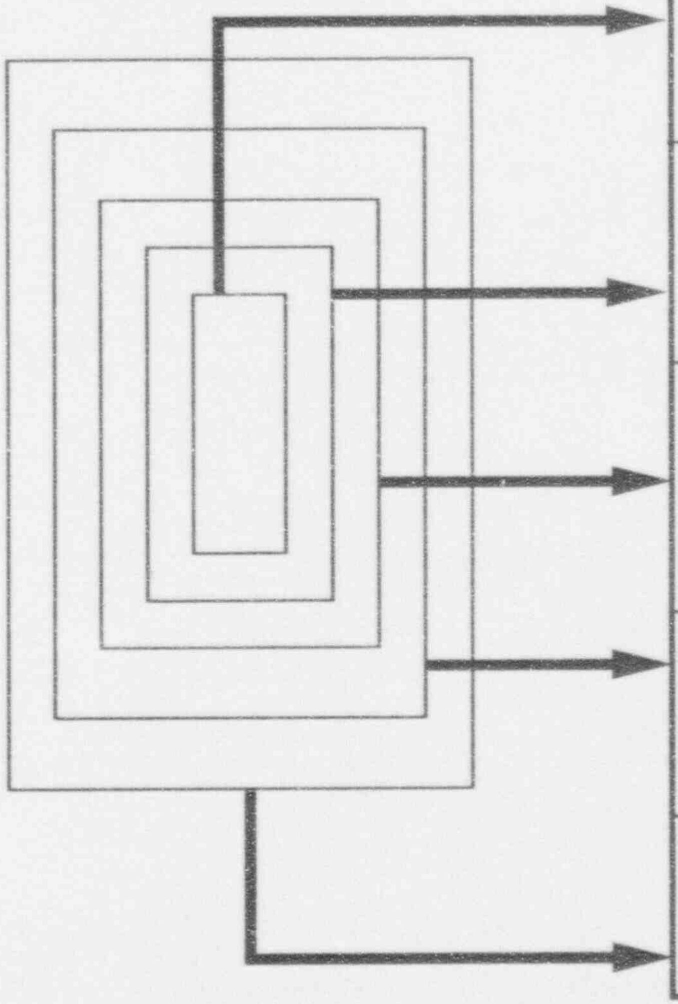
ALWR protection systems will make extensive use of digital technology rather than the analog technology typical of present-day LWRs. Digital systems are arguably more tolerant of environmental temperature effects than analog systems, in which posit e temperature feedback effects can lead to localized heating and thermal runaway in marginally designed systems. Still, the problem of system failures due to temperature effects is very real. For example, I&C system personnel in one process industry indicated that their distributed processing units start having problems when the ambient temperature reaches 90°F, even though the system specifications indicate adequate system functionality up to 120°F. Generally, the equipment becomes unreliable, developing random failures such as intermittent ability to keep up with the incoming data stream. I&C personnel at this plant indicated that an optimum temperature for the system seemed to be 72°F, and plant personnel would become concerned if the temperature reached 80°F. This example underscores the importance of environmental qualification programs for digital safety-related systems.

Safety systems such as protection cabinets are environmentally qualified at the cabinet level rather than at the component level. That is, environmental qualification tests typically involve the *total equipment*, not the individual electronic components inside the cabinet. Nevertheless, environmental reliability must be built into the system at various levels. This is depicted in Figure 3.8, which illustrates the various levels of protection against the environment for the actual circuits/components performing a safety-related function.

The first level of environmental protection is provided by the heating, ventilation, and air-conditioning (HVAC) system in the room or enclosure where the safety-related equipment is installed. While the HVAC system controls the environmental parameters such as humidity, temperature, and airborne particulates, the room itself may serve as a radiation shield for the equipment and a level of protection against the spread of smoke and fire in case a fire occurs. With respect to present-day LWRs, cabinets for all the (four) protection channels are typically located in the same room [Figure 3.9(a)]. The room is typically served by two separate HVAC systems, each of which is capable of maintaining the required environmental conditions. This ensures that failure of one HVAC will not adversely affect protection system functions. While HVAC system configurations for ALWRs may differ from manufacturer to manufacturer, at least one configuration divides the protection channels into two fire zones, as shown in Figure 3.9(b). Fire Zone A includes two rooms, each housing the cabinets for one protection channel. Fire zone B includes a similar set of rooms ıor the other two protection channels. Each of the two fire zones is serviced by a separate and independent HVAC system. Suitable controls are provided such that, in case of fire in one "protection cabinet room," appropriate dampers are closed so as to prevent smoke and particulates from entering into the other protection channel room serviced by that HVAC system.

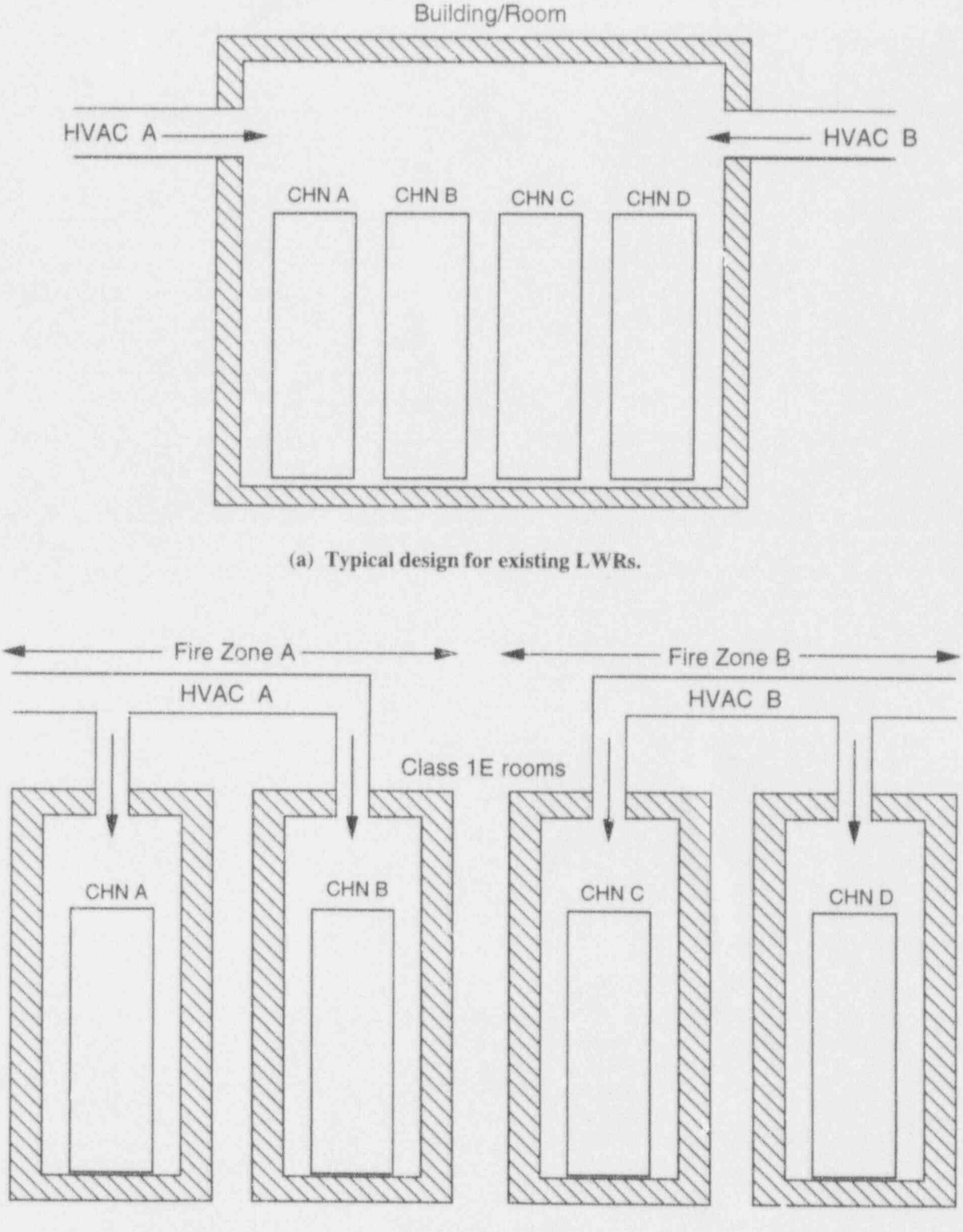
The next level of protection for the protection channel electronics is provided by the cabinet itself. Various design features such as fans, filters, and EMI/RFI shielding should be considered in the cabinet design. The fans and fan

PROTECTION HIERARCHY



	Stressors	Environmental controls
Electronic component	• Radiation • Heat dissipation • Vibration	• Type (TTL, CMOS) • Packaging (insertion mount, surface mount, chip on board)
Circuit board	• Heat • EMI/RFI effects • Smoke, particulates. corrosive gases, vibration	• Heat sinks • Shielding • Board layout (wire trace material coating)
Module/Rack	• Internally generated heat • EMI/RFI effects • Smoke, particulates, corrosive gases, vibration	• Fans • Shielding • Board enclosure design (e.g., inner foam cover)
Cabinet Class 1E system is qualified at this level	• Temperature • Humidity • Particulates • Corrosive gases • Seismic events • EMI/RFI	• Fans, filters • Cabinet design • Shielding
Room	• Temperature • Particulates • Radiation • Humidity	• HVAC, filtering • Fire protection • Shielding (gamma) • Location

Figure 3.8 Levels of protection against environmental stressors for safety-related electronic hardware



(a) Typical design for existing LWRs.

(b) Design for a selected ALWR.

Figure 3.9 Simplified diagram of HVAC system connections to protection rooms

filters provide additional protection by drawing air away from sensitive components in case of smoke and by trapping smoke particulates. The bottom shelf of a cabinet may be raised off the floor to prevent submersion in standing water. Holes may also be provided on this shelf to drain standing water. With regard to this, cable conduits connected to cabinets help to prevent standing water if connections are made from the bottom of the cabinet.

Depending on the system design, the next level of protection may be modules, racks, or circuit boards inside the cabinet. Circuit boards may be mounted vertically to limit soot, dust, and water accumulation. Modules may be designed in such a manner as to reduce smoke and particulate deposits in case of fire.

The final level of environmental protection for system components is at the chip level. Thermal management problems at the chip level become increasingly significant as clock frequencies increase, while more circuitry is crammed onto microprocessors and other integrated circuits. Moreover, as the number of on-chip I/Os increase, new and often complex schemes must be used to make the necessary connections between closely packed circuits. This has led to increasingly sophisticated packaging technologies. Thermal protection at the microcircuit level, however, is the responsibility of packaging engineers and not system design engineers. Thus the ALWR designer has to ensure that chips used for the design of a safety-related system have undergone adequate electronic stress screening and other quality assurance tests.

Environmental protection of safety-related electronic systems should be viewed from a defense-in-depth point of view, with the top levels of defense being the HVAC and fire protection systems. While a risk assessment of ALWR HVAC systems was not an objective of this study, our initial study of the HVAC system design indicates that the defense-in-depth approach should give adequate protection to microprocessor-based, safety-related electronics. The representative case studied (briefly described above) appears to be capable of isolating redundant safety channels from the detrimental effects of smoke and heat. It should also be noted that, in general, physical separation and fire protection requirements, rather than environmental qualification of the Class 1E equipment, should be relied upon to mitigate the consequences of a fire.

3.4 Functionality and Fault-Tolerance Issues of ALWR Protection Systems

The use of digital computers in safety-critical applications elicits requirements not necessarily applicable to analog safety systems. New approaches must sometimes be used in an effort to meet required criteria. In the development of a microprocessor-based safety-critical system, the hardware design is typically performed separately from the software design. This approach is both convenient and necessary to ensure both a highly reliable digital design, as well as highly reliable software. However, the overall safety of the microprocessor-based system is ensured by addressing the reliability of the *total system*. Typically, this is done by bringing the hardware and software designs together during the *integration phase* of the system's development. This approach is outlined in a number of Institute of Electrical and Electronics Engineers (IEEE) standards and is also recommended in draft standard P-7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."[39]

One reason for the exercise of caution in the introduction of software into safety-critical systems is the potential for common-cause failure due to the software. In an *integrated* system, however, it becomes difficult (and perhaps meaningless) in many instances to identify a particular system performance failure as being clearly software or hardware related. This is especially true of applications in which the "software" becomes an intimate part of the hardware (referred to as *firmware*), as in microprocessor-based protection systems proposed for ALWRs. For example, consider the situation in which some of the functions performed by the analog instrument string shown in Figure 2.7 are now performed in software. These functions will include A/D conversion of the input signal, linearization and scaling to engineering units, square root computation to extract flow information from the signal, comparison of the digital value to its set point, and the initiation of a trip/no trip signal. These computational functions will typically reside in firmware, meaning that the program required to perform the function is permanently "burned" into hardware (e.g., EPROM). The microprocessor reads and performs the instructions previously embedded in the EPROM but will manipulate the input data acquired in real time and stored in random access memory, or RAM. Two types of system failures may therefore be postulated:

1. Environmental stressors may give rise to a fault in one (or more) of the cells in the RAM. If the affected cell belongs to a byte of RAM that holds *data*, this fault may result in a system malfunction (due to manipulation of erroneous data) even though the "software" (i.e., the algorithm embedded in EPROM) was generated correctly. Has a "software" or a "hardware" error occurred?

2. Environmental stressors may give rise to a fault in one (or more) of the cells in the EPROM. If the affected cell belongs to a byte of EPROM that holds an *instruction* or an *address*, this would almost certainly result in a system malfunction, as a result of the microprocessor's execution of an erroneous instruction. Although this could be termed a software error, the error actually resulted from a *hardware* fault rather than an inherent "bug" in the software.

The two malfunction scenarios postulated above illustrate that in evaluating the performance of a microprocessor-based system, it is sometimes difficult–and not especially helpful–to differentiate software faults from hardware faults. When dealing with the performance of an overall system–after it is designed and constructed–the real issues are *functionality* and *fault tolerance*, not hardware vs software.[1] From this point of view, we examined the approaches taken by various ALWR manufacturers in applying microprocessor-based technology in safety systems. The objective was to examine further all aspects related to the widespread application of digital and other "new" hardware in the power plant environment.

3.4.1 Independence of Safety Channels

One significant aspect of the application of digital computers in safety systems is that they permit a greater level of interchannel communication as well as communication between safety and nonsafety computers. An issue of concern is the potential loss of a safety function as a result of this communication activity. With the older, hardwired analog systems, electrical isolation between safety channels, or between safety and nonsafety systems, was a primary requirement as an aid in maintaining channel independence. Requirements for physical separation and electrical isolation are stipulated in IEEE Standard 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." With microprocessor-based systems, da or communication isolation must also be considered, in addition to electrical isolation.

In digital systems proposed for ALWRs, communication between safety channels typically is required for voting, which is implemented in software. In some cases, the communication is also used for detecting faults. The following considerations result from these possible communication activities:

1. Failure in one channel should not prevent another channel from performing its safety function.

2. A protection channel should not require input from another to perform its function, except for the purposes of voting.

3. Any automatic surveillance testing should not prevent a safety channel from performing its safety function.

One way of achieving this is to adopt a *separation of function* approach, using separate, independent processors to perform trip functions, communication functions, and surveillance testing functions. This separation of functions should prevent the safety processor from "hanging up" due to communication faults. Communication based on dedicated processors can be structured to ensure reliable communication. The physical link between the channels must provide the electrical isolation (via optical isolators or fiber-optic cable), while the separate communication processor provides the necessary data isolation. As a minimum, a processor performing a separate function should be on a separate card.

[1] It should be emphasized that the above discussions do not in any way decrease the desirability of requiring *software* V&V to be performed during the (protection system) design process. Software V&V must be performed in order to have adequate confidence that software bugs have, in fact, been reduced to an acceptable level (approaching, but never attaining, zero). However, the real issues following system integration become functionality and fault tolerance rather than software and hardware.

While other approaches might be possible, our study of protection systems proposed for ALWRs revealed that, in general, the separation of function approach is being followed to maintain channel independence.

3.4.2 Diversity

Diversity with regard to safety systems may be viewed as different ways of providing the same safety function in order that the potential for common-mode failures is reduced. Functional diversity may be achieved by monitoring different process parameters in a safety channel, thereby enabling diverse processes to act as redundant scram initiators (e.g., steam generator water level, pressurizer pressure, etc., all in a single channel). Hardware diversity may be achieved by employing equipment from different manufacturers in each safety channel (e.g., pressure transmitters from different manufacturers in different safety channels). With processor-based systems, software diversity may be accomplished by using different compilers and different programmers for each safety system. However, some industry experts, both domestic and foreign, have expressed doubts as to whether software diversity actually contributes significantly to safety system reliability, as well as to a reduction in the potential for common-mode failures. While some studies show that about 80% of all software errors are traceable to misinterpretation of the (software) requirements specifications,[40] no study has been done to date, to the authors' knowledge, which indicates that software diversity can significantly reduce the probability of common-mode failure.

In analog systems, each instrument string in a protection channel is typically implemented with separate analog components. With microprocessor-based systems, however, a single multiplexer-A/D converter arrangement may be used to sample values from several safety parameters, and software is then used to perform many of the functions formerly performed with discrete analog components. The issue raised here is the potential failure of a safety channel due to a failure in either the multiplexer or the A/D converter, thereby rendering all associated process inputs ineffective. In such a case, a significant motivation for maintaining functional diversity in the first place--reduction of the safety system susceptibility to common-cause failures--would have been effectively negated.

Our study indicates that ALWR manufacturers generally will not employ software diversity in the implementation of the plant protection system. However, software diversity will be used (in addition to hardware diversity) in the implementation of control system I&C on the one hand and protection system I&C on the other. That is, different software programmers, hardware components, etc., will be used in the control and protection system implementations to reduce the probability of failure of both control and protection systems due to common causes.

With regard to the probability of common-cause failure due to multiplexing of trip variables, the approach generally used by ALWR manufacturers to reduce this probability is to divide the trip variables into two groups within each protection division, with each group monitored by a separate processor. Independence is maintained from the transmitters to the voting logic.

It is the opinion of the authors that since software diversity has not been shown to reduce common-mode failure, the probability of common-mode failure of the redundant system due to software errors should be accounted for in the evaluation of a safety system. One way is to use the defense-in-depth approach as described in NUREG-0493.[41]

3.4.3 Capability for Test and Calibration

While the test and calibration sources provided for analog safety systems are typically external to the safety system, computer-based safety systems are capable of providing internal test, diagnostic, and calibration features. For example, internal diagnostic methods can be used to monitor the "health" of different processor/memory boards and to perform software checks to ensure that the proper software is executing. Internal calibration methods may be used to compensate for gain and bias errors of associated signal-conditioning and A/D converter circuitry. While such techniques improve system operation, their use also raises new issues. For example, if an internal voltage reference source is used for system calibration and steps are not taken to ensure the integrity of the source, it could invalidate all the values of the safety parameters being monitored in that channel. This could result in corrupted data being sent to other channels in the case of a system that employs interchannel communication.

Our study of ALWR protection systems indicates that both on-line and off-line testing methods are to be incorporated in ALWR safety system designs. However, the degree of sophistication differs from manufacturer to manufacturer. Off-line testing methods may be used to automatically test a safety channel, usually during maintenance periods. On-line testing methods, on the other hand, will perform a certain amount of diagnostics when the channel is active. In the case of one manufacturer, we ascertained that the on-line diagnostics include power-up tests (RAM, EPROM, etc.), crystal time base checks, checks for "reasonability of calculations," and gain and bias compensation checks. The tests also include error checking on the data links, such as cyclic redundancy checks on the transmitted data, as well as tests by a transmitting channel to ascertain that the transmitted signal has been properly received by the receiving channels.

While the on-line diagnostics functions of microprocessor-based systems are considered an enhancement over their analog counterparts, an overriding issue is that the diagnostic function should not adversely affect the performance of the safety channel. While our system level study indicates this to be the case in general, a more detailed study was considered warranted but found to be outside the scope of this study, since it should involve a detailed study of the software.

3.4.4 Application of the Single-Failure Criterion to Computer-Based Safety Systems

Section 5.1 of IEEE Standard 603-1980 states the single-failure criterion as follows:

> The safety system shall perform all safety functions required for a design basis event in the presence of: (1) any single *detectable failure* within the safety systems concurrent with all identifiable but nondetectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions which cause or are caused by the design basis event requiring the safety functions.

A *detectable failure* is a "...failure that can be identified through periodic testing or can be revealed by an alarm or anomalous indication."[42] Detectability of failures is a function of system design and the level of sophistication of the tests performed. In computer-based systems the migration of many of the safety system functions into software, the increased complexity of the functions that are possible in software compared to what can be done in analog systems (self-diagnostics, self-calibration, as well as calculation of trip functions), and the unique and sometimes complex failure mechanisms that can arise in software systems all contribute to making the detection of failures more difficult. To increase the likelihood of identifying all detectable failures, the system hardware architecture should be kept simple and system V&V must be highly reliable. Keeping the hardware simple suggests the use of a deterministic computer (i.e., one that is noninterrupt driven). Such a system has a continuous execution cycle, and the designer can trace what the computer will be executing at any point in time. In effect, a deterministic computer is somewhat analogous to an analog system that consists of a string of components, with one output providing an input to the next. This implementation approach increases the likelihood that the causes and effects of failures can be identified. In the evaluation of a computer-based safety system, therefore, the issue of whether a deterministic or nondeterministic system has been employed in the system design should be considered.

The quality of the V&V performed for a system is crucial in the identification of detectable failures and is the most significant contributing factor to the reliability of the computer safety system. While the software V&V procedures employed by reactor manufacturers are not a part of this study, we were able to ascertain from a systems point of view that the protection system software presently being proposed does not use any operating system, which tends to increase system overhead and time response; nor are any interrupt mechanisms employed with regard to the reactor trip functions.

3.4.5 Fault Tolerance to EMI/RFI

An environmental stressor of particular interest in microprocessor-based protection systems is EMI/RFI. The survey of LERs discussed in Chap. 2 suggested that EMI/RFI may be a significant problem in current power plants. The increased use of microprocessors and digital circuitry, combined with the use of higher clock frequencies, faster logic families, and lower-level logic voltages, may result in a greater susceptibility to upsets and malfunctions due to the effects of EMI/RFI. In fact, recent experiences[43] have shown that inoustrial systems using the faster logic families generally have a greater susceptibility to the effects of EMI and therefore must be protected so that extraneous noise is not misinterpreted by the hardware as legitimate logic signals. While several standards exist and are used by reactor equipment manufacturers for EMI/RFI qualification of their digital equipment, no specific guidelines are presently available, to the authors' knowledge, that sets limits and criteria for the nuclear power plant environment. IEEE Standard 1050, *Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, was developed to provide guidance specific to a power generating plant for the design of grounding systems for I&C equipment. For the most part, IEEE 1050 is accurate in its treatment of electromagnetic compatibility (EMC) design and installation practices and applicable to the nuclear power plants environment. In addition, MIL-STD-461C, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference,* and MIL-STD-462, *Measurement of Electromagnetic Interference Characteristics*, are considered applicable to the needs of the nuclear industry. MIL-STD-461C and -462 were developed for use by the U.S. Department of Defense agencies to evaluate EMC. Applying to both equipment designs and procurement specifications, the purpose of the standards is to ensure that equipment and subsystems are compatible with their intended electromagnetic operating and that EMI effects are considered early in the design process.

A standard applicable to the nuclear industry should include guidance on EMI, electromagnetic susceptibility, ESD, high-frequency transients, surge withstand, and lightning effects.

The need for the development of regulatory guidance on EMI/RFI emissions and susceptibility is recognized by the NRC. Under the auspices of the NRC, Oak Ridge National Laboratory is presently conducting a separate study aimed at establishing the technical basis for acceptance criteria to immunize digital systems against EMI.[16]

3.5 A Methodology for the Qualification of New I&C Technologies for Nuclear Power Plants

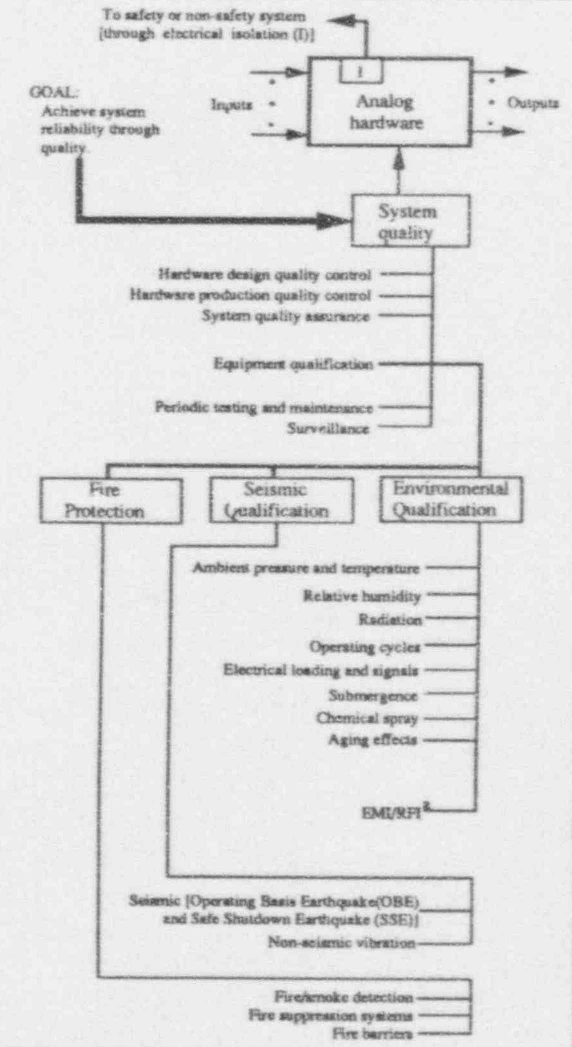
In this section, we summarize our study by proposing a methodology for qualifying a safety system involving new I&C technologies. The methodology identifies when accelerated aging may be needed prior to qualification testing.

It should be realized that environmental qualification addresses only one aspect of the overall goal of developing adequate confidence that a safety system (containing digital I&C) will perform as intended under any DBE. Qualification is, of course, performed on the finished product and is aimed at identifying any age-related degradation that could precipitate a common-cause failure in all redundant equipment during a DBE. Random failures are addressed by surveillance and diagnostic programs. However, the probability of either random or common-cause failure is a function of the quality built into the components of the product. For example, a semiconductor manufacturer should typically perform extensive burn-in and stress screening tests on a number of samples to initially qualify the components. Use of highly reliable components is, of course, the first step in maintaining quality at various levels of design, implementation, and operation of the safety system.

The overall process of achieving high reliability in a present-day (analog) safety system is depicted in Figure 3.10. The figure also identifies the most significant standards related to the particular "qualification" activity. Figure 3.11 identifies areas in these activities that could be (or are being) strengthened for application to microprocessor-based safety systems.

As illustrated in the figures, equipment qualification is generally handled under environmental, seismic, and fire protection criteria and standards. Environmental qualification methods are embodied in IEEE Standard 323-1974, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, which is endorsed by Regulatory Guide 1.89, *Qualification of Class 1E Equipment for Nuclear Power Plants*. IEEE Standard 323-1983 provides further clarification of these environmental qualification procedures. Although NRC has not specifically endorsed the 1983 version, it has commented that IEEE Standard 323-1983 neither alters the industry guidance provided nor alters the NRC's endorsement of acceptable qualification methods. Type testing is the most frequently used method of equipment qualification and involves subjecting the equipment to the environments and operating conditions for which it was designed. It also includes the concept of aging, in which the equipment is

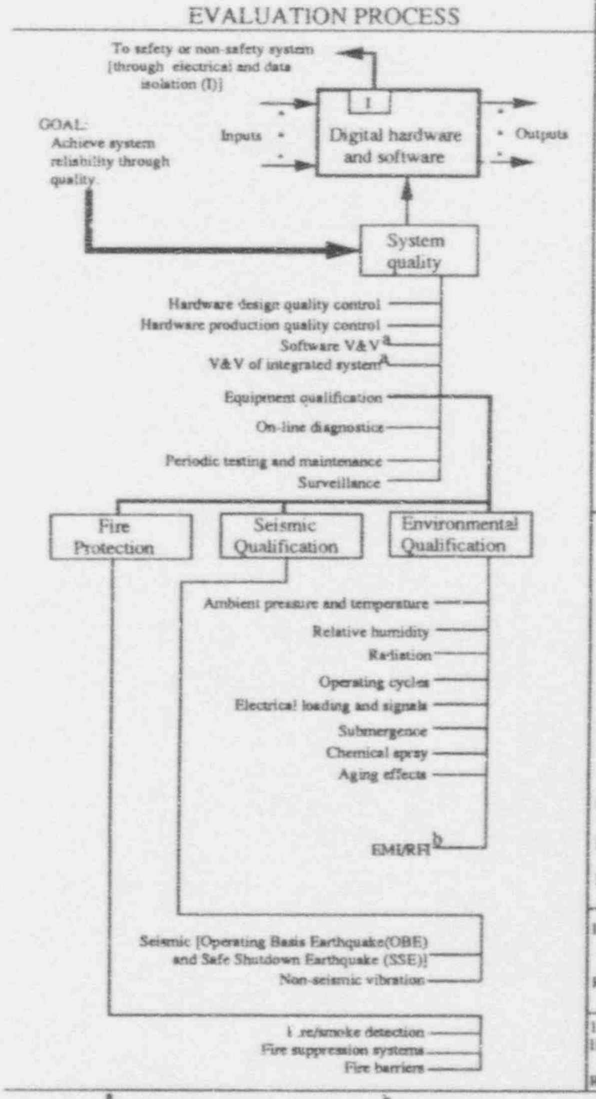
EVALUATION PROCESS


To safety or non-safety system
[through electrical isolation (I)]
I
GOAL:
Achieve system reliability through quality.
Inputs
Analog hardware
Outputs
System quality
Hardware design quality control
Hardware production quality control
System quality assurance
Equipment qualification
Periodic testing and maintenance
Surveillance
Fire Protection
Seismic Qualification
Environmental Qualification
Ambient pressure and temperature
Relative humidity
Radiation
Operating cycles
Electrical loading and signals
Submergence
Chemical spray
Aging effects
EMI/RFI[a]
Seismic [Operating Basis Earthquake(OBE) and Safe Shutdown Earthquake (SSE)]
Non-seismic vibration
Fire/smoke detection
Fire suppression systems
Fire barriers

APPLICABLE CODES AND STANDARDS	COMMENTS
	Diagram represents a generalized safety instrumentation and control system consisting of ans log and electromecha ical components. Interfaces to other safety systems or non-safety systems typically employ electrical isolation.
ASME NQA-1-1989, "Quality Assurance Program Requirements for Nuclear Facilities." IEEE Std 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Powe: Generating Stations." Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems."	
IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."	
IEEE Std 627-1980, "IEEE Standard for Design Qualification of Safety System Equipment Used In Nuclear Power Generating Stations." IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants."	EMI testing is typically addressed on an individual equipment basis, as necessary.
IEEE Std 1050-1989, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations." MIL-STD 461C, "Electromagnetic Emission and Susceptibility Requirements for the Control of EMI." MIL-STD-462, "Measurement of Electromagnetic Interference Characteristics."	Other standards such as SAMA PMG 33.1, ANSI/IEEE C62.43, and !EEE Std 472, are used.
IEEE Std 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations." Regulatory Guide 1.100, "Seismic Qualification of Electrical Equipment for Nuclear Power Plants."	
10 CFR 50, App. A; 10 CFR 50.48; 10 CFR 50, App. R. IEEE Std 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." Regulatory Guide 1.75, "Physical Independence of Electric Systems."	General Design Criterion 3 of 10 CFR 50, Appendix A, requires systems important to safety to be designed to minimize the probability and effects of fires and explosions. The specific requirements for fire protection are given in Appendix R.

[a] EMI/RFI = Electromagnetic interference/radio frequency interference.

Figure 3.10 The overall evaluation process to achieve safety system reliability in present-day nuclear power plants


EVALUATION PROCESS
To safety or non-safety system [through electrical and data isolation (I)]
I
GOAL: Achieve system reliability through quality.
Inputs
Digital hardware and software
Outputs
System quality
Hardware design quality control
Hardware production quality control
Software V&V[a]
V&V of integrated system[a]
Equipment qualification
On-line diagnostice
Periodic testing and maintenance
Surveillance
Fire Protection
Seismic Qualification
Environmental Qualification
Ambient pressure and temperature
Relative humidity
Radiation
Operating cycles
Electrical loading and signals
Submergence
Chemical spray
Aging effects
EMI/RFI[b]
Seismic [Operating Basis Earthquake(OBE) and Safe Shutdown Earthquake (SSE)]
Non-seismic vibration
I .re/smoke detection
Fire suppression systems
Fire barriers

APPLICABLE CODES AND STANDARDS	COMMENTS
ASME NQA-1-1989, "Quality Assurance Program Requirements for Nuclear Facilities." IEEE Std 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." ANSI/IEEE-ANS 7-4.3.2-1982, "Application Criteria for Digital Computers in Safety Systems of Nuclear Power Facilities." Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Regulatory Guide 1.152, "Criteria for Programmable Digital Computer Software in Safety-Related Systems of Nuclear Power Plants."	Diagram represents generalized, microprocessor-based safety instrumentation and control (I&C) system. Interfaces to other safety systems or non-safety systems are typically by fiber optic links. In a microprocessor-based safety system, the concept of data isolation should also be considered in addition to electrical isolation. That is, there should be data isolation between the safety software and the communication software. Failure of the communication software should have no effect on the capability of the protection system to perform its safety function. ANS/IEEE-7-4.3.2 - 1982 is inadequate in addressing issues relating to microprocessor-based I&C. These issues have been addressed in IEEE 7-4.3.2 - 1993.
IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."	On-line diagnostics methods can reduce stress on (digital) safety system I&C by reducing the number of periodic maintenance schedules required. This advantage could be reflected in current periodic maintenance requirements.
IEEE Std 627-1980, "IEEE Standard for Design Qualification of Safety System Equipment Used In Nuclear Power Generating Stations." IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Pow:r Generating Stations." Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for N::clear Power Plants." Regulatory Guide 1.100, "Seismic Qualification of Electrical Equipment for Nuclear Power Plants."	EMI testing is typically not included in the environmental qualification process. It is addressed on an individual equipment basis, as necessary. However, the unpredictable failure modes of microprocessor-based systems require all (digital) safety I&C to be *environmentally* qualified against EMI/RFI.[b]
IEEE Std 1050-1989, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations." MIL-STD 461C, "Electromagnetic Emission and Susceptibility Requirements for the Control of EMI." MIL-STD-462, "Measurement of Electromagnetic Interference Characteristics."	Other standards such as SAMA PMC 33.1, ANSI/IEEE C62.43, and IEEE Std 472, are used. However, specific criteria for EMI/RF I[b] qualification for the nuclear power industry is lacking. Specific EMI/RFI requirements are addressed in a companion document, NUREG/CR-5941, *Technical Basis for Regulatory Guidance on Electromagnetic and Radio-Frequency Interference in Safety-Critical I&C Systems.*
IEEE Std 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations." Regulatory Guide 1.100, "Seismic Qualification of Electrical Equipment for Nuclear Power Plants."	
10 CFR 50, App. A; 10 CFR 50.48 IEEE Std 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." Regulatory Guide 1.75, "Physical Independence of Electric Systems."	Fire and its effects (smoke, heat, ignition explosions, toxic gases) on safety-related equipment is a fire protection concern and not necessarily an environmental qualification issue.

[a] V&V = Verification and validation

[b] EMI/RFI = Electromagnetic interference/radio frequency interference.

Figure 3.11 The overall process for evaluating digital safety systems with possible enhancements for greater assurance of correct functionality and high reliability

put in a condition that simulates its expected end of qualified life. In this study, we identified environmental conditions and aging stressors to which major components in ALWR protection channels will be subjected and compared them to environmental conditions and stressors in present-day nuclear power plants. We concluded that many of the environmental stressors are likely to be similar. However, EMI/RFI may be of particular interest as an environmental stressor for microprocessor-based I&C systems. Regardless of whether a microprocessor-based system is likely to be more or less susceptible to EMI/RFI than its analog counterpart, the fundamental problem that remains is the unpredictable behavior response of a software-based digital system to EMI/RFI upsets. Thus, qualification criteria should include EMI/RFI tests with the intent of demonstrating that the protection system will *fail safe* for the worst-case EMI/RFI conditions to which the system is likely to be exposed. Currently, EMI/RFI susceptibility tests are generally not included in the environmental qualification process. Rather, EMI/RFI is addressed on an individual equipment basis as necessary, such as to demonstrate physical independence of Class 1E and non-Class 1E circuitry in a microprocessor-based protection system.

Seismic qualification criteria are embodied in IEEE Standard 344-1987, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.* This standard is endorsed by Regulatory Guide 1.100, *Seismic Qualification of Electrical Equipment for Nuclear Power Plants.* Seismic testing is typically performed as part of an overall qualification program and is designed to demonstrate the capability of the equipment to perform its safety function during and after the time it is subjected to the forces resulting from a defined safe-shutdown earthquake (SSE). The requirements for seismic qualification of microprocessor-based I&C equipment appear to be no different from those for analog I&C equipment, and so continued endorsement of the standard seems appropriate.

The basic design requirements for protection against fire are stipulated in General Design Criterion 3 of Appendix A of 10 CFR 50 and IEEE Standard 384, *Independence of Class 1E Equipment and Circuits.* General Design Criterion 3 (Appendix A of 10 CFR 50) requires that structures, systems, and components important to safety be located to minimize the probability and effects of fires and explosions. IEEE Standard 384 requires that an electrically generated fire in a Class 1E division shall not result in the loss of function in the redundant Class 1E division. In addition to these requirements, Appendix R of 10 CFR 50 requires a defense-in-depth approach to be taken to (1) prevent fires from starting; (2) detect rapidly, control, and extinguish promptly those fires that do occur; and (3) provide protection for structures, systems, and components important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent safe shutdown of the plant.

A fire protection system should be capable of detecting, containing, and suppressing a fire. In addition, the system should be capable of isolating redundant safety channels from the detrimental effects of smoke, heat, and the potential generation of toxic gases. In general, physical separation and fire protection requirements, rather than environmental qualification of the Class 1E equipment, should be relied upon to mitigate the consequences of a fire.

While Figures 3.10 and 3.11 provide an overall picture of the protection and reliability mechanisms designed to ensure a reliable safety system, ***our main emphasis in this section is the evaluation of the need for accelerated aging in the environmental qualification process for safety-related I&C equipment not covered under 10 CFR 50.49,*** **Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants.** Safety-related equipment "located in a mild environment"[1] is not addressed within the scope of 10 CFR 50.49.

As we have indicated elsewhere in this document, many of the environmental stressors experienced by safety systems of ALWRs at their proposed locations are likely to be similar to those of present-day plants. However, a new technology introduced into a so-called "mild" environment may be subject to new and significant degradation mechanisms that could lead to common-cause failures under postulated service conditions. On the other hand, it can be argued that accelerated aging may not be needed in a qualification process for equipment that does not exhibit any significant age-related degradation, if the equipment has a proven track record in similar environments in the nonnuclear industry. We propose a methodology based on an analysis of the effect of stressors using the

[1] 10 CFR 50.49 defines a mild environment as "an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences."

concept of *aging fraction* and the determination of a *threshold* for each of the stressors that the I&C system will experience under both normal and abnormal service conditions. This methodology is illustrated in Figure 3.12 and explained in the text that follows. The boxed/circled numbers in Figure 3.12 correspond to the numbered sections below to facilitate comparisons. The discussion on fiber-optic transmission systems is used wherever applicable to illustrate the methodology.

1. *Identify all stressors that can degrade the equipment under both normal and abnormal service conditions.*

Stressors include (but are not limited to) temperature, humidity, pressure, vibration, EMI/RFI, electrical loading, chemical spray, and maintenance and the synergistic effects involving two or more of these. An example of maintenance stress is stress experienced by a fiber-optic cable/connector assembly as it undergoes frequent connection and disconnection in the course of maintenance throughout its service life.

> Using the preceding review of fiber-optic communication systems and the proposed location of ALWR protection cabinets, temperature, humidity, radiation, and maintenance stress will all be identified as stressors. Even though the equipment may be well designed and perform reliably, all possible stressors that can degrade the equipment under both normal and abnormal conditions should be identified during this step.

2. *For each stressor, determine whether a threshold exists below which the stressor has been demonstrated not to cause significant age-related degradation.*

An age-related degradation mechanism is significant if in the normal and abnormal service environment it causes degradation during the installed life of the equipment that progressively and appreciably renders the equipment vulnerable to failure to perform its safety function(s) under DBE conditions. We propose here a quantitative measure for *significant* age-related degradation: an aging mechanism may be considered significant if the ratio of the number of failures due to the aging mechanism to the total number of failures (both random and age-related) is greater than 0.1 (10%). In a study focusing on reactor protection systems,[6] assessments were made of the relative number of occurrences of age-related failures vs other failures. In that study a quantity, *aging fraction*, was defined for a particular piece of equipment as

Aging fraction = (failures due to aging)/(total failures).

It was found that different types of I&C equipment had similar aging fractions ranging between 0.2 and 0.4. While this study was performed using the NPRDS database, another study using the LER database produced similar results,[7] despite differences between the studies regarding what constitutes aging effects. An aging fraction of 0.1 therefore appears to be a (conservative and) reasonable figure to use when evaluating any new I&C technology being introduced into the nuclear power plant environment. One advantage of using this quantitative measure for evaluating the likely impact of stressors on new safety-related I&C systems is that it provides an empirical basis for comparing any new I&C technology to present-day Class 1E I&C systems. Since the data used in both studies above were Class 1E equipment in which the effect of aging had been taken into consideration during qualification, it suggests that:

> *Any new technology that can be shown to have an aging fraction of less than 0.2 in its service environment is not likely to have significant age-related degradation mechanisms that will increase the probability of common-cause failures beyond what is currently attainable in Class 1E systems.*

If the environmental temperature under both normal and abnormal service conditions for some I&C equipment is *T* and it can be shown that the aging fraction for that equipment in such an environment is 0.1 or better, then the threshold temperature for the equipment is *T*.

The fundamental concern of qualification is to ensure that Class 1E equipment can perform its safety function(s) with no failure mechanism, due to design or manufacture, that could lead to common-cause failures under postulated service conditions. The object of *accelerated aging*, in a program of equipment qualification, "is to put a

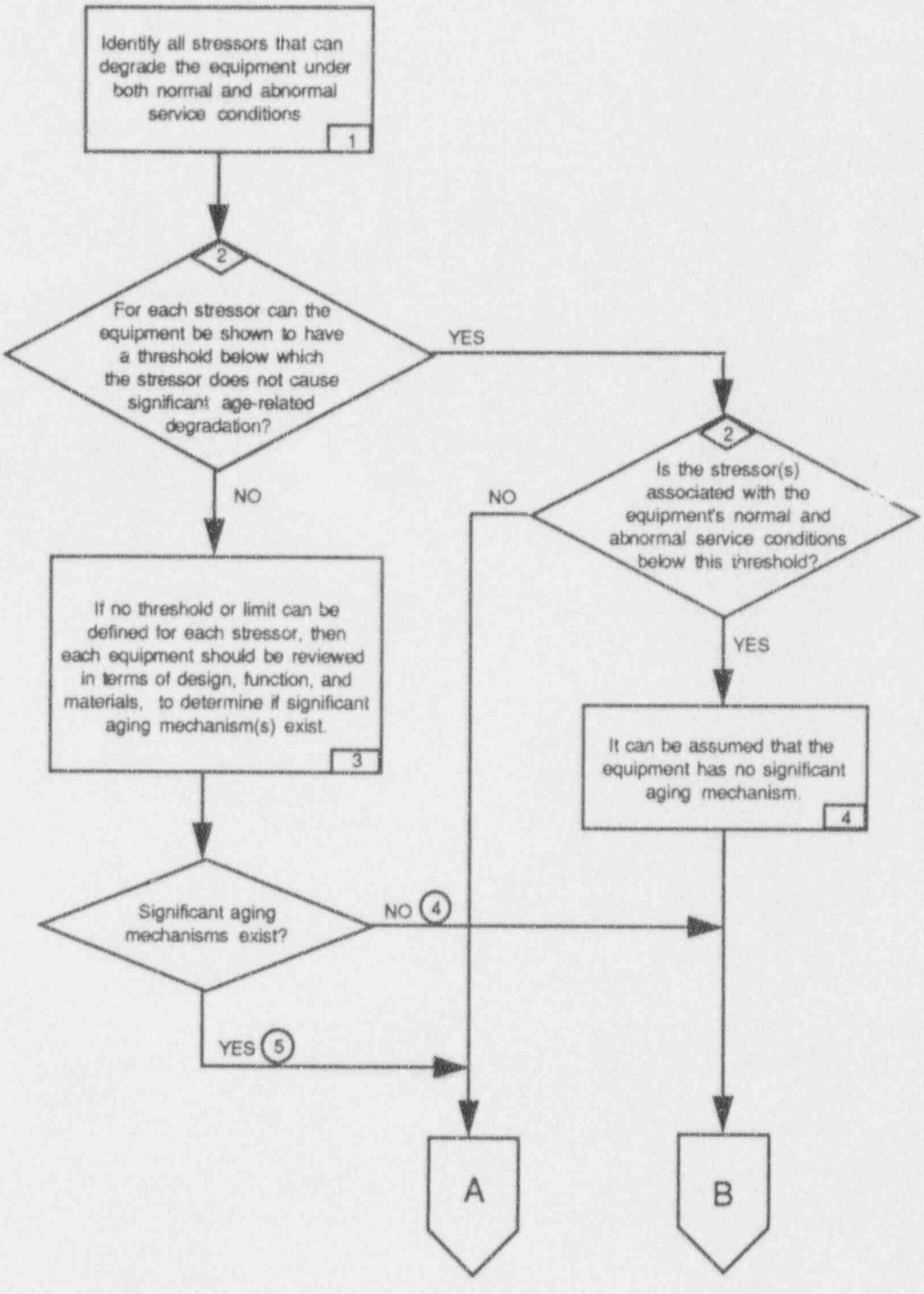

Identify all stressors that can degrade the equipment under both normal and abnormal service conditions
1
2
For each stressor can the equipment be shown to have a threshold below which the stressor does not cause significant age-related degradation?
YES
NO
2
Is the stressor(s) associated with the equipment's normal and abnormal service conditions below this threshold?
NO
YES
If no threshold or limit can be defined for each stressor, then each equipment should be reviewed in terms of design, function, and materials, to determine if significant aging mechanism(s) exist.
3
It can be assumed that the equipment has no significant aging mechanism.
4
Significant aging mechanisms exist?
NO 4
YES 5
A
B

Figure 3.12 A methodology for determining if accelerated aging is required during qualification testing for safety-related I&C equipment not covered under 10 CFR 50.49

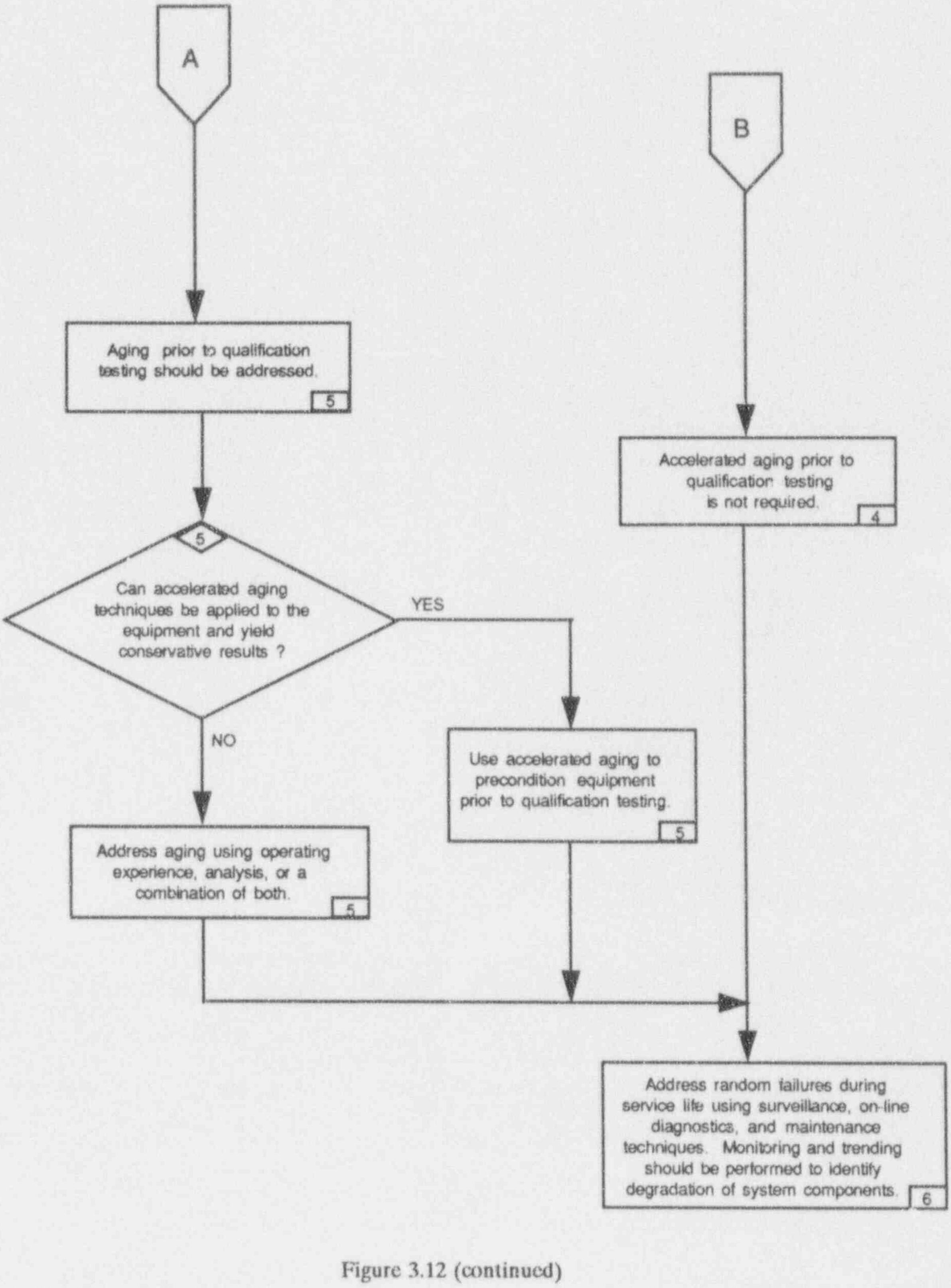

A
B
Aging prior to qualification testing should be addressed.
5
Accelerated aging prior to qualification testing is not required.
4
5
Can accelerated aging techniques be applied to the equipment and yield conservative results ?
YES
NO
Use accelerated aging to precondition equipment prior to qualification testing.
5
Address aging using operating experience, analysis, or a combination of both.
5
Address random failures during service life using surveillance, on-line diagnostics, and maintenance techniques. Monitoring and trending should be performed to identify degradation of system components.
6

Figure 3.12 (continued)

specimen in a condition simulating its ability to function as required during and following a design basis accident that may occur after as much as forty years of service."[9]

Industry consensus appears to be that radiation is not considered a significant aging mechanism for electronic equipment at locations experiencing an integral dose of less than 100 Gy. Available data indicate that this is likely to be the case for fiber-optic components also. In general, however, the impact of stressors should be analyzed on a case-by-case basis. Equipment located in any environment, whether mild or harsh, may or may not experience significant age-related degradation, depending on a number of factors such as the technology used. In some cases, degradation may be accelerated because of poor design or selection of (electronic) components. For example, poor design may result in localized heating on a board in a cabinet, causing identical boards in all redundant systems to degrade and eventually fail even though each redundant cabinet may be specified to operate in a mild environment. Therefore, in determining a threshold for a particular stressor, the actual operating characteristics of the *components*, as well as the operating environment at the board level, should be considered. Note that this does not suggest that qualification should be performed at the board level—only that board-level operating conditions should be considered in the determination of a threshold. For example, the environmental temperature at the location of an I&C cabinet may be 75°F, but temperature conditions *inside* the cabinet may be significantly higher.

In the application of any new I&C technology in Class 1E systems, the burden of proof (for the nonexistence of a significant age-related degradation mechanism) is on the user to show that the aging fraction is 0.1 or better.

> From the preceding review on the effect of some stressors on optical fiber communication systems, we can infer that when such systems are used in control room temperature, humidity, and radiation environments, they are <u>likely</u> to perform reliably. However, with the possible exception of radiation effects with regard to fiber-optic <u>cables</u>, no temperature or humidity thresholds have been shown to exist in the literature for the communication system components. Further analysis will therefore have to be done, as suggested in subsequent steps.

3. *If no threshold or limit can be defined for each stressor, review the equipment in terms of design, function, and materials to determine the existence of significant aging mechanisms.*

For example, as has been suggested in item 2, a piece of electronic equipment may be said to be operating below its "radiation threshold" if it can be shown that the equipment is not likely to experience a radiation dose above 100 Gy under postulated service conditions, including a DBE. If no such threshold has already been established for the stressor under consideration, then equipment may be analyzed in terms of design, function, and materials to determine the existence/nonexistence of significant aging mechanisms. Note that this implies a determination of the existence or nonexistence of a threshold for that stressor. The primary source for a determination may be research data based on failure rate data in *similar* environments in the nonnuclear industry, materials, technology used, reliability data, operating experience, and/or analysis. Note that if field failure rate data are used, age-related failure rates will typically depend upon the integrated or synergistic effect of all the environmental stressors (e.g., humidity *and* temperature) experienced during the normal service life of the equipment. In this instance, *threshold* as defined in item 2 above should be understood to mean the threshold for that *environment*, not just for a single stressor.

> The aging fraction of a piece of I&C equipment can be estimated if a suitable database exists. However, since fiber-optic systems are relatively new in nuclear power plants, no such database exists. The methodology suggests that we can take credit for data available for similar or more harsh environments in the nonnuclear industry. The telecommunications industry makes extensive use of fiber-optic cables and has been compiling field failure information through an organized reporting program since 1986. The failure reports include both aerial and underground cables. Analysis of over 650 failure data reported from 1986 through 1993 showed the following:
>
> - 58% of all reported failures were due to cable dig-ups. A dig-up is damage to cable during an attempt to penetrate the ground.
>
> - 7.4% of all cable failures were due to installation error.

- Extreme temperatures other than steam leaks accounted for 1.7% of all reported failures. One failure occurred when cold weather caused an aerial cable jacket to shrink, placing pressure on the fibers.

- 3.2% of all reported failures were due to fire. In some of these failures the fibers themselves remained unbroken, although the cable was practically destroyed. Failures in such cases were caused by high loss in the unbroken fibers.

- The rest of the failures (accounting for 29.7% of all failures) were due to damage caused by power line contacts, firearms, vehicle damage, and rodents.

From the preceding data, age-related failures for underground and aerial fiber-optic cables with regard to environmental temperature can be expected to be fairly low (less than 10% of all failures). Since both the normal and abnormal environmental temperatures for both underground and aerial fiber-optic cables are worse than those expected in the control room, we may conclude that fiber-optic cables in the latter environment may not experience significant age-related degradation with regard to temperature.

Similar analysis should be performed for all stressors the equipment is likely to experience under normal and abnormal service conditions.

4. *Accelerated aging need not be performed for equipment with no significant aging mechanism.*

It is the opinion of the authors that accelerated aging need not be considered in a qualification program if it can be shown that age-related degradation is not a significant contributing factor to common-cause failures and that all random, age-related failures can be adequately detected through surveillance and diagnostic techniques. Notice that the "vagueness" associated with "significant" has been removed by introducing the concepts of aging fraction[6] and threshold. The fundamental idea is that if both of these parameters can be ascertained for the I&C equipment, *and* if it can be shown that both the normal and abnormal service conditions of the equipment are below the threshold, then employing accelerated aging during qualification testing is not likely to reduce the probability of common-cause failure.

5. *If accelerated aging cannot be shown to yield conservative results, alternative means should be used in equipment qualification.*

If significant aging mechanisms exist, then accelerated aging prior to qualification testing should be required. Accelerated (thermal) aging is typically employed in accordance with IEEE 323-1974 and Reference 9 to precondition equipment. The Arrhenius equation is the physical model typically used in accelerated aging. However, one of the major problem areas is the adequacy of this model in simulating actual equipment aging. This is especially true of electronic systems, where the different components making up a subsystem have different activation energies and different degradation mechanisms. Another problem is synergism, because of which the effect of the *simultaneous* application of radiation and temperature may be different from the effect of the *sequential* application typically employed. For example, evidence to date shows that the order of application of the stressors to electrical cables may be significant.[10]

While the consensus of industry experts appears to be that current aging methodologies tend to yield conservative results (at least with regard to cables), it is the opinion of the authors that this tendency has not been shown to be the case for electronic equipment. In addition, it will not necessarily be the case for other technologies that will be introduced in power plant environments in the future. We propose in this methodology that if the use of accelerated aging techniques cannot be shown to yield conservative results, or valid results that may be correlated with real time, then aging should be addressed using operating experience, analysis, or both.

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

Since aging is present in any I&C equipment, this methodology does not imply that the effects of aging should not be considered during the *service life* of the equipment. Condition monitoring and trending should be used to identify end-of-life of the component. The use of microprocessors can enable advanced and on-line diagnostics to be performed, improving the ability to detect both random and impending (age-related) failures beyond present capabilities.

3.6 Concluding Remarks

In this chapter, I&C systems and components proposed to be used in ALWR protection systems were identified. The study indicates that the major *new* components will be optical fibers and the extensive application of microprocessors in safety systems. The more significant Class 1E applications of optical fibers in proposed ALWRs appear to be as data links between protection system divisions or as a communication network (FDDI) over which multiplexed data are carried to protection or engineering safety system processing units. A study of the impact of stressors on optical fiber cables in their proposed locations indicate that, with the likely exception of maintenance aging, age-related degradation is likely to be minimal. This is because appreciable degradation due to the stressors (e.g., radiation) seems to occur at much higher stress levels than the proposed locations indicate. This suggests that given good design choices and installation procedures, fiber-optic components and communication systems are likely to perform reliably in their proposed operating environments. However, periodic surveillance testing and condition monitoring in accordance with IEEE Standard 338 are recommended.

Based on the results of this study, a methodology for equipment qualification of new I&C technologies for application in safety systems has been proposed. The methodology basically identifies when accelerated aging may be needed prior to qualification testing.

4 Conclusions

This study has presented an evaluation of the protection system I&C for ALWRs in terms of the effects of stressors, the environment, and distribution of function. Analog trip systems in present-day plants were reviewed and compared with microprocessor-based trip systems proposed for ALWRs. The comparisons enabled the identification of unique qualification and functional issues characterizing the application of advanced I&C systems in nuclear power plants.

The study also identified optical fiber systems as a technology that is relatively new to the nuclear power plant environment and examined the failure modes and age-related degradation mechanisms associated with optical fibers and components. The data were then used to recommend a methodology for the qualification of new technologies for power plant applications.

Other findings and conclusions from the study are as follows:

1. The type of transmitters, sensing lines, and cabling, up to the multiplexing and sampling components, are likely to be the same for ALWRs as for existing LWRs. Environmental conditions (temperature, humidity, radiation, etc.) for the instrumentation are also likely to be very similar. However, a potential issue for ALWR safety systems may be increased susceptibility to EMI and RFI because of the increased use of microprocessor-based technology. While digital systems generally have higher noise margins than their analog counterparts, the trend toward the use of higher clock frequencies, lower logic levels, and ever denser packages leads to greater probability for upsets. First, the increasing levels of integration tend to decrease the noise immunity of the digital devices. Second, some logic families have rather poor worst-case noise margins to start with [e.g., 0.12 V for emitter coupled logic and 0.1 V for gallium arsenide (GaAs)]. On-chip protection methods help to protect the devices against interference-induced damage, but they have not eliminated *upset* problems. In fact, even fault-tolerant systems in general do not achieve reliable systems performance in some high-EMI environments. Thus, it appears that while safety systems in ALWRs will have to be qualified to the same environment as current LWRs, EMI/RFI emissions and susceptibility criteria and guidelines specific to the nuclear power plant environment should be considered. Specific EMI/RFI

requirements are addressed in a companion document, NUREG/CR-5941, *Technical Basis for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems.*[15]

2. The protection systems of ALWRs employ a voting scheme (two-out-of-four) similar to present-day (analog) implementations. The essential difference, however, is that the voting will be performed in software rather than in hardware and will in some cases involve software data communication among the channels. This cross-communication could be a source of problems and should require close review. Failure modes in which a processor waits indefinitely for information from another channel, or erroneous data are communicated to the other channels without being noticed, are of concern and will require consideration in appropriate standards and regulatory guides. For example, processors performing communication functions may be required to be different from processors performing protection system functions.

3. In existing plants, physical separation and fire protection requirements, rather than environmental qualification of the Class 1E equipment per se, are generally relied upon to mitigate the consequences of a fire. This approach also appears to have been followed for the next generation of nuclear power plants.

5 Recommendations for Further Research

Although optical fiber cables have been shown to perform adequately under adverse radiation conditions, the *long-term* performance of fiber-optic interfaces such as connections, sources, and detectors under similar conditions has not been adequately characterized. Research is needed to characterize the performance of these interfaces in radiation environments.

Because of the increased complexity and uncertainties associated with microprocessor-based protection systems, there is a need to evaluate and verify *experimentally* the functional behavior and failure modes of a typical microprocessor-based protection system as a result of the application of environmental stressors such as temperature, humidity, vibration, radiation, and the presence of smoke and chemical contaminants.

The limitations associated with accelerated aging, sequential vs simultaneous testing, and synergistic effects, especially with regard to microprocessors, need to be adequately characterized in anticipation of such systems being employed in adverse environments in future power plants.

6 References

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

2. *U.S. Code of Federal Regulations*, 10 CFR 50.62, 1991.

3. E. J. Siskins et al., *Analysis of Utility Industry Data Systems*, EPRI NP-1064, Electric Power Research Institute, April 1979.

4. *U.S. Code of Federal Regulations*, 10 CFR 50.72, 1991.

5. M. K. Comer et al., *Human Reliability Data Bank for Nuclear Power Plant Operations*, NUREG/CR-2744/2, U.S. Nuclear Regulatory Commission, February 1983.

6. P. T. Jacobs, *An Interim Assessment of Reactor Protection Aging*, NUREG/CP-0082, U.S. Nuclear Regulatory Commission, July 1984.

7. *Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U.S. Commercial Nuclear Power Plants*, NUREG/CR-1740, U.S. Nuclear Regulatory Commission, 1984.

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

9. *A Review of Equipment Aging Theory and Technology*, NP-1558, Electric Power Research Institute, September 1980.

10. R. L. Clough and K. T. Gillen, *Radiation-Thermal Degradation of PE and PVC: Mechanism of Synergism and Dose Rate Effects*, NUREG/CR-2156, Sandia National Laboratories, June 1981.

11. A. C. Gehl and E. W. Hagen, *Aging Assessment of Reactor Instrumentation and Protection System Components*, NUREG/CR-5700, U.S. Nuclear Regulatory Commission, July 1992.

12. L. Meyer, *Nuclear Plant Aging Research on Reactor Protection Systems*, NUREG/CR-4740, Idaho National Engineering Laboratory, January 1988.

13. G. J. Toman, *Inspection, Surveillance, and Monitoring of Electrical Equipment in Nuclear Power Plants, Volume 2, Pressure Transmitters*, NUREG/CR-4257, Oak Ridge National Laboratory, August 1986.

14. C. W. Mayo et al., *Radiation Hardening of Smart Transmitters*, EPRI NP-7172, Electric Power Research Institute, February 1991.

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

16. P. D. Ewing, K. Korsah, and Christina Antonescu, "Immunizing Digital Systems Against Electromagnetic Interference," pp. 757–765 in *Proceedings of the 2nd ASME/JSME Nuclear Engineering Joint Conference*, Vol. 2, San Francisco, March 21–24, 1993.

17. Dan Wilkinson and Larry Wray, *Integrated Instrumentation and Control Upgrade Plan*, NP-7343, Rev. 2, Electric Power Research Institute, December 1991.

18. D. M. Fleetwood et al., "High-Temperature Silicon-on-Insulator Electronics for Space Nuclear Power Systems: Requirements and Feasibility," *IEEE Trans. Nucl. Sci.*, **NS-35**(5), 1099 (1988).

19. J. L. Leray et al., "CMOS/SOI Hardening at 100 Mrad(S_iO_2)," *IEEE Trans. Nucl. Sci.*, **NS-37**(6), 2013 (1990).

20. O. Flament et al., "High Total Dose Effects on CMOS/SOI Technology," *IEEE Trans. Nucl. Sci.*, **NS-35**(3), 376 (1992).

21. J. M. Weiss and R. L. Shepard, "Evaluation of Advanced Pressure Sensor Technology," pp. 2.01–2.09 in *Proceedings of the 8th Power Plant Dynamics, Control & Testing Symposium*, Vol. 1, May 27–29, 1992.

22. *Oil Loss Syndrome in Rosemount Pressure Transmitters*, compiled by Analysis and Measurements Corporation, 9111 Cross Park Drive, Knoxville, TN 37923, August 1991.

23. M. J. Matthewson and C. R. Kurkjian, "Environmental Effects on the Static Fatigue of Silica Optical Fiber," *J. Am. Ceram. Soc.*, **71**(3), 177–83 (1988).

24. G. D. Brown et al., "Temperature and Humidity Testing of Fiber-Optic Components," *Proc. Int. Society Optical Eng. (SPIE)*, **1174**, 171–6 (1989).

25. K. M. Doty and K. J. Long, "Prediction of Shipboard Fiber-Optic Cable Service Life," *Proc. Int. Society Optical Eng. (SPIE)*, **1174**, 205–18 (1989).

26. Branko Leskovar, "Radiation Effects on Optical Data Transmission Systems," *IEEE Trans. Nucl. Sci.*, **36**(1) (February 1989).

27. *Impact of Fiber Optics on System Reliability and Maintainability*, RADC-TR-88-124, Rome Air Development Center, June 1988.

28. H. Okuda et al., "Radiation Effects on InGaAsP/InP DH LEDs (λ_p = 1.3 μm)," p. 209 in *46th Meeting of the Japan Society of Applied Physics*, 3a-N-1, 1985.

29. C. E. Barnes, "The Effects of Radiation on Optoelectronic Devices," pp. 18–25 in *Proceedings of SPIE–Fiber Optics in Adverse Environments III*, Vol. 721, 1986.

30. *Optical Fibers in Radiation Environments*, EPRI-TR-100367, Electric Power Research Institute, 1992.

31. *Lightguide Digest*, Issue No. 1, AT&T Network Systems, Morristown, NJ (1992).

32. N. J. Bonanno et al., "Handling Optical Fiber During Splicing," *Lightwave*, p. 39 (November 1993).

33. W. Lakas, "New Fiber-Optic Ribbon Cable Design," pp. 4–10 in *Intl. Wire and Cable Symposium Proceedings*, 1986.

34. T. Matsuo, "Composite Submarine Cable Containing Optical Fibers and Pilot Pairs," pp. 123–30 in *Intl. Wire and Cable Symposium Proceedings*, 1986.

35. "Single-Mode Progress: From the Lab to the Field," pp. 71–80 in *Photonics Spectra*, Staff Report, April 1986.

36. B. H. Rose and C. E. Barnes, "Proton Damage Effects on Light-Emitting Diodes," *J. Appl. Phys.*, **53**(3), 1772–1780 (1982).

37. Kofi Korsah and Christina Antonescu, "A Survey of Issues Associated with Microprocessor-Based Protection System Hardware," pp. 751–56 in *Proceedings of the 2nd ASME/JSME Nuclear Engineering Joint Conference*, Vol. 2, San Francisco, March 21–24, 1993.

38. *U.S. Code of Federal Regulations*, 10 CFR 50.49, 1991.

39. J. R. Matras, "Technical Note: Rewriting the Standard on the Functional Requirements for Computers Used in Safety Systems of Nuclear Power Plants," *Nucl. Safety*, **32**(3), 375–79 (1991).

40. *Computers in Nuclear Power Plant Operations*, U. S. Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, Bethesda, MD, September 22, 1992.

41. *A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System*, NUREG-0493, U.S. Nuclear Regulatory Commision, March 1979.

42. Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," IEEE Standard 603-1980.

43. J. Hyne, "Electromagnetic Compatibility in Instrumentation," pp. 127–30 in *Conference on Measurement Instrumentation and Digital Technology*, Melbourne, Australia, October 1984.

NUREG/CR-5904
ORNL/TM-12164
Distribution Category 1RM, 1RV

INTERNAL DISTRIBUTION

1. J. L. Anderson
2. S. J. Ball
3. R. E. Battle
4. M. E. Buchanan
5. N. E. Clapp
6–7. R. L. Clark
8. P. D. Ewing
9. D. N. Fry
10. R. A. Hess
11. D. E. Holcomb
12. S. W. Kercel
13. R. A. Kisner
14–25. K. Korsah
26. R. C. Kryter
27. D. W. McDonald
28. G. N. Miller
29. G. A. Murphy
30. C. E. Pugh
31. R. L. Shepard
32–33. R. T. Wood
34. D. F. Craig
35–36. Central Research Library
37. Y-12 Technical Reference Section
38–39. Laboratory Records Department
40. Laboratory Records ORNL–Record Copy
41. ORNL Patent Section
42. I&C Division Publications Office

EXTERNAL DISTRIBUTION

43. B. Chexal, Electric Power Research Institute, 3412 Hillview Avenue, Palo Alto, CA 94303
44. V. Radeka, Brookhaven National Laboratory, Instrumentation Division, 535-B, Upton, NY 11973
45. M. Sevik, Carderock Division, Naval Surface Warfare Center. Code 1900, Bethesda, MD 20084-5000
46. R. M. Taylor, Leeds and Northup, Sunneytown Pike, North Wales, PA 19454
47. Revis W. James, Electric Power Research Institute, 3412 Hillview Avenue, P.O. Box 10412, Palo Alto, CA 94304-1395
48. Albert J. Machiels, Electric Power Research Institute, 3412 Hillview Avenue, P.O. Box 10412, Palo Alto, CA 94304-1395
49. H. L. Magleby, Idaho National Engineering Laboratory, MS 2406, P.O. Box 1625, Idaho Falls, ID 83415
50. John Matras, Science Applications International Corporation, Las Vegas, NV 89109
51. Barry Simon, General Electric Company, 175 Cartner Avenue, MC 765, San Jose, CA 95125
52. G. Sliter, Electric Power Research Institute, 3412 Hillview Avenue, P.O. Box 10412, Palo Alto, CA 94303
53. Tom Staff, Combustion Engineering, 1000 Prospect Hill Road, P.O. Box 500, Windsor, CT 06095-0500
54. J. W. Tills, Institute for Nuclear Power Operations, 1100 Circle 75 Parkway, Atlanta, GA 30339-3064
55. David Vaglia, Westinghouse Electric Corporation, P.O. Box 355, Pittsburgh, PA 15230-0355
56. Christina Antonescu, U.S. Nuclear Regulatory Commission, RES/EMEB, MS NLS 217B, 5650 Nicholson Lane, Rockville, MD 20852
57. Mathew Chiramal, U.S. Nuclear Regulatory Commission, NRR/HICB, MS 8H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
58. Frank Coffman, U.S. Nuclear Regulatory Commission, RES/HFB, NLN 316, 5650 Nicholson Lane, Rockville, MD 20852
59. Joseph P. Joyce, U.S. Nuclear Regulatory Commission, NRR/HICB, MS 8H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
60. Jerry L. Mauck, U.S. Nuclear Regulatory Commission, NRR/HICB, MS 8H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 10852
61. W. Russell, U.S. Nuclear Regulatory Commission, NRR/ADT, 12G18, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852
62. A. C. Thadani, U.S. Nuclear Regulatory Commission, NRR/DSSA, MS 8E2, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852

63. M. Vagins, U.S. Nuclear Regulatory Commission, ORR, Chief Electrical & Mechanical Engineering Branch, 5650 Nicholson Lane, Rockville, MD 20852

64. J. P. Vora, U.S. Nuclear Regulatory Commission, RES/EMEB, 5650 NIcholson Lane, Rockville, MD 20852

65. J. Wermiel, U.S. Nuclear Regulatory Commission, NRR/HICB, MS 8H3, 1 White Flint North, 11555 Rockville Pike, Rockville, MD 20852

66. C. Michelson, Advisory Committee on Reactor Sa'eguards, 20 Argonne Plaza White 365, Oak Ridge, TN 37830

67. Richard J. Blauw, Commonwealth Edison, 125 South Clark Street, Chicago, IL 60690-0767

68. Tom Starr, Combustion Engineering, Inc., 1000 Prospect Hill Road, P.O. Box 500, Windsor, CT 06095-0500

69. Ron Reeves, Tennessee Valley Authority, 1101 Market Street, Chattanooga, TN 37402

70. Assistant Manager for Energy Research and Development, U.S. Department of Energy, Oak Ridge Operations Office, P.O. Box 2001, Oak Ridge, TN 37831-8600

71-73. Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, TN 37831

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

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

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

NUREG/CR-5904
ORNL/TM-12164

2. TITLE AND SUBTITLE

Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors

3. DATE REPORT PUBLISHED

MONTH	YEAR
April	1994

4. FIN OR GRANT NUMBER
L1798

5. AUTHOR(S)

K. Korsah, R. L. Clark, R. T. Wood

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

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

Oak Ridge National Laboratory
Oak Ridge, TN 37831-6050

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

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

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

A study of significant "new" technologies proposed for use in safety-related instrumentation and controls (I&C) systems of advanced light-water reactors (ALWRs) was performed as part of the *Qualification of Advanced Instrumentation and Control Systems* project conducted for the Office of Nuclear Regulatory Research of the U.S. Nuclear Regulatory Commission (NRC). Templates showing digital protection systems of some ALWR designs and the effect of expected environmental stressors on system components were developed to illustrate functional and qualification issues.

The study also identified optical fiber systems as technologies that are relatively new to the nuclear power plant environment, and examined the failure modes and age-related degradation mechanisms associated with fiber optic cables and components. The data were then used to propose a methodology for identifying circumstances in which accelerated aging should be used in an equipment qualification program for "new" I&C technologies.

An analysis of the *licensee event report* database over a 10-y period (1982-1991) performed under this study showed that the fraction of EMI/RFI-related protection system events is significant compared to traditionally recognized environmental stressors such as elevated temperature. The problem is likely to be even more significant for ALWR safety systems due to the increased use of microprocessor-based technology and software. Thus, it appears that while safety systems in ALWRs will have to be qualified to the same environment as current LWRs, EMI/RFI emissions and susceptibility criteria and guidelines specific to the nuclear power plant environment should be considered. Specific EMI/RFI requirements are addressed in a companion document, NUREG/CR-5941, *Electromagnetic and Radio-Frequency Interference in Safety-Critical I&C Systems*.

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

accelerated aging
age-related degradation
common cause failure
digital trip system
fiber optic communications
fault tolerance
environmental stressors
multiplexing equipment

13. AVAILABILITY STATEMENT
Unlimited

14. SECURITY CLASSIFICATION
(This Page)
Unclassified
(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

NUREG/CR-5904 FUNCTIONAL ISSUES AND ENVIRONMENTAL QUALIFICATION OF DIGITAL PROTECTION SYSTEMS OF ADVANCED LIGHT-WATER NUCLEAR REACTORS APRIL 1994