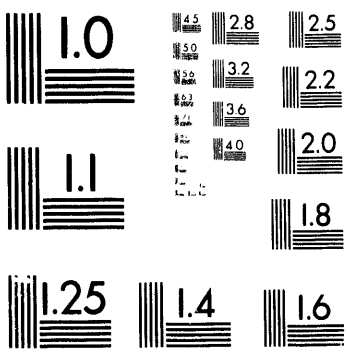

1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0

1 of 6

NUREG/CP-0134

International Atomic Energy Agency Specialists Meeting on Experience in Ageing, Maintenance, and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability

Held at
Rockville, Maryland
May 5–7, 1993

Manuscript Completed: October 1993
Date Published: October 1993

Sponsored by
International Atomic Energy Agency
Vienna, Austria
Electric Power Research Institute
Palo Alto, California
Oak Ridge National Laboratory
Oak Ridge, Tennessee
U. S. Nuclear Regulatory Commission
Washington, D. C.

Proceedings Compiled by
U.S. Nuclear Regulatory Commission



MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Abstract

This report presents the proceedings of the Specialist's Meeting on Experience in Aging, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability that was held at the Ramada Inn in Rockville, Maryland on May 5-7, 1993. The Meeting was presented in cooperation with the Electric Power Research Institute, Oak Ridge National Laboratory and the International Atomic Energy Agency. There were approximately 65 participants from 13 countries at the Meeting. The program chairman was Jerry L. Mauck of the U.S. Nuclear Regulatory Commission.

TABLE OF CONTENTS

	Page
Preface	ix
Introductory Session	xi
Opening Address: Conference Co-Chairman **A. Kossilov**	1
International Atomic Energy Agency (IAEA) "Experience in Ageing, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability"	
Schedule of Main Activities of Working Group in 1993	9
Jerry Mauck, U.S. Nuclear Regulatory Commission (USNRC) "Computer Software Review Procedures"	11
Dan Wilkinson, Electric Power Research Institute (EPRI) "U.S. Utility I&C Upgrade Initiative"	21
Dwayne N. Fry, U.S. Department of Energy Oak Ridge National Laboratory (ORNL) "Aging, Maintenance, and Modernization of Instrumentation at the ORNL High Flux Isotope Reactor"	35
Session #1 **Standards**	42
"License Renewal" - **Scott Newberry**, U.S. NRC	43
"Cable Aging Tests" - **George Hubbard**, U.S. NRC	69
"In-Situ Measurement of Response Time of RTDs and Pressure Transmitters in Nuclear Power Plants" - **H. M. Hashemian** and **J. L. Riner**, Analysis and Measurement Services Corporation	89
Session #2 **Ageing and Maintenance**	148
"Pilot Studies on Management of Ageing of NPP I&C Components" **S.G. Burnay**, United Kingdom, **K. Simola**, Finland, **A. Kossilov**, IAEA, **J. Pachner**, IAEA	149
"Effects of Normal Aging on Calibration and Response Time of Nuclear Plant RTDs and Pressure Sensors" - **H. M. Hashemian** and **J. L. Riner**, Analysis and Measurement Services Corporation	157

Table of Contents
Page two

Session #2 (Continued) Page

"Validation of On-Line Monitoring Techniques for In-Situ Testing of Calibration Drift of Process Instrumentation Channels in Nuclear Power Plants" - **H. M. Hashemian, D. W. Mitchell, D. V. Stansberry**, Analysis and Measurement Services Corporation..... 209

Session #3 **Ageing and Maintenance**..... 262

"Predictive Maintenance of Electrical Components Through Computer-Controlled Acquisition and Trending of Standard Circuit Parameters" - **Gregory Allan** and **Thomas J. Weir** CM Technologies..... 263

"The Effects of Aging on Electrical and I&C Components: Results of U.S. Nuclear Plant Aging Research" - **Satish K. Aggarwal**, U.S. NRC, and **William E. Gunther**, Brookhaven National Laboratory..... 277

"Rosemount Transmitters - Supplement to Bulletin 90-01" - **Deirdre Spaulding**, U.S. NRC..... 285

Session #4 **Modernization**..... 305

"Account of Requirements for Modernization in VPBER-600 Enhanced Safety Reactor Instrumentation and Control System Development" - **S. L. Shashkin, A. B. Pobedonostsev, V. V. Drumov**, OKB Mechanical Engineering, Nizhny Novgorod, Russia and **A. G. Chudin**, Ministry of Nuclear Energy of Russian Federation, Moscow, Russia..... 307

"Regulatory Requirements for Replacement of Analog Systems With Digital Upgrades" - **Paul J. Loeser**, U.S. NRC..... 315

Session #5 **Modernization**..... 333

"Addressing the Susceptibility of Digital Systems to Electromagnetic Interference" - **Paul D. Ewing, Kofi Korsah,** and **Christina Antonescu**, Oak Ridge National Laboratory..... 335

"Life Extension Activities and Modernization Strategies for Instrumentation & Control Systems of Research and Power Reactors in India" - **S. P. Chaganty** and **B. R. Bairi**, Bhabha Atomic Research Centre, Bombay, India.....349

"Regulatory Perspective on Digital Instrumentation and Control Systems for Future Advanced Nuclear Power Plants" - **Matthew Chiramal**, U.S. NRC.....363

Table of Contents
Page three

Page

Session #6 **Modernization**.....391

"Experience in Installing a Microprocessor-based Protection System on a UK Nuclear Power Plant" - **C. D. Jones**, Nuclear Electric Plc, Dungeness 'B' Power Station and **I. C. Smith**, AEA Technology, U.K.....393

"Reactor Safety Instrumentation of Paks NPP" - **Sandor Elo** and **Karoly Hamar**, Hungarian Atomic Energy Commission.....405

"Strategy to Safety Grade Systems Replacements" - **Dr. Michael Stimler**, **Kevin E. Sullivan**, and **Irfan Trebincevic**, SIEMENS, Germany..... 421

Session #7 **Modernization**..... 461

"Instrumentation and Control System Upgrade Plan for Operating PWR Plants in Japan" - **Hirofumi Ishii**, Mitsubishi Atomic Power Industries, Inc., Tokyo, Japan..... 463

"Modernization of the Borssele NPP Reactor Protection System" - **IJ. van der Plas**, Ministry of Social Affairs and Employment, The Netherlands..... 479

"The Role of International Standards in the Design of Modern I&C Systems for Nuclear Power Plants" - **John M. Gallagher**, U.S. NRC.....489

Session #8 **Modernization Issues**.....503

"Software Maintenance and Re-Validation for Nuclear Power Plants" - **R. G. Phoenix**, Rolls Royce and Associates, UK..... 505

"Reliability Analysis of Microprocessor-Based Control and Protection Systems in Nuclear Power Plants" - **John S. Wiesemann**, **Glenn E. Lang**, and **Gilbert W. Remley**, Westinghouse Electric Corporation.....515

"Recent Activities Within Nuclear Electric Related to the Qualification of Digital Systems and the Extension of Maintenance Intervals" - **G. P. Holt**, Nuclear Electric, UK..... 531

"Qualification Issues Associated with the Use of Advanced Instrumentation and Control Systems Hardware in Nuclear Power Plants" - **Kofi Korsah**, Oak Ridge National Laboratory, and **Christina Antonescu**, U.S. NRC..... 547

List of Participants..... 561

PREFACE

The International Atomic Energy Agency (IAEA) Specialists' Meeting on "Experience in Ageing, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability" took place in Rockville, MD at the Ramada Inn, May 5-7, 1993. This Specialists' Group is under the Nuclear Power Plant Control and Instrumentation International Working Group. The International Atomic Energy Agency, the U.S. Nuclear Regulatory Commission, the Electric Power Research Institute, and the Oak Ridge National Laboratory sponsored the meeting. Representatives from Austria, Finland, Germany, Hungary, India, Japan, The Netherlands, Spain, Sweden, Switzerland, United Kingdom, and the United States attended.

28 papers were presented. The opening papers were presented by Dr. Andrei N. Kossilov of the International Atomic Energy Agency; Jerry L. Mauck, U.S. Nuclear Regulatory Commission; C. Dan Wilkinson, Electric Power Research Institute; and Dwayne N. Fry, U.S. Department of Energy - Oak Ridge National Laboratory.

Many of the participants arrived a little early and attended the U.S. Nuclear Regulatory Commission's large **Regulatory Information Conference (RIC)** being held across the street at the Holiday Inn Crowne Plaza from May 4-5, 1993. The "Digital Instrumentation and Control Systems" breakout session at the RIC held on May 4, 1993 was of particular interest to the group.

The highlights of the IAEA May 7 banquet were the presentations by Carlton R. Stoiber, Director, Office of International Programs, U.S. Nuclear Regulatory Commission, and William T. Russell, Associate Director for Inspection and Technical Assessment, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission. The meeting concluded Friday afternoon, May 7.

INTRODUCTORY SESSION

Experience in Ageing, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability

Computer Software Review Procedures

U.S. Utility I&C Upgrade Initiative

Aging, Maintenance and Modernization of Instrumentation at the ORNL High Flux Isotope Reactor

Specialists' Meeting

on

EXPERIENCE IN AGEING, MAINTENANCE AND MODERNIZATION OF INSTRUMENTATION AND CONTROL SYSTEMS FOR IMPROVING NUCLEAR POWER PLANT AVAILABILITY

5 to 7 May 1993, Rockville, Maryland, USA

Welcoming Address

A. Kossilov

International Atomic Energy Agency

Mr. Chairman, Ladies and Gentlemen,

It is my pleasure to welcome you on behalf of the International Atomic Energy Agency to this Specialists' Meeting on "Experience in Ageing, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability".

The meeting is being held within the framework of the programme of the International Working Group on Nuclear Power Plant Control and Instrumentation and is convened with the support of the US Nuclear Regulatory Commission, the Electric Power Research Institute and the Oak Ridge National Laboratory.

Before continuing, let me first express the Agency's gratitude to the Government of the USA for hosting this meeting, and for providing the opportunity to participants from all over the world to exchange information and experience.

Automation of large, complex industrial processes is an established feature of modern society. In the development of nuclear power plants throughout the world there has been an increasing trend towards the use of automation. However, special features of nuclear power plants require that increased attention be paid to important factors relevant to automation. These factors include:

- The need to achieve and maintain high levels of safety and reliability

- The need to increase the reliability of electricity production from nuclear power plants

- The need to control plant operations (including maintenance) with increasing optimization in order to improve plant performance and plant life

- Increases in plant size and complexity and hence capital investment, which require increased levels of protection and assurance

- Requirements in monitoring and instrumentation technology, which generate increased amounts of data and the consequent need to process and handle this information.

Therefore the task you have before you this week - increasing understanding of the proper role of instrumentation and control in nuclear power plants - is both important and timely.

The advances in computer technology have been phenomenal in recent years. The use of powerful personal computers and workstations is widespread in all sectors of industry. In nuclear power technology computers are used in design, engineering, operation and maintenance, and their role has grown steadily in the last decade. The use of computers has been extended from its traditional role in the manipulation of large quantities of numerical data and mathematical equations to its more current role of fast and accurate processing of information and knowledge. Digital technology has been increasingly recognized as a valuable tool for the support and enhancement of human capability in the areas of monitoring, diagnostics, control, maintenance, surveillance and communication.

Many functions in nuclear power plants are performed by a combination of human actions and automation. Increasingly, computer-based systems are used to support operation and maintenance personnel in the performance of their tasks. There are many benefits which

can accrue from the use of computers, but it is important to ensure that the design and implementation of the support system and the task to be performed places the person in the correct role in relation to the machine; that is, in an intellectually superior position, with the computer serving the human. In addition, consideration must be given to such important factors as computer system integrity, software validation and verification and consequences of error. To achieve a balance between computer and human actions, the design process must consider each operational function as pertaining either to computer or to human operation or, what is more common in nuclear plants, to a combination of human and computer functions.

The impact of computer systems on safety must not be forgotten. The features that produce the financial benefits may act either to improve safety, if correctly implemented, or to reduce safety, if poorly conceived and executed.

Fortunately, many of the features of computerized process control systems can, if properly designed and engineered, have a positive impact on safety. Calculations can be performed in real time which enable safety margins to be determined more precisely. Plant health monitoring can be integrated into the control structures. Unsolicited changes in plant status can be detected. Many of these safety improvements flow from the increase in information gathering and manipulation. With regard to the human operator, it is possible to automate more of his tedious routine tasks or those tasks that require a rapid response under difficult circumstances. A well-structured operator console with properly organized data presentation will have a significant positive effect on safety.

The current IAEA programme on control and instrumentation, nuclear power plant computerization and man-machine interface studies promotes technical information exchanges among Member States with major research and development programmes, offers assistance to Member States with an interest in exploratory or research programmes, and publishes reports available to all Member States interested in the current status of development. The IAEA activities are co-ordinated by the International Working Group on Nuclear Power Plant Control and Instrumentation (IWG-NPPCI) which meets periodically to review the national

programmes of the countries, and to advise the IAEA on its technical meetings and activities where current progress, problems and operating experience are discussed.

Since not all countries have adequate resources for work in the man-machine interface field, it was recommended by the members of the IWG-NPPCI that the IAEA could provide a great service by co-ordinating information on the topic. The hosting of conferences, the convening of technical committees to analyse and summarize the state of the art and the publishing of status documents would provide significant assistance to Member States. Such information exchange would also help in reducing the duplication of efforts by Member States.

In the past 15 years or so, there has been a steady increase in both the production, reliability and safety of computer-based equipment used to automate plants. As a result, there has been less resistance to the use of automation. By suitable design, using redundant, diverse or distributed systems, design availability and reliability targets can be readily met. Availabilities in excess of 98-99% are commonly achieved.

As digital technology becomes increasingly available and economical, there is a trend by designers to produce more integrated systems which encompass many aspects of plant monitoring and control. Additional operator support functions are being incorporated, particularly to support fault identification and analysis and to extend critical function monitoring and present procedures on graphical CRT displays. These developments are taking place in many design organizations and utilities throughout the world and reflect a desire on the part of all operating staff and managements to provide improved monitoring of plant operations and added assurances regarding safety. Increased use is also being made of robotics for maintenance activities, particularly in areas of the plant with arduous conditions.

The use of expert systems with artificial intelligence and techniques has become more of a working reality. Many applications are employing such devices in non-critical operational roles, such as personal advice consultation systems, diagnostic features, rule compliance monitors, etc. In some cases, such devices are being evaluated in roles critical for safety. Developments are expected to appear in areas such as rule-based monitoring and

abnormality diagnosis, together with the creation of advanced information systems which embody information filtering, reduction and processing features.

The increasing use of computer capability to enhance operator performance has led to changes in the role of operating staff from the traditional role of equipment operator to a new role of high-level information system manager. Computer-based support systems provide increased operator support via improved information displays which aid the perception of the operating state. Incorporating fast, real-time simulators into the normal control interface is another possibility under consideration. This could make it possible to predict the results of operator actions and thus, to improve the quality of decision-making, particularly in complex situations.

A key feature of operator support systems is their ability to structure data to increase its relevance to a given situation. This can improve the user's ability to identify the state of the plant's functional systems and components, as well as to identify faults and diagnose them. Operator support systems can also assist the user in planning and implementing corrective actions. In addition to improving availability, operator support systems can be increasingly used to improve safety. Also, applications are being developed to aid maintenance and to extend the lifetime of the plant components.

Taking these developments and objectives into account, the Agency has started in 1992 the Co-ordinated Research Programme on "Operator Support Systems in Nuclear Power Plants" which will provide guidance and technology transfer in the development and implementation of operator support systems, including the experience with man-machine interface and closely related issues such as control and instrumentation, the use of computers and operator qualification.

The present situation in the nuclear industry is characterized by a decreasing number of new plants and an increasing amount of installations where backfitting measures are to be expected. Instrumentation and control equipment in nuclear power plants have a special role, because their technological life span is about ten years and the innovation time even shorter. Considering the fact that the mechanical systems of the plant are designed for a lifetime of

30 to 60 years, the instrumentation and control equipment, or part of it, has to be backfitted or modernized several times in order to achieve the required availability and safety.

The need for frequent backfitting of instrumentation and control systems arises from specific conditions:

- Rapid obsolescence of technologies as a consequence of which new designs with new operational characteristics have to be employed

- The high potential for improving and broadening I&C application to achieve improved on-site operational benefits at relatively low cost.

- New regulatory requirements.

The main idea of upgrading the instrumentation and control systems in nuclear power plants is to take advantage of modern technology to improve plant availability and to reduce instrumentation and control's contribution to escalating operating and maintenance costs. Modern instrumentation and control technology, using analog and digital equipment to the best advantage, brings increased reliability and safety.

The IAEA programme intends to define the steps to be followed when modernizing the instrumentation and control equipment and systems including the computers and software used for data logging and information processing. This programme extends from planning and organization to technical realization. Emphasis should be placed upon problem areas and how they were solved, and on where and how improvements could be made by introducing new equipment or systems.

The main objective of this meeting is to provide a forum for exchange of information among the participating experts from member states through their interactions both at this meeting and later through the publication of the meeting's proceedings which will reach a much wider audience. I believe that the information exchange in the coming days will make an important contribution to reaching our common goal of achieving a high level of nuclear

performance and safety. The results of this meeting should help to clarify the main issues for future work, both for you and for us in the IAEA.

Concluding, I wish to express our gratitude to the US Nuclear Regulatory Commission, the Electric Power Research Institute and the Oak Ridge National Laboratory for all arrangements which have been made, especially to the representative of the USA to the International Working Group on Nuclear Power Plant Control and Instrumentation, Mr. J.L. Mauck, also to Mr. C.D. Wilkinson of the Electric Power Research Institute, and Mr. D.N. Fry of the Oak Ridge National Laboratory and their colleagues who all did an excellent job in organizing the meeting.

And, to all of you, I wish a successful and productive meeting.

1993-04-28
AKossilov/jd/usa-wa

IAEA
International Working Group on Nuclear Power Plant Control and Instrumentation (IWG-NPPCI)

THE MAIN ACTIVITIES IN 1993

1. SPM on Experience in Ageing, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability, 5-7 May, 1993, Rockville, Maryland, USA

2. SPM on Operator Support Systems in Nuclear Power Plants, 17-21 May, 1993, Moscow, Russia

3. SPM on Improvements in Nuclear and Radiation Instrumentation for Nuclear Power Plants: Impact of experience and New Technologies, 18-20 October 1993, Paris, France

4. Technical Committee (IWG) on Nuclear Power Plant Control and Instrumentation, (Regular Meeting of the IAEA IWG-NPPCI), 21-22 October 1993, Paris, France

5. Consultancy on Guidelines for validation, verification and licensing of software related to control and instrumentation, 14-18 June 1993, Vienna, Austria

6. Technical Committee Meeting on Reliability of Computerized Safety Systems (in co-operation with the Division of Nuclear Safety), 21-25 June 1993, Vienna, Austria

7. Interregional Training Course on NPP Control and Instrumentation, 19 April-19 May 1993, Karlsruhe, Germany

8. Technical Committee Meeting on the Use of Diagnostic Systems to Monitor Performance of Safety Related Equipment (in co-operation with Division of Nuclear Safety), 11-15 October 1993, Vienna, Austria

---

SPM - Specialists Meeting

For detailed information please contact:

Mr. A. Kossilov
Scientific Secretary (IWG-NPPCI)
IAEA, P.O. Box 100
Vienna International Centre
Wagramerstrasse 5
A-1400 Vienna
Austria
Tel: 1 2360 ext. 2796 **Telex: 1-12645**
Fax: 1 234 564 **E-mail: NEI@IAEA1**

COMPUTER SOFTWARE REVIEW PROCEDURES

J. L. Mauck
U.S. NUCLEAR REGULATORY COMMISSION
INSTRUMENTATION AND CONTROLS BRANCH

INTRODUCTION

Future trends are toward increased use of computer based designs to encompass more plant instrumentation and control (I&C) functions and to ensure that the latest I&C requirements are met. An important consideration for these applications is computer architecture designs that permit easy change or addition, thus minimizing equipment obsolescence. These trends affect both control and safety system functions in many applications in nuclear power plants. Plants in the United Sates that have implemented computer retrofits are listed in the attached table.

With the proper hardware design, the use of software in instrument control can provide excellent functional performance while allowing for rapid, minimum impact changes in instrument function when needed. Incorporating new computer based technology within safety-related system nuclear power plants introduces a positive potential for improving overall system performance, while at the same time creating, a potential for introducing new system failure modes within the computer software architecture.

The Nuclear Regulatory Commission (NRC) review performed on the hardware portion of the computer is consistent with that which has been performed for past analog systems. That is, our review of the computer hardware should lead to the a conclusion that the appropriate 10 Code of Federal Regulation (CFR) 50 General Design Criteria (GDC) are met, including applicable Institute of Electronic and Electrical Engineers (IEEE) standards and the appropriate regulatory guides. In particular, IEEE-279-1971 requirements have to be met including manual initiation capabilities, control/protection system interactions, physical separation and independence and testability.

The one area that is not sufficiently covered by the regulatory criteria used in past staff reviews was the validity, qualification level, and reliability of resident software. Standards and regulations have emerged which impose new guidance for independent V&V on software intended to be used to perform safety related functions. Acceptable system V&V has been recognized as a means to bridge the gap between known hardware safety requirements and the software qualification requirements needed for safety systems. A previously planned, systematic, independent V&V effort integrated with system development offers a means for formal documented developmental steps, better hardware and software interfaces, and a configuration management of system documentation. These records will provide a mechanism for regulatory review and approval.

DISCUSSION

The importance of digital systems reliability and in particular a strong software development and maintenance program, cannot be over emphasized when considering the potential for software

initiated failures. This presents a summary of the NRC criteria and review approach used for digital retrofit reviews. This description is not all inclusive of the questions asked and material reviewed and referenced, but does cover the major areas.

Currently, the NRC uses Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants" and ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations" for guidance when performing reviews of digital systems. Although other software standards such as ANSI/IEEE Std. 1012-1986, "IEEE Standard for Software Verification and Validation Plans," and ASME NQA-2a-1990, Part 2.7, "Quality Assurance Requirements of Computer Systems for Nuclear Facility Applications, American Society of Mechanical Engineers" are used for reference, licensees are generally held responsible for conforming to ANSI/IEEE-7-4.3.2-1982.

The staff performs a detailed review of the system design process and the software verification and validation program. At this stage, the staff is looking programmatically at the design process and making comparisons to the applicable review guidance. The staff reviews available information on the software and hardware history including previous software and hardware failures. The staff reviews the specific plant application including any special features that were required. The staff reviews the specific verification and validation (V&V) performed on the software used in the application. This is a detailed review and includes (1) following the code development, (2) examining the vendor/licensee interface and feedback process, (3) reviewing software problem/error reports and resulting corrections, (4) comparing the V&V process to ANSI/IEEE ANS-7-4.3.2-1982, (5) interviewing personnel involved in the process, (6) verifying the independence of the software verifiers, (7) reviewing the development of the functional requirements and subsequent software development documents, (8) reviewing software life-cycle and future vendor/licensee interface, and (9) reviewing the verification and validation results. The staff also performs a "thread audit" which consists of picking a sample of plant parameters and tracing the software implementation of these parameters from the purchase specification and development of the functional requirements to the writing and testing of the code. This review includes (1) reviewing actual sections of the code on a sample basis, (2) examining the various levels of software development documents and comparing them to the code, (3) examining problem reports and verifying the corrections, (4) examining the engineering cross-discipline interfaces to ensure that nuclear specific needs were correctly incorporated into the code, (5) examining the licensee interface to ensure plant specific requirements are correctly incorporated, (6) ensuring that the verification and validation process is followed according to the vendor's plan, and (7) reviewing the final results of the process. Finally, the software and hardware are reviewed as a system looking for potential timing and software/hardware problems. At the end of the review, all of the information is collated to establish a benchmark for assessing the software safety system performance and reliability.

1. Licensee/Vendor Interface

Experience with computer projects has demonstrated that the development of computer system functional requirements can have a significant impact on the quality and safety of the

implemented system. (ANSI/IEEE ANS-7-4.3.2-1982, Sec. 3) In fact, there have been recent software failures attributed to software functional requirements and system specifications that did not accurately reflect plant specific idiosyncrasies. This has placed additional emphasis on the importance of the licensee/vendor interface during software development and is an important factor when assessing software reliability and quality. The staff considers the correctness of the functional requirements by reviewing the process for the development of these requirements, concentrating on the licensee/vendor interface, the changes that were made, and the qualifications of the personnel involved. Personnel from all relevant disciplines should have been part of the process.

2. Verification and Validation Organization

The verification group shall be independent of the design team and shall have technical qualifications comparable to the design team. (ANSI/IEEE ANS-7-4.3.2-1982, Sec. 7.1) The verification and validation (V&V) organization should be independent from the software development group with separate supervisory engineers and composed of personnel with comparable technical qualifications to the development group. The development group should submit the code to the V&V group after writing and debugging the code. The V&V group should then review the code according to the V&V plan and produces a V&V report. Communications between the software development group and V&V personnel should be documented in written, traceable reports. In order to be acceptable, the independence of the V&V group and the V&V personnel should conform to ANSI/IEEE-ANS-7-4.3.2-1982. Additional guidelines for this portion of the review can be found in ANSI/IEEE 1012, "IEEE Standard for Software Verification and Validation Plans" and IEC 880, "Quality Assurance Requirements of Computer System at Nuclear Facility Applications".

3. Verification and Validation Program Review

The verification and validation (V&V) of the digital system is a formalized program that includes detailed procedures and policies for technical review and audit functions, software reviews and audits, software test and analysis, dynamic system testing simulating normal and design basis events, and an independent stage-to-stage verification performed by knowledgeable individuals. (ANSI/IEEE-ANS-7-4.3.2-1982, Sec. 3.7) The vendors V&V program should be described in documentation submitted to the staff. The V&V group should perform several tasks before they approve the release of the software code including: (1) document code reviews; (2) test case development; (3) verification and validation testing; and (4) abnormal conditions review. After the development group submits the code to the V&V group, each independent verifier should receive one or more modules on which a document code review and evaluation is performed. The evaluation is based upon the module's conformance to the functional requirements and the design and coding standards.

Although the verifier's primary focus at this stage is a comparison between the functional requirements document and the code, the software development documentation should also be verified for consistency and integrity starting from the functional requirement and including the

system design requirement, the system design specification, and the functional decomposition document.

After completing the walk-through of the design documents and the source code walkthrough, the verifier develops two types of test cases, i.e. verification tests and validation tests.

The method and rigor used for verification tests is a function of the safety classification of the software module as defined by ANSI/IEEE Std. 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronic Engineers." By this standard, software associated with the actuation and/or implementation of reactor trips, engineered safety features, and information displays for manually controlled actions receives the highest level of verification. The verification tests are further partitioned into structural testing and functional testing. Guidelines for testing methods can be found in IEEE 829, "Software Test Documentation".

The structural testing (whitebox) ensures that all source lines meet the intended design specification. To determine the rigor and method of this testing, the verifier follows an established set of criteria based on the software uniqueness and complexity. After applying the criteria, the verifier should then read the code and derive the structural test cases that will exercise all of the statements. Next the verifier performs either manual structural testing or computer emulation. For bounded input values, the verifier chooses values to exercise the lower limit, the upper limit and at least one random intermediate value. Particular attention should be given to out-of-range and other abnormal input variables such as negatives and zeros. The functional testing is similar to the structural testing except that the functional properties are the basis for the functional testing and are provided by the Design Specification.

When software errors or coding discrepancies are found, the verifiers should generate either a Procedure Problem Report or a Generic Problem Report. Each software module contains several procedures so that a Procedure Problem Report concerns defects in the smallest software unit. A Generic Problem Report pertains to problems that cross module boundaries and involve multiple modules. A log of the reports should be kept and their status tracked by the V&V group. The developer has the responsibility to resolve these reports and if a code modification is required, the verifier performs regression testing until the module satisfactorily passes the test. The Lead Verifier ensures that no problem reports remain open upon release of the module.

Once the verification results are accepted, the software is installed in the target hardware and the verifiers should check hexadecimal and check sum values for consistency. The hardware/software should then be validated.

The validation process emphasizes the system functionality of the target hardware/software. The major phases of the validation testing are: (1) "top-down" functional requirements testing; (2) Abnormal conditions review of the design and its implementation; and (3) specific MMI testing.

The Validation Test Engineer derives test cases from the decomposition of the functional requirements into sub-requirements and looks for functional and abnormal conditions to test. Once the tests are derived, a Validation Test Technician executes the tests on the verified

software now residing in the final target hardware. The Validation Test Engineer then reviews the test results.

An abnormal conditions review can also be used to ensure that the design operates properly under abnormal-mode conditions and to ensure that the system rejects unpermitted inputs (including out of range inputs). This review is primarily directed at the internal structure of the system software and is used to complement the functional testing and evaluate integrated system integrity.

As part of the programmatic review of the V&V program, the staff reviews software development documents, interviews V&V managers, and reviews various V&V summaries and reports. The staff also randomly samples problem reports. In the reports reviewed, defects are documented and analyzed for significance.

Based upon the above review and comparison of the V&V Process/Plan to ANSI/IEEE ANS-7-4.3.2-1982, the staff confirms that the licensee/vendor program as reviewed, complies with Regulatory Guide 1.152 and ANSI/IEEE ANS-7-4.3.2-1982. To obtain a benchmark for evaluating V&V effectiveness and the licensee application, the staff then performs a "thread audit." Guidelines for this portion of the software review can be found in ANSI/IEEE 1012 and IEC 880.

4. NRC Thread Walk-through

The staff conducts a "thread audit" walk-through of a chosen parameter. The "thread audit" traces the software development of the chosen parameters and includes reviewing the software development documentation, sections of the code and comparing the software development documentation to the code. The thread audit includes the validity test of the functional requirements and how they relate to the software requirements. While performing this review, the staff confirms that all errors have corresponding problem reports and appear to be identified by the V&V process when applied to the functional code. If these problems are not identified by V&V, they present the staff with two concerns. The first is a question regarding verification thoroughness and effectiveness which is discussed in the defense-in-depth section below. The second is whether flawed development documents and comment errors could mislead a software writer during future code revisions. Therefore, the staff should ask how these errors will be resolved, and for an analysis of the root cause of the errors.

Based on the "thread audit" and the V&V program reviewed above, the staff confirms that the licensee application complies with Regulatory Guide 1.152 and ANSI/IEEE AN-7-4.3.2-1982.

5. Configuration Management

All software code and software documentation should be kept under strict configuration management control. Any software changes other than tunable parameters should be made through a licensee controlled modification program that has a librarian to control changes to the

code. When software is changed, the licensee should execute an analysis tool to determine the side effects resulting from code changes and to evaluate the impact on the code. Furthermore, all modified code should be subject to verification and validation as described above. The configurations management plan should follow the guidelines of IEEE 828-1983, "Software Configuration Management Plans".

CONCLUSION

Based on the foregoing review, the staff will confirm that the licensee/vendor verification and validation plan/program complies with Regulatory Guide 1.152 and ANSI/IEEE AN-7-4.3.2-1982 and that the licensee's application of the verification and validation plan/program meets its functional and design requirements.

The following are plants in the United States that have performed analog to digital modifications for Safety Systems

REVIEW PERFORMED

PLANT	SYSTEM	VENDOR	YEAR
Haddem Neck	Reactor Trip System	Foxboro Spec 200 μ	1990
Zion	Signal conditioning and bistable portion of Reactor Trip System	Westinghouse Eagle 21	1992
Watts Bar	RTD Bypass	Westinghouse Eagle 21	1989
Sequoyah	Signal conditioning and bistable portion of Reactor Trip System	Westinghouse Eagle 21	1990
Turkey Point	Emergency Diesel Generator sequencer and RTD bypass	Allen Bradley / Eagle 21	1991
South Texas	Qualified Safety Parameter Display System	Westinghouse	1987
ANO2 San Onofre Palo Verde	Core Protection Calculator upgrade	Combustion Engineering	1990

The following are plants in the United States that have performed analog to digital modifications for Safety Systems

REVIEW PERFORMED (Continued)

Big Rock Point	Neutron Flux Monitoring	General Electric NUMAC	1989
Vogtle & Beaver Valley	Plant Safety Monitoring System	Westinghouse	1987 1989
Turkey Point	Load Sequencer	Allen Bradly PLC	1992
Prairie Island	Load Sequencer	Allen Bradly PLC	1993
Haddam Neck	Aux Feed	Woodward	1992
Prairie Island, Diablo Canyon, Ginna, Salem	Feedwater (trip Removal)	Westinghouse / DPF	1989/ 1993

The following are plants in the United States that are performing analog to digital modifications for Safety Systems

UNDER REVIEW

D.C. Cook	Signal Conditioning and Bistable portion of the Reactor Trip System	Foxboro Spec 200μ	1993
Brunswick	leak detection	GE NUMAC	1993
Browns Ferry	Radiation Monitoring	GE NUMAC	1993
Diablo Canyon	Signal Conditioning and bistable portion of the Reactor Trip System	Westinghouse Eagle 21	1994
Kewaunee	Radiation	Nuclear Research	1994
Watts Bar	Signal Conditioning and Bistable Portion of the Reactor Trip System	Westinghouse Eagle 21	1993
Palo Verde	DAFAS /ATWS (Safety)	Modicon PLC	1992

The following are plants in the United States that have performed analog to digital modifications for Safety Systems

NO REVIEW PERFORMED

Numerous	Rad Monitoring	Unknown
Numerous	ATWS Systems/Safety NM-Safety	Westinghouse Allen Bradly Foxboro Custom, etc.
Peach Bottom	Signal Conditioning and Bistable Portion of Trip Systems	Foxboro

US Utility I&C Upgrade Initiative

presented to
IAEA Specialists Meeting
on
Experience in Ageing, Maintenance and Modernization of I&C Systems

Rockville, MD
May 5, 1993

Dan Wilkinson
EPRI

Background

- **I&C Initiative — Why?**
  - Address growing obsolescence
  - Improve availability, reliability, safety
  - Provide industry-focus on I&C
- **Strategic Goal**
  - I&C modernization in 10 nuclear plants by year 2000

Background (cont.)

Industry Benefits From This Initiative

- Coordinated strategy involving US utilities, vendors, government, standards groups and foreign participants
- Utility driven results in a timely manner
- Greater standardization of modern technology
- Lower cost to utilities (single vs. multiple users)
- Generic regulatory review to optimize cost and schedule for acceptance
- More reliable vendor pool

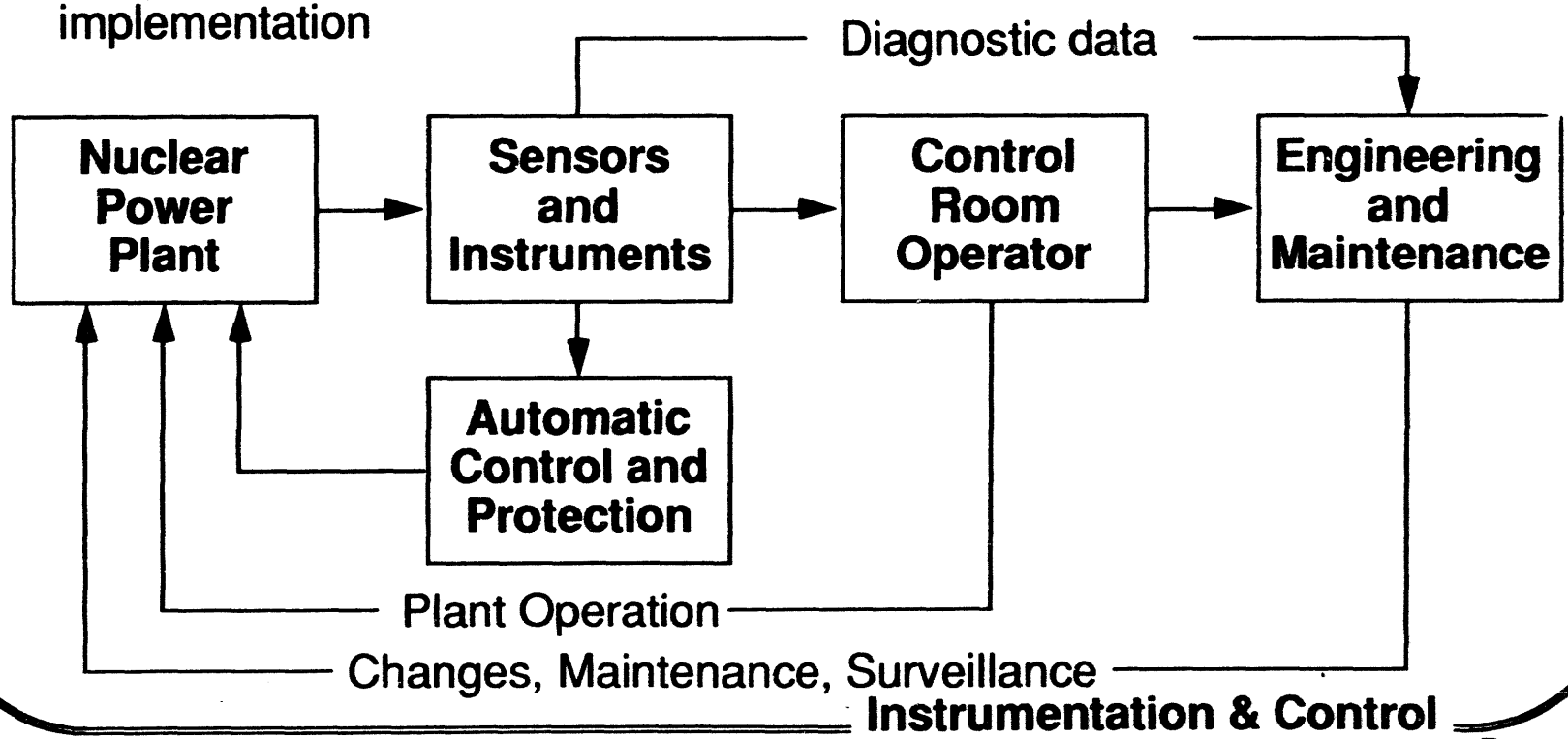
Integrated Instrumentation and Control

Overall
- Software V&V
- Communications
- Stds. & requirements
- Integrated I&C plan implementation

- Instrumentation
- Control & Protection

- Man/Machine Support Systems

- Maintenance



I&C Upgrade

- Experience Evaluation
  - NSAC 153, Vol. I, I&C Workshop
  - NSAC 153, Vol. II, Recommendations
- Industry Plan
  - NP7343, Rev. 3, Dec., 1992
- Upgrade Methodologies & Guidelines
- Demonstration Plants

OBJECTIVES OF UPGRADE DEMONSTRATIONS

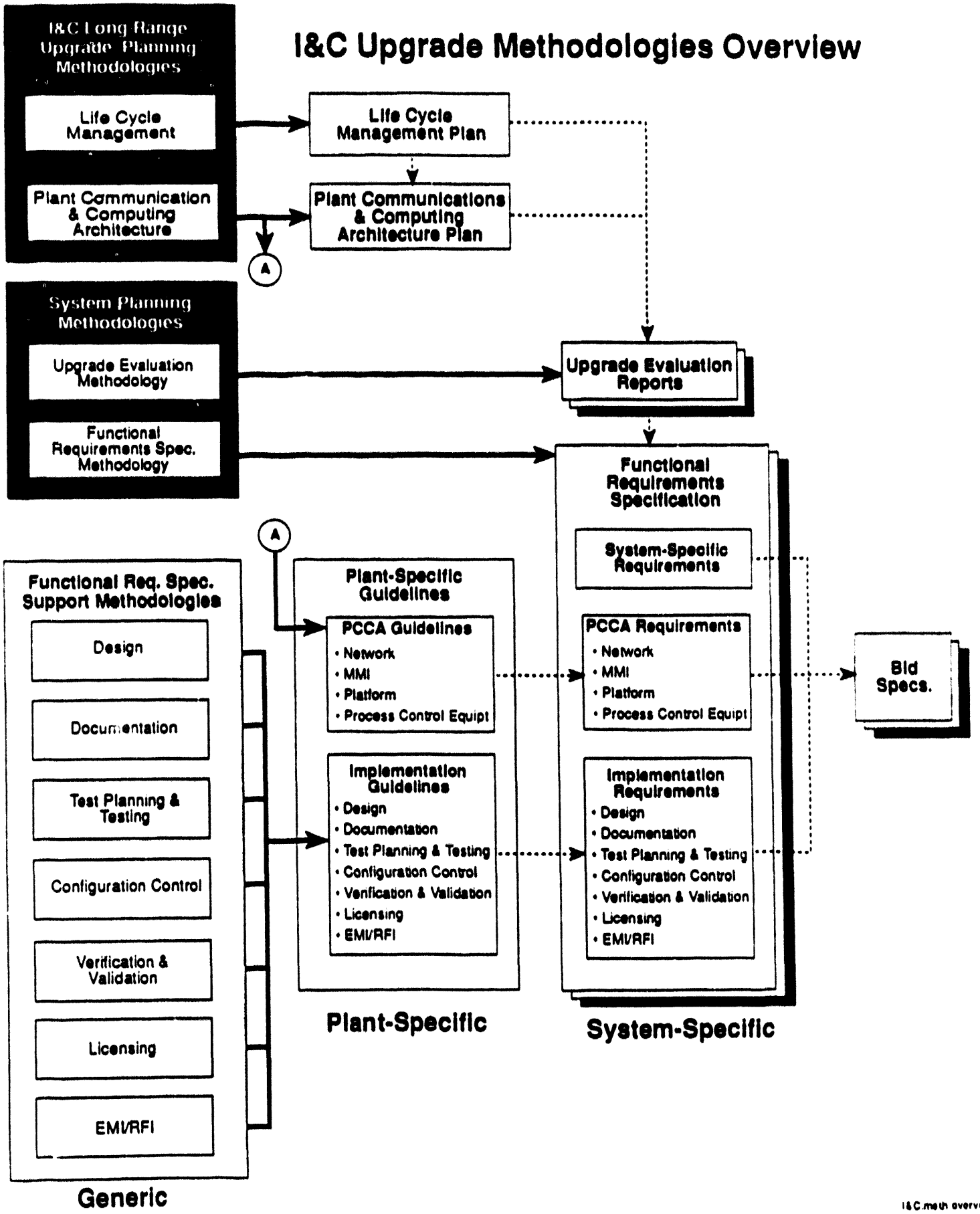
- Address obsolescence
- Improve reliability and functionality
- Plant-wide integration of modern technology and R&D results
- Develop generic methodologies, guidelines, and information
- Demonstrate generic applicability - all four NSSS types
- Obtain feedback for needed R&D projects
- Develop stable regulatory approach for digital technology

Bottom Line:
Reduce costs and shorten "learning curve" for modernizing I&C

Demonstration Plant Planning

- Focus of upgrade planning
  - Life cycle planning
  - Communication network architecture
  - System evaluation
  - Generic and specific licensing activities
  - Plant specific upgrade plan
  - Sharing lessons learned and methodologies
- Demonstration plant technical interaction group
- Upgrade ten plants by 2000

I&C Upgrade Methodologies Overview

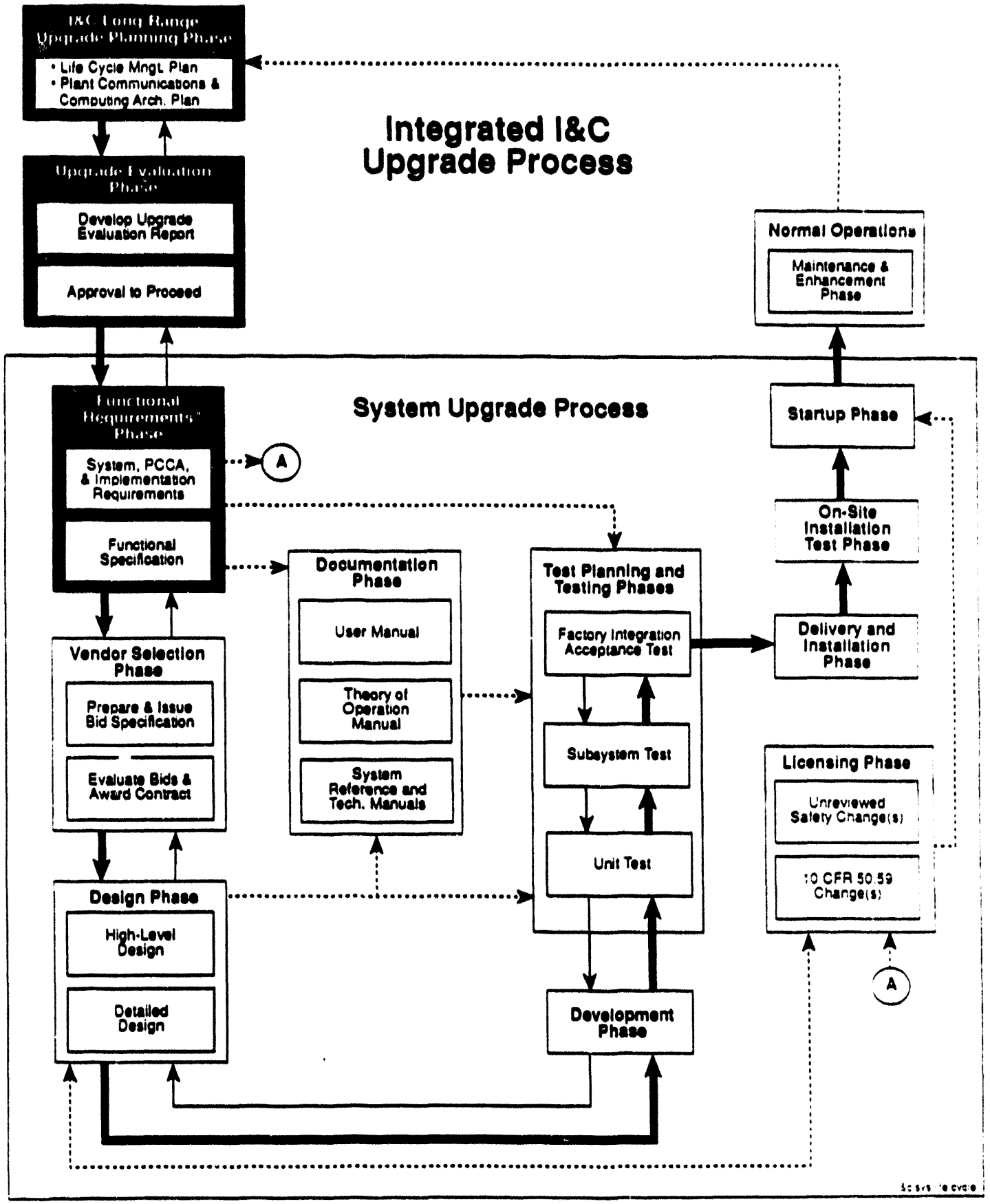


Shaded Areas Indicate Methodologies Needed For Developing:

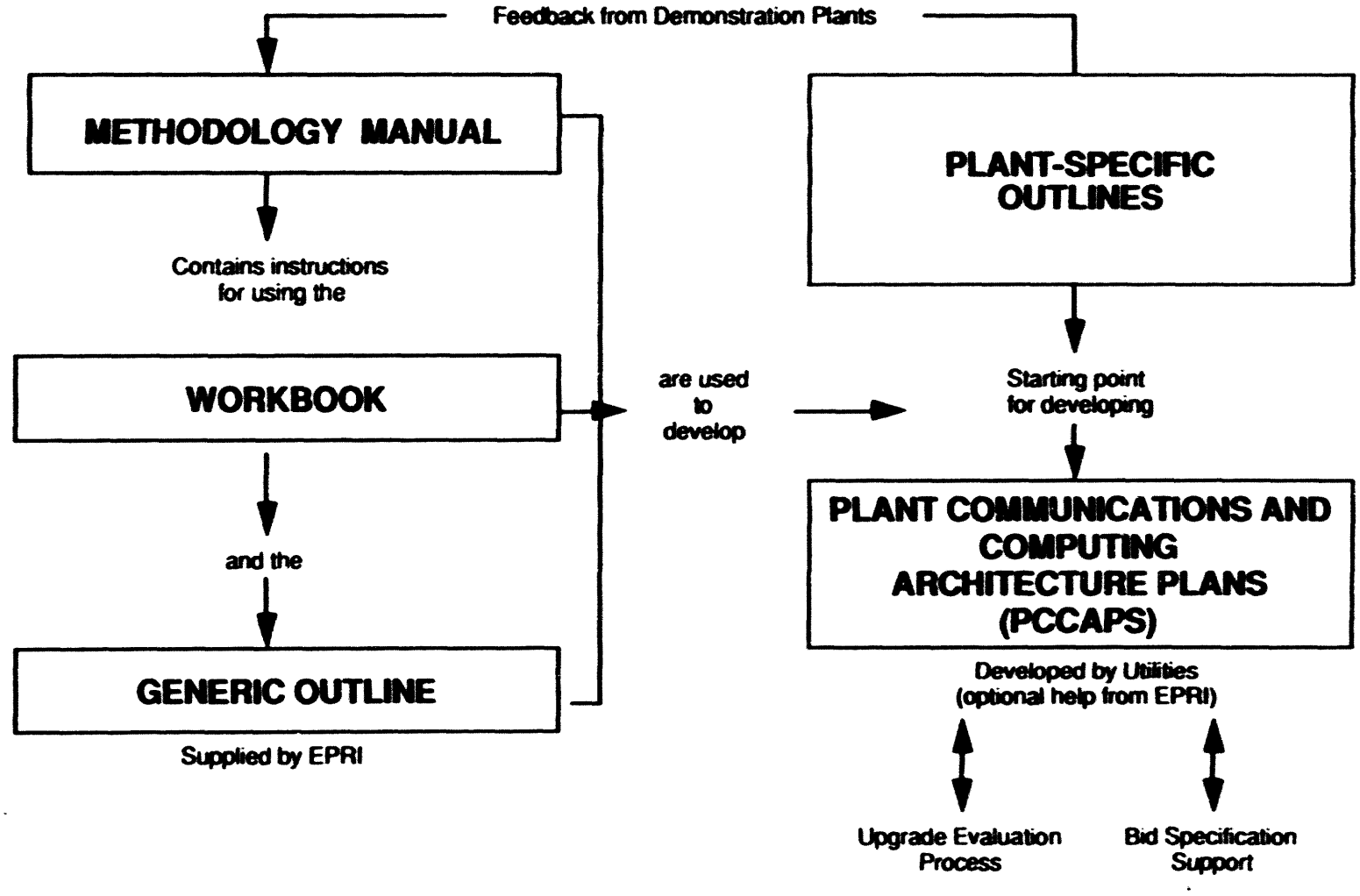
- Plans, Architecture Guidelines, and System Documents
- Vendor Implementation Guidelines

Main Path

Output Input


I&C Long Range Upgrade Planning Phase
• Life Cycle Mngt. Plan
• Plant Communications & Computing Arch. Plan
Integrated I&C Upgrade Process
Upgrade Evaluation Phase
Develop Upgrade Evaluation Report
Approval to Proceed
Normal Operations
Maintenance & Enhancement Phase
System Upgrade Process
Functional Requirements Phase
System, PCCA, & Implementation Requirements
Functional Specification
A
Startup Phase
On-Site Installation Test Phase
Documentation Phase
User Manual
Theory of Operation Manual
System Reference and Tech. Manuals
Test Planning and Testing Phases
Factory Integration Acceptance Test
Subsystem Test
Unit Test
Delivery and Installation Phase
Vendor Selection Phase
Prepare & Issue Bid Specification
Evaluate Bids & Award Contract
Licensing Phase
Unreviewed Safety Change(s)
10 CFR 50.59 Change(s)
Design Phase
High-Level Design
Detailed Design
Development Phase
A
Shaded Areas Indicate Methodologies Needed For Developing:
Plans, Architecture Guidelines, and System Documents
Vendor Implementation Guidelines
Main Path
Feedback
Output Input

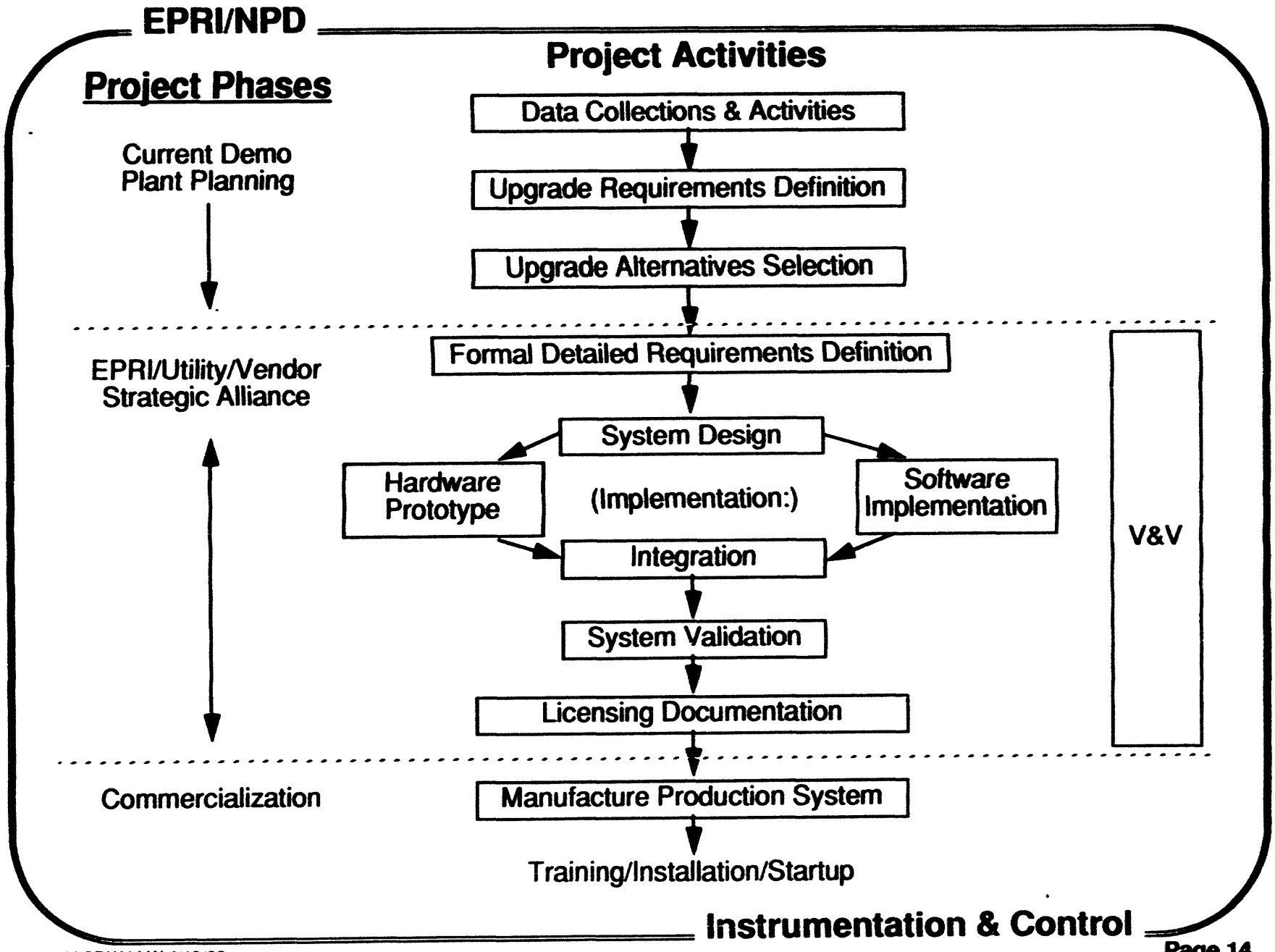
Plant Communications and Computing Architecture Plan Methodology



Instrumentation & Control

Plant Upgrade Planning

- TVA - Browns Ferry 2 (GE-BWR)
- BG&E - Calvert Cliffs 1 & 2 (CE-PWR)
- NSP - Prairie Island 1 & 2 (W-PWR)
- Entergy - ANO 1 & 2 (B&W-PWR, CE-PWR)


EPRI/NPD
Project Activities
Project Phases
Data Collections & Activities
Current Demo
Plant Planning
Upgrade Requirements Definition
Upgrade Alternatives Selection
Formal Detailed Requirements Definition
EPRI/Utility/Vendor
Strategic Alliance
System Design
Hardware
Prototype
(Implementation:)
Software
Implementation
V&V
Integration
System Validation
Licensing Documentation
Commercialization
Manufacture Production System
Training/Installation/Startup
Instrumentation & Control

Demonstration Plant Strategic Alliances Project Funding

Cost Sharing	Tailored Collaboration EPRI	Utility	Vendor
Development			
Specification	←	33.3%	→
Design	←	33.3%	→
Implementation	←	33.3%	→
Prototype			
Qualification	←	33.3%	→
Verification & Validation	←	33.3%	→
Licensing Support	←	33.3%	→
Production	Receive Royalty	Quantity Discount	Pay Royalty

EPRI Strategic Alliance Demo Plant Strategy Benefits

DEMO UTILITY

- Reduction of cost and risk
- Increased standardization and user base
- Shorter development time
- Open system compatible
- Addresses licensing issues

EPRI

- Reduced R&D base budget
- Improved commercialization
- Faster technology deployment

VENDOR

- Reduced development cost
- Increased market potential
- Faster technology deployment

AGING, MAINTENANCE AND MODERNIZATION OF INSTRUMENTATION AT THE ORNL HIGH FLUX ISOTOPE REACTOR

D. N. Fry

Reactor Systems Section

Instrumentation and Controls Division

ornl

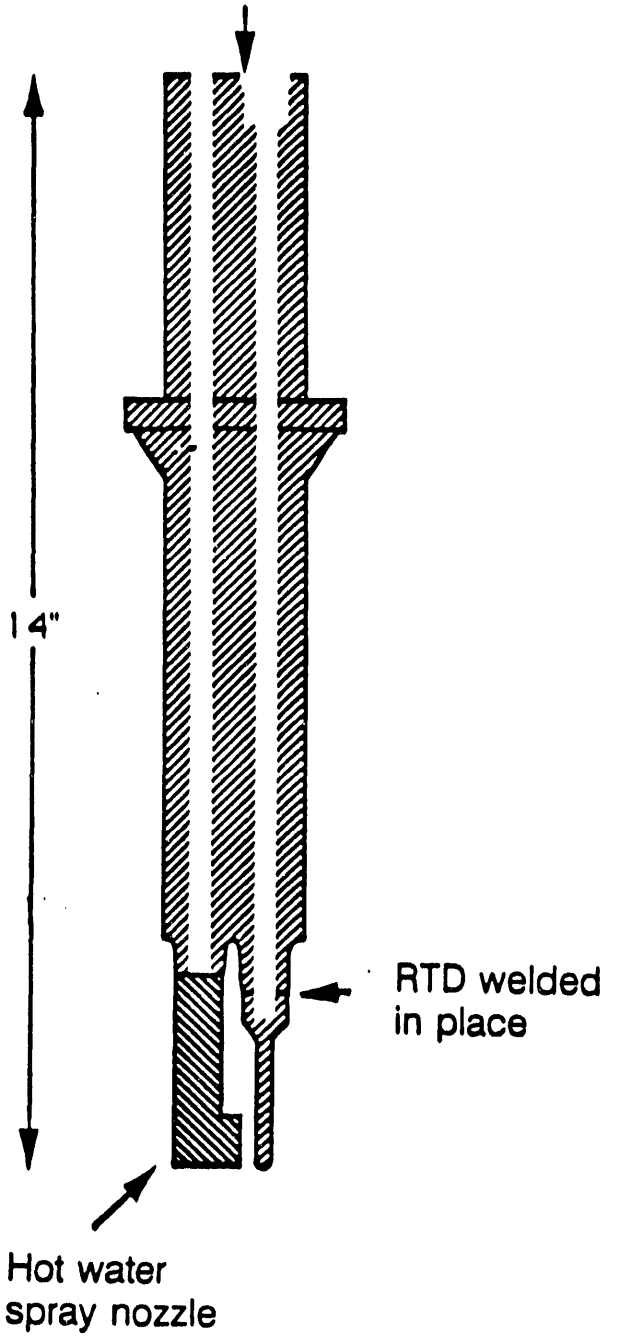
Presented to
Nuclear Power Plant Control and Instrumentation
Specialists Meeting

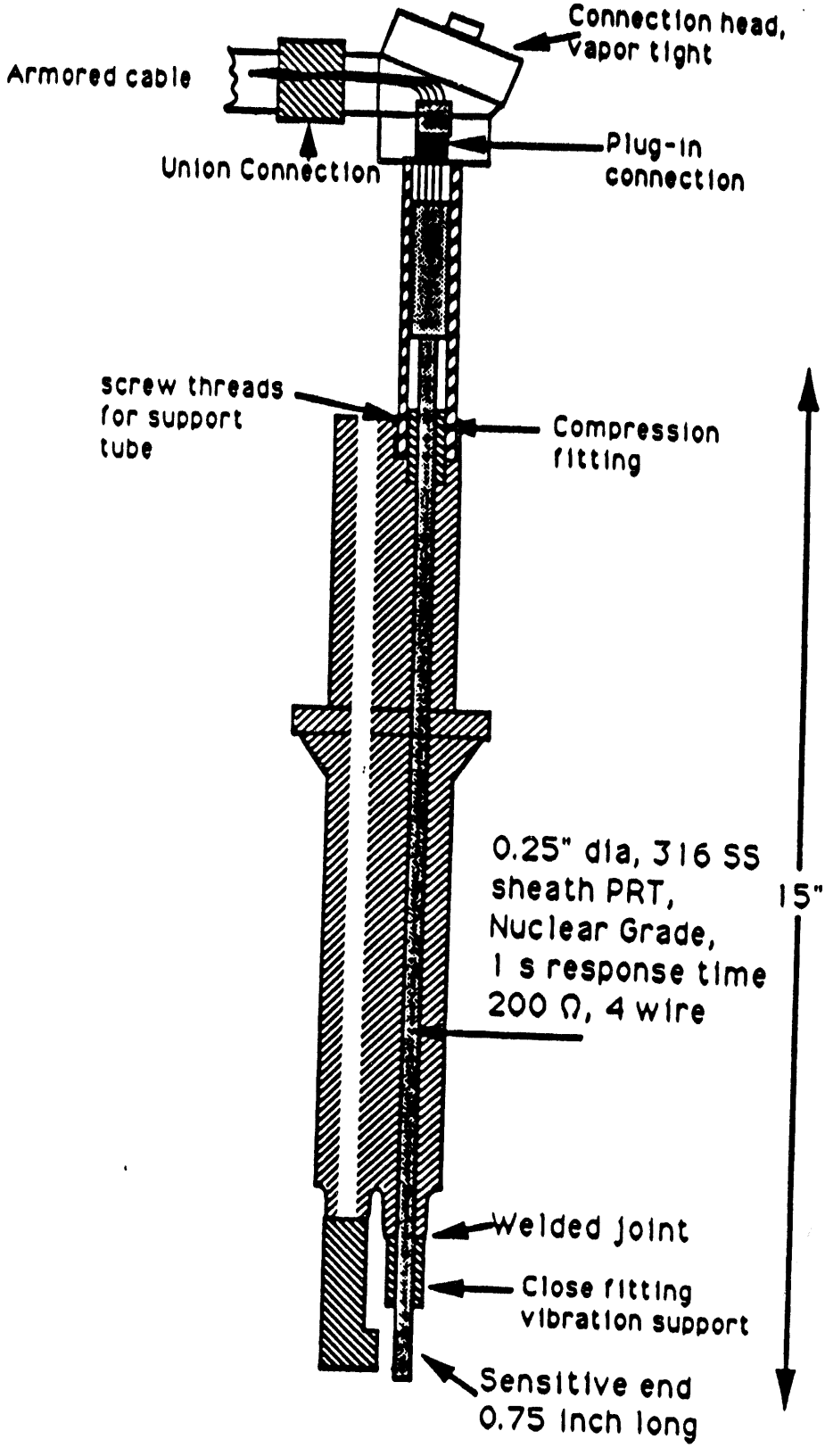
May 5-7, 1993
Rockville, Maryland

Aging of the Temperature Detectors in HFIR Is Providing an Opportunity to Upgrade the System Design

- RTDs originally installed are approaching the limit of their useful lives
- The inventory of spare RTDs that resulted from replacements of RTDs that failed over 30 years of operation has been depleted
- Safety, reliability and continuity of HFIR operation are vital
  - Replace old technology (3-wire system) with 4-wire commercial grade system
  - Improve RTD lifetimes by redesigning the assemblies that house and protect the RTDs
  - Improve ease of maintenance

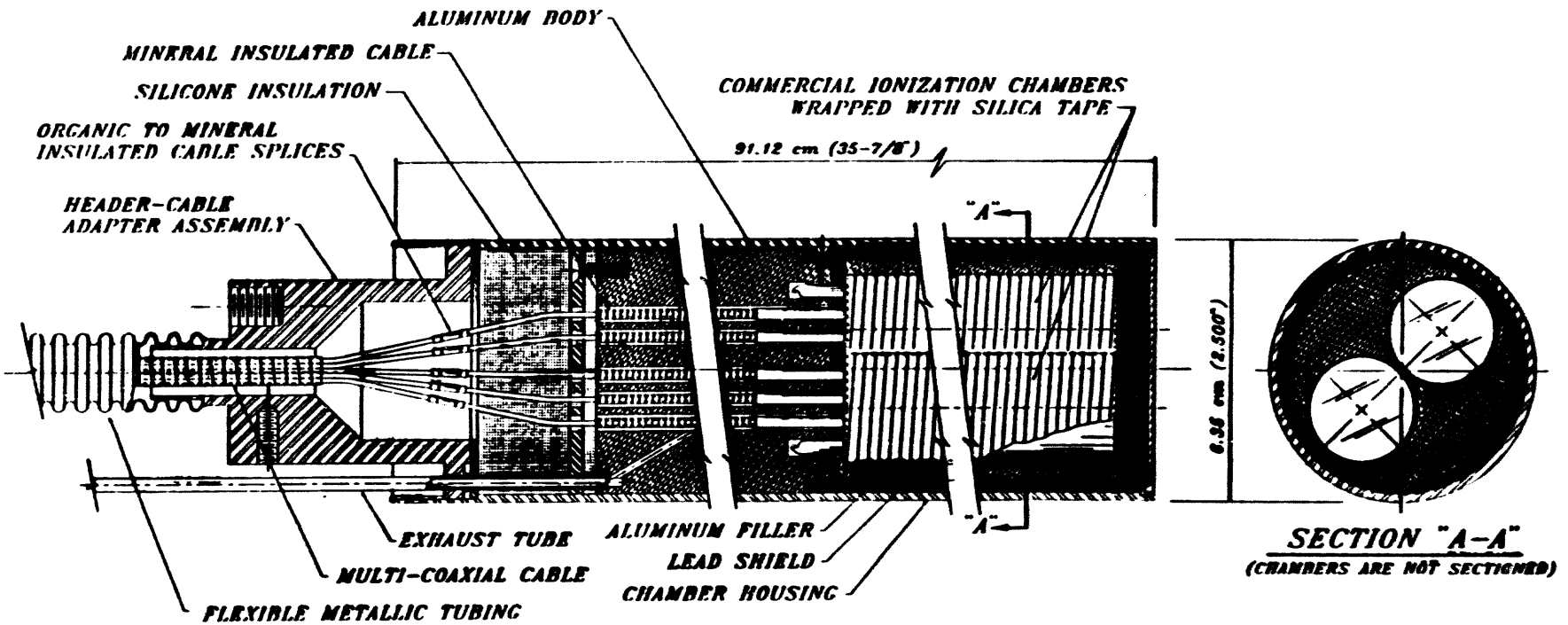
Existing Resistance Temperature Device (RTD), 3 wire, Ni coil, Bridge Balance System




Connection head, vapor tight
Armored cable
Union Connection
Plug-in connection
screw threads for support tube
Compression fitting
0.25" dia, 316 SS sheath PRT, Nuclear Grade, 1 s response time 200 Ω, 4 wire
15"
Welded joint
Close fitting vibration support
Sensitive end 0.75 inch long

Aging of the Neutron Detectors for the HFIR Control and Protection Channels Provides an Opportunity to Upgrade the Detection System Design

- There is a need to have replacement ionization chambers for those that have either failed in operation or are approaching the end of their useful lives
- Fabrication capabilities and facilities are limited and manufacturing costs are extremely high for procurement of ionization chambers of the original design
- Safety, reliability, and continuity of HFIR operation are vital
  - Replaced complex detector design having four sensitive volumes with a simple design of two volumes: one for control and one for protection
  - Eliminated unnecessary sensitive volumes devoted to gamma compensation and high voltage monitoring
  - Designed a two-detector system into the same housing as the original using commercial, nuclear grade neutron detectors



CCC IONIZATION CHAMBER FOR HFIR

HIGH FLUX ISOTOPE REACTOR PROTECTION SYSTEM UPGRADE

PROBLEM: THE REACTOR SUFFERS FROM SPURIOUS ROD DROPS OCCURRING DURING WEEKLY SURVEILLANCE TESTING

CAUSE: THE HFIR USES COINCIDENCE MAGNETS FOR ITS 2/3 LOGIC

DUE TO THE MAGNET DESIGN, THE RELEASE TIME OF THE SAFETY PLATES IS APPROXIMATELY 4 TIMES FASTER WHEN ONE OF THE THREE MAGNET COILS IS DEENERGIZED
(NORMAL CONDITION FOR SAFETY TESTING)

SOLUTION: PERFORM THE 2/3 LOGIC ELECTRONICALLY INSTEAD OF MAGNETICALLY TO KEEP THE RELEASE TIME CONSTANT DURING ALL PLANT CONDITIONS

IMPLEMENTATION:

A NEW INSTRUMENT MODULE WILL BE ADDED TO EACH SAFETY CHANNEL TO PERFORM THE SYSTEM 2/3 LOGIC

TO AVOID ELECTRICAL INTERACTION BETWEEN CHANNELS AND POSSIBLE ELECTRICAL FAULTS , THE LOGIC SIGNALS WILL BE VISIBLE LIGHT TRANSMITTED THROUGH 1000 MICRON FIBERS

THE RELEASE TIME OF THE MAGNETS WILL BE MAINTAINED AT 4 MILLISECONDS FOR BOTH 2/3 AND 3/3 CONDITIONS

PROTOTYPE MODULES HAVE UNDERGONE 6 MONTHS OF TESTING INCLUDING ENVIRONMENTAL TESTING

INSTALLATION OF THE NEW SYSTEM PREDICTED IN EARLY 1994

SESSION 1

STANDARDS

License Renewal

Cable Aging Tests

In-Situ Measurement of Response Time of RTDs and Pressure Transmitters in Nuclear Power Plants



LICENSE RENEWAL

SCOTT NEWBERRY

May 5, 1993

PURPOSE

PROVIDE AN OVERVIEW OF LICENSE RENEWAL

* WHAT IS LICENSE RENEWAL?

* SIGNIFICANCE OF LICENSE RENEWAL

* KEY ELEMENTS OF LICENSE RENEWAL
  - 10 CFR PART 54
  - 10 CFR PART 51
  - INDUSTRY REPORTS

* SUMMARY

REQUIREMENTS FOR LICENSE RENEWAL

STATE REQUIREMENTS:

- ENVIRONMENTAL
- PUBLIC HEALTH
- FINANCIAL

OTHER FEDERAL AGENCIES:

- ENVIRONMENTAL
- PUBLIC HEALTH

NRC REQUIREMENTS:

10 CFR PART 54 -- REACTOR SAFETY

10 CFR PART 51 -- ENVIRONMENTAL

WHAT IS LICENSE RENEWAL?

ATOMIC ENERGY ACT - 40 YR LICENSE TO OPERATE

ATOMIC ENERGY ACT ALLOWS RENEWAL

NEW LICENSE TO OPERATE FOR UP TO 20 YEARS AFTER ORIGINAL 40 YEARS

LICENSE APPLICATION & NRC APPROVAL

ALLOWS PUBLIC PARTICIPATION

REGULATIONS APPLICABLE TO LICENSE RENEWAL
- 10 CFR PART 54
- 10 CFR PART 51

WHAT IS LICENSE RENEWAL?

LICENSE RENEWAL

VS

LIFE EXTENSION (PLEX)

SIGNIFICANCE OF LICENSE RENEWAL

ENERGY PERSPECTIVE

100,000 MEGAWATTS OF NEW ELECTRICITY NEEDED BY YEAR 2000 (U.S. DOE ESTIMATE)

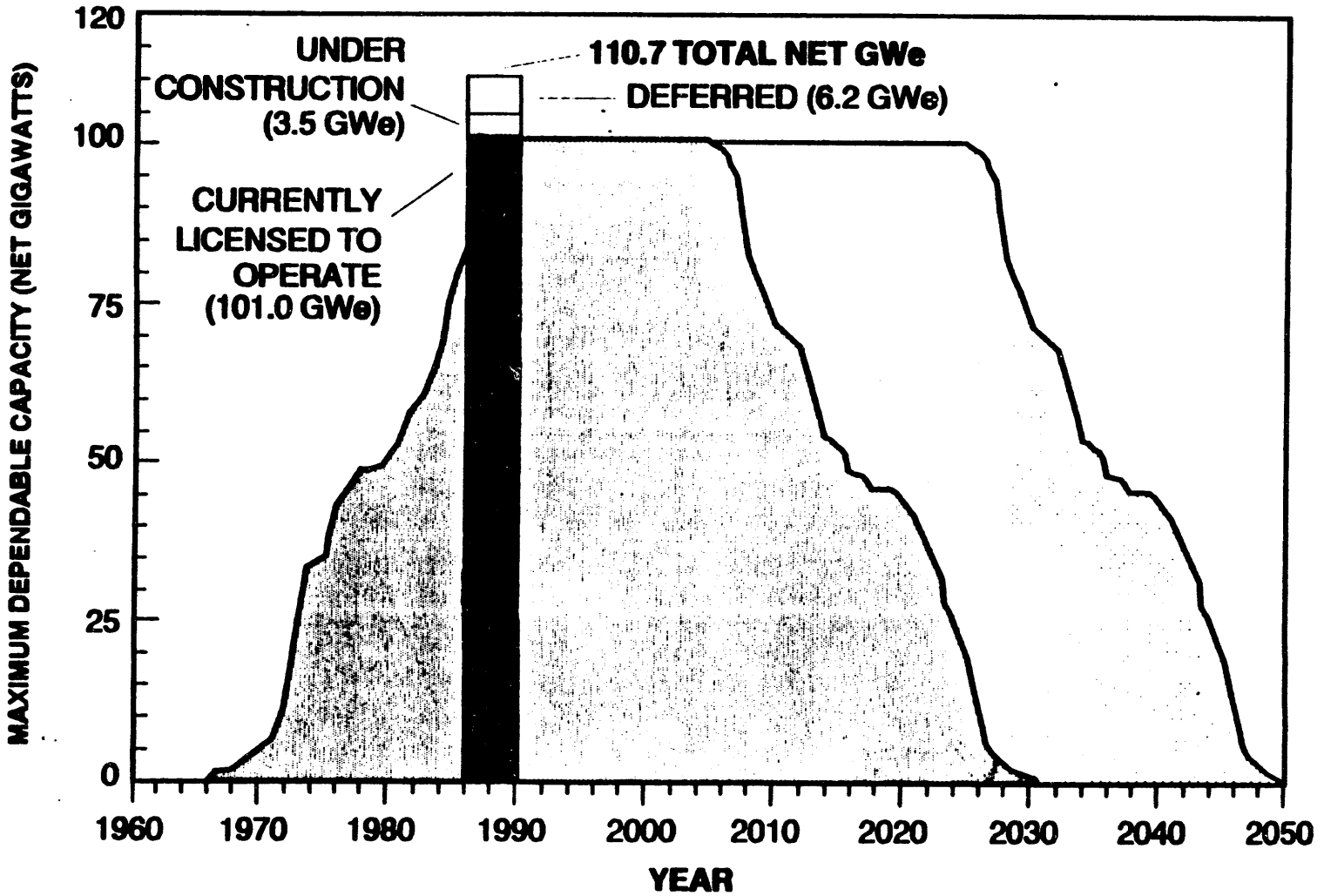
FEW BASE LOAD GENERATING PLANTS ORDERED OR PLANNED, EITHER FOSSIL OR NUCLEAR

110 LICENSED NUCLEAR POWER PLANTS

* ABOUT 20% OF CURRENT U.S. SUPPLY

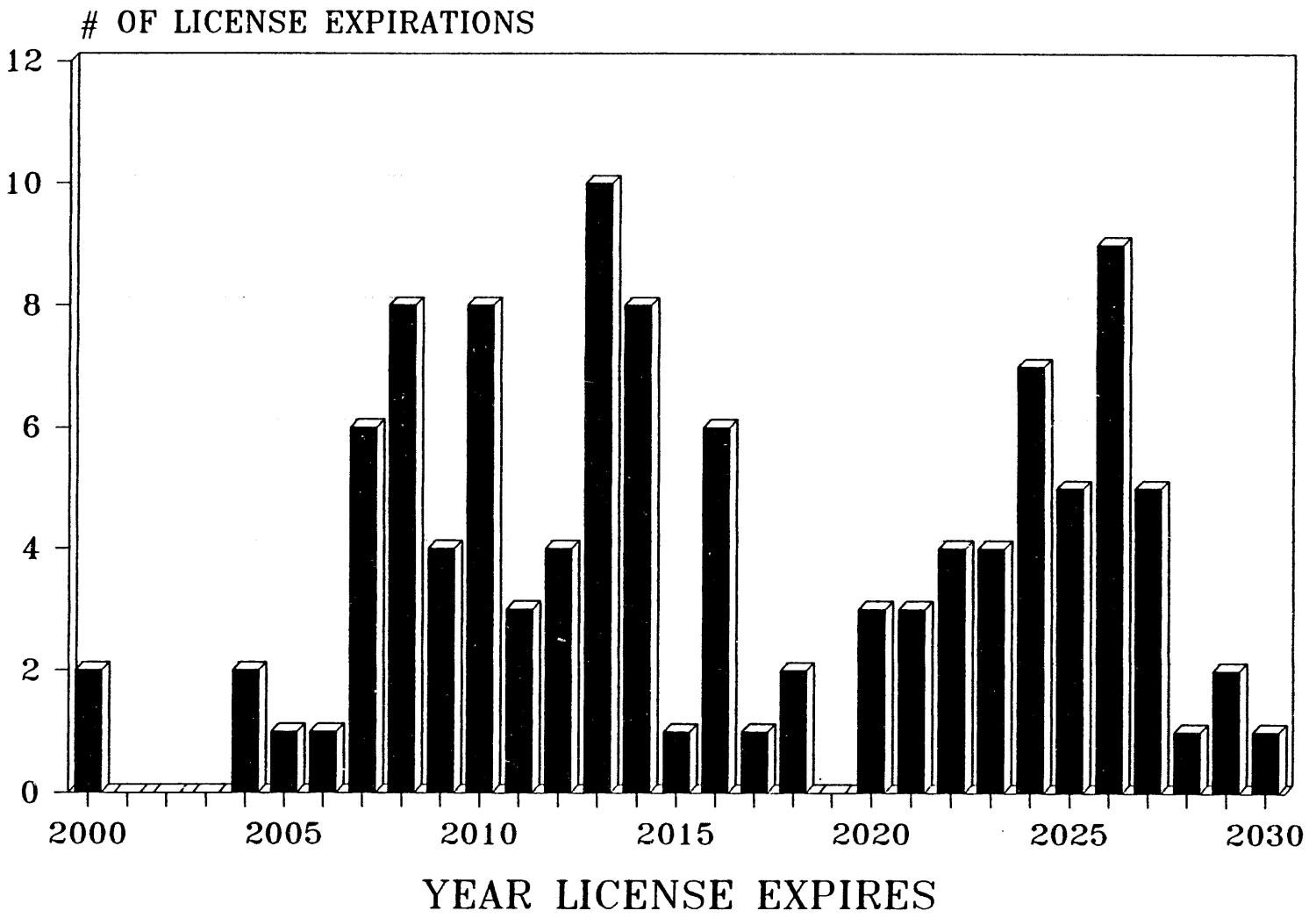
* LICENSES START TO EXPIRE IN YEAR 2000

U.S. Commercial Nuclear Power Reactor Generating Capacity

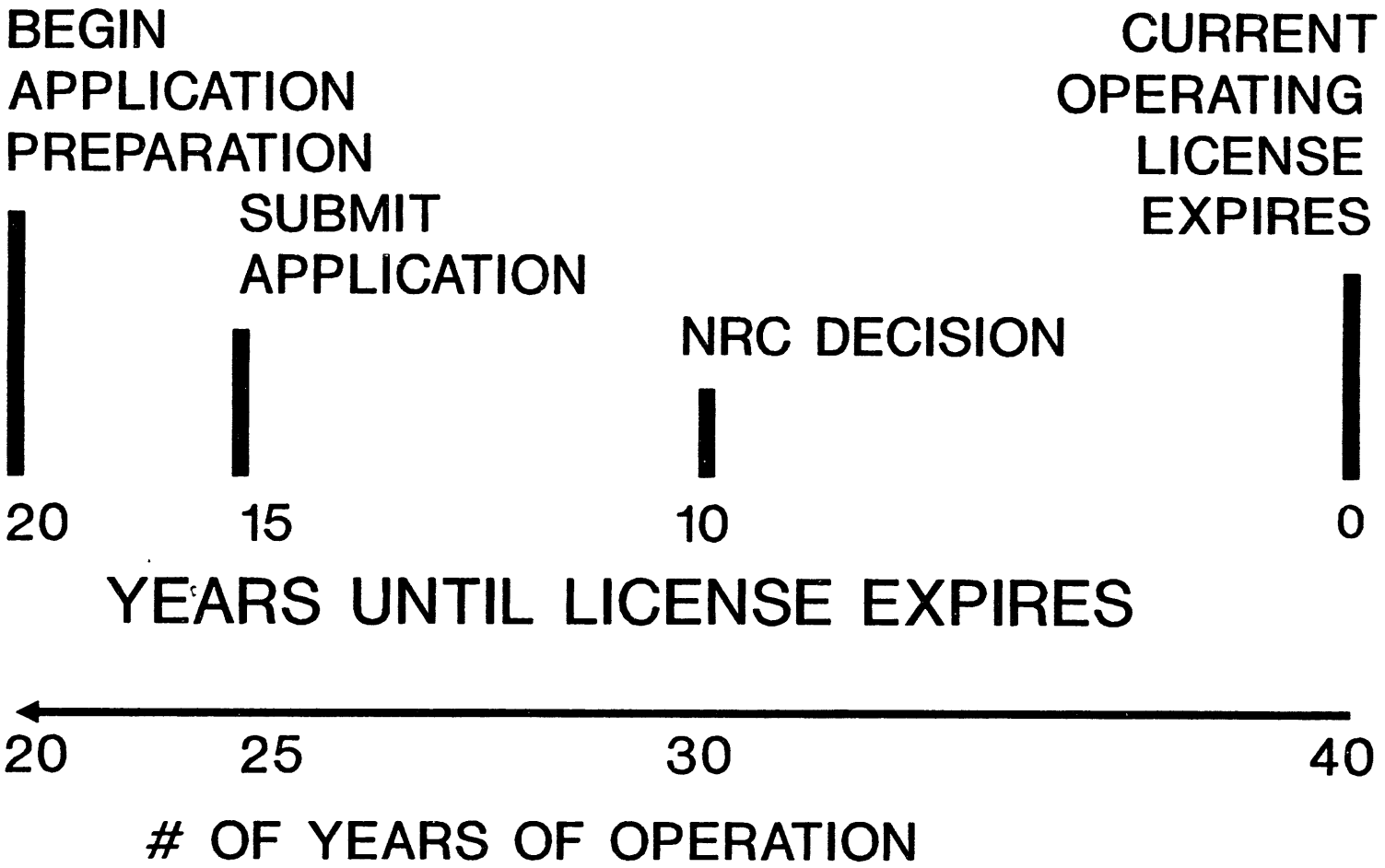


Source: Nuclear Regulatory Commission and Compiled Licensee Data

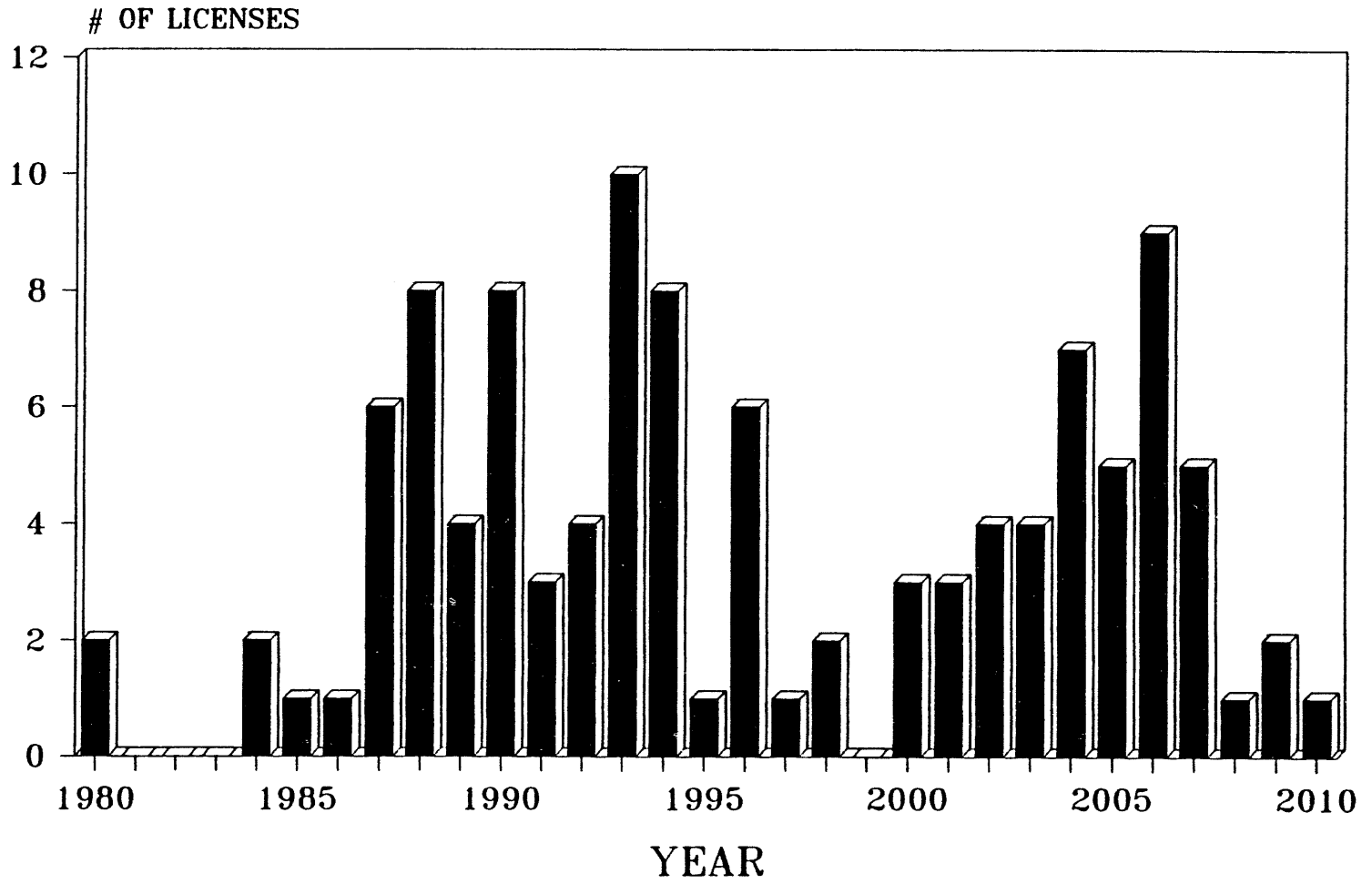
LICENSE EXPIRATIONS PER YEAR



LICENSE RENEWAL TIMELINE



LICENSE RENEWAL EFFORT
Year Application Preparation Begins



KEY ELEMENTS OF LICENSE RENEWAL

LICENSE RENEWAL ACTIVITIES

* 10 CFR PART 54 (TECHNICAL REQUIREMENTS)
  - REGULATORY GUIDE DEVELOPMENT
  - STANDARD REVIEW PLAN FOR LICENSE RENEWAL

* 10 CFR PART 51 (ENVIRONMENTAL REQUIREMENTS)
  - REGULATORY GUIDE AMENDMENTS
  - ENVIRONMENTAL STANDARD REVIEW PLAN

* INDUSTRY REPORT DEVELOPMENT AND REVIEW

* LEAD PLANT REVIEWS

10 CFR PART 54

LICENSE RENEWAL PRINCIPLES

PHILOSOPHY FOUNDED ON 2 KEY PRINCIPLES:

1. REGULATORY PROCESS ASSURES THAT CURRENT LICENSING BASIS PROVIDES AND MAINTAINS AN ACCEPTABLE LEVEL OF SAFETY

   - WITH THE POSSIBLE EXCEPTION OF AGE-RELATED DEGRADATION UNIQUE TO THE PERIOD OF EXTENDED OPERATION

2. CURRENT LICENSING BASIS MUST BE MAINTAINED DURING THE RENEWAL TERM

   - THE INTEGRATED PLANT ASSESSMENT (IPA) IS A DETAILED SYSTEMATIC REVIEW OF AGING AND IDENTIFIES ADDITIONAL AGING MANAGEMENT ACTIONS

REGULATORY GUIDANCE DOCUMENTS

REGULATORY GUIDE (DG 1009)

* LICENSEE GUIDANCE ON FORMAT & CONTENT OF APPLICATION

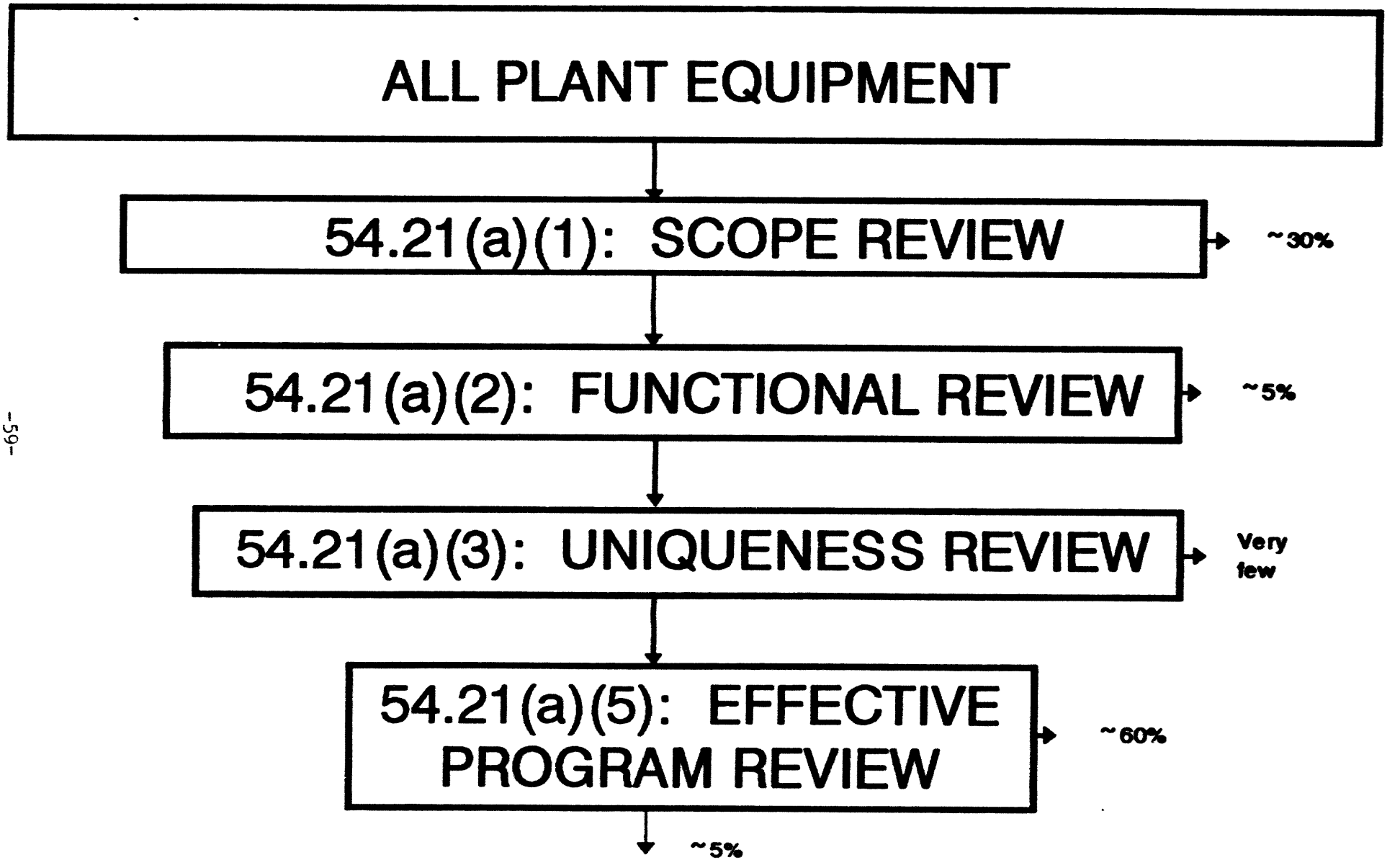
* ASSURES QUALITY & UNIFORMITY OF LICENSEE SUBMITTALS

STANDARD REVIEW PLAN FOR LICENSE RENEWAL (NUREG 1299)

* NRC STAFF REVIEW GUIDANCE

* FOCUSES REVIEW OF APPICATION & ASSURES CONSISTENCY OF REVIEWS

FIGURE 1: INTEGRATED PLANT ASSESSMENT (IPA)



EXAMPLES OF PUBLIC PARTICIPATION

FEDERAL REGISTER NOTICES

- NOTICE OF "TENDERED APPLICATION"
- NOTICE OF DOCKETING APPLICATION
- NOTICE OF TIMELY & SUFFICENT APPLICATION
- ISSUANCE OF RENEWED LICENSE or DENIAL

PUBLIC DOCUMENT ROOM

- APPLICATION
- FEDERAL REGISTER NOTICES
- CORRESPONDENCE BETWEEN NRC/APPLICANT
- SAFETY EVALUATION REPORT
- ENVIRONEMNTAL IMPACT STATEMENT

PUBLIC MEETINGS WITH APPLICANT

OPPORTUNITY FOR HEARINGS (10 CFR 2.758 & 54.29)

10 CFR PART 51

NATIONAL ENVIRONMENTAL POLICY ACT (NEPA)

* REQUIRES FEDERAL AGENCIES TO TAKE ENVIRONMENTAL FACTORS INTO ACCOUNT IN THEIR DECISIONMAKING & TO DOCUMENT THAT PROCESS IN A DETAILED STATEMENT

* NRC IMPLEMENTS NEPA THROUGH 10 CFR PART 51: ENVIRONMENTAL PROTECTION REGULATIONS FOR LICENSING & RELATED REGULATORY FUNCTIONS

* 10 CFR PART 51 IS CONSISTENT WITH THE COUNCIL ON ENVIRONMENTAL QUALITY (CEQ) REGULATIONS IMPLEMENTING NEPA: 40 CFR PARTS 1500-1508

10 CFR PART 51

CURRENTLY REQUIRES THAT AN ENVIRONMENTAL IMPACT STATEMENT (EIS) BE PREPARED AS PART OF A LICENSE RENEWAL REVIEW

PROPOSED AMENDMENT:

* REVIEW UP FRONT AS MANY ENVIRONMENTAL ISSUES ASSOCIATED WITH LICENSE RENEWAL AS POSSIBLE (ENHANCE REGULATORY EFFICIENCY)

* DEFINE ENVIRONMENTAL ISSUES THAT NEED TO BE REVIEWED AS PART OF PLANT SPECIFIC LICENSE RENEWAL REVIEW

INDUSTRY REPORTS

INDUSTRY REPORTS (IRs)

* INDUSTRY INITIATIVE TO EVALUATE DEGRADATION ISSUES
* 10 TECHNICAL REPORTS ON A VARIETY OF STRUCTURES AND COMPONENTS
* ATTEMPTS TO EVALUATE ISSUES GENERICALLY
* IRs CONTAIN TECHNICAL INFORMATION THAT MAY BE UTILIZED DURING THE INTEGRATED PLANT ASSESSMENT
* LICENSEES TO PROVIDE PLANT SPECIFIC INFORMATION TO DEMONSTRATE THAT THE INFORMATION & CORRESPONDING CONCLUSIONS CONTAINED IN THE IR ARE APPLICABLE TO ITS FACILITY

INDUSTRY REPORTS (IRs)

- CABLE IN CONTAINMENT
- CLASS 1 STRUCTURES

- BWR REACTOR PRESSURE VESSEL (RPV)
- BWR RPV INTERNALS
- BWR PRESSURE BOUNDARY
- BWR CONTAINMENT

- PWR REACTOR PRESSURE VESSEL
- PWR RPV INTERNALS
- PWR REACTOR COOLANT SYSTEM
- PWR CONTAINMENT

LICENSE RENEWAL SUMMARY

LICENSE RENEWAL SUMMARY

* TWO MAJOR RULEMAKINGS

  - 10 CFR PART 54

    TO ESTABLISH PROCEDURES, CRITERIA, & STANDARDS GOVERNING LICENSE RENEWAL FOR NUCLEAR PLANTS

  - 10 CFR PART 51

    TO EVALUATE GENERIC ENVIRONMENTAL ISSUES & DETERMINE THE ISSUES TO BE EVALUATED DURING EACH LICENSE RENEWAL APPLICATION

* 10 INDUSTRY REPORTS

* ONGOING DISCUSSIONS WITH PUBLIC & INDUSTRY
  - SECY-93-049: ISSUED MARCH 1, 1993
  - SECY-93-113: ISSUED APRIL 30, 1993

Cable Aging Tests

George Hubbard
Division of Systems Safety and Analysis
U.S. Nuclear Regulatory Commission

May 5, 1993

AGING, CONDITION MONITORING, AND LOSS-OF-COOLANT ACCIDENT (LOCA) TESTING OF CLASS 1E ELECTRICAL CABLES

NUREG/CR-5772

Purpose: Assess accident performance of cables aged slowly with simultaneous thermal and radiation exposure.

Cables tested:

- **Crosslinked Polyolefin Cables (Volume 1)**
- **Ethylene Propylene Rubber Cables (Volume 2)**
- **Miscellaneous Cable Types (Volume 3)**

NUREG/CR-5772
(Continued)

Pre-aging:

- Simultaneous thermal and radiation aging
- 9 Krad/hr (90 Gy/hr) dose rate, 100°C for 3 months, 6 months, or 9 months (Arrhenius equivalent of 55°C for 20, 40, or 60 years)
- Accident dose rate was 0.6 Mrad/hr (6 kGy/hr)

Aging time	Approximate total dose
3 months	123 Mrad (1.23 MGy)
6 months	132 Mrad (1.32 MGy)
9 months	159 Mrad (1.59 MGy)

LOCA Test: Similar to IEEE 323-1974, Appendix A, accelerated post-LOCA, no chemical spray

NUREG/CR-5772 RESULTS

Summary of Tested (T), Failed (F), and Marginal Insulation Resistance (IR)* Cables

Cable Type	20 T--F/IR	40 T--F/IR	60 T--F/IR
Firewall III, M	3--0/0	3--0/0	6--1/0
Brand Rex, M	3--0/0	3--0/0	3--0/0
Polyset, M	3--0/0	3--0/0	6--0/0
Raychem, S	2--0/0	2--0/0	3--0/0
Anaconda, M	6--0/0	6--0/0	6--0/0
Anaconda, S	1--0/0	1--0/0	1--0/0
BIW Bostrad, M	2--0/2	2--0/2	4--0/4
BIW Bostrad, S	2--0/1	2--0/2	2--0/2
Okonite, S	3--0/0	3--0/0	4--1/0
Dekorad, M	4--1/0	4--0/0	4--2/0
Dekorad, S	2--0/0	2--0/0	2--0/0
Kerite, S	2--0/0	2--0/2	3--0/3
Coaxial, S	2--0/2	2--0/2	2--0/2
Silicone, S	2--0/0	2--0/0	2--0/0
**Kapton, S	2--1/0	2--1/?	2--1/0
Totals	39--2/5	39--1/8	50--5/11

S Single conductor cables
M Multiconductor cables
* Minimum IR lower than 2500 ohm-1000 ft for instrument cable, 500 ohm-100 ft for control cable, or 10^7 ohm-1000 ft for coaxial cable.
** Failed cables in 40 and 60 were damaged prior to accident test.
? No IR measurements were possible

NUREG/CR-5772 RESULTS
(Continued)

- Cable type may be a factor in surviving LOCA test. Some types showed no failures, even at 60-year equivalent aging, while other types failed after only 20 years.

DAMAGED CABLE TEST

Purpose: Determine the minimum insulation thickness needed to survive a LOCA test at the end of qualified life.

Cables tested:

- **Ethylene Propylene Rubber with bonded Hypalon jacket**
- **Silicone Rubber with fiberglass jacket**
- **Crosslinked Polyethylene Rubber with no jacket**

DAMAGED CABLE TEST
(Continued)

Radiation aging: 300 Krad/hr (3 kGy) for 433 hours, 130 Mrad (1.3 MGy) total dose

Thermal aging: 158°C for 336 hours

Arrhenius equivalent age: 40 years at 69°C

LOCA Test: Similar to IEEE 323-1974, Appendix A, accelerated post-LOCA, no chemical spray

DAMAGED CABLE TEST RESULTS

All bonded jacket cables failed during LOCA test

After thermal and radiation aging:

- **Damaged bonded jacket samples had cracks through to the conductor (away from damaged areas).**

- **No cracks on the undamaged bonded jacket cables.**

DAMAGED CABLE TEST RESULTS
(Continued)

LOCA performance of bonded jacket cables:

- **Insulation resistance was monitored continuously during the test.**
- **Cables with through-wall cracks after aging failed within five days of the start of the LOCA test (IR decreased to 100 ohms).**
- **The undamaged cable failed earlier than many of the damaged cables (6 1/2 hours after the start of the second transient).**

After the LOCA test the insulation on all bonded jacket cable samples had split down the length of the cable and bare conductor was visible.

COMMUNICATION TO INDUSTRY

The NRC has recently issued the following information notices on cable failures:

- **IN 92-81, "Potential Deficiency of Electrical Cables with Bonded Hypalon Jackets"**

- **IN 93-33, "Potential Deficiency of Certain Class 1E Instrumentation and Control Cables"**

CONCLUSIONS

Failures of qualified cables raised concerns relative to artificial aging methods and adequacy of qualification test results.

The tests do not prove or disprove the adequacy of current qualification practices or requirements.

As a result of these test failures, the NRC will review:

- Uncertainty in artificial aging for qualification
- Adequacy of Environmental Qualification requirements to ensure that equipment will perform its safety function to the end of qualified life.
- Condition monitoring to determine actual aging of installed cables

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, D.C. 20555

April 28, 1993

NRC INFORMATION NOTICE 93-33: POTENTIAL DEFICIENCY OF CERTAIN CLASS 1E INSTRUMENTATION AND CONTROL CABLES

Addressees

All holders of operating licenses or construction permits for nuclear power reactors.

Purpose

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice to alert addressees to a potential deficiency in the environmental qualification of certain Class 1E instrumentation and control cables. It is expected that recipients will review the information for applicability to their facilities and consider actions, as appropriate to avoid similar problems. However, suggestions contained in this information notice are not NRC requirements; therefore, no specific action or written response to this notice is required.

Description of Circumstances

Sandia National Laboratories, under contract to the NRC, tested cables to determine the long-term aging degradation behavior of typical instrumentation and control cables used in nuclear power plants and to determine the potential for using condition monitoring for assessing residual life. The results of this testing are described in NUREG/CR-5772, "Aging, Condition Monitoring, and Loss-of-Coolant Accident (LOCA) Tests of Class 1E Electrical Cables," Volumes 1, 2, and 3. The tests were conducted on cross-linked polyolefin/polyethylene, ethylene propylene rubber, and miscellaneous Class 1E cable types. The test program generally followed the guidance of Institute of Electrical and Electronics Engineers (IEEE) Standard 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and IEEE Standard 383-1974, "IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections." IEEE Standard 323-1974 is an industry-established standard endorsed by the NRC for qualifying Class 1E equipment for nuclear power generating stations, and IEEE Standard 383-1974 is an industry-established standard for type test of Class 1E electric cables, field splices, and connections for nuclear power generating stations.

The test program consisted of two phases; both phases used the same test specimens. Phase 1 consisted of simultaneous thermal and radiation aging of the cables at approximately 100 °C (212 °F) and 0.10 kGy per hour (10 kilorads per hour), respectively. Three different sets of cable specimens were tested in this phase: one was aged to a nominal lifetime of 20 years, a second to 40 years, and a third to 60 years. Phase II was a sequential accident exposure consisting of 1100 kGy (110 megarads) of high-dose-rate irradiation

9304230163

at the rate of 6 kGy per hour (600 kilorads per hour) followed by a simulated exposure to LOCA steam. The test profile was similar to the one given in IEEE Standard 323-1974 for "generic" qualification. The cables were energized at 110 V dc during the accident simulation. Insulation resistance was measured on line throughout the test. No chemical spray was used during the steam exposure, but a post-LOCA submergence test was performed on the cables that were aged to a nominal equivalent of 40 years.

Cable types that failed during the accident tests or that exhibited marginal insulation resistances were Rockbestos Firewall III, BIW Bostrad 7E, Okonite-Okolon, Samuel Moore Dekoron Dekorad Type 1952, Kerite 1977, Rockbestos RSS-6-104/LE Coaxial, and Champlain Kapton. The list of cables included in the test program and a summary of the test results from NUREG/CR-5772 are shown in Attachments 1 and 2, respectively.

In addition, the Sandia National Laboratories (under contract to NRC) has also tested cables in a separate program to determine the minimum insulation thickness necessary for installed cable to perform its intended function should the insulation be damaged during installation, maintenance, or other activities. During LOCA testing, all 10 of the Okonite-Okolon cable samples failed. The results of this test program are summarized in NRC Information Notice 92-81, "Potential Deficiency of Electrical Cables With Bonded Hypalon Jackets," issued on December 11, 1992.

Discussion

The Sandia National Laboratories test results from NRC-sponsored programs raise questions with respect to the environmental qualification (EQ) of certain cables that either failed or exhibited marginal insulation resistance values. The staff reviewed the test data and noted that cable types identified as Firewall III, Okonite, Dekorad, and Kapton failed during the simulated accident exposure, while BIW Bostrad, Rockbestos Coaxial, and Kerite exhibited marginal insulation resistances. It should be noted that the insulation resistance of the Rockbestos coaxial cables may be too low to meet specifications for use in General Atomics radiation monitor circuits, depending on the environment to which the cable will be exposed. The low insulation resistance of these Rockbestos coaxial cables was the subject of a 10 CFR Part 21, "Reporting of Defects and Noncompliance," notification by General Atomics dated March 28, 1989.

As part of the NRC-sponsored aging research program, the Sandia National Laboratories searched licensee event reports (LERs) to find LERs that might be related to cable aging. In NUREG/CR-5461, "Aging of Cables, Connections, and Electrical Penetrations Assemblies Used in Nuclear Power Plants," the Sandia National Laboratories concluded that although cables are highly reliable

devices under normal plant operating conditions, with no evidence of significant increases in failure rate with aging, the performance experience with these components under actual accident conditions is small. The current LER data provide a very limited database for this purpose. The only significant data for cables subjected to design-basis events comes from EQ testing.

Depending on the application, failure of these cables during or following design-basis events could affect the performance of safety functions in nuclear power plants. NRC Generic Letter 88-07, "Modified Enforcement Policy Relating to 10 CFR 50.49, 'Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants'," provides relevant information on dealing with potential EQ deficiencies. In Generic Letter 88-07, the NRC stated, in part:

> When a potential deficiency has been identified by the NRC or licensee in the equipment (i.e., a licensee does not have an adequate basis to establish qualification), the licensee is expected to make a prompt determination of operability (i.e., the system or component is capable of performing its intended design function), take immediate steps to establish a plan with a reasonable schedule to correct the deficiency, and have written justification for continued operation, which will be available for NRC review.
>
> The licensee may be able to make a finding of operability using analysis and partial test data to provide reasonable assurance that the equipment will perform its safety function when called upon. In this connection, it must also be shown that subsequent failure of the equipment, if likely under accident conditions, will not result in significant degradation of any safety function or provide misleading information to the operator.

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please contact one of the technical contacts listed below or the appropriate Office of Nuclear Reactor Regulation (NRR) project manager.

Brian K. Grimes, Director
Division of Operating Reactor Support
Office of Nuclear Reactor Regulation

Technical contacts: Paul Shemanski, NRR
(301) 504-1377

Ann Dummer, NRR
(301) 504-2831

Satish Aggarwal, RES
(301) 492-3829

Attachments:
1. "Cables Included in the Test Program"
2. "Summary of Tested, Failed, and Marginal Insulation Resistance Cables"
3. List of Recently Issued NRC Information Notices

CABLES INCLUDED IN THE TEST PROGRAM

	Supplier	Description
1.	Brand Rex	30 mil XLPE Insulation, 60 mil CSPE Jacket, 12 AWG, 3/C, 600 V
2.	Rockbestos	Firewall III, 30 mil XLPE Insulation, 45 mil Neoprene Jacket, 12 AWG, 3/C, 600 V
3.	Raychem	Flamtrol, 30 mil XLPE Insulation, 12 AWG, 1/C, 600 V
4.	Samuel Moore	Dekoron Polyset, 30 mil XLPO Insulation, 45 mil CSPE Jacket, 12 AWG, 3/C and Drain, 600 V
5.	Anaconda	Anaconda Y Flame-Guard FR-EP, 30 mil EPR Insulation, 45 mil CPE Jacket, 12 AWG, 3/C, 600 V
5a.	Anaconda*	Anaconda Flame-Guard EP, 30 mil EPR Insulation, 15 mil Individual CSPE Jackets, 45 mil Overall CSPE Jacket, 12 AWG, 3/C, 1000 V
6.	Okonite	Okonite-Okolon, 30 mil EPR Insulation, 15 mil CSPE Jacket, 12 AWG, 1/C, 600 V
7.	Samuel Moore	Dekoron Dekorad Type 1952, 20 mil EPDM Insulation, 10 mil Individual CSPE Jackets, 45 mil Overall CSPE Jacket, 16 AWG, 2/C TSP, 600 V
8.	Kerite	Kerite 1977, 70 mil FR Insulation, 40 mil FR Jacket, 12 AWG, 1/C, 600 V
8a.	Kerite	Kerite 1977, 50 mil FR Insulation, 60 mil FR Jacket, 12 AWG, 1/C, 600 V
9.	Rockbestos	RSS-6-104/LE Coaxial Cable, 22 AWG, 1/C Shielded
10.	Rockbestos	30 mil Firewall Silicone Rubber Insulation, Fiberglass Braided Jacket, 16 AWG, 1/C, 600 V
11.	Champlain	5 mil Polyimide (Kapton) Insulation, Unjacketed, 12 AWG, 1/C
12.	BIW**	Bostrad 7E, 30 mil EPR Insulation, 15 mil Individual CSPE Jackets, 60 mil Overall CSPE Jacket, 16 AWG, 2/C TSP, 600 V

* This cable was only used for the multiconductor samples in the 3-month chamber.

** The IR values in BIW Report B915 are approximately one order of magnitude higher than the values observed during the Sandia National Laboratories testing.

Summary of Tested (T), Failed (F), and Marginal Insulation Resistance (IR)* Cables

Cable Type		Pre-aged 20 years T--F/IR	40 years T--F/IR	60 years T--F/IR
Firewall III	M	3--0/0	3--0/0	6--1/0
Brand Rex	M	3--0/0	3--0/0	3--0/0
Polyset	M	3--0/0	3--0/0	6--0/0
Raychem	S	2--0/0	2--0/0	3--0/0
Anaconda	M	6--0/0	6--0/0	6--0/0
Anaconda	S	1--0/0	1--0/0	1--0/0
BIW Bostrad	M	2--0/2	2--0/2	4--0/4
BIW Bostrad	S	2--0/1	2--0/2	2--0/2
Okonite	S	3--0/0	3--0/0	4--1/0
Dekorad	M	4--1/0	4--0/0	4--2/0
Dekorad	S	2--0/0	2--0/0	2--0/0
Kerite	S	2--0/0	2--0/2	3--0/3
Coaxial	S	2--0/2	2--0/2	2--0/2
Silicone	S	2--0/0	2--0/0	2--0/0
Kapton**	S	2--1/0	2--1/?	2--1/0
Totals		39--2/5	39--1/8	50--5/11

* Minimum IR lower than 2500 ohm-1000 ft for instrument cable, 500 ohm-1000 ft for control cable, or 10^7 ohm-1000 ft for coaxial cable.

** Failed cables that were pre-aged to 40 and 60 years were damaged prior to accident test.

? No IR measurements were possible.

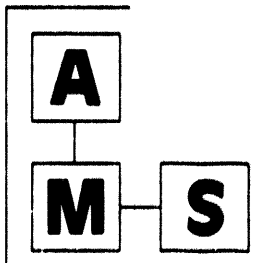
S Single conductor cables

M Multiconductor cables

LIST OF RECENTLY ISSUED NRC INFORMATION NOTICES

Information Notice No.	Subject	Date of Issuance	Issued to
93-32	Nonconservative Inputs for Boron Dilution Event Analysis	4/21/93	All holders of OLs or CPs for pressurized water reactors (PWRs).
93-31	Training of Nurses Responsible for the Care of Patients with Brachytherapy Implants	04/13/93	All U.S. Nuclear Regulatory Commission medical licensees.
93-30	NRC Requirements for Evaluation of Wipe Test Results; Calibration of Count Rate Survey Instruments	04/12/93	All U.S. Nuclear Regulatory Commission medical licensees.
93-29	Problems with the Use of Unshielded Test Leads in Reactor Protection System Circuitry	04/12/93	All holders of OLs or CPs for nuclear power reactors.
93-28	Failure to Consider Loss of DC Bus in the Emergency Core Cooling System Evaluation May Lead to Nonconservative Analysis	04/09/93	All holders of OLs or CPs for nuclear power reactors.
93-27	Level Instrumentation Inaccuracies Observed during Normal Plant Depressurization	04/08/93	All holders of OLs or CPs for nuclear power reactors.
93-26	Grease Solidification Causes Molded Case Circuit Breaker Failure to Close	04/07/93	All holders of OLs or CPs for nuclear power reactors.
93-25	Electrical Penetration Assembly Degradation	04/01/93	All holders of OLs or CPs for nuclear power reactors.

OL = Operating License
CP = Construction Permit



ANALYSIS AND MEASUREMENT SERVICES CORPORATION

AMS 9111 CROSS PARK DRIVE / KNOXVILLE, TN 37923 USA (615) 691-1756

In-Situ Measurement of Response Time of RTDs and Pressure Transmitters in Nuclear Power Plants

H. M. Hashemian
J. L. Riner

Analysis and Measurement Services Corporation
AMS 9111 Cross Park Drive
Knoxville, TN 37923 USA
Phone: (615) 691-1756
Fax: (615) 691-9344

Presented At

International Atomic Energy Agency Specialist Meeting on
Experience in Ageing, Maintenance and Modernization
of Instrumentation and Control Systems for
Improving Nuclear Power Plant Availability

ABSTRACT

Response time measurements are performed once every fuel cycle on most safety-related temperature and pressure sensors in a majority of nuclear power plants in the United States. This paper provides a review of the methods that are used for these measurements. The methods are referred to as the Loop Current Step Response (LCSR) test, which is used for response time testing of temperature sensors, and noise analysis and power interrupt (PI) tests, which are used for response time testing of pressure, level, and flow transmitters.

1. INTRODUCTION

This paper presents the principle of the modern techniques for testing the response time of Resistance Temperature Detectors (RTDs), and pressure, level and flow transmitters in nuclear power plants. The significance of these techniques is that they permit in-situ testing at process operating conditions and thereby provide the actual in-service response times of the sensors.

For RTDs, a method called the LCSR test has been developed and validated for remote measurement of response time while the RTD remains installed in an operating process. The LCSR test is based on applying an electric current to the RTD's extension leads to produce Joule heating (I^2R) in the sensing element. This heating produces an internal temperature transient in the RTD that can be analyzed to provide the RTD response time.

The validity of the LCSR method has been established through laboratory research and the method has been used extensively in the nuclear power industry for the last fifteen years. To date, about sixty nuclear power plants in the United States and several plants in other countries depend on the LCSR method for RTD response time measurements. These measurements are usually performed once every fuel cycle to verify that the safety system RTDs meet the response time requirements.

For response time testing of pressure transmitters, a method called noise analysis was developed and validated. The method is based on analyzing the natural fluctuations that exist at the output of pressure transmitters while the plant is operating. These fluctuations are analyzed in the frequency domain by a fast fourier transform analysis or in time domain by autoregressive modeling to give the response time of the transmitters.

In addition to the noise analysis technique, a method called the PI test is available for response time testing of pressure transmitters. However, this method is applicable only to force-balance transmitters. The PI test is based on analyzing the output of the transmitter after the power to the transmitter has been switched OFF and then ON. Like the LCSR test and noise analysis, the PI method has been validated for use in nuclear power plants.

2. RTD RESPONSE TIME TESTING METHODS

The response time of an RTD can be measured in a laboratory using a method called the plunge test. The test provides a baseline response time value which is useful for comparing a group of RTDs or thermowells to ensure that they provide comparable and consistent response times. The

plunge test is also useful for testing the response times of RTDs of different design or manufacturers to determine which design or manufacturer provides a better response time.

The plunge test results have very little bearing on the response time of an RTD after it is installed in an operating process. Due to the effect of installation and process conditions, the response time of an installed RTD can only be identified by in-situ testing using the LCSR method. The principles of the plunge and LCSR tests are covered in the following sections.

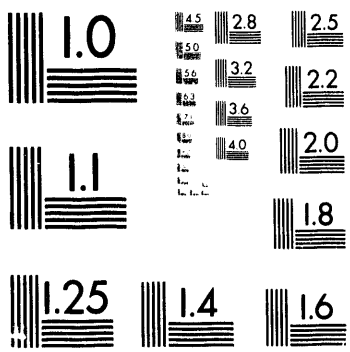
2.1 Plunge Test

The response time of a temperature sensor is classically measured in a laboratory environment using a method called the plunge test. In this test, the sensor is exposed to a sudden change in temperature and its output is recorded until it reaches steady-state. The analysis of a plunge test to obtain the time constant of a sensor is simple. For example, if the sensor output transient is recorded on a strip chart recorder, the time constant is identified by measuring the time that corresponds to 63.2 percent of the final value)Figure 1 .

It should be noted that although the definition of time constant as illustrated in Figure 1 is analytically valid only for a first order system, it is conventionally used for empirically establishing the response time of most temperature sensors regardless of the dynamic order. Therefore, all references to the terms "response time" or "time constant" in this paper correspond to this definition regardless of the type or size of the sensor, the test condition, or the test method being used)whether it is the plunge or the LCSR test .

The time constant obtained by the plunge method is a relative index which should be accompanied by a description of the test conditions. This is important because the response time of temperature sensors is strongly dependent on the properties of the final medium in which they are plunged. The type of medium)air, water, etc. and its velocity, temperature, and pressure must always be specified with the response time results. The fluid velocity is usually the most important factor followed by temperature and then pressure. These parameters affect the film heat transfer coefficient on the sensor surface which is related to the response time. Higher fluid velocities increase the film heat transfer coefficient on the surface of the sensor and reduce the response time. Temperature, however, has a mixed effect. On the one hand, temperature acts in the same manner as fluid velocity, i.e., it increases the film heat transfer coefficient and reduces the response time. On the other hand, high temperatures can affect the material properties inside the sensor and either increase or decrease the response time. Pressure does not usually affect the sensor response time except for its effect on the fluid properties that control the surface heat transfer coefficient. In addition to process effects, the response time of RTDs usually depends on installation, especially when the sensor is installed into a thermowell. Figure 2 shows the response time of two different temperature sensors as a function of the flow rate and temperature of the media in which the sensors were tested.

Because of the effect of process conditions on response time, a standard has been devised by the American Society for Testing and Materials)ASTM for the laboratory plunge testing of RTDs.[1] The standard specifies that laboratory plunge tests shall be performed in water flowing at 3 feet per second)approximately 1 meter per second at ambient temperature and pressure conditions. Referred to as ASTM Standard E644, the standard is intended to ensure that laboratory response time measurements are performed in a uniform set of conditions throughout the industry to provide a basis for comparing the response times of various RTDs from various manufacturers.


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3

2 of 6

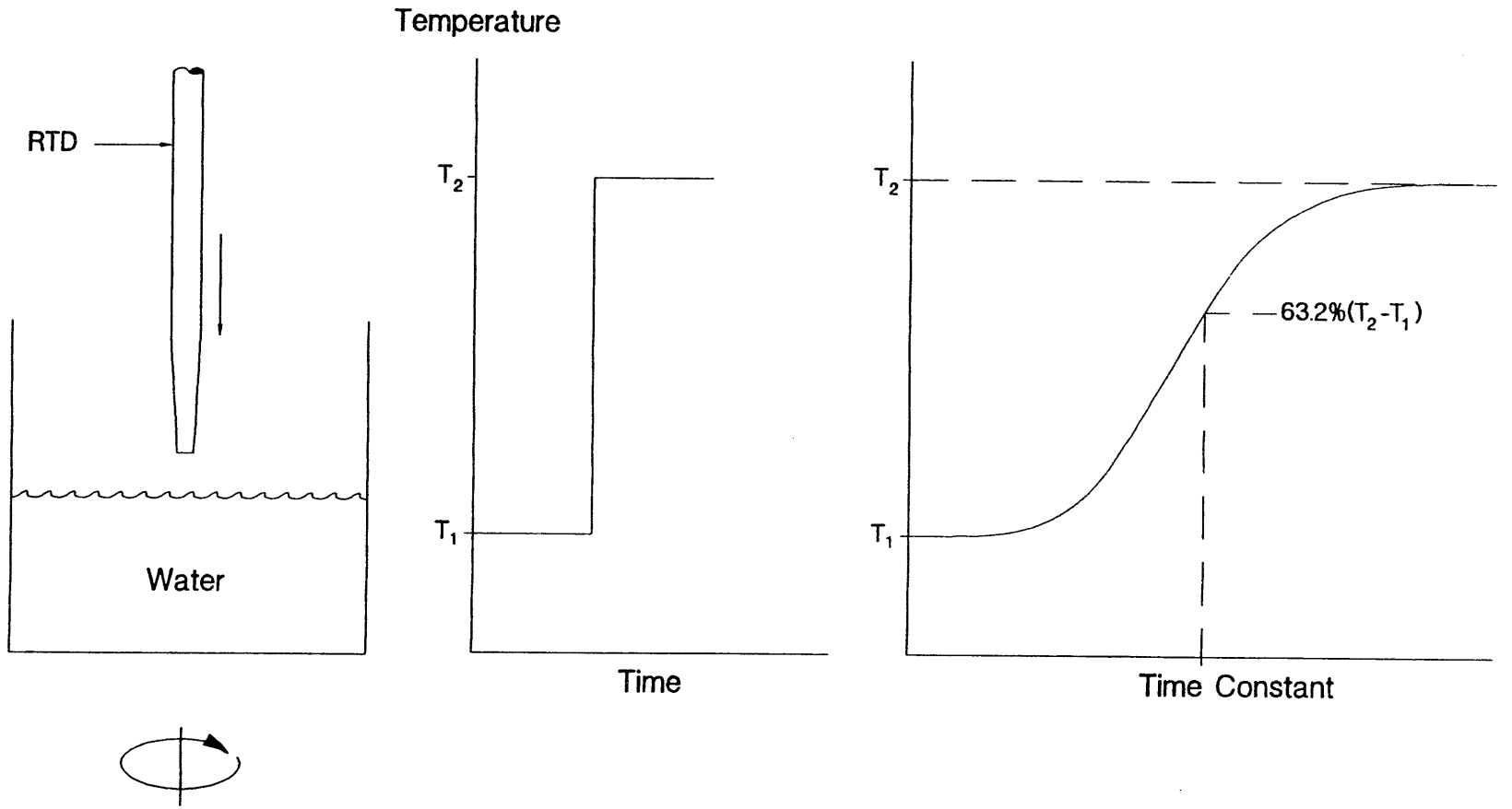


Figure 1. Illustration of Principle of Plunge Test and Measurement of Response Time in Terms of Time Constant.

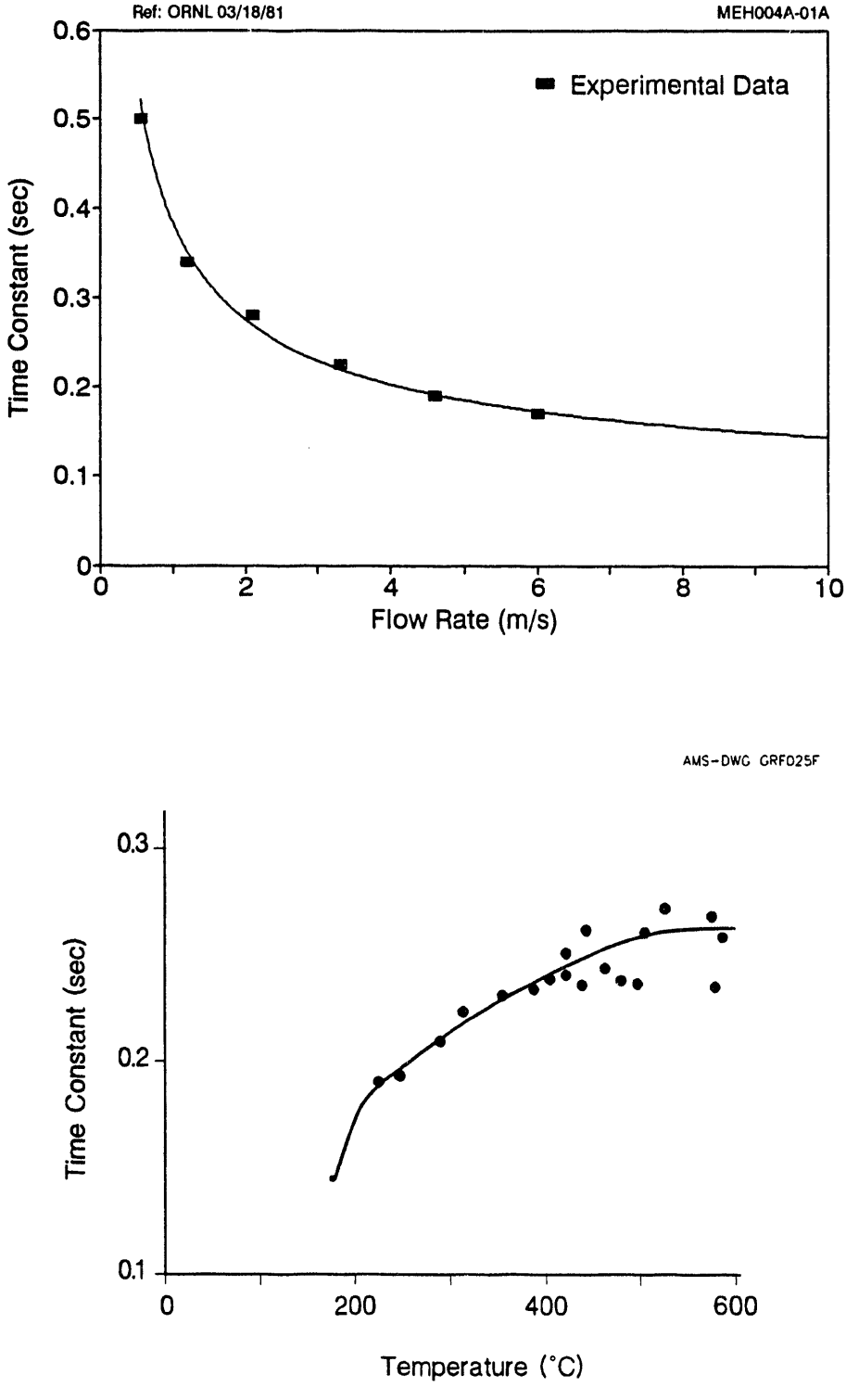


Figure 2. Effect of Fluid Flow and Fluid Temperature on Response Time of Temperature Sensors.

2.2 LCSR Test

Since the response time of a temperature sensor is strongly affected by process conditions, laboratory measurements such as plunge tests in a reference condition cannot provide accurate information about the "in-service" response time of the sensor. Therefore, an in-situ method that can be implemented at process operating conditions must be used. The LCSR method was developed to provide the in-situ response time testing capability that is needed to measure the in-service response times of RTDs.

The LCSR test is performed by connecting the RTD to one arm of a Wheatstone bridge and changing the bridge current from a few milliamperes to a level of about 40 to 80 milliamperes (Figure 3). The step change in current produces Joule heating in the RTD element and causes its resistance to increase in proportion to the RTD's ability to dissipate the heat to the environment. The transient change in RTD resistance produces a transient voltage signal at the output of the Wheatstone bridge which is referred to as the LCSR transient or the LCSR data for the RTD. This transient is then analyzed to provide the response time of the RTD under the conditions tested. The analysis involves fitting the LCSR transient to a heat transfer model to transform the internal heating data to yield the transient response time of the RTD as if it was exposed to a sudden change in the surrounding temperature. The details of the LCSR transfunction are covered in Reference 2.

The advantage of the LCSR test is that it permits on-line testing of installed RTDs from outside the reactor containment and provides the actual "in-service" response times of the RTDs. The test accounts for all installation effects on the RTD time constant. This includes the effect of the thermowell if one is used, the fit between the RTD and the thermowell, and all process condition effects such as the process temperature, pressure, and flow.

The accuracy of the LCSR results is better than $\pm$ 10 percent for RTDs which meet the LCSR assumptions. [2]

2.3 LCSR Validation

The validity of the LCSR test depends on two assumptions about the physical location of the sensing element in the sensing tip of the sensor. The two assumptions are:

1. The heat transfer between the sensor and its surrounding fluid must be one dimensional (radial).

2. The sensing element of the sensor must be located at the center of the sensor assembly or there must be little heat capacity between the sensing element and the centerline of the sensor assembly.

These assumptions must be satisfied for the heat transfer to and from the sensing element to be unidirectional and for the LCSR transient to be transformable to the plunge test transient. The only reliable and practical method to ensure that these assumptions are adequately satisfied and that the LCSR test is valid for the RTD is to perform experimental measurements. The validation should involve a plunge test followed by a LCSR test performed under the same test conditions on each RTD design to be validated. The LCSR data is then analyzed, and the response time

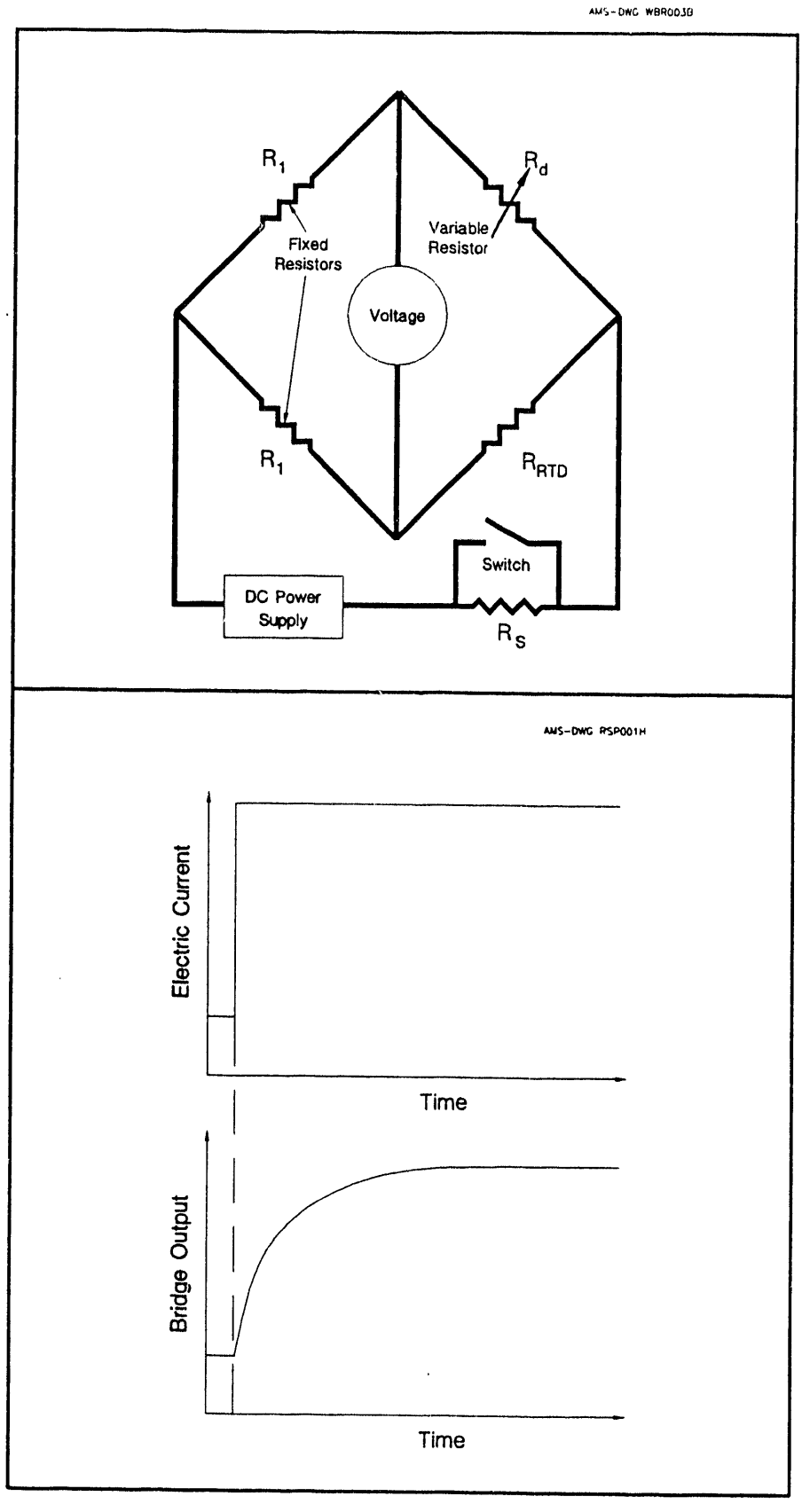


Figure 3. Illustration of Test Equipment and Principle of LCSR Method for RTDs.

result is compared with that of the corresponding plunge test result to establish the validity and determine the accuracy of the LCSR method for the sensor design being validated.

Table 1 presents typical validation results for representative RTDs tested in the laboratory in room temperature water at a flow velocity of 3 feet per second (~1 meter/second). The reasonable agreement between the plunge and the LCSR test results shown in this table indicates that the sensors shown are in-situ testable by the LCSR method.

Table 1

LCSR Validation Results for RTDs in Room Temperature Water Flowing at 3 feet/second

RTD Number	Response Time (sec) Plunge	LCSR	Percent Difference
1	7.1	7.2	1.4
2	6.3	6.6	4.8
3	4.9	4.9	0.0
4	5.2	5.3	1.9
5	2.8	2.6	-7.1
6	3.1	3.1	0.0
7	0.38	0.42	10.5
8	4.8	4.5	-6.3
9	4.6	4.2	-8.7
10	2.0	2.1	5.0
11	3.5	3.4	-2.9
12	2.7	2.9	7.4
13	11.7	12.3	5.1
14	2.0	2.1	5.0

The above results include various models of RTDs manufactured by Conax, RdF, Rosemount, and Weed. These four manufacturers provide almost all the RTDs that are used for safety-related temperature measurements in the U.S. nuclear power plants. LCSR validation tests have also been performed on RTDs used in nuclear power plants outside the U.S. An example is the Degussa RTDs used in several plants in Europe. Two models of this RTD have been successfully validated for LCSR testability.

In addition to the laboratory validation tests described above, the LCSR method has been validated in a test loop that simulated the conditions of a Pressurized Water Reactor (PWR). Sample results of these tests are shown in Table 2 for four RTDs of the types used in nuclear power plants. [3] The results listed under plunge test in Table 2 were actually obtained by

sudden injection of cold water upstream of the RTDs as installed in the test loop. A high speed reference thermocouple was attached to the tip of each RTD, and its output was used as the timing signal for the injection tests. The water in the test loop during the LCSR validation experiments was at a temperature of about 536°F (280°C), a pressure of approximately 2,320 psi (160 bars), and a flow velocity of approximately 16 to 20 feet per second (approximately 5 to 6 meter/second).

Table 2

Sample LCSR Validation Results for RTDs in PWR Conditions

RTD Number	Time Constant (sec) Plunge	LCSR	Percent Difference
1	6.2	5.9	-4.8
2	4.1	3.7	-9.8
3	8.8	8.4	-4.5
4	0.14	0.13	-7.1

3. RESPONSE TIME TESTING METHODS FOR PRESSURE TRANSMITTERS

The response time testing methods for pressure transmitters may be divided into two groups of tests as follows: 1) on-line methods which are based on new technologies developed or validated in the last five years, and 2) conventional methods which have been used since testing began about twenty years ago. Both the on-line methods and conventional methods are currently used in both PWRs and BWRs.

The advantage of the on-line methods is that they permit remote testing of pressure transmitters at normal operating conditions while the conventional tests require physical access to each transmitter and cannot usually be performed while the plant is operating. The disadvantage of the on-line methods is that they require sophisticated computer-aided data acquisition, data analysis, and interpretation techniques as opposed to the conventional methods which provide the response time of the transmitter directly. A description of the conventional methods and the on-line methods follows.

3.1 Conventional Methods

The conventional methods for response time testing of pressure transmitters usually involve a hydraulic pressure generator to produce a test signal in the form of a step or ramp. The ramp test is more commonly used than the step test because design basis accidents in nuclear power plants usually assume pressure transients which approximate a ramp.

Figure 4 shows a simplified diagram of a hydraulic pressure generator. The pressure test signal, as generated by this equipment, is applied to the transmitter under test and simultaneously to a high speed reference transmitter. The outputs of the two transmitters are recorded on a dual channel strip chart recorder or a similar device and used to identify the response time of the transmitter. Figures 5 and 6 show photographs of commercial equipment used to perform the ramp test. The first photograph is that of the original equipment developed under a research project sponsored by the Electric Power Research Institute (EPRI) about twenty years ago. [4] The second photograph is that of a new light-weight model developed in response to the nuclear industry's need for a more portable unit. This equipment can produce pressure signals which range from inches of water to several thousand psi.

Although, plants have been switching from conventional tests to on-line tests, there are transmitters in nuclear power plants which cannot be tested with the on-line methods. For example, the containment pressure transmitters in PWRs cannot be tested on-line using the noise analysis technique because there is no process noise to drive the transmitter. If these transmitters are force-balance, then they can be tested on-line using the PI method described later in this paper. Otherwise, the tests must be performed using the conventional ramp or step tests. Plants also use the conventional test methods to bench test a replacement transmitter before it is installed.

Figure 7 shows how the response time (τ) of a pressure transmitter is determined from the ramp test data. This response time value is sometimes referred to as the asymptotic ramp time delay. In practice, however, the response time of a pressure transmitter is usually defined as the time delay between the response of the reference transmitter and the test transmitter as they pass through a setpoint. This response time should have nearly the same value as the response time shown in Figure 7, provided that the transmitter is linear and has a nonoscillatory response. For step tests, the response time is determined in either of two ways: 1) the time required for the transmitter to pass through a setpoint, in which case the response time is referred to as "time to trip", or 2) the time required for the transmitter output to reach 63.2 percent of its final steady-state value. The latter definition corresponds to the response time of a first order system, and is used in defining the step response of pressure transmitters, even though pressure transmitters are not necessarily first order.

3.2 On-Line Methods

Two methods have been developed and validated for response time testing of pressure transmitters as installed in operating processes. These methods are referred to as the noise analysis and power interrupt (PI) tests. The noise analysis technique can be used for response time testing of most pressure transmitters, but the PI test is applicable only to force-balance pressure transmitters. Force-balance pressure transmitters are also testable by the noise analysis technique, but the PI test is more often used than noise analysis. This is because the PI test is a simpler test, and usually takes less time to perform than noise analysis, except for when noise analysis tests are performed on several transmitters at a time. A description of the noise analysis and PI tests follows.

3.2.1 Description of Noise Analysis Technique

The noise analysis technique is based on analyzing the natural fluctuations that exist at the output of pressure transmitters while the plant is operating. These pressure fluctuations (noise)

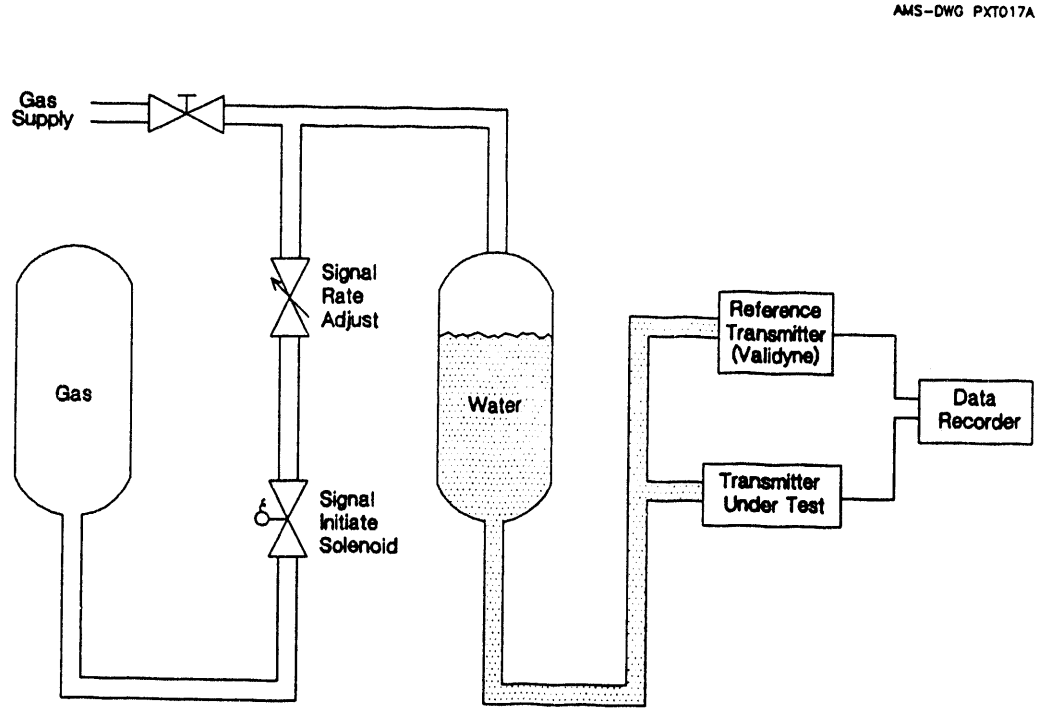


Figure 4. Principle of Operation of Pressure Signal Generator.

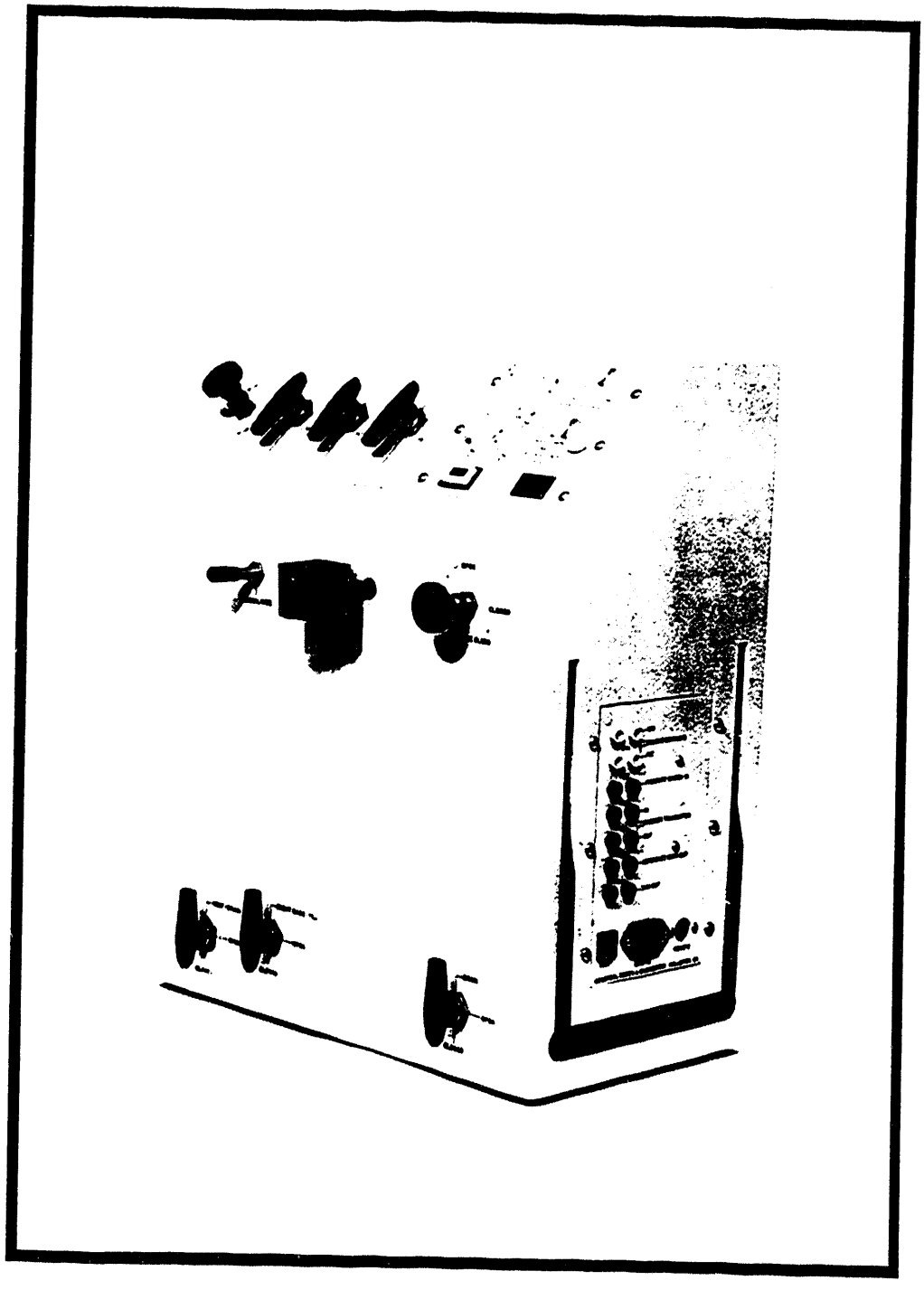


Figure 5. Original Version of Pressure Signal Generator.

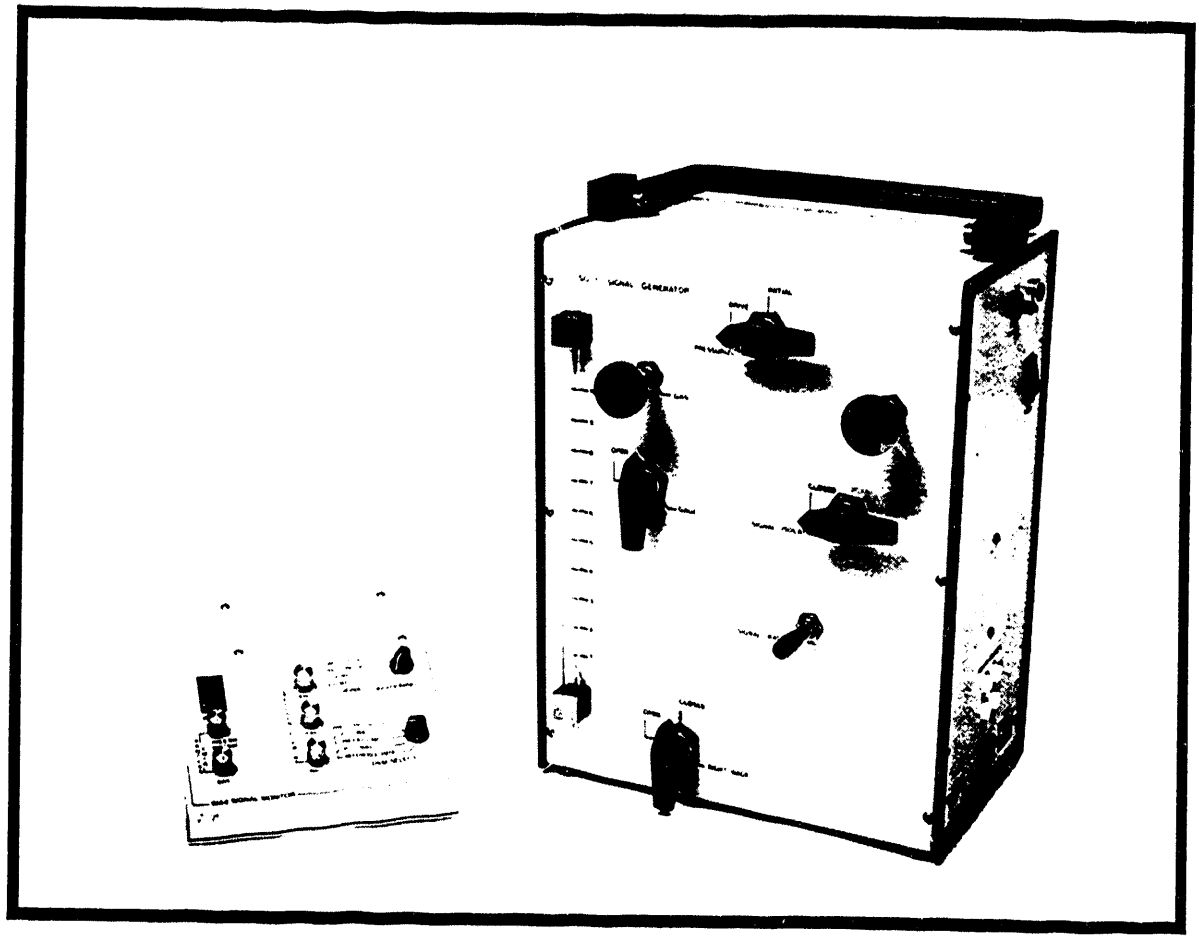


Figure 6. New Light-Weight Version of Pressure Signal Generator.

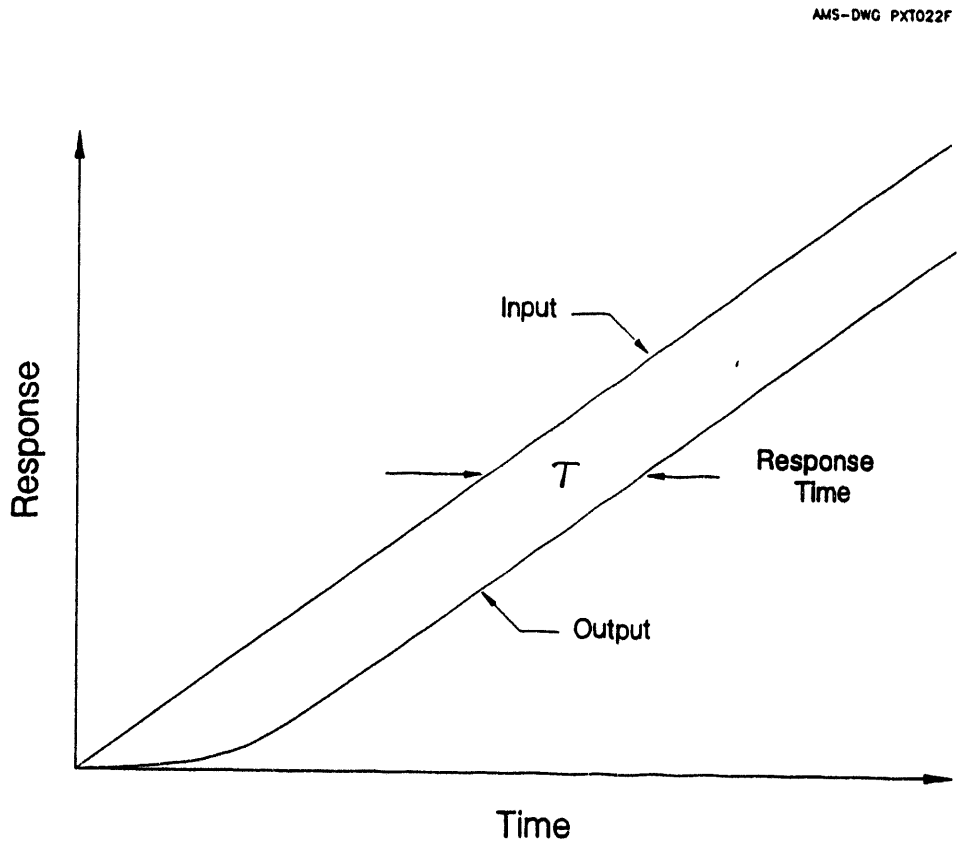


Figure 7. Illustration of Ramp Response.

are usually due to turbulence induced by the flow of water in the system, random heat transfer in the core, and other naturally occurring phenomena. The noise is superimposed on the DC output of the transmitter as shown in Figure 8. It is extracted from the transmitter output by removing the DC component of the signal, and amplifying the AC component. The DC component is removed by passing the sensor output through a high-pass filter, or adding a negative bias to the output. This leaves the AC component which is amplified and then passed through a low-pass filter for anti-aliasing and removal of high frequency electrical noise and interferences. The signal is then digitized by an analog to digital converter and subsequently analyzed. Figure 9 shows a photograph of the AMS noise test equipment. This equipment consists of a multichannel signal conditioning unit and a data acquisition and analysis computer. The signal conditioning unit contains a signal isolation device and a programmable filter/amplifier system. Several transmitters can be tested at a time using this equipment.

The noise analysis technique is advantageous in nuclear power plant applications because it is a passive test that can be performed remotely from the control room, does not interfere with plant operation, does not involve radiation exposure to the test personnel, and can be performed on several transmitters at a time. The test requires approximately one hour for each group of transmitters regardless of the number of transmitters in the group. Figure 10 shows the equipment set-up for testing of each transmitter. Figure 11 shows a 50 second trace of a raw noise data record for a pressure transmitter in a nuclear power plant. For each transmitter, 30 to 60 minutes of such noise data is recorded and analyzed to obtain the response time of the transmitter.

The analysis of noise data is performed in the frequency domain and/or time domain, and is based on the assumption that the dynamic characteristics of the transmitter are linear. The frequency domain and time domain analyses are independent methods for response time determination of pressure transmitters, and it is usually helpful to analyze the data with both methods and average the results.

For frequency domain analysis, the Power Spectral Density (PSD) of the noise signal is obtained through a Fast Fourier Transform (FFT) algorithm. An appropriate mathematical function is then fit to the PSD from which the response time of the transmitter is calculated. The PSDs of nuclear plant pressure transmitters have various shapes depending on the plant, the transmitter installation and service, the process conditions, and other effects. Figure 12 shows three PSDs of the shapes usually seen in nuclear power plants.

In the time domain analysis, the raw noise data is processed with a univariate autoregressive (AR) modeling program to obtain the impulse response (i.e., response to a narrow pressure pulse) and then the step response of the transmitter from which the transmitter response time is calculated. After the data is analyzed in the frequency domain and time domain, the response time results are averaged, and the average value is reported as the response time of the transmitter tested.

The in-plant noise tests for each transmitter are often repeated for three frequency bands from near DC to 10 Hz, 100 Hz, and 1000 Hz to cover the entire frequency spectrum over which the sensor response time may lie. The data for each of the frequency bands are analyzed separately, the outliers are rejected, and the remaining results are averaged to provide a single frequency domain and a single time domain result. These two results are then averaged together as appropriate to give the response time of the transmitter.

AMS-DWG PXT093G

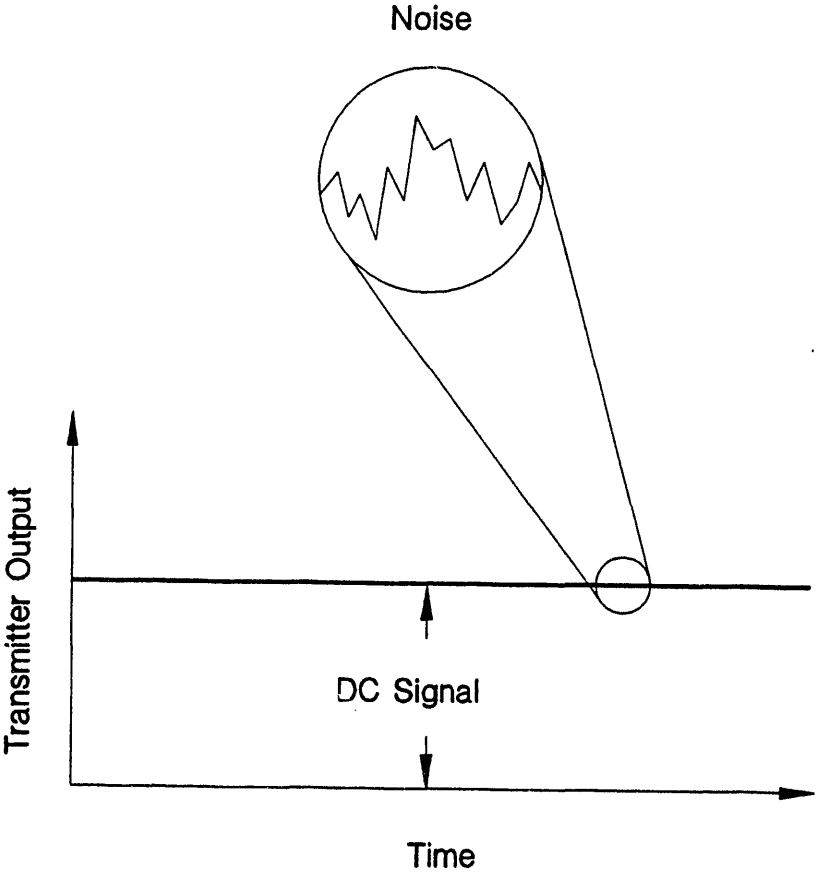


Figure 8. Illustration of Process Noise on the DC Output of a Pressure Transmitter.

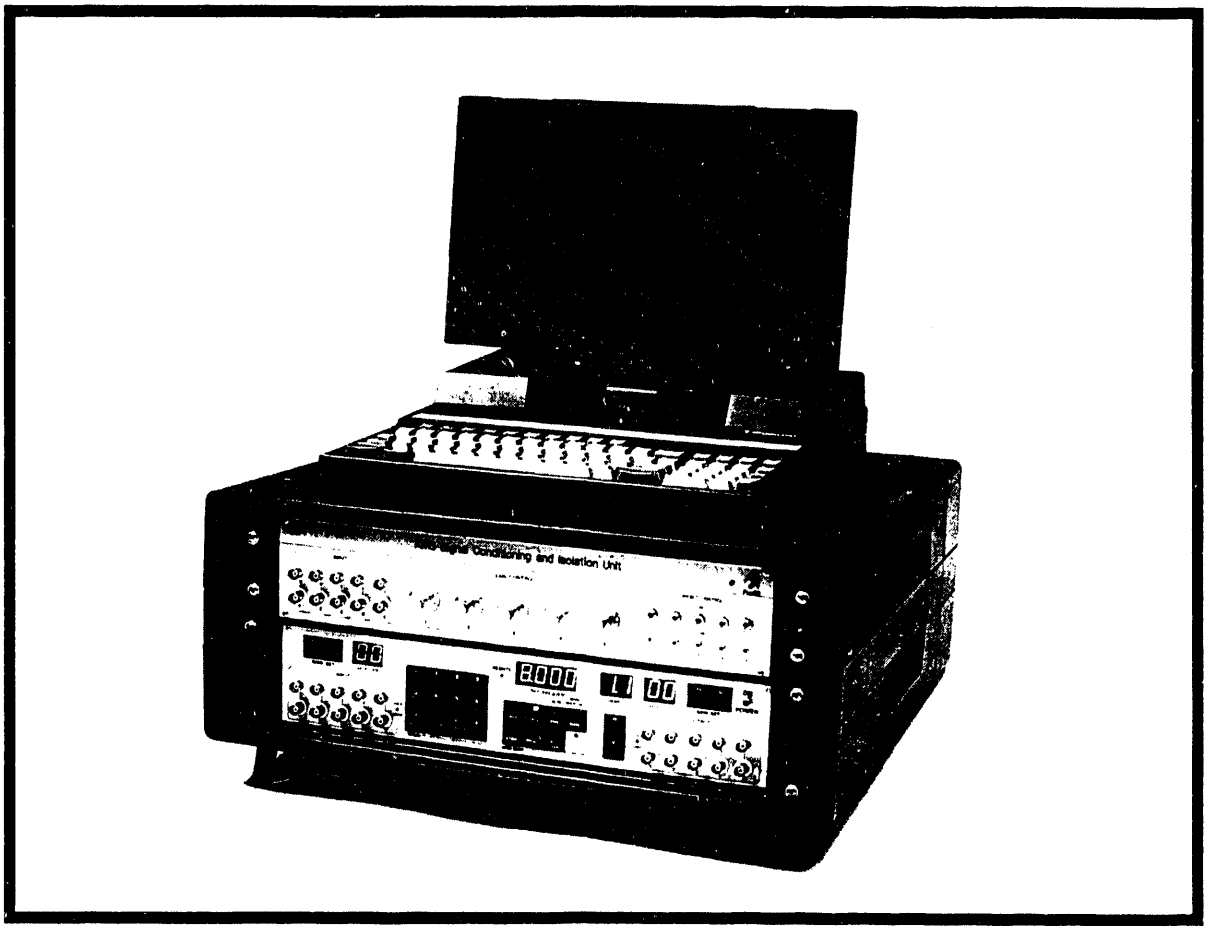


Figure 9. Integrated Equipment for Noise Data Acquisition and Data Analysis.

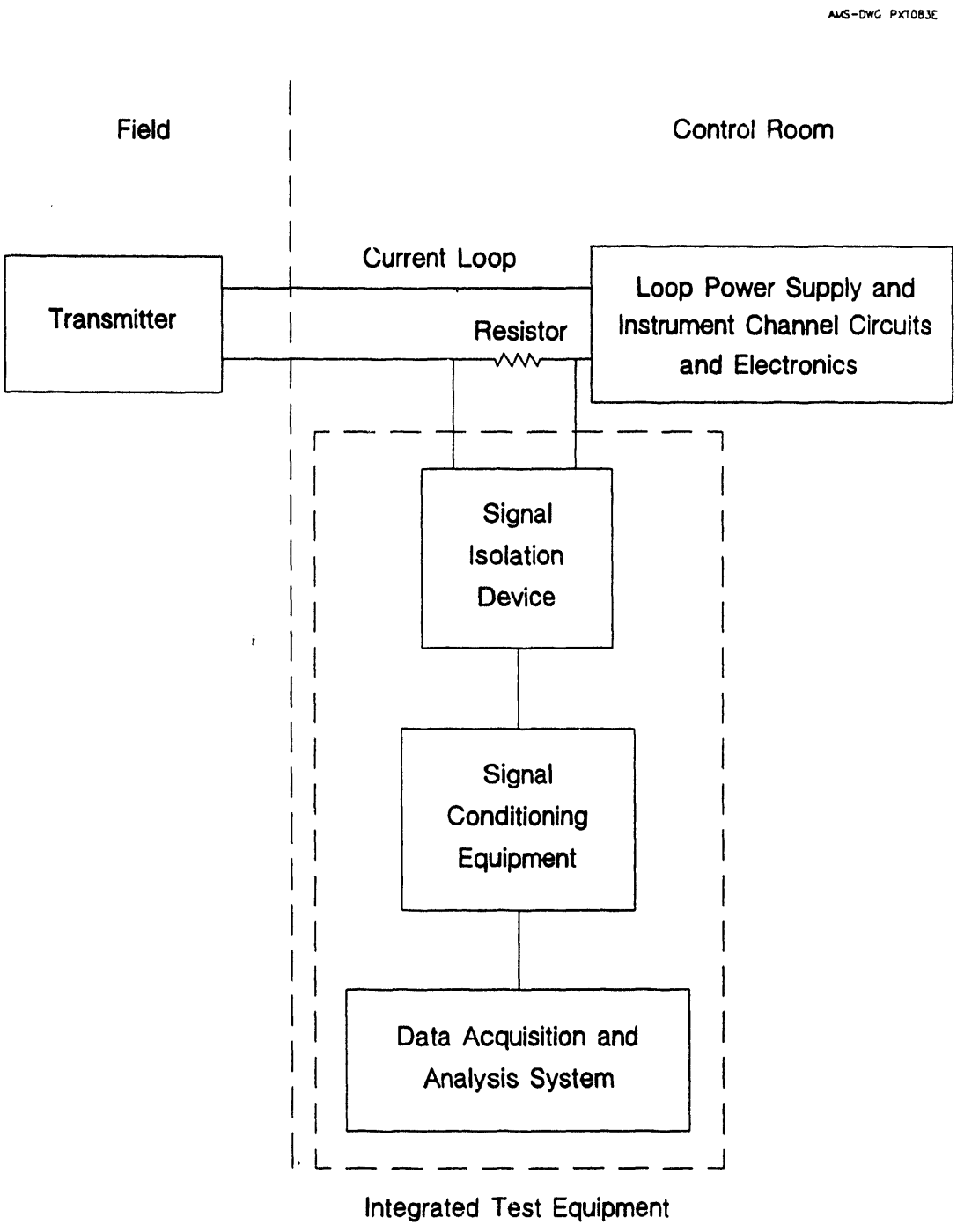


Figure 10. Equipment Set-Up for On-Line Measurement of Response Time of Pressure Transmitters.

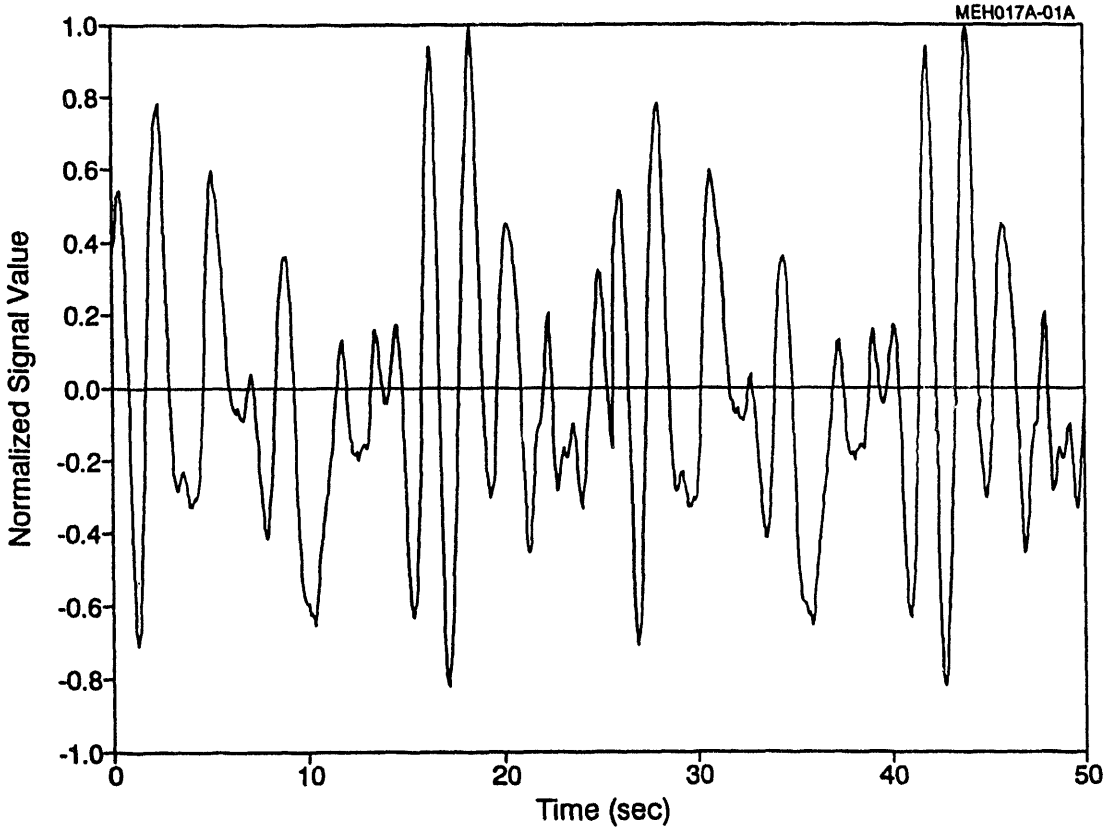


Figure 11. A 50 Second Portion of a Noise Data Record.

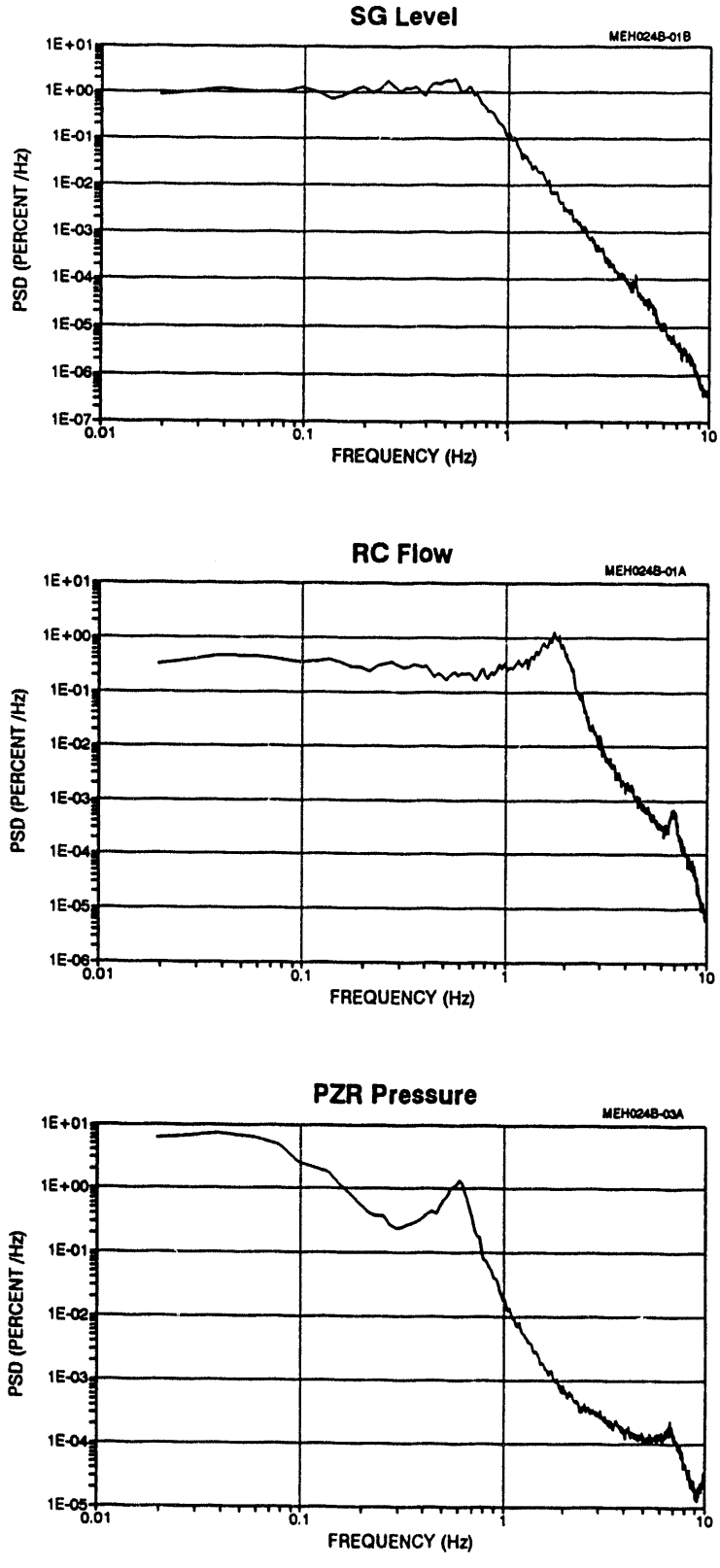


Figure 12. Typical PSDs of Nuclear Plant Pressure Transmitters.

The validity of the noise analysis technique has been examined by laboratory testing of representative Barton, Foxboro, Rosemount, Tobar (Veritrak), Fischer & Porter, Schlumberger (Bailey), and Statham (Gould) pressure transmitters of the types used in nuclear power plants.[5,6] Based on the results of the laboratory validation tests, the noise analysis technique has been found to be generally successful in providing the response times of pressure transmitters to within better than ± 0.10 seconds of the results that are obtained by the conventional ramp or step tests. For in-plant tests, experience has shown that the noise analysis method generally provides conservative response time results, provided that the process noise that excites the transmitter is free of interfering resonances. In some situations, the bandwidth of the process noise that drives the transmitters may be much smaller than the frequency response of the transmitter. In these situations, the PSD of the transmitter noise signal would be dominated by the process bandwidth and would therefore result in an excessively conservative response time value for the transmitter.

Prior to any time domain or frequency domain analysis, the suitability of the noise data for a reliable analysis must be examined by a computer scanning and screening of the raw data. This is accomplished using data qualification algorithms that check for the stationarity and linearity of the data. This includes plotting the Amplitude Probability Density (APD) of the data for inspection for skewness and nonlinearity as well as calculating the skewness, flatness, or other descriptors of the noise data record to ensure that the data record has a normal distribution and does not contain saturated blocks and other undesirable characteristics. Figure 13 shows two APDs for a normal and a skewed noise signal. A large skewness is usually indicative of nonlinearity of the transmitter or the noise data.

3.2.2 Power Interrupt Technique

The power interrupt (PI) test is a method for in-situ response time testing of force-balance pressure transmitters. The test is based on a momentary interruption of the electrical supply power normally used to activate the transmitter. It is performed by turning the power to the transmitter OFF for a few seconds and then ON. As soon as the power is turned off, the lever system in the transmitter deflects until it comes to a physical stop inside the transmitter. When the power is turned ON, the force motor brings the lever system back to the equilibrium position. While the system is returning to the equilibrium position, the transmitter will output a transient signal which can be analyzed to give the response time of the transmitter. This response time corresponds to the response time which would be obtained using the conventional step or ramp tests.

The PI transient typically begins with switching spikes followed by a ramp output which lasts until the force motor has built up enough force to move the mechanical system of the transmitter away from the stop and back to the equilibrium position. The rate of this ramp signal is referred to as the critical ramp rate.

The ramp output of a transmitter in the PI test is followed by a transient which contains the response time of the transmitter. This transient is separated from the ramp output by a numerical algorithm. It is then analyzed by a mathematical fitting procedure to give the response time of the transmitter.

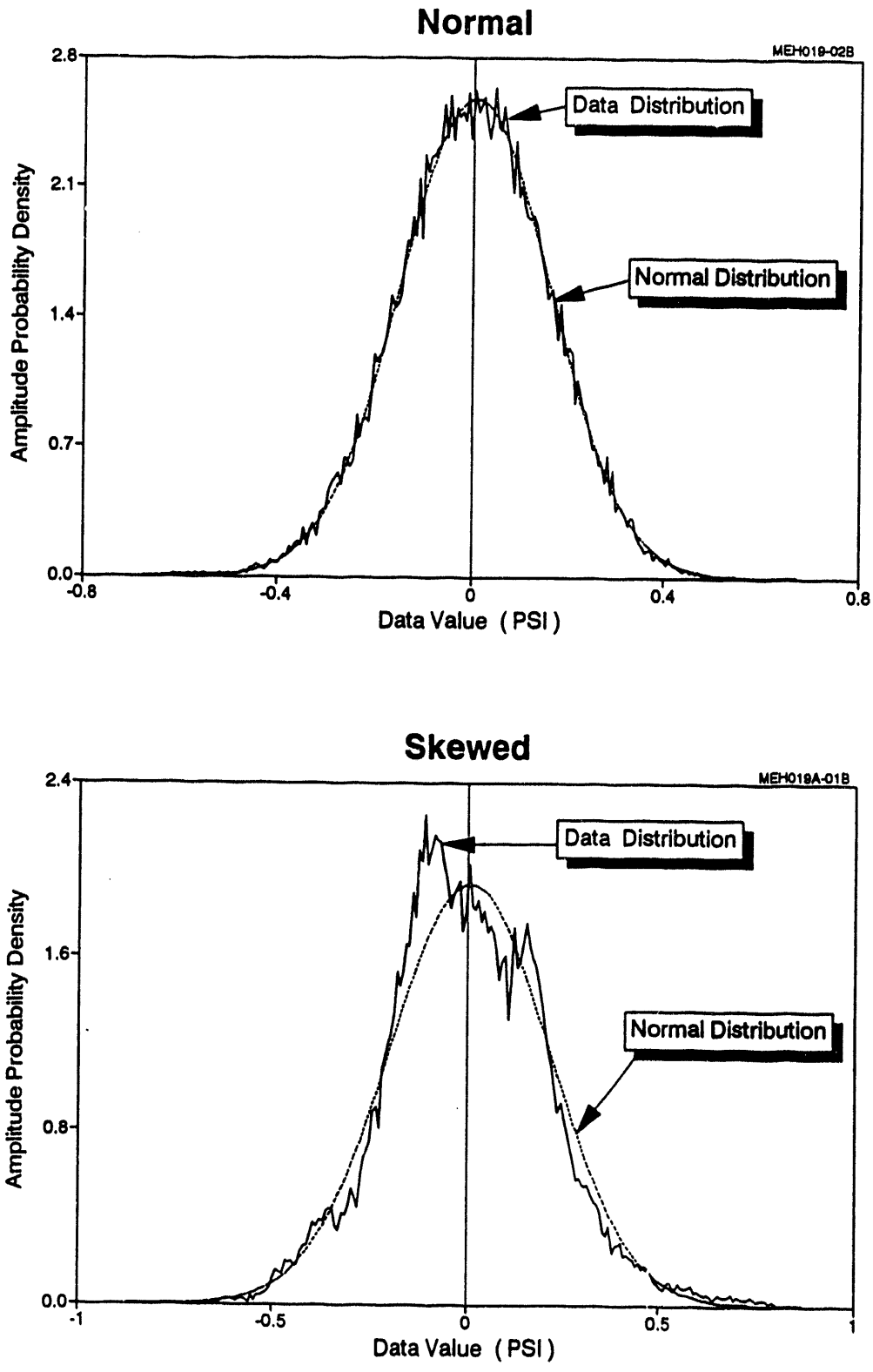


Figure 13. Normal and Skewed Noise Signal APDs.

Figure 14 shows three commonly encountered PI transients we have observed to date in nuclear power plants. The three PI transients include one that is clean and free of any noise or fluctuations, one that contains some low frequency oscillations, and one that has an overshoot. The effect of the noise and fluctuations can often be reduced by repeating the PI tests several times, analyzing the individual tests, and averaging the results. In the standard procedure for the PI test, the test is usually repeated ten times for each transmitter, and the response time results of the individual tests are averaged to give the response time of the transmitter.

The PI test accounts for the response time of both the mechanical and the electronic components in the transmitter and thereby gives the response time of the complete electromechanical system of the transmitter. The validity of the PI test has been examined in laboratory tests by comparing the results of the PI test with those of the conventional ramp or step tests performed on a number of force-balance pressure transmitters. The laboratory validation tests have shown that the PI method is generally successful in providing the response time of force-balance pressure transmitters to within better than ± 0.10 seconds of corresponding response time values obtained from the conventional methods provided that: 1) the dynamic characteristics of the transmitters are predominantly linear, and 2) the step or ramp pressure signals used in the conventional tests are not so large as to cause the mechanical system of the transmitter to come to a physical stop inside the transmitter. The second assumption may be restated as follows: the PI test results correspond to the results of the conventional tests for a ramp input pressure with a ramp rate that is less than the critical ramp rate of the transmitter. More specifically, in expressing response time results from the PI test, it is assumed that the response time of interest in meeting a plant's technical specification is the response which would be obtained using an input ramp signal with a ramp rate that is less than the critical ramp rate of the transmitter.

4. CONCLUSION

The response times of temperature and pressure sensors in nuclear power plants can be measured remotely from the control room area while the plant is operating. The test methods which can be used for these measurements were described in this paper. These methods have been validated and commercial equipment and services have been developed for routine testing in nuclear power plants.

5. REFERENCES

1. ASTM Standard E644-86, Standard Methods for Testing Industrial Resistance Thermometers, 1988 Annual Book of ASTM Standards, Vol. 14.03-14, American Society for Testing and Materials (1986).

2. HASHEMIAN, H.M., PETERSEN, K.M., Loop Current Step Response Method For In-Place Measurement of Response Time of Installed RTDs and Thermocouples, Seventh International Symposium on Temperature, Vol. 6, American Institute of Physics, New York, NY (1992).

3. HASHEMIAN, H.M., JACQUOT, J.P., and GUERIN, B., Preliminary Report: Response Time Testing of Resistance Temperature Detectors (RTDs) in EDF Test Loop, EDF Report Number HP/236/79/04, Electricite de France, Paris, France (1978).

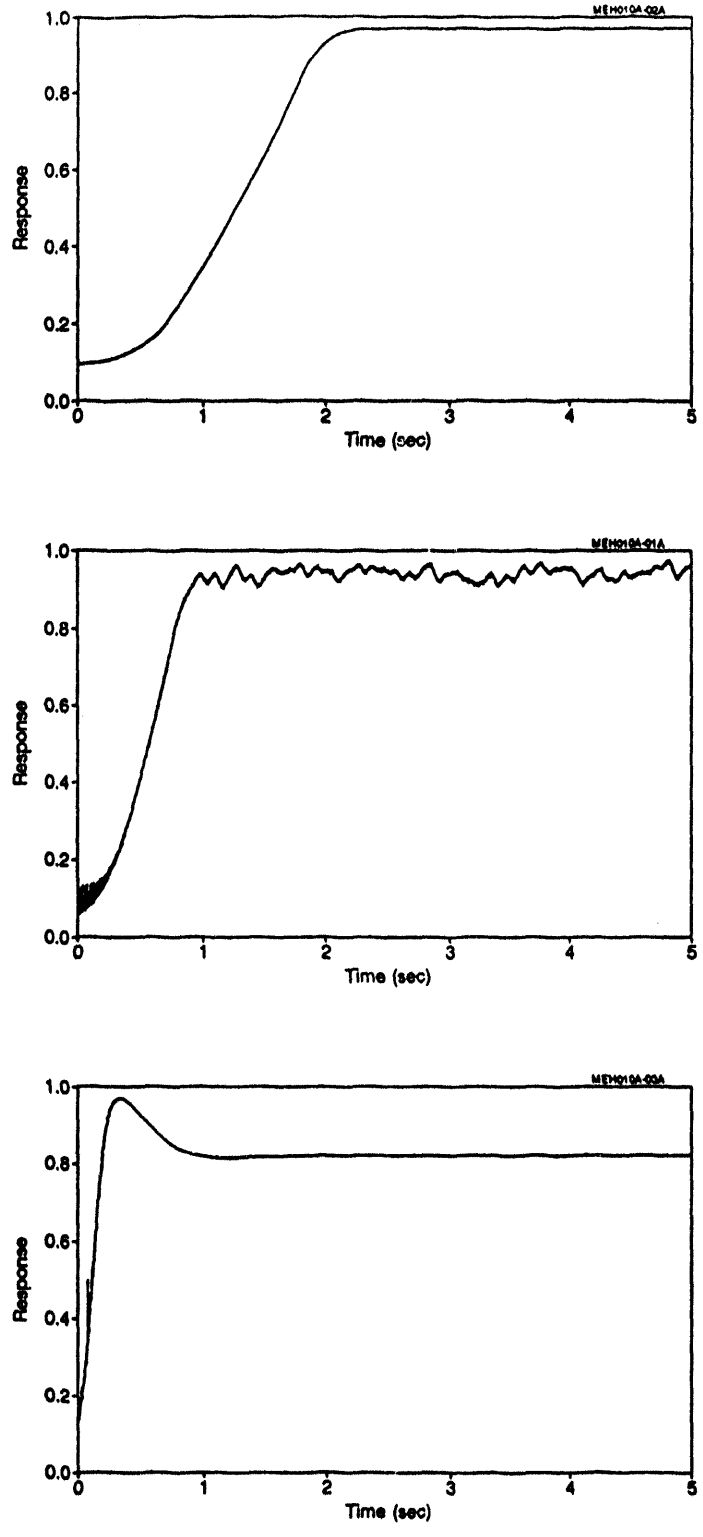


Figure 14. Typical PI Test Transients from Response Time Testing of Force-Balance Pressure Transmitters in Nuclear Power Plants.

4. FOSTER, C.G, et. al., Sensor Response Time Verification, Report No. NP-267, Electric Power Research Institute, Palo Alto, California (1976).

5. HASHEMIAN, H.M., et. al., Effect of Aging on Response Time of Nuclear Plant Pressure Sensors, NRC Report Number NUREG/CR-5383, U.S. Nuclear Regulatory Commission, Washington, D.C. (1989).

6. H. M. HASHEMIAN, et. al., Long Term Performance and Aging Characteristics of Nuclear Plant Pressure Transmitters, NRC Report Number NUREG/CR-5851, U.S. Nuclear Regulatory Commission, Washington, D.C. (1993).

FIGURES

Figure 1. Illustration of Principle of Plunge Test and Measurement of Response Time in Terms of Time Constant.

Figure 2. Effect of Fluid Flow and Fluid Temperature on Response Time of Temperature Sensors.

Figure 3. Illustration of Test Equipment and Principle of LCSR Method for RTDs.

Figure 4. Principle of Operation of Pressure Signal Generator.

Figure 5. Original Version of Pressure Signal Generator.

Figure 6. New Light-Weight Version of Pressure Signal Generator.

Figure 7. Illustration of Ramp Response.

Figure 8. Illustration of Process Noise on the DC Output of a Pressure Transmitter.

Figure 9. Integrated Equipment for Noise Data Acquisition and Data Analysis.

Figure 10. Equipment Set-Up for On-Line Measurement of Response Time of Pressure Transmitters.

Figure 11. A 50 Second Portion of a Noise Data Record.

Figure 12. Typical PSDs of Nuclear Plant Pressure Transmitters.

Figure 13. Normal and Skewed Noise Signal APDs.

Figure 14. Typical PI Test Transients from Response Time Testing of Force-Balance Pressure Transmitters in Nuclear Power Plants.

ANALYSIS AND
MEASUREMENT SERVICES
CORPORATION

AMS 9111 CROSS PARK DRIVE / KNOXVILLE, TN 37923 USA (615) 691-1756

IAEA1-5

IN-SITU MEASUREMENT OF RESPONSE TIME OF RTDs AND PRESSURE TRANSMITTERS IN NUCLEAR POWER PLANTS

H. M. Hashemian

Presented At

IAEA Specialists Meeting
Ramada Inn at Congressional Park
Rockville, Maryland
May 5-7, 1993

IAEA1-7

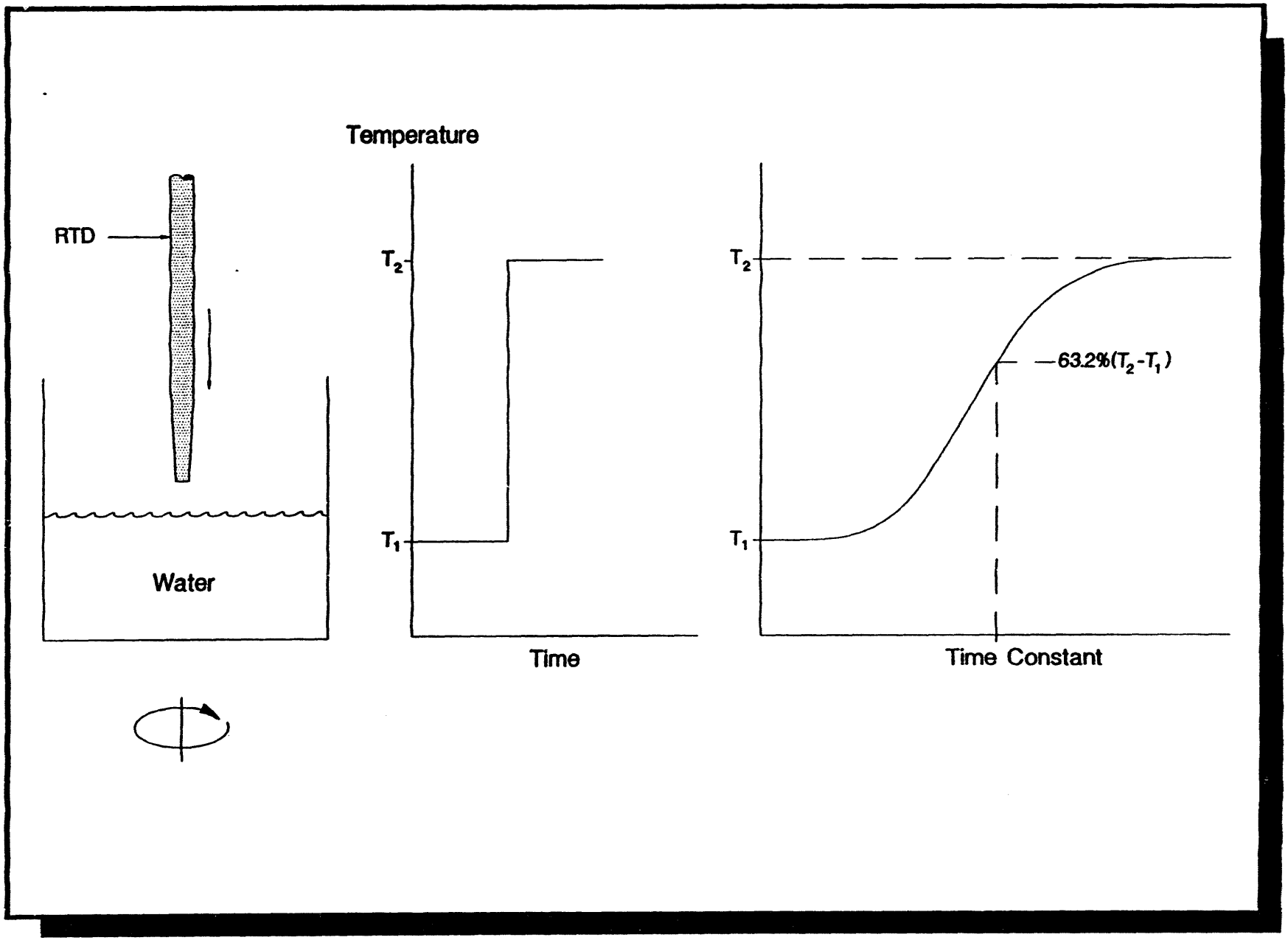
RESPONSE TIME TESTING METHODS

RTDs

- Plunge Test
- LCSR Test

Pressure Transmitters

- Noise Analysis
- PI Test


Temperature
RTD
Water
T_2
T_1
Time
T_2
T_1
63.2%(T_2-T_1)
Time Constant

TIME CONSTANT AS A FUNCTION OF ENVIRONMENT

Sensor #	Time Constant (sec) Water	Air
RTDs		
1	2.0	14.4
2	2.7	22.0
3	3.6	24.0
Thermocouples		
1	1.3	15.0
2	1.3	14.8
3	2.0	15.3

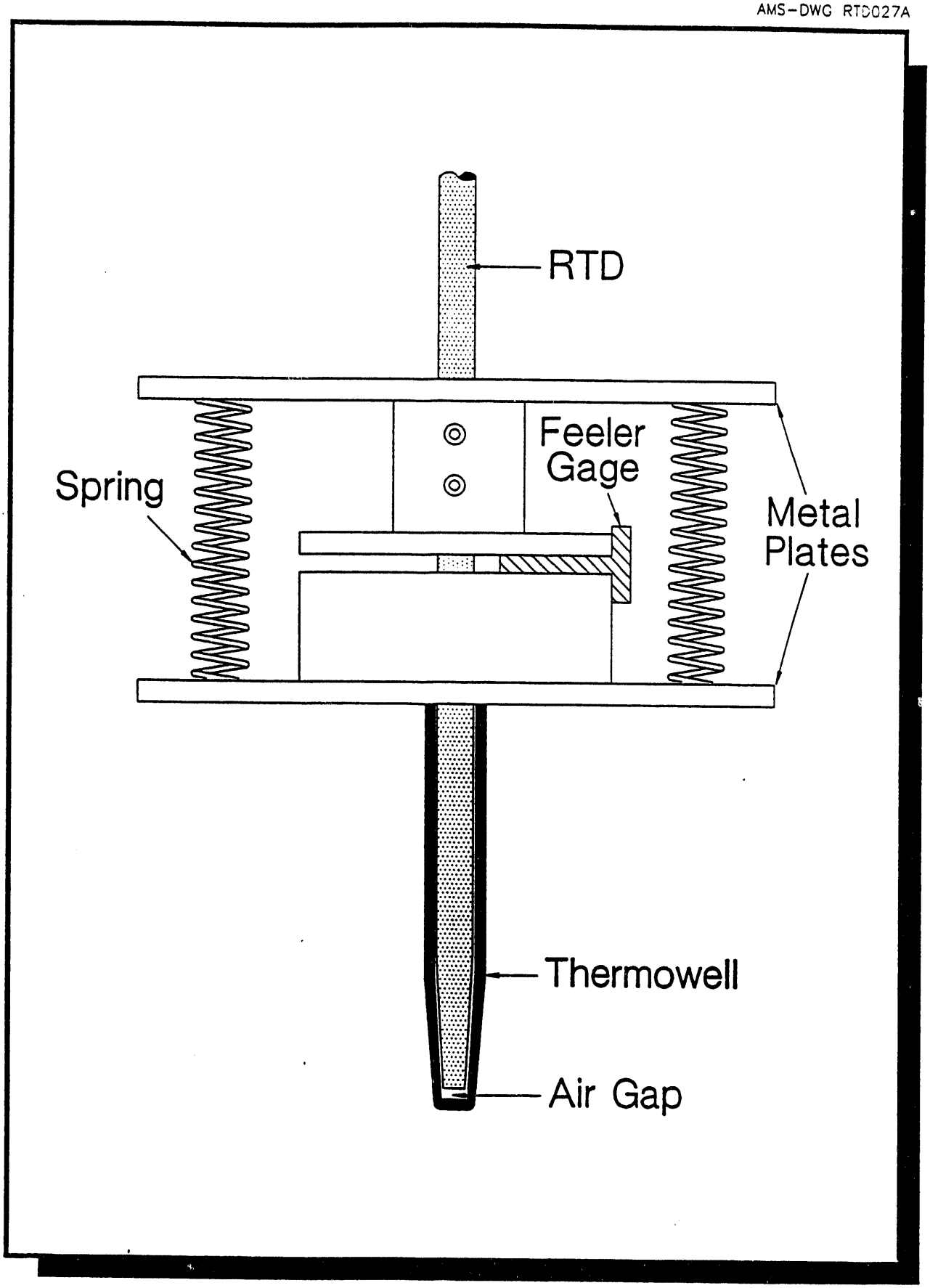
Water at 1 m/s. Air at 16 m/s.

RTD Time Constants With and Without Thermowell

RTD I.D.	Time Constant (sec) No Well	Well #1	Well #2	Well #3
1	1.7	4.8	5.2	6.0
2	1.8	3.6	4.1	4.6
3	1.9	4.4	4.9	5.9

Note: Above results are for three identical RTDs tested in three identical thermowells.

AMS-DWG RTD027A



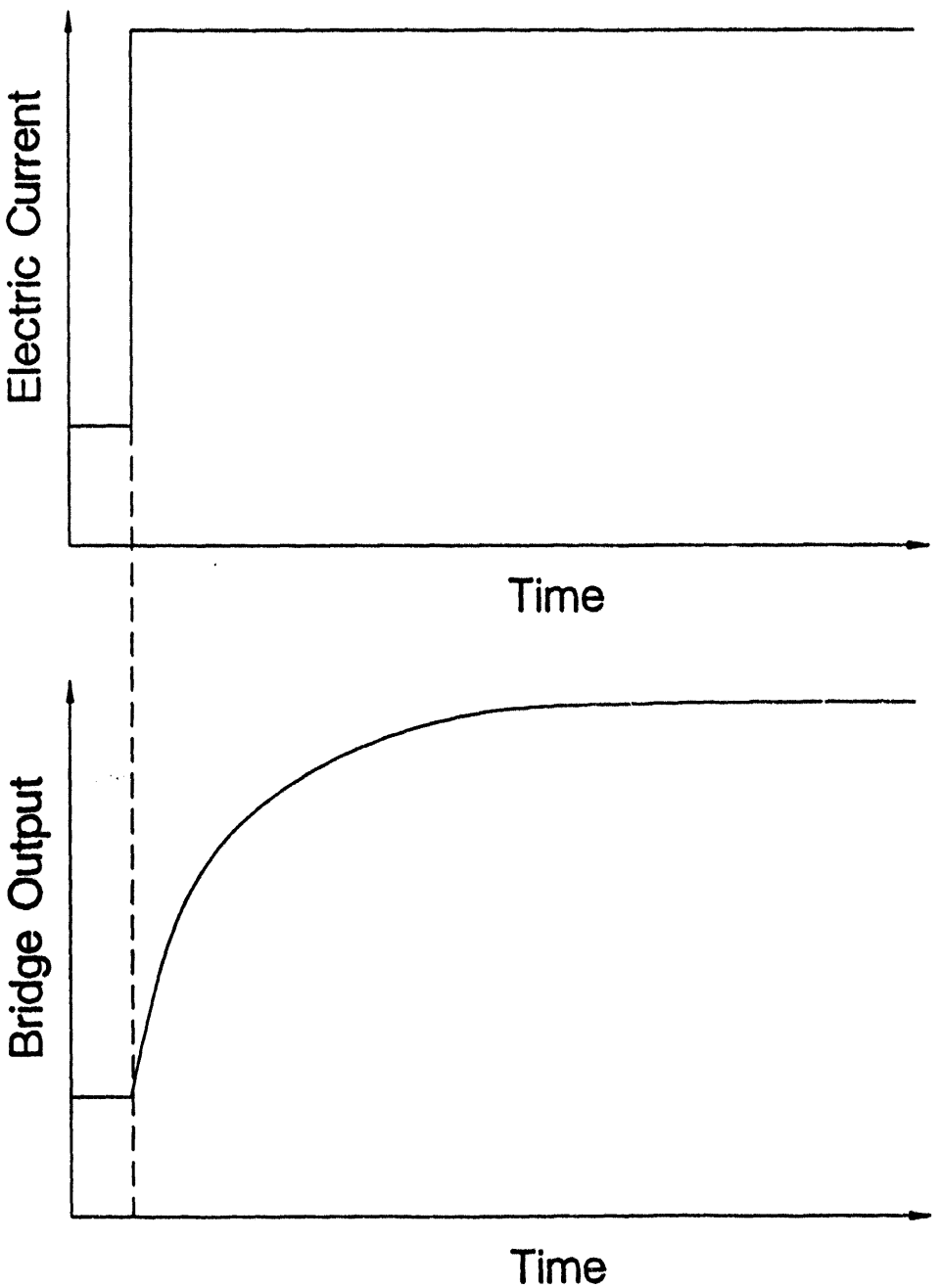
Response Time Changes in Well-Type RTDs

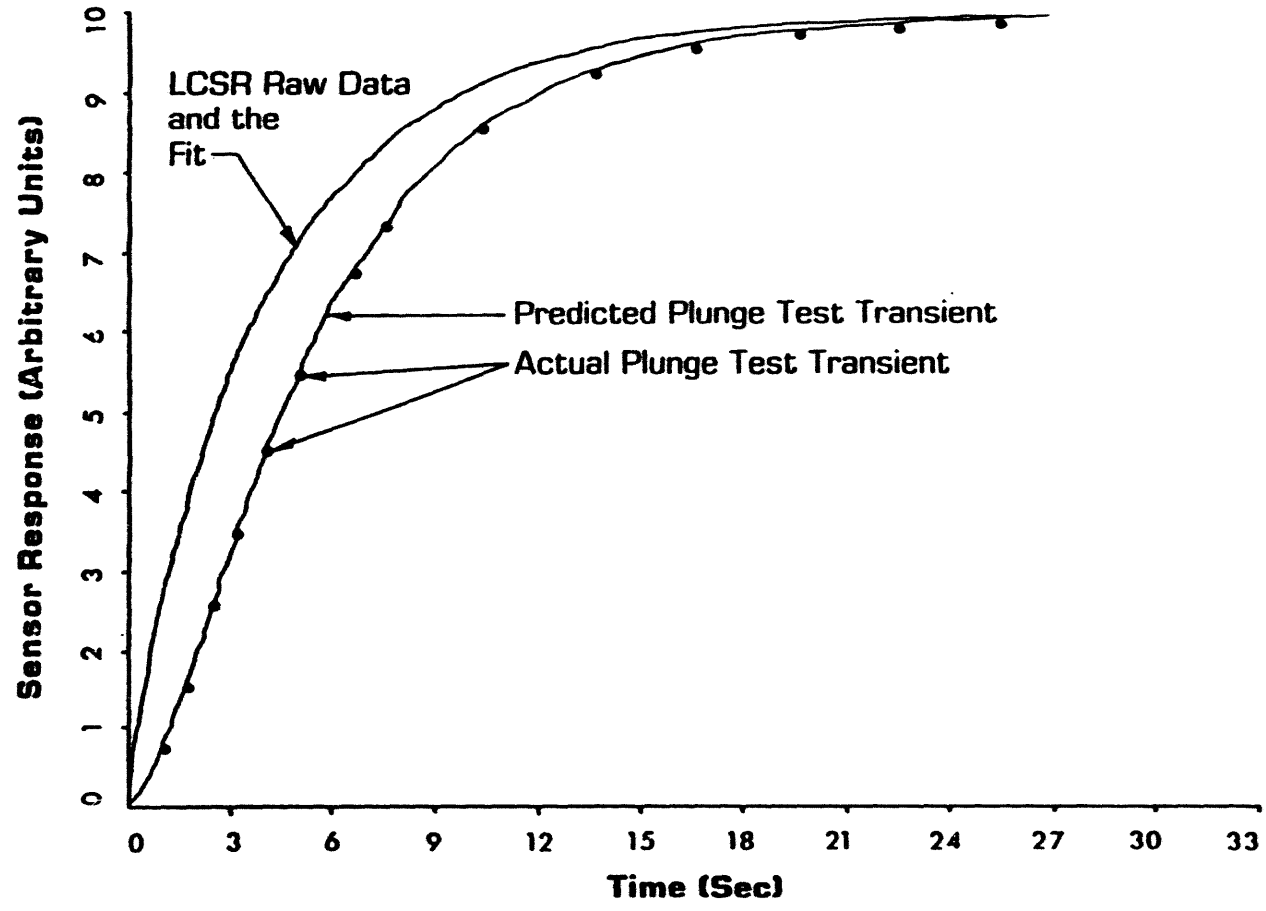
Gap Size (mm)	Time Constant (Seconds)
0	6.3
0.006	7.1
0.010	8.0
0.016	8.9
0.022	9.5
0.035	10.5

In water @ 1 meter/sec.

Loop Current Step Response Test (LCSR)

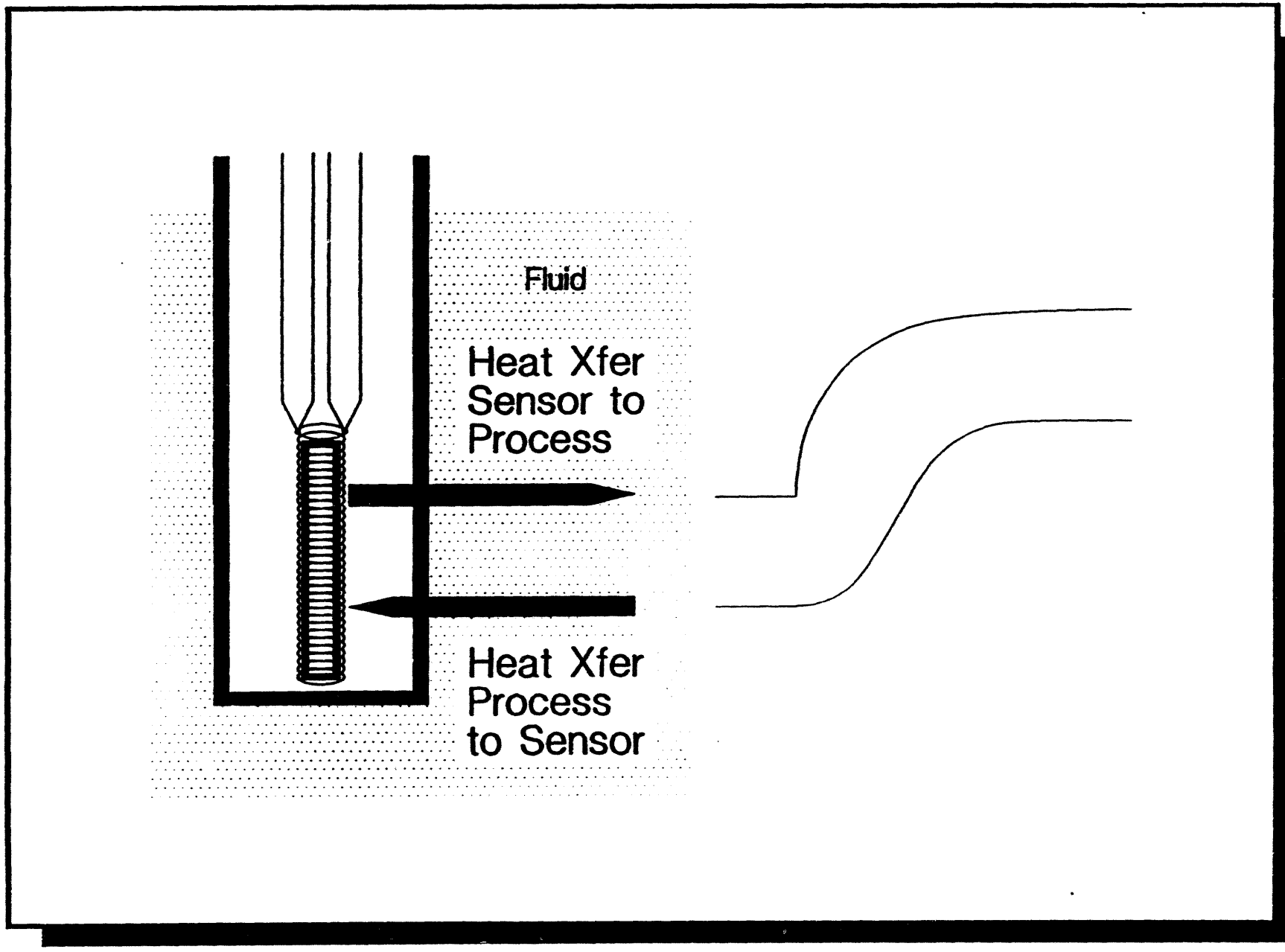
Illustration of the LCSR Test





LCSR Test Results for a Laboratory Test of Rosemount 104ADA RTD.

AMS-DWG RSP006A



Laboratory Validation of LCSR Test

RTD Model	Time Constant (sec) Plunge	LCSR	Percent Difference
176KF	0.38	0.42	+10.5
104ADA (no well)	3.1	3.1	0.0
104ADA (well)	7.1	7.2	+1.4
104VC (no well)	2.3	2.1	- 8.7
104VC (well)	5.3	5.5	+3.8
Sostman 8606	2.0	2.1	+5.0
177GY (El. 1)	5.8	6.2	+6.9
177GY (El. 2)	6.1	6.3	+3.3

Reference: EPRI Report No. NP-1486

Examples of LCSR Validation Results

Rosemount RTDs	Time Constant (sec) Plunge Test	Time Constant (sec) LCSR Test	Percent Difference
Laboratory Conditions			
104AFC	5.3	5.2	-1.8
104 & NS	3.9	3.9	0.0
177HW	11.7	12.3	+5.1
176KF	0.42	0.41	-2.4
PWR Operating Condtions			
104AFC	6.2	5.9	-4.8
104 & NS	4.1	3.7	-9.8
177HW	8.8	8.4	-4.5
176KF	0.14	0.13	-7.1

Reference: EPRI Report No. NP-1486

LCSR Validation Results

Item	Time Constant (sec) Plunge	LCSR
1	6.8	7.0
2	6.3	6.6
3	7.3	7.6
4	4.9	4.9
5	5.2	5.3
6	4.6	4.7
7	2.8	2.6
8	2.7	2.4
9	2.6	2.5
10	3.5	3.2
11	2.9	2.7
12	3.5	3.3
13	4.8	4.5
14	4.6	4.2
15	2.0	2.1
16	3.5	3.4
17	2.7	2.9
18	6.6	6.3
19	4.6	5.0
20	5.9	6.1

Above results include various models of RdF, Weed, Conax, and Sostman RTDs. References are APS8402, DPC8702, PGE 7/88 Notebook, LPL8302 & 862, MIL8801, PSG8803, Conax File, etc.

RESPONSE TIME TESTING OF PRESSURE TRANSMITTERS IN NUCLEAR POWER PLANTS

TEST METHODS

Conventional Methods

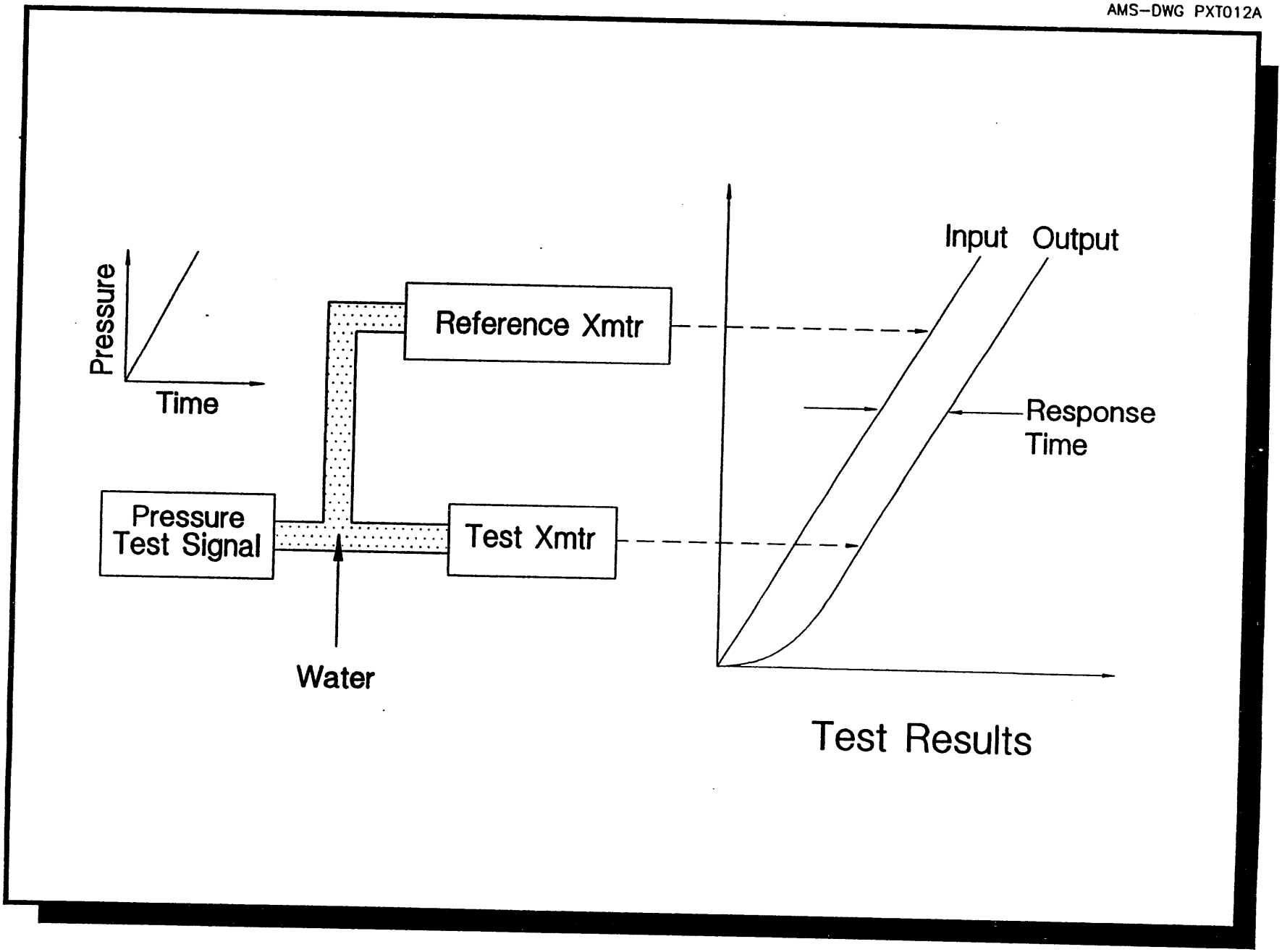
- Substitute Process Variable Test (Step Test, Ramp Test, etc.)

In-Situ Methods

- Noise Analysis Technique
- Power Interrupt Test

Conventional Test Procedure

- Valve-off the sensing lines
- Inject a test signal to the transmitter
- Measure the transmitter delay with respect to a high speed reference transmitter


Pressure
Time
Reference Xmtr
Pressure
Test Signal
Test Xmtr
Water
Input
Output
Response
Time
Test Results

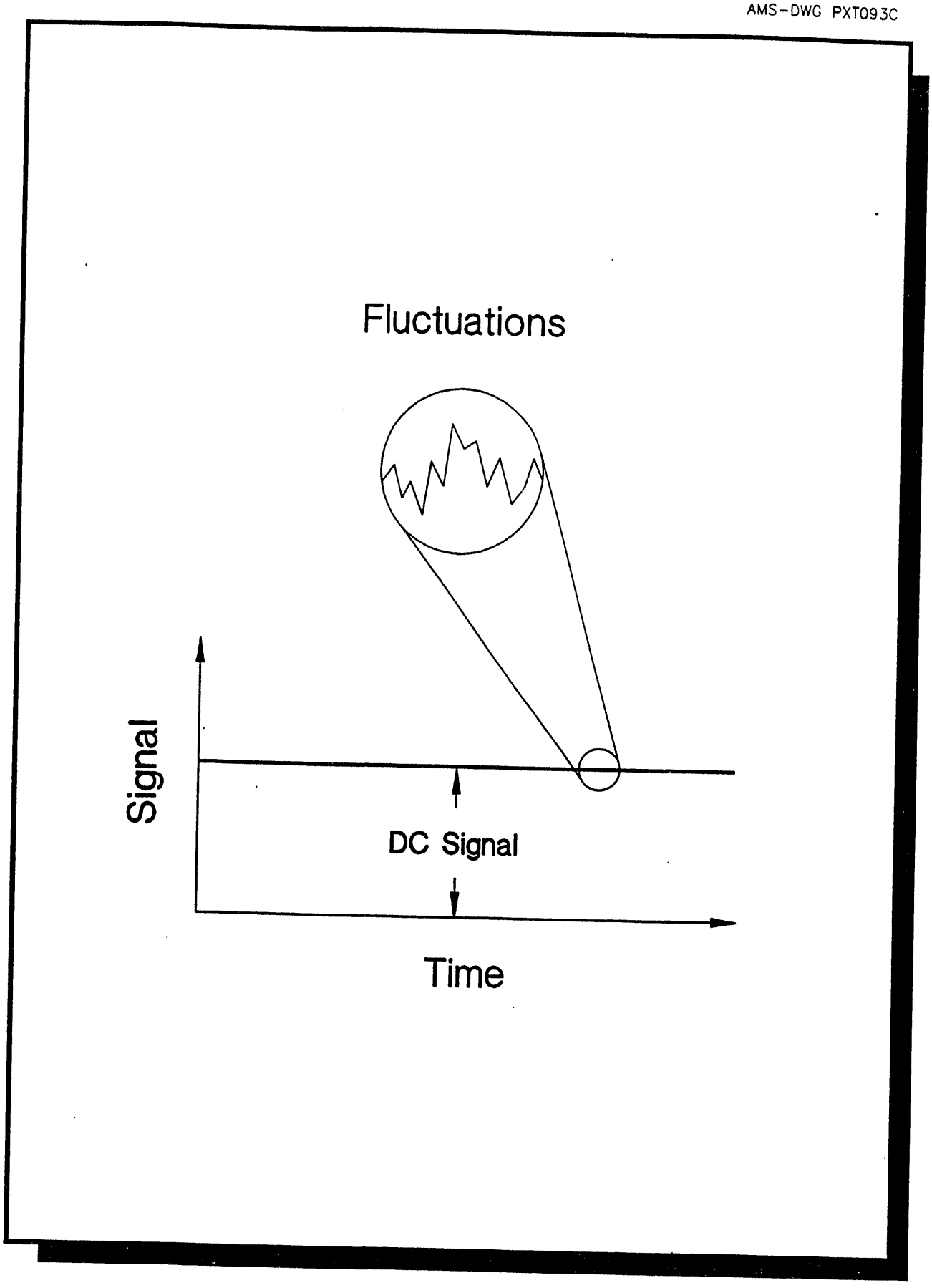
ON-LINE METHODS

POWER INTERRUPT TEST

Applicable to force balance transmitters. Have been validated for Foxboro and Fischer & Porter transmitters.

NOISE ANALYSIS

Applicable to all transmitters. Results include any delays due to sensing lines.


Fluctuations
Signal
DC Signal
Time

ANALYSIS OF NOISE DATA TO OBTAIN RESPONSE TIME

Time Domain

- Data Qualification
- Autoregressive Modeling (AR)

Frequency Domain

- FFT
- PSD
- Function Fit

VALIDATION PROCESS

- Laboratory Validation
- In-Plant Implementation
- Equipment/Software Validation
- Documentation
- Routine In-Plant Measurements

Noise Analysis Validation Results

BARTON

Tag	Response Time (sec) Ramp	Noise	Difference (sec)
PS19	.05	.11	.06
PS20	.17	.18	.01
PS23	.17	.22	.05
PS29	.12	.12	.00
PS30	.12	.16	.04
PS34	.11	.13	.02
PS36	.11	.13	.02
PS38	.12	.15	.03
PS40	.11	.14	.03
PS41	.11	.14	.03

Noise Analysis Validation Results

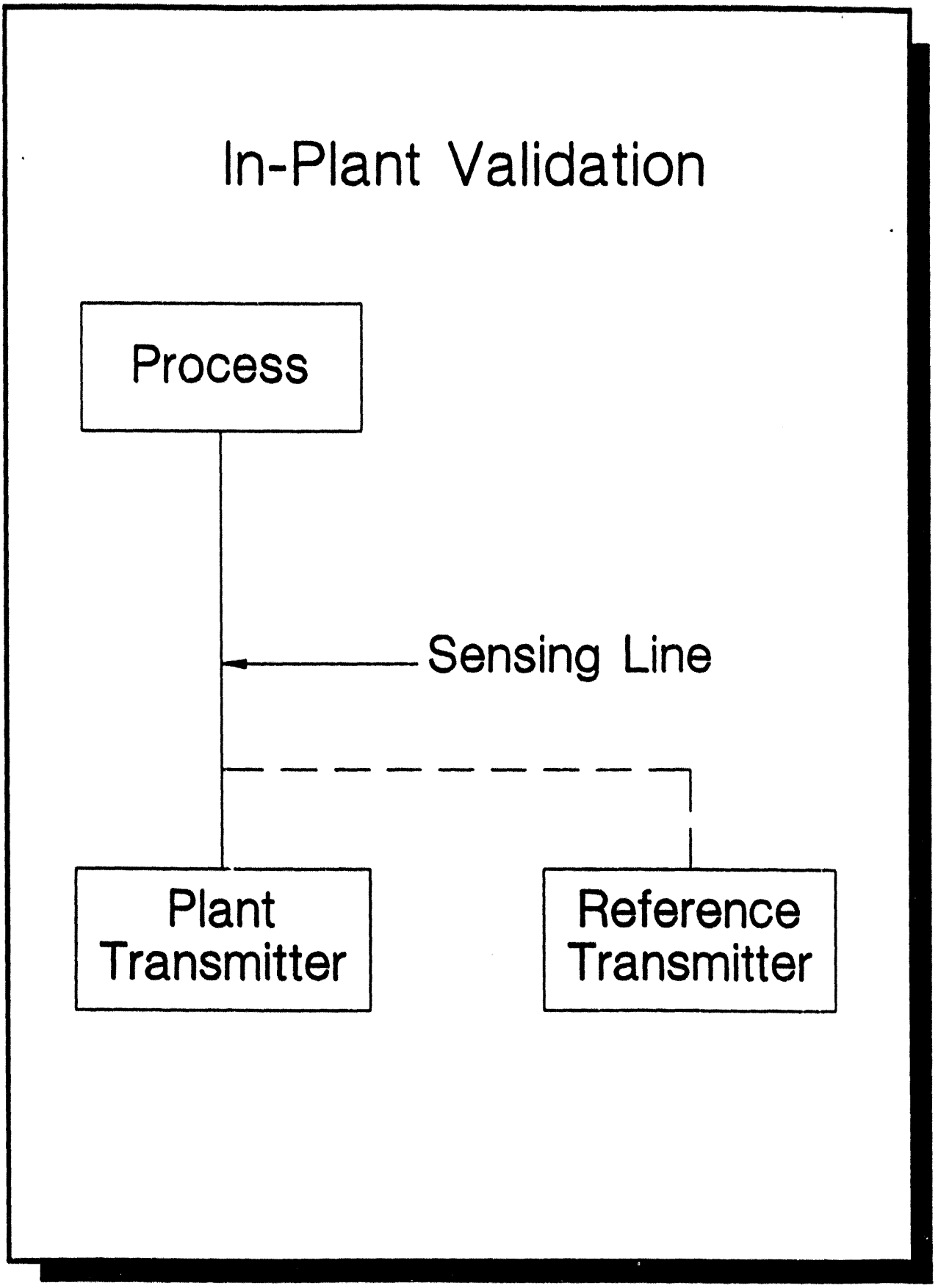
ROSEMOUNT

Tag	Response Time (sec) Ramp	Noise	Difference (sec)
PS7	.05	.05	.00
PS12	.32	.31	-.01
PS21	.07	.09	.02
C10	.08	.04	-.04
G1151	.07	.05	-.02
C17	.11	.04	-.07
C18	.10	.07	-.03
C20	.11	.10	-.01
C26	.09	.08	-.01
C35	.09	.09	.00
C36	.10	.10	.00
C40	.09	.10	.01

HOST UTILITY PLANTS FOR FIELD VALIDATION OF NOISE ANALYSIS

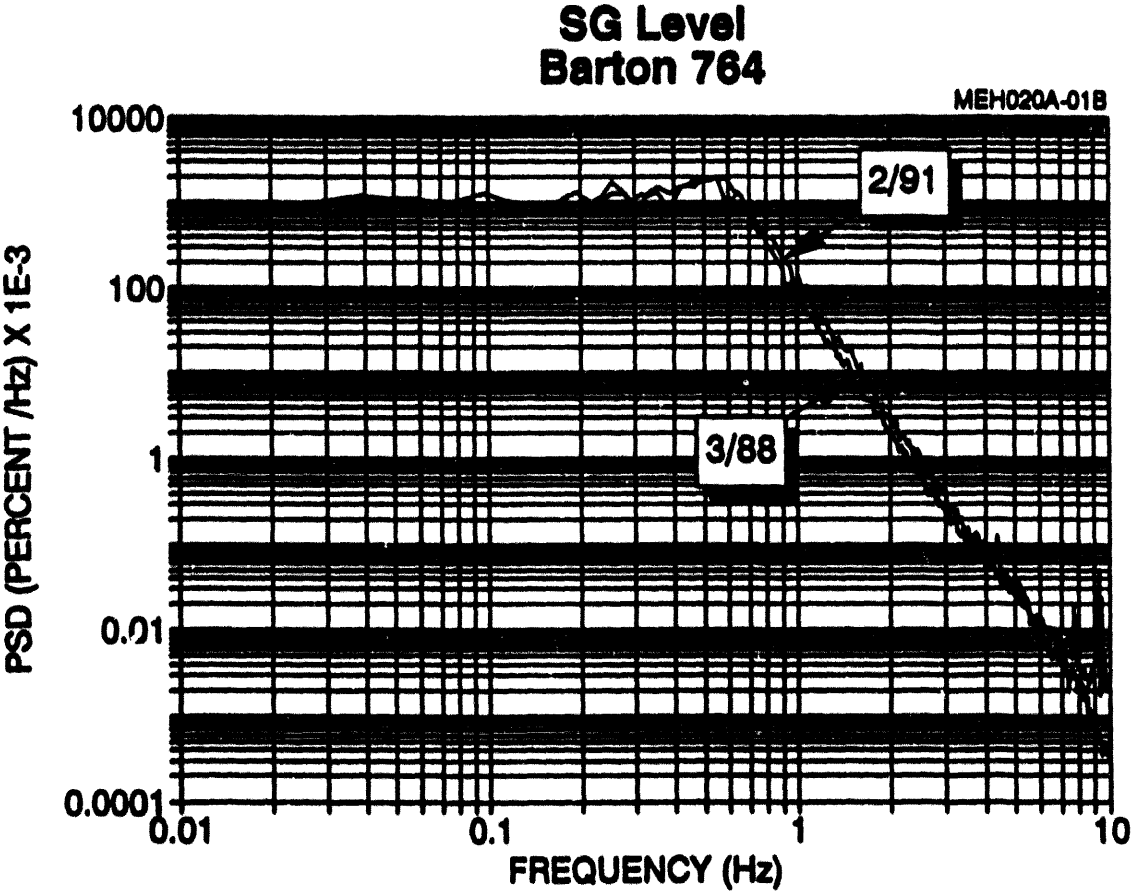
- Catawba I
- Catawba II

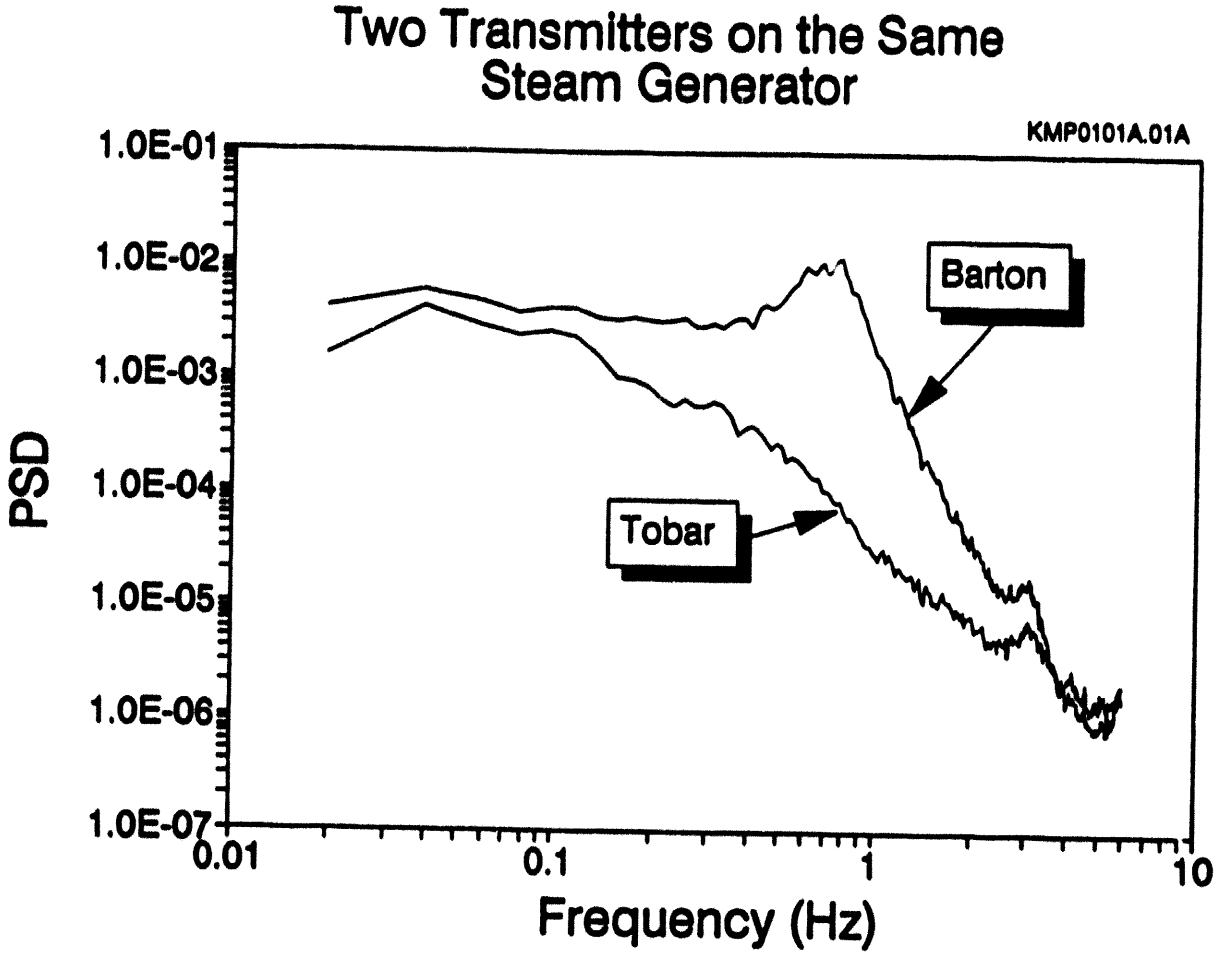
- Byron I
- Byron II


In-Plant Validation
Process
Sensing Line
Plant Transmitter
Reference Transmitter

EXAMPLE OF IN-PLANT NOISE ANALYSIS VALIDATION RESULTS

Transmitter Manufacturer	Response Time (sec)	
	Noise	Direct
Rosemount	0.06	0.08
Veritrak	0.11	0.11
Rosemount	0.13	0.11
Veritrak	0.27	0.13

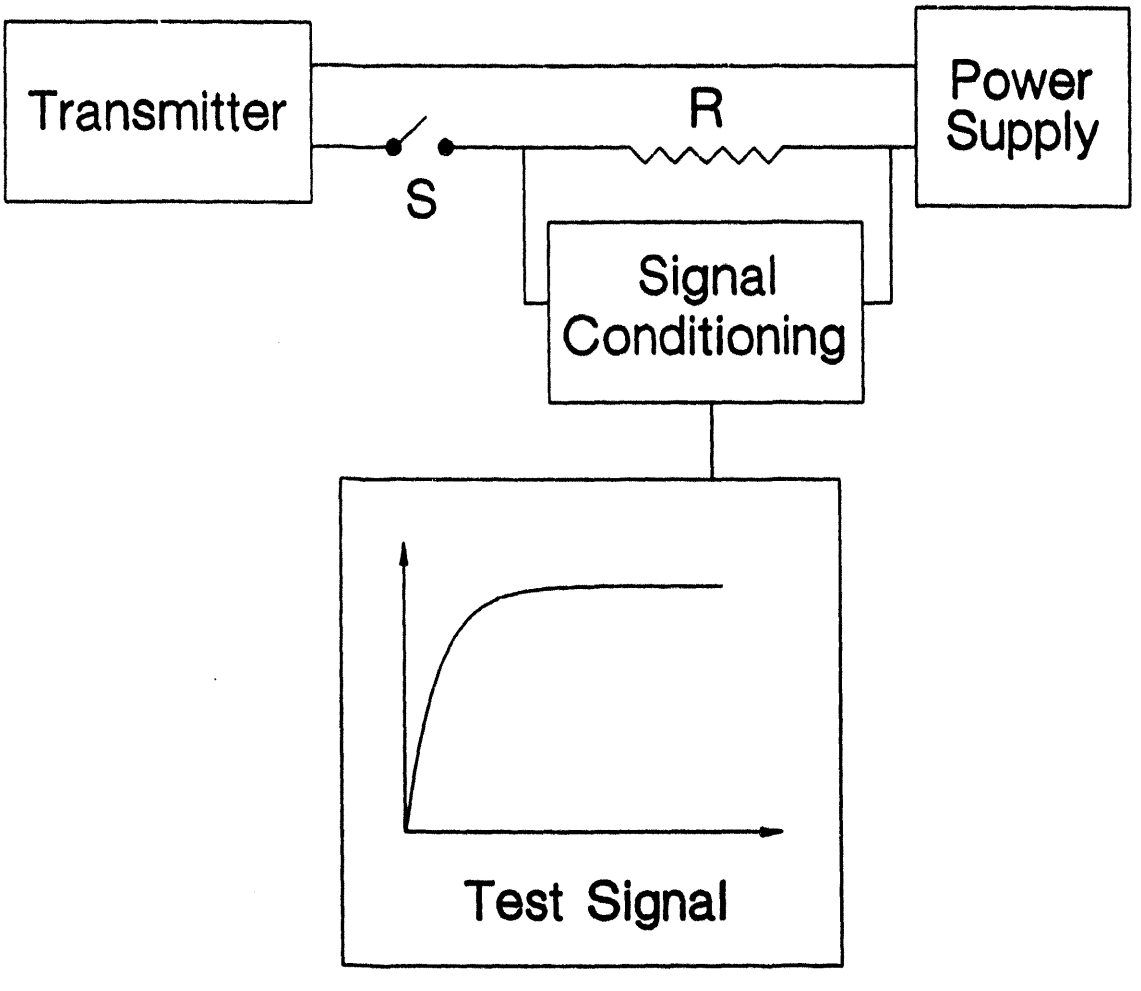

SG Level
Barton 764
MEH020A-01B
10000
100
1
0.01
0.0001
2/91
3/88
PSD (PERCENT /Hz) X 1E-3
0.01
0.1
1
10
FREQUENCY (Hz)


Two Transmitters on the Same
Steam Generator
KMP0101A.01A
1.0E-01
1.0E-02
1.0E-03
1.0E-04
1.0E-05
1.0E-06
1.0E-07
PSD
Barton
Tobar
0.01
0.1
1
10
Frequency (Hz)

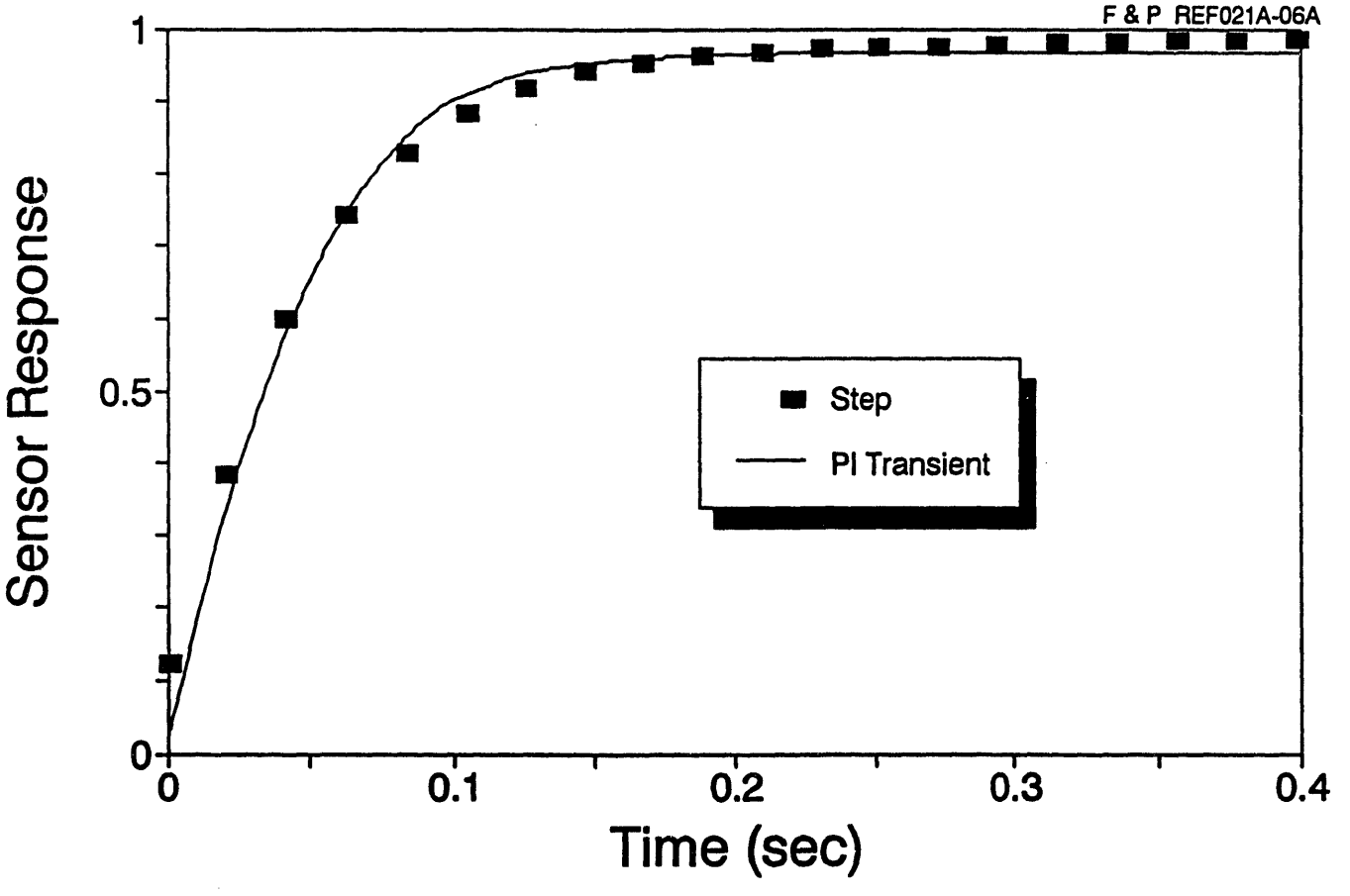
POWER INTERRUPT TEST (PI)

AMS-DWG PXT015A

PI Test Setup



Comparison of Step and PI Transients



CONCLUSIONS

- Response Time of RTDs and Pressure Transmitters can be Tested Remotely While the Plant is Operating
- The On-Line Testing Techniques have been Validated for use in Nuclear Power Plants
- LCSR Test is used in About 60 Plants in the U.S. and Several Plants in Other Countries
- The Noise Analysis and PI Tests are used in About 30 Plants in the U.S. and a Few Plants in Europe

SESSION 2

AGEING AND MAINTENANCE

Pilot Studies of Management of Ageing of Nuclear Power Plant Instrumentation and Control Components

Effects of Normal Aging on Calibration and Response Time of Nuclear Plant RTDs and Pressure Sensors

Validation of On-Line Monitoring Techniques for In-Situ Testing of Calibration Drift of Process Instrumentation Channels in Nuclear Power Plants

PILOT STUDIES OF MANAGEMENT OF AGEING

OF NUCLEAR POWER PLANT INSTRUMENTATION AND CONTROL COMPONENTS

For Presentation at the IWG/NPPCI Specialists Meeting on
Experience in Ageing, Maintenance and Modernization of
Instrumentation and Control Systems for Improving
Nuclear Power Plant Availability
5-7 May 1993, Rockville, Maryland, USA

S.G. Burnay[1], K. Simola[2], A. Kossilov[3] and J. Pachner[3]

1 AEA Technology
Harwell Laboratory, B 401.8
Didcot, Oxfordshire, OX11 ORA, UK

2 Technical Research Centre of Finland, VTT
Laboratory of Electrical and Automation Engineering
P.O. Box 34
SF-02150 Espoo, Finland

3 International Atomic Energy Agency
P.O. Box 100
Vienna International Centre
A-1400 Vienna, Austria

PILOT STUDIES ON MANAGEMENT OF AGEING OF NUCLEAR POWER PLANT INSTRUMENTATION AND CONTROL COMPONENTS

INTRODUCTION

Ageing[1] in NPPs must be effectively managed to ensure that required safety margins are maintained throughout plant service life, including any extended life. Many organizations in Member States are developing the necessary technical basis for managing nuclear power plant ageing.

To facilitate the exchange of information and collaboration among these organizations the IAEA initiated in 1989 work on pilot studies on management of ageing of NPP components. In November 1989, a methodology for performing ageing management studies [1] was developed, four safety significant NPP components were chosen for the studies, and common technical issues to be addressed in the pilot studies were identified. The four NPP components representing different safety functions and materials that were selected on the basis of their safety significance and their susceptibility to different types of ageing degradation are the primary nozzle of a reactor vessel; a motor operated isolating valve; the concrete containment building; and instrumentation and control cables within the containment.

[1] In this paper ageing is used to mean the process by which the physical characteristics of a component, system or structure change with time or use; this process may proceed by a single ageing mechanism or by a combination of several ageing mechanisms.

The objectives of the pilot studies are, for each component to identify dominant ageing mechanisms, and to identify or develop an effective strategy for managing ageing effects caused by the identified mechanisms.

The pilot studies are being implemented in two phases using the methodology for ageing management studies documented in [1]. Phase I pilot studies (i.e. interim ageing studies) were completed through Technical Committee Meetings of November 1990 and October 1991, and Phase II studies (i.e. comprehensive ageing studies) are being implemented through IAEA Co-ordinated Research Programmes (CRPs).

Work performed in Phase I consisted of a review of current understanding of ageing and methods for monitoring and mitigation of this ageing for the four selected NPP components, and identification of relevant knowledge and technology gaps, and a formulation of recommendations for follow-up work in the form of a work statement for Phase II studies. Results of this work are presented in [2]. Together with results to be obtained from Phase II studies they will provide the technical basis for managing ageing of the selected NPP components.

PILOT STUDY ON MOTOR OPERATED ISOLATION VALVES

Motor operated isolating valves perform an essential safety function in nuclear power plant safety systems under accident conditions. Both the motor actuator and the valve itself are susceptible to several types of ageing degradation. The aim of the pilot study on motor operated isolation valve is to improve the understanding and management of MOV ageing and thus to help assure required MOV performance.

In Phase I of the MOV ageing management study, the current understanding of MOV ageing and methods for monitoring and mitigating the ageing gaps were recognized and a research plan for Phase II study was prepared based on these findings. The results of Phase I are documented in [2]. The objective of the Phase II study is to fill the knowledge and technology gaps identified in the interim ageing study.

As there are various types and manufacturers of MOVs, it was decided that the pilot study would not be addressed to any specific valve design and no joint testing or laboratory research work was planned for the pilot study. The aim is rather to develop generic guidelines for MOV ageing management with appropriate monitoring techniques and maintenance procedures. The objectives and tasks of the pilot study are shortly described in the following:

Understanding MOV ageing

The first objective in the study is to improve understanding of MOV ageing mechanisms and effects, and thus help assure functionality of MOVs under both normal operating and accident conditions. This task will be addressed by the exchange of information of laboratory testing and plant operating experiences. The need of a common database on ageing experiences should also be discussed in the early stage of the research programme.

Monitoring of MOV ageing

The aim is to identify effective and practical methods for monitoring of MOV ageing capable of timely detection of MOV anomalies attributable to age related degradation. Information on current testing and inspection methods will be exchanged in the early stage of the pilot study. The work should be focused on the evaluation and development of diagnostic systems for early detection of degradation and identification of the probable cause of degradation.

Risk and reliability assessment

Guidelines for risk and reliability assessment of MOV ageing should be developed. Probabilistic ageing models, that take into account the effects of maintenance, can be used in the planning of maintenance schedules and in the prediction of MOV performance. Statistical analyses of operating experience require data of good quality. It is thus important to evaluate the current data collection systems to identify whether they fulfill the requirements for the model applications. Age-related MOV reliability data can also be used in time dependent probabilistic safety evaluations of the plant.

Qualification methods

The objective is to improve MOV qualification methods and formulate MOV qualification guidelines. In the information exchange on qualification practices, the emphasis should be put on techniques used to account for MOV ageing. It would be desirable to determine by qualification test whether, after actual in-plant ageing, the ageing degradation has affected the original qualification.

Maintenance procedures

The last of the five objectives is to establish guidelines for effective MOV maintenance to alleviate ageing effects and concerns. Information should be collected on valve maintenance practices and methods and experiences on maintenance optimization. The maintenance guidelines will conclude the findings of the above-mentioned four other tasks with the intention to summarize enhanced methods and practices for mitigating ageing degradation.

The five objectives described above are addressed in parallel in the beginning of the pilot study. Depending on the specific areas of interest of the participants, the pilot study may be focused on some selected topics. It is desired that the research programme would have participants from utilities, manufacturers, regulatory bodies, and research laboratories.

During the first year of the three-year research programme, the participants are pursuing their individual research plans. In the first Research Co-ordinated Meeting to be held in October/November 1993, the participants will present the progress of their work. This meeting will focus on the exchange of information on the five topics, and the proceeding of the pilot study will be discussed and agreed.

Organizations from Canada, Czechoslovakia, Finland, India and Russia have submitted proposals for research agreements. Organizations from France, Germany, Sweden and the USA have indicated their interest in the research programme. Other Member States Organizations are invited to participate in the pilot studies.

PILOT STUDIES ON IN-CONTAINMENT I&C CABLES

Cables are vital components of instrumentation and control systems in nuclear power plants in that they are the linking elements between sensors, actuators and their associated control and monitoring equipment. Cables can be located both inside and outside containment and are required to be qualified for use under both normal service conditions and under accident and post-accident conditions, but the majority of I&C cables used in-containment are based on polymeric materials.

Phase I of the pilot study on I&C cables has summarized the current state of knowledge on the degradation of polymeric cable materials and identified technology and knowledge gaps relating to management of I&C cables. During this phase of the pilot study, a plan of research to fill these gaps has been found; this plan is the basis for the Phase II studies.

Because of the wide range of polymeric cable materials in use in NPPs, it is not feasible to carry out the Phase II studies on all of the types. To bring the overall programme to a manageable size, the work has been restricted to 3 polymer types, representing the cable materials most commonly in use world-wide. These materials are - XLPE (cross-linked polyethylene), EPR (ethylene propylene co-polymers) and EVA (ethylene vinyl acetate polymers).

The objectives and tasks in Phase II of the pilot study on I&C cables are summarized in the following section:

Objectives

The objectives listed below were identified by the working group in Phase I as being most important in the management of cable ageing.

1) To validate predictive cable ageing models which can take into account synergistic effects which take place when long-term radiation and thermal ageing of cables occurs in real plant environments.

2) To provide practical guidelines and procedures for assessing and managing ageing of I&C cables in real plant environments.

Tasks

The following tasks have been identified in the Phase II programme and will spread between the participants in the CRP. There are two main strands to the programme which will run in parallel during the first 2 years of the programme.

1) Cable testing programme:

   a) Samples of real-time aged cables of the types identified above are to be procured from NPPs. The data on actual environmental conditions to which these cables have been exposed will also need to be known i.e. temperature, dose rate, total dose, humidity, presence of chemicals etc. In addition, unaged cables of the same materials will need to be procured. These reference cables may come from the original manufacturer, from stored material or from a very mild environment area in the NPP, such as a control room area.

   b) The reference cables will be subjected to a range of sequential and combined environment tests to obtain data for comparison with the real-time aged cables. Measurements will include both electrical and mechanical properties.

   c) The data from both the real-time aged and laboratory aged cables will be used to evaluate currently available lifetime prediction models and assess their suitability for use in cable management programmes.

2) Data collection:

   a) Data on the degradation of XLPE, EPR and EVA cable materials under conditions relevant to NPPs will be collected from the literature world-wide. Participants will be encouraged to include unpublished data and operating experience from their own countries in the data collection.

b) Where possible, the collected data will also be used in assessment of lifetime prediction models for these materials.

3) Guidelines development:

Using the data collected on the three materials from the literature and operating experience, combined with the data from the comparison of real-time aged cables with accelerated testing, a guidelines document will be produced. This document will aim to provide guidelines for the assessment and management of I&C cables and include practical test methods for the prediction of cable lifetimes.

At present, the pilot study on I&C cables has participants from UK, Germany, Canada and India; in addition, organizations in Russia, France, Hungary, USA and Sweden have indicated an interest in joining the programme. Additional participants in this area would be welcome.

REFERENCES

[1] International Atomic Energy Agency, Methodology for the Management of Ageing of Nuclear Power Plant Components Important to Safety, Technical Report Series No. 338 (1992)

[2] International Atomic Energy Agency, Pilot Studies on Management of Ageing of Nuclear Power Plant Components, IAEA-TECDOC-670 (1992)

/jd/2062r

ANALYSIS AND
MEASUREMENT SERVICES
CORPORATION

AMS 9111 CROSS PARK DRIVE / KNOXVILLE. TN 37923 USA (615) 691-1756

Effects of Normal Aging on Calibration and Response Time of Nuclear Plant RTDs and Pressure Sensors

H. M. Hashemian
J. L. Riner

Analysis and Measurement Services Corporation
AMS 9111 Cross Park Drive
Knoxville, TN 37923 USA

Phone: (615) 691-1756
Fax: (615) 691-9344

Presented At

International Atomic Energy Agency Specialist Meeting on
Experience in Ageing, Maintenance and Modernization
of Instrumentation and Control Systems for
Improving Nuclear Power Plant Availability

ABSTRACT

Resistance temperature detectors (RTDs) and pressure, level, and flow transmitters provide a majority of the vital signals for the control and safety of nuclear power plants. Therefore, it is crucial to ensure that the performance of these sensors are maintained at an acceptable level while the plant is operating.

Since aging has the potential to cause performance degradation in RTDs and pressure transmitters, several research projects have been sponsored by the U.S. Nuclear Regulatory Commission (NRC) to study the aging characteristics of these sensors and ensure that adequate test methods and test frequencies are followed by the nuclear industry to ensure safety. The details of these projects are summarized in this paper.

1. INTRODUCTION

This paper presents the key results of four experimental research projects conducted for the NRC on aging of safety system RTDs and pressure transmitters in nuclear power plants. Each project was conducted in two phases. A Phase I feasibility study followed by a comprehensive research and development effort in Phase II. The results of these projects have been published in the following NRC reports: [1,2,3,4]

1. NUREG/CR-4928, "Degradation of Nuclear Plant Temperature Sensors," June 1987.

2. NUREG/CR-5560, "Aging of Nuclear Plant Resistance Temperature Detectors," June 1990.

3. NUREG/CR-5383, "Effect of Aging on Response Time of Nuclear Plant Pressure Sensors," June 1989.

4. NUREG/CR-5851, "Long Term Performance and Aging Characteristics of Nuclear Plant Pressure Transmitters," March 1993.

The overall purpose of these projects has been to determine if the current nuclear practice of response time testing and calibration performed once every fuel cycle is adequate for management of aging of the safety-related RTDs and pressure transmitters. In addition, the response time and calibration test methods for RTDs and pressure transmitters were evaluated and validated as necessary. The projects summarized in this paper were performed under a special U.S. government program that promotes the commercialization of federally-funded research and development efforts. As such, commercial testing services and integrated equipment and procedures were developed during the course of these projects to provide the nuclear industry with a reliable means of testing for any aging degradation that may occur in the RTDs or pressure transmitters.

2. AGING CHARACTERISTICS OF RTDs

2.1 Definition of Performance

The performance of an RTD is characterized by its accuracy and response time. Accuracy is a measure of how well the RTD may indicate a static temperature and response time defines how quickly the RTD may detect a temperature change. The accuracy and response time of RTDs are generally independent.

The deterioration of accuracy is called calibration drift or calibration shift and the deterioration of response time is called response time degradation. Accuracy can be restored by recalibration if the RTD is stable, but response time is an intrinsic characteristic that cannot be altered once the RTD is manufactured. In the case of thermowell-mounted RTDs, however, response time degradation due to movements of the RTD in its thermowell can sometimes be reversed.

2.2 Definition of Aging

The term aging used in this paper refers to decalibration or response time degradation of RTDs with time in normal environments and under normal operating conditions in the primary coolant system of Pressurized Water Reactors (PWRs). These conditions are summarized in Table 1.

Table 1

Normal Aging Conditions for Primary Coolant RTDs in PWRs

Temperature Range	300 to 320°C
Temperature Cycling Conditions	Shutdowns, Start-ups, Plant Trips
Temperature Fluctuations	± 0.5°C
Containment Temperature Range	50 to 60°C
Storage Temperature	Ambient Temperature (approx. 20°C)
Containment Humidity Range	10 to 90%
Vibration Sources	Flow Induced Vibration Vibration of Nearby Machinery
Sources of Mechanical Shock	Shock in Shipping, Handling, Installation, and Plant Trips

The definition of aging mentioned above is based on NRC's definition of aging which is, "the cumulative degradation that occurs with the passage of time in a component, system, or structure which can, if unchecked, lead to loss of function and impairment of safety". Since the performance of RTDs is tested periodically, the degradation does not accumulate. Therefore, the word cumulative was deleted in our definition. Furthermore, we concentrated on the aging that

occurs in an 18 month period, the length of a typical PWR fuel cycle and the period of time between periodic response time and cross calibration tests currently performed in nuclear power plants.

2.3 Effects of Aging on Performance

Normal aging of RTDs occurs from long-term exposure to any combination of heat, humidity, vibration, temperature cycling, and mechanical shock. Nuclear radiation can also affect RTD performance, but this was not studied to limit the project scope and concentrate on aging effects that are believed to have major effects. Since primary coolant RTDs are remote from the reactor core, they are normally unaffected by nuclear radiation except for gamma which may cause degradation in the insulation and other RTD materials.

2.3.1 Effects of Aging on Calibration

A significant calibration shift should not occur in an RTD as long as the sensing element is not stressed or contaminated after calibration and the insulation material is kept in place and dry. Any new stress, contamination, or metallurgical changes in the sensing element or moisture in the insulation material can cause a calibration shift.

Stress results from any combination of heat, vibration, temperature cycling, and mechanical shock. The effect of temperature is the most important. This is because the RTD materials have different thermal expansion coefficients causing the element to experience stress whenever the temperature changes. The resistance of the sensing element increases with tension stresses and decreases with compression stresses. For small temperature variations, the stress reverses itself but for large ones, the effect is not reversible except by annealing. Chemical contamination and oxidation of the sensing element results from long-term exposure to high temperatures. To avoid oxidation, RTDs may be built with reducing atmosphere in the sheath. However, this leads to contamination due to migration of metal ions from the sheath to the sensing element at temperatures above 500°C.

Metallurgical changes such as grain growth occur at temperatures above 420°C. Cold working (or work hardening) results from vibration and mechanical shock and can be eliminated by annealing, which requires heating the RTD above 400°C.

The insulation resistance of an RTD decreases as moisture enters the sheath. The electrical resistance of an RTD is a parallel combination of two resistances: the sensing element and the insulation resistance (Figure 1). The insulation resistance is normally high compared to that of the sensing element and has a negligible effect on resistance measurement. However, with moisture, the insulation resistance decreases and causes the RTD to indicate a lower temperature than normal.

At high temperatures, moisture in the RTD is not normally a major concern because water vapor is likely to diffuse out of the RTD. However, since at high temperatures the insulation resistance significantly decreases, any remaining moisture in the RTD may have a significant impact on the insulation resistance value.

AMS-DWG RTD023D

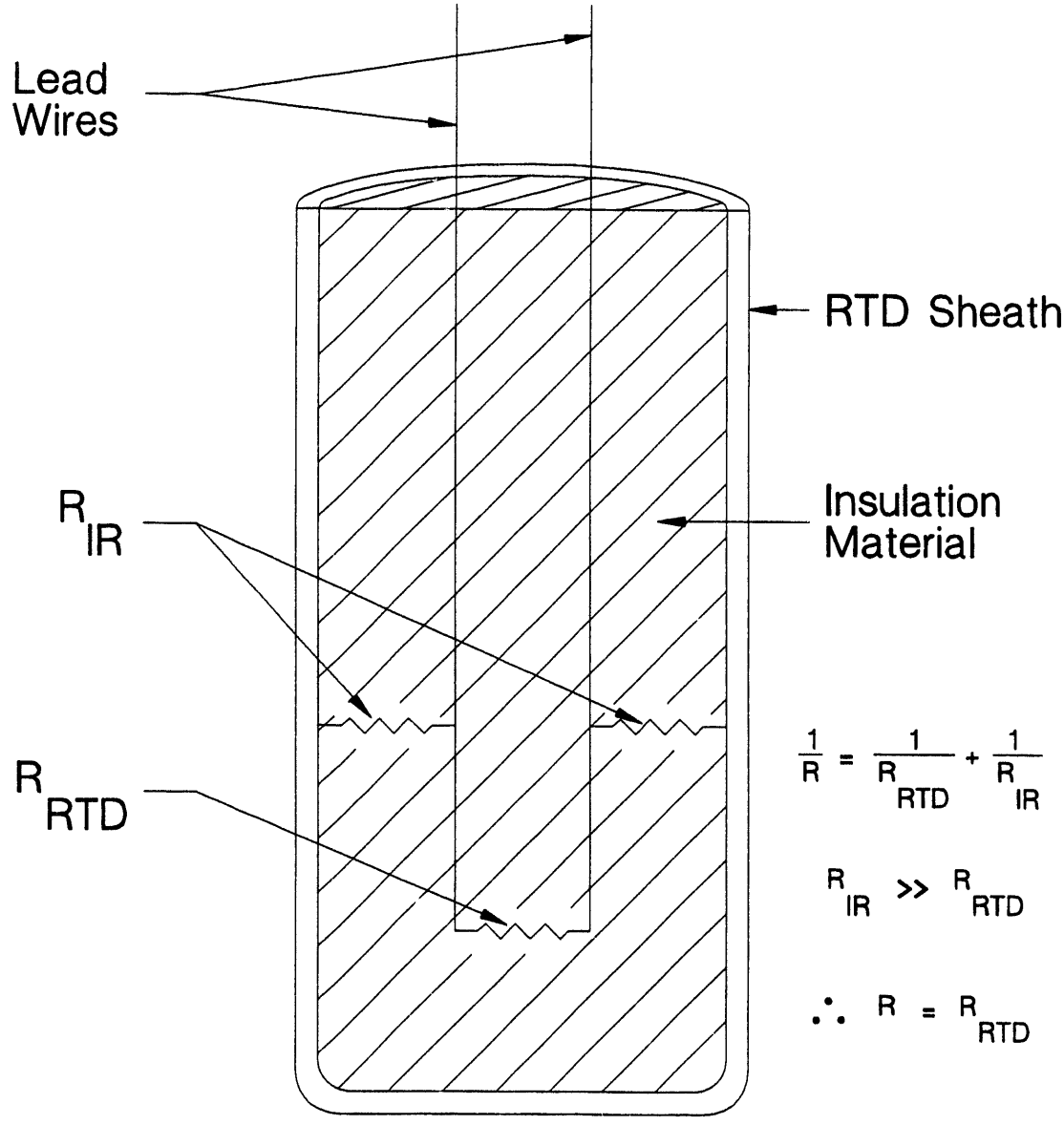


Figure 1. Electrical Resistances of an RTD.

2.3.2 Effects of Aging on Response Time

Response time degradation results from changes in the heat transfer properties of the insulation material. Gaps and cracks which may develop in the insulation materials from long-term exposure to high temperature, vibration, and temperature cycling are detrimental to dynamic performance. If moisture enters the RTD, the response time may decrease at the cost of a calibration shift. Although improvement in response time with age is possible, an RTD whose response time continues to decrease with age could be suffering from degradation of insulation resistance.

A major cause of response time degradation in nuclear plant RTDs is due to changes that can occur in the RTD/thermowell interface in thermowell-mounted RTDs. Experience has shown that air gaps in the RTD/thermowell interface play a major role in controlling the overall response time of the RTD (Figure 2). Changes of as little as a few hundredths of a millimeter in the size of the air gap caused by vibration, shock, and other mechanical effects during plant operation, installation, handling, or dimensional tolerances will change the response time significantly. If the RTD is spring-loaded into the thermowell, mechanical effects may change the insertion length or the contact pressure, increase the size of the air gap in the thermowell, and result in a response time increase.

2.4 Aging Test Results

The first step in performing the RTD aging project was to set up a laboratory with calibration and aging equipment and to obtain nuclear grade RTDs. The project was started with fifty-one nuclear grade and seventeen commercial grade RTDs. The commercial grade RTDs were included for comparison purposes. Of the fifty-one nuclear grade RTDs, twenty-one were dual element providing a total of seventy-two independent RTD elements. These RTDs were used in one or more of the five aging categories: thermal aging, vibration aging, humidity aging, thermal cycling, and high temperature testing. The project focussed on the effects of aging on RTD calibration more so than RTD response time. As such, the results presented here are concentrated on the effects of aging on calibration. However, in presenting the conclusions of the RTD aging project, the response time issue is also included.

Next, a computer-based automatic calibration and monitoring system and procedure were developed. The RTDs were calibrated and placed in two furnaces at approximately 320°C, the primary coolant temperature in most PWRs. The RTDs were monitored in the furnaces using a computer scanning system which measured and stored their loop resistance, insulation resistance, open circuit voltage, and lead wire resistance. These measurements helped identify and characterize the failures when they occurred. Once every one or two months, the RTDs were removed from the furnaces and calibrated to quantify any drift. The thermal aging process was continued for 18 months, equivalent to a typical PWR fuel cycle. Of thirty RTD elements tested for thermal aging, two failed, six showed drift in the range of 0.6 to 3.0°C, but the remaining twenty-two drifted less than 0.2°C over the entire thermal aging period. The average positive and negative drift of the unfailed RTDs as a function of calibration interval is given in Figure 3. Each calibration interval corresponds to one to two months. The results show that after an apparent burn-in period which lasted until the fifth calibration or approximately nine months into the aging process, the RTDs stabilized in a drift band of ± 0.2°C. Note that the results are presented in terms of an average drift band rather than a drift rate because the calibration changes as a function of time were random and not systematic and we could not therefore arrive at a drift rate.

AMS-DWG RTD019D

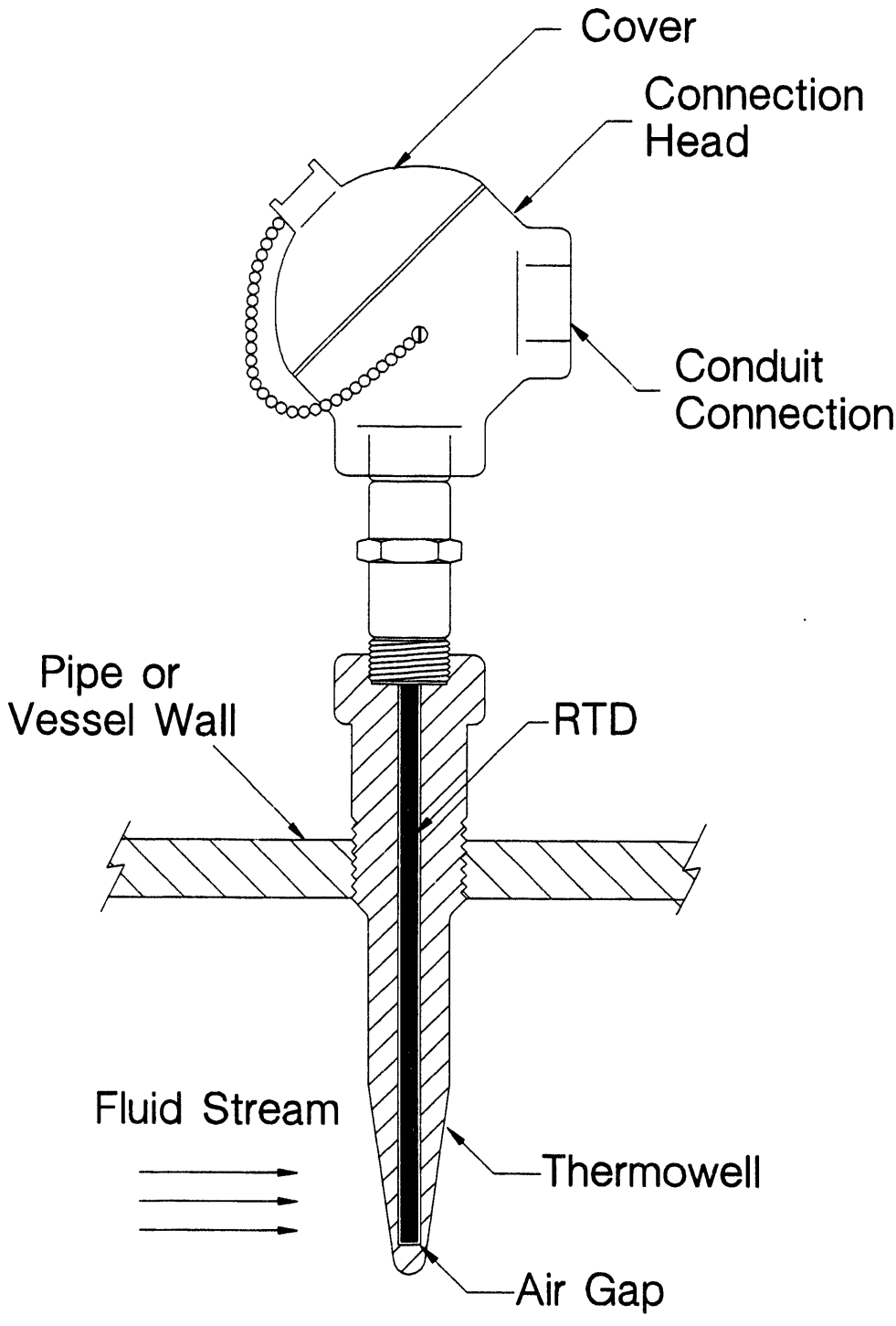


Figure 2. A Typical RTD in Thermowell Installation.

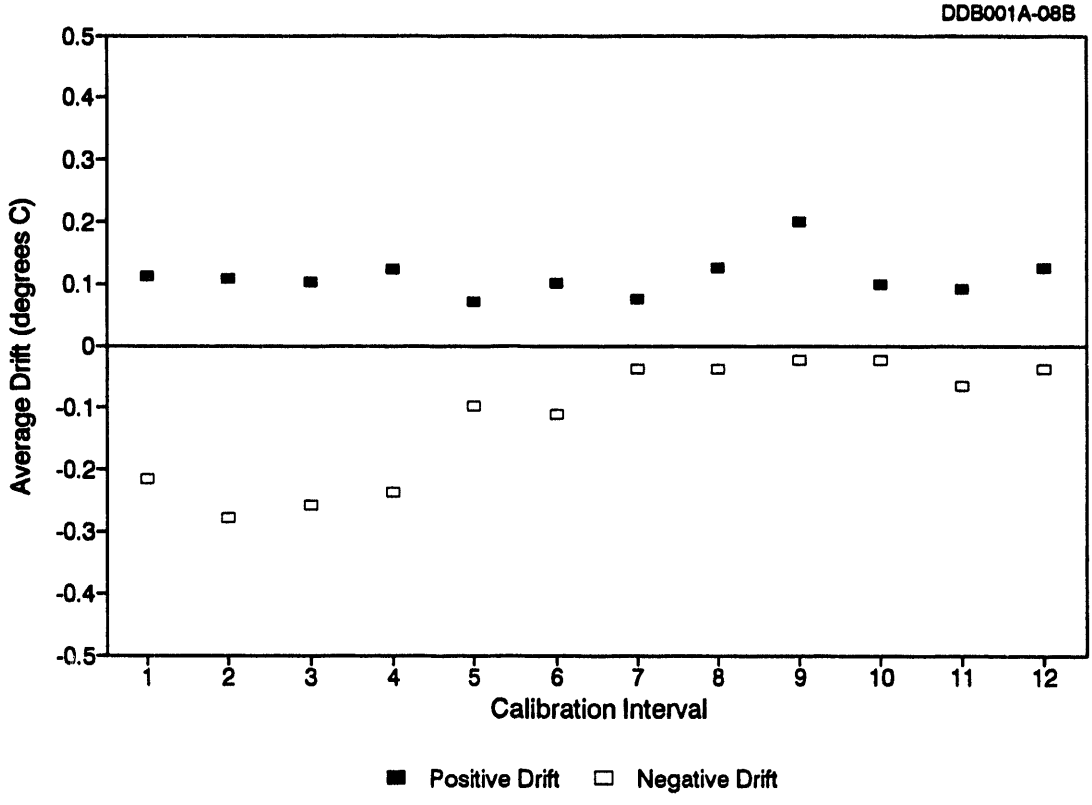


Figure 3. Average Drift of the Test RTDs as a Function of Time in the Aging Furnace.

The RTDs were then stored at room temperature, pressure, and humidity, and periodically tested for shelf-life drift. The results showed that the RTDs are not immune to degradation during storage. This problem can be resolved by recalibrating the RTDs shortly before they are installed in the plant.

The aging of the RTDs was continued to identify the effects of vibration, humidity, mechanical shock, high temperature, and thermal cycling. These effects could not be combined and were performed individually on a group of RTDs at a time. These tests resulted in three more failures, but did not increase the average drift of the RTDs beyond that of thermal aging. The results are summarized in Figure 4 along with the duration of each test. Although the duration of the tests other than thermal aging were short, a thorough analysis of the data indicated that the drifts would probably plateau at the average values shown in Figure 4. Furthermore, it was determined that the aging effects are interactive rather than accumulative and that if the aging effects are combined in a single test, the results would not have exceeded the drift bands shown in Figure 4.

In addition, a number of RTDs removed from operating nuclear power plants after 2 to 5 years of service were tested to determine the drift of naturally aged RTDs. The results are shown in Figure 5. The drift results are mostly within ± 0.2°C which is consistent with the laboratory aging test results.

2.5 Testing Intervals and Replacement Schedules

The current industry practice for verifying adequate RTD accuracy and response time is to perform on-line cross calibration and response time testing at least once every fuel cycle. In light of the results generated in the aging project discussed here and elsewhere, this practice is reasonable unless there are plant specific problems requiring more frequent testing or the RTDs are suspected of deficiencies in design, fabrication, or installation. For example, in one plant, a small margin between the required response time and the nominal response time of primary coolant RTDs, in addition to a history of response time problems due to degradation of a thermal compound used in the thermowell, required periodic response time testing to be performed once every one or two months.

The data available on drift and response time degradation of RTDs including those discussed in this paper are so random that a reliable rate of change for either calibration or response time of RTDs can not be established. Therefore, RTD replacement schedules should be based on performance problems identified during the periodic in-plant tests. For example, an RTD that has consistently shown measurable monotonic drift in either positive or negative directions should be replaced. Any RTD that has suffered a shift of more than 1°C should be replaced. Any major change or consistent increases in response time of well-type RTDs should be followed by an attempt to clean and reseat the RTD in the cleaned thermowell. This may or may not resolve the problem. If not, the RTD and sometimes even the thermowell may have to be replaced. Any direct immersion RTD that has been found to have an unacceptable response time should be replaced as there is no other way to restore the response time of direct immersion RTDs.

Those RTDs that consistently pass response time and calibration testing can be kept and used in the plant for their design life as specified by the manufacturer. Typical design life of nuclear grade RTDs is 10 to 40 years depending on the type of sensor and conditions of use.

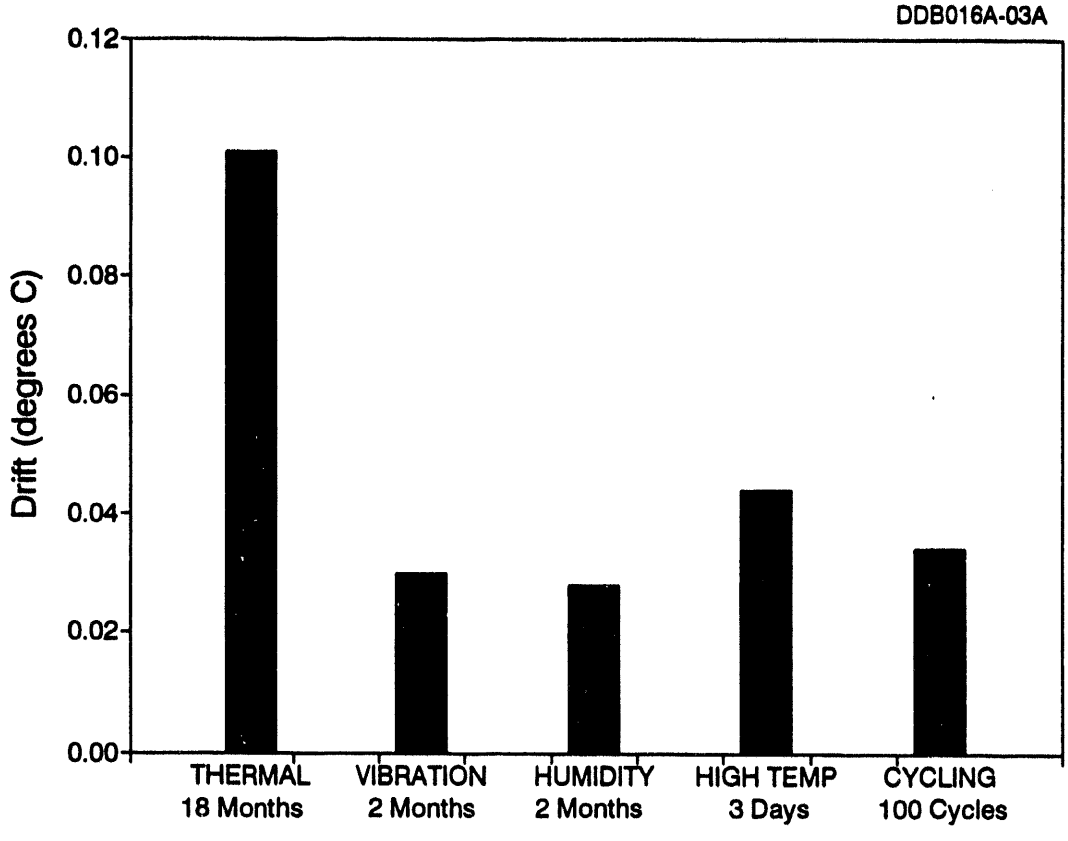


Figure 4. Summary of Aging Test Results.

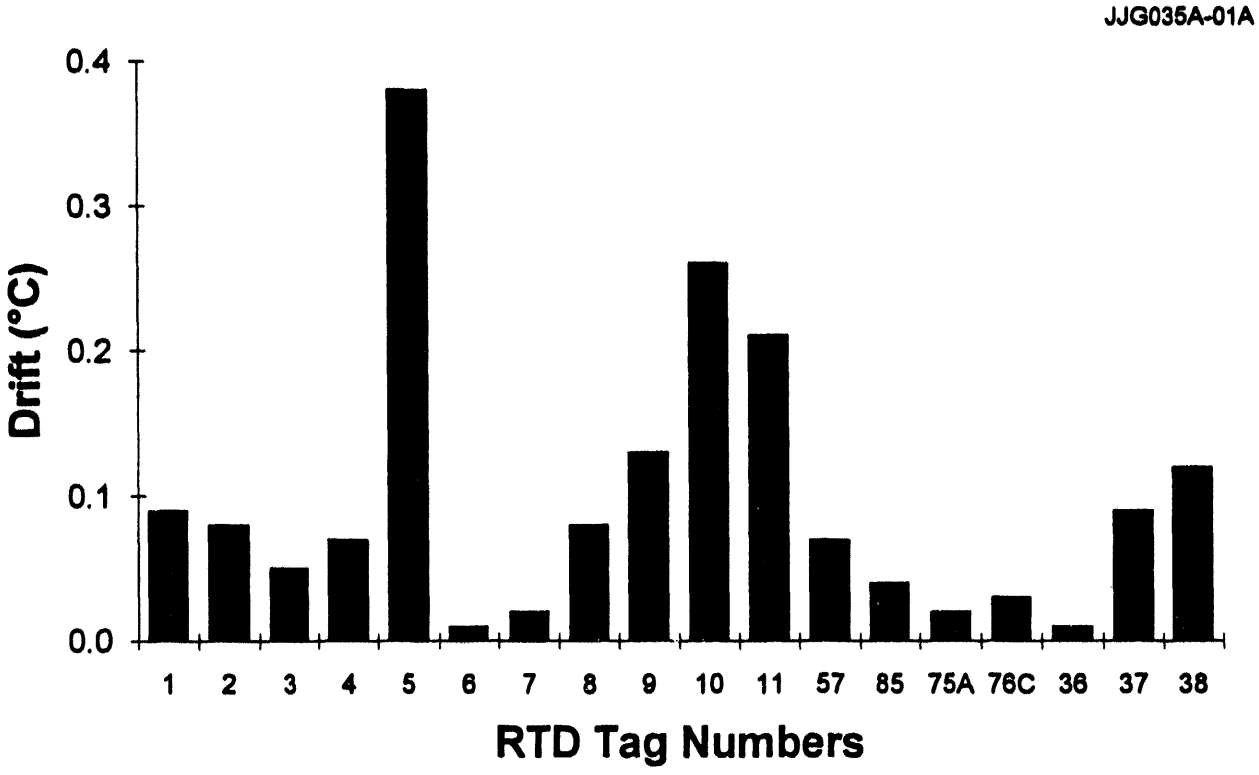


Figure 5. Drift of Naturally Aged RTDs.

2.6 Conclusions on Aging of RTDs

The calibration and response time of RTDs are affected by aging even at normal operating conditions. However, the aging is manageable by periodic tests performed once every fuel cycle.

If an RTD has been in storage for more than two years, it should be recalibrated before it is installed in the plant. The same argument applies to RTDs that have been inactive such as those installed in a non-operating plant for a period of more than two years. The stability of these RTDs may be improved if they are first annealed and then calibrated.

The drift of nuclear grade RTDs was found to generally lie in a ± 0.2°C band. A drift band is used instead of a drift rate because the drift of RTDs does not occur in a monotonic fashion to provide a unique value for calibration changes as a function of time.

3. AGING CHARACTERISTICS OF PRESSURE TRANSMITTERS

Aging degradation may occur in a pressure transmitter when the material in the transmitter is exposed to a stress for a period of time. Typical aging mechanisms that can cause a material's mechanical strength or pnysical properties to degrade include thermal, mechanical, or electrical fatigue, wear, corrosion, erosion, embrittlement, diffusion, chemical reaction, cracking or fracture, surface contamination, etc. These degradations may result from exposure to any combination of the following stressors: heat, humidity, vibration, radiation, mechanical shock, thermal shock, temperature cycling, pressure cycling, testing, electromagnetic interferences, etc.

Examples of how aging stressors may affect the integrity of a pressure transmitter during a period of normal plant operation are presented below:

- Radiation. Ionizing radiation plays a role in aging of equipment that is located in the reactor containment. Materials such as organic fluids, elastomers, and plastics that are used in construction of some transmitters are especially susceptible to radiation damage. Radiation can cause embrittlement and cracking of seals, especially in the presence of heat; increase the viscosity of fill fluids; and affect the transmitter's electronics, especially the integrated circuit components.

- Temperature. Temperature is one of the dominant stressors in pressure transmitters. Temperature predominantly affects the transmitter's electronics. The ambient temperature in the reactor containment is about 120°F ±20°F (about 50°C ±10°C) during normal operating conditions. Long term exposure to such temperatures is detrimental to the life of the transmitter. Temperature also affects other stressors. For example, detrimental effects of humidity are often increased at higher temperatures because of higher diffusion rates.

- Pressure. Pressure transmitters are continuously exposed to small pressure fluctuations during normal operation and large pressure surges during reactor trips and other events. Water hammer, for example, is a well-known phenomenon in nuclear power plants which can degrade the performance of pressure transmitters. Other pressure-induced degradations occur during calibration and maintenance when transmitters are inadvertently overpressurized or cycled with pressures that are above or below their normal range. Cyclic

pressures accelerate the normal wear and loosening of parts in the mechanical systems of transmitters.

- Humidity. Humidity affects the operation of a transmitter's electronics and can cause corrosion in other parts of a transmitter. Moisture sources and sinks exist within the transmitter and are therefore unavoidable. The humidity levels inside reactor containment are in the range of 10 to 100 percent. The higher humidities are encountered due to leaking valve seals or broken water or steam lines. Some moisture will leak into transmitters because the organic polymer seals used in most transmitters cannot provide perfect sealing under long-term exposure to the temperatures that exist around pressure transmitters. A significant degrading effect of humidity is short circuits in the transmitter electronics. In addition, moisture weakens the dielectric strength of insulators.

- Vibration. Vibration generated by nearby machinery during plant operation is transmitted to pressure transmitters through the building structure. The vibration of concern in this aging project was not that of seismic events which are addressed during the qualification of pressure transmitters. Normal vibration can produce mechanical fatigue and loosen or disintegrate the transmitter components.

- Maintenance. An example of a maintenance induced problem that occasionally occurs in pressure transmitters is with test pressures that are inadvertently applied to the wrong side of the transmitter during calibration activities. Another example is when isolation and equalizing valves are not manipulated in the correct sequence to prevent exposure of the transmitter to sudden changes in pressure. Furthermore, excessive calibration and other maintenance activities can contribute to the wear and tear of transmitter components. For example, calibration potentiometers, and other components on circuit cards may wear-out after a few years of service due to periodic calibrations.

3.1 Effects of Aging on Calibration and Response Time

The stresses experienced by nuclear plant pressure transmitters during a long period of normal plant operation can cause performance degradation in the mechanical and electronic components of the transmitter and result in steady-state (calibration) and dynamic (response time) performance problems. A few examples of potential effects of some of the most dominant stressors are listed in Table 2 and discussed below.

3.1.1 Aging Effects on Mechanical Components

Some examples of the mechanical components of pressure transmitters susceptible to aging degradation during normal operation include the following:

- Permanent deformation of sensing elements due to pressure surges during reactor trips and maintenance. This will affect both the calibration and response time of pressure transmitters.

- Failure of the bellows: Bellows can rupture and cause leaks resulting in false pressure indications or total failure of transmitters.

- Degradation or leakage of fill fluid: The fill fluid (usually oil) in pressure transmitters can suffer degradation due to radiation and heat or may leak out. If the degradation affects fluid

Table 2

Examples of Aging Effects That Can Cause Performance Degradation in Pressure Transmitters

Degradation	Potential Cause	Predominantly Affected Performance		
		Calibration	Response Time	Total Failure
1. Partial or total loss of fill fluid	• Manufacturing flaws • High pressure	✓	✓	✓
2. Degradation of fill fluid	• Viscosity changes due to radiation and heat		✓	
3. Wear, friction, and sticking of mechanical linkages (especially in force balance transmitters)	• Pressure fluctuations and surges • Corrosion and oxidation		✓	
4. Failure of seals allowing moisture into transmitter electronics	• Embrittlement and cracking of seals due to radiation and heat	✓		✓
5. Leakage of process fluid into cell fluid resulting in temperature changes in sensor, viscosity changes in fill fluid, etc.	• Failure of seals • Manufacturing flaws • Rupture of sensing elements	✓	✓	✓
6. Deformation of sensing element resulting in changes in stiffness	• Pressure cycling • Overpressurization • Vibration	✓	✓	
7. Changes in values of electronic components	• Heat, radiation, humidity • Changes in power supply voltages • Maintenance	✓		
8. Changes in spring constants of bellows and diaphragms	• Mechanical fatigue • Pressure cycling	✓	✓	
9. Blockage of holes in ceramic inserts in sensing modules (Rosemount transmitters) or crimped capillaries	• Normal aging • Manufacturing flaws • Mishandling		✓	
10. Drift of damping resistors	• Thermal fatigue • Radiation effects • Vibration		✓	
11. Failure of transmitter electronics	• Normal aging			✓

properties, changes in response time will result. Any leakage of the fill fluid may be accompanied by changes in both response time and calibration.

- Degradation of diaphragm due to work hardening. Work hardening may cause cracks in the diaphragm and change its stiffness. This will result in response time changes and can also affect the transmitter calibration.

- Friction in mechanical linkages due to corrosion can cause response time degradation and may also affect the transmitter calibration.

- Failure of seals. Seals can harden or crack allowing moisture to leak into the transmitters and affect the transmitter calibration.

- Loosening of mechanical components in force-balance transmitters due to pressure fluctuations, surges, and mechanical vibration can result in calibration and response time problems.

- Blockages in capillary tubes and other passageways restricting the flow of fill fluid in oil filled systems.

3.1.2 Aging Effects on Electronics

The electronic components of pressure transmitters include numerous resistors, capacitors, diodes, and integrated circuits that are used for signal conversion, signal conditioning, and linearization of the transmitter's output. In some transmitters, 10 to 20 resistors are used to maintain the linearity of the transmitter output in addition to resistors and capacitors to control the transmitter "zero" and "span." Almost all these components are affected by long-term exposure to temperature, humidity and radiation. Any significant change in the value of electronic components can cause calibration shifts and in some cases response time changes.

3.2 Aging Test Results

The effects of normal aging on the performance of representative nuclear plant pressure transmitters were studied in a series of laboratory measurements. The transmitters were first calibrated and response time tested, then aged in simulated plant conditions for up to one year. Following this aging, the calibration and response time tests were repeated and the results were compared with the original unaged test results to determine if significant changes or failures had occurred due to the aging. The results of the aging tests are presented here in terms of aging effects on complete transmitter assemblies.

The project involved fifty-seven pressure transmitters representing eight manufacturers. The aging processes included heat and humidity levels corresponding to normal operating conditions of nuclear power plants, heat and humidity simulating the extremes of normal conditions, normal vibration, pressure cycling, and overpressurization. The aging tests conducted in this project were focused on determining gross malfunctions more so than identifying small changes or verifying manufacturer's specifications. The goal was to determine if pressure transmitters are resilient enough to justify the testing frequencies of once every fuel cycle or every 18 to 24 months that are currently practiced by the nuclear power industry.

Since the project focused on determining gross and unusual transmitter behavior, instead of presenting the results in terms of numerical changes in zero, span, and response time of the transmitters, the following qualitative criteria were used to present the results.

1. For the steady-state results, the transmitter instabilities or their deviations from a reference transmitter or a normal value were categorized as "High", "Medium" and "Low" corresponding respectively to gross malfunction or failure, degraded but acceptable performance, and readily acceptable performance.

2. For the response time results, the degradations were categorized again as "High", "Medium", and "Low" corresponding respectively to more than 50 percent increase in response time, 20 to 50 percent increase, or less than 20 percent increase. The response times of nuclear plant pressure transmitters are usually very small (30 to 300 milliseconds). Therefore, increases of up to 50 percent may correspond to a very small change in actual response time. In addition, the inherent repeatability problems with response time testing of pressure transmitters usually make it impractical to distinguish differences of less than 20 percent for those transmitters which have a small response time.

The aging test results are summarized in Table 3 in terms of the aging conditions, the aging periods and percentages of transmitters that were affected, not affected, or failed due to aging. The results in the last six columns in Table 3 were averaged as shown in the results section at the bottom of the table. Both straight and weighted averages were calculated. The straight averages use the sum of the percentages in each column divided by six. The weighted averages are calculated as follows: multiply the percentages by the corresponding number of transmitters, sum the results for each column, and divide the sum by 74. Note that some transmitters were exposed to more than one stressor. That is, the total number of transmitters involved was less than 74.

The results in Table 3 also include those of the Phase I project performed on seventeen pressure transmitters as documented in Reference 3.

The results in terms of weighted averages are shown graphically in Figure 6. Overall, 5 to 7 percent of the transmitters failed from a calibration standpoint due to aging, 35 to 40 percent were affected by aging but not severely, and 55 to 58 percent were not affected by aging at all. The effects of aging on response time were even less than the effects on calibration. Less than five percent failed from a response time standpoint, 12 to 14 percent were moderately affected, and 83 to 84 percent were unaffected. Although the number of transmitters and the duration of the aging tests were limited and no radiation effects were included, the results obtained here are consistent with the experience of the nuclear power industry. The experience of the nuclear power industry is documented in Reference 4 in terms of a search of the Licensee Event Report (LER) database, a search of the Nuclear Plant Reliability Data System (NPRDS) database, and a survey of the Instrumentation and Control personnel in twenty-four nuclear power plant units.

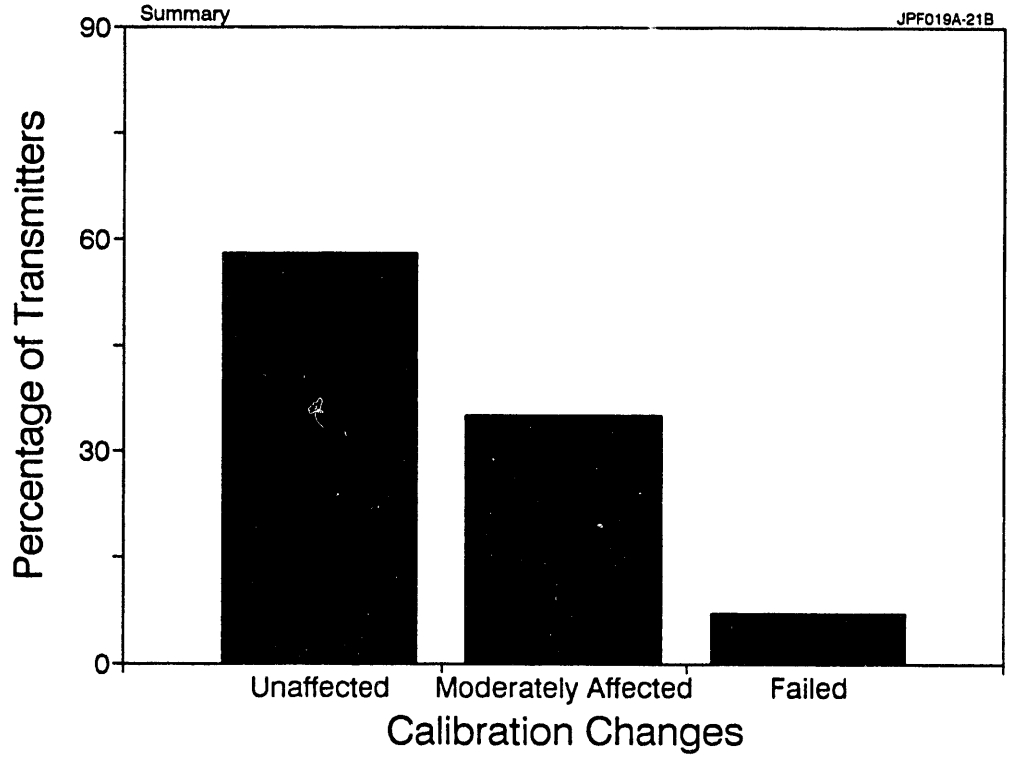
3.3 Aging of Pressure Sensing Lines

A potential problem with the performance of pressure sensing systems that was discovered in this project is the effect of sensing line blockages on response time due to gradual buildup of boron, crud, and other particles in the reactor water. Figure 7 shows how sensing line blockages may affect the response time of some of the most widely used pressure transmitters

Table 3

Summary of Aging Test Results

Aging Stressor	Duration (Month)	Aging Conditions	Number of Transmitters Involved	Aging Test Results					
				Effect on Calibration			Effect on Reeponee Time		
				Not Affected	Moderately Affected	Failed	Not Affected	Moderately Affected	Failed
1. Normal Heat & Humidity	6-12	110°F, 65% RH	23	61%	35%	4%	87%	4%	9%
2. Extremes of Normal Heat & Humidity	3	150°F, 90% RH	11	73%	18%	9%	64%	27%	9%
3. Vibration	2	3 mils at 20 Hz	7	0	100%	0	57%	43%	0
4. Pressure Cycling	2	50% of Span: 100K to 500K Cycles	8	63%	37%	0	100%	0	0
5. Overpressurization	0.5	1000 psi	8	75%	25%	0	100%	0	0
6. Phase I Results	see Reference 3		17	59%	23%	18%	88%	12%	0
Average Results of All Laboratory Aging Tests Performed in This Project									
Straight Average				55	40	5	83	14	3
Weighted Average				58	35	7	84	12	4



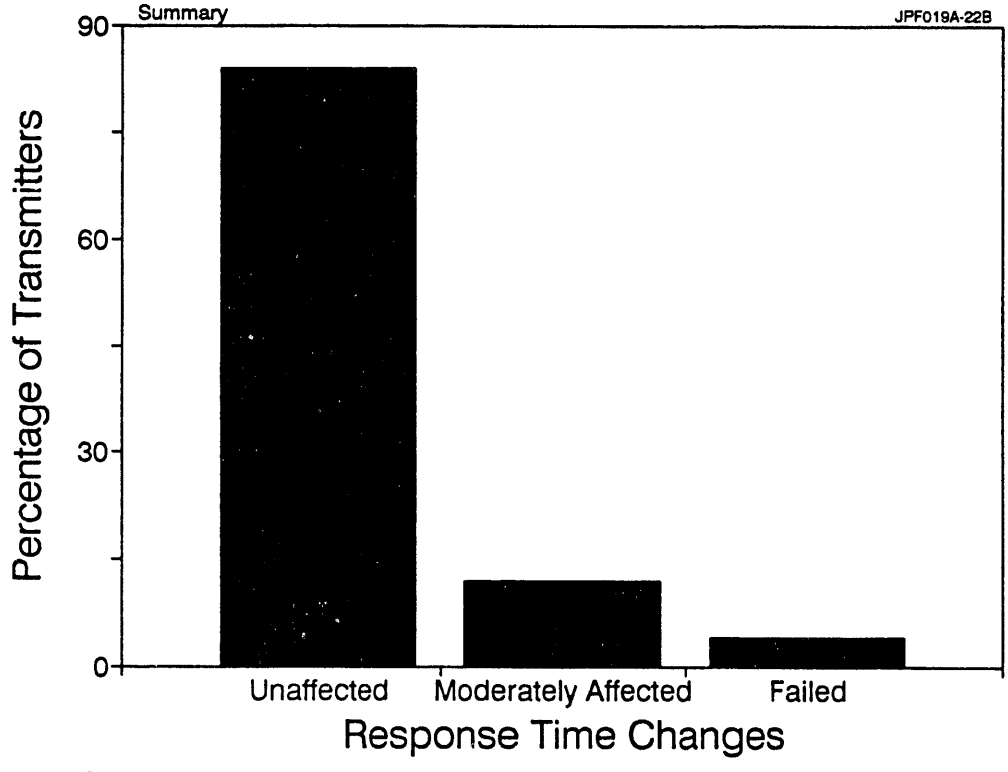


Figure 6. Overall Results of Aging Effects on Transmitter Calibration and Response Time.

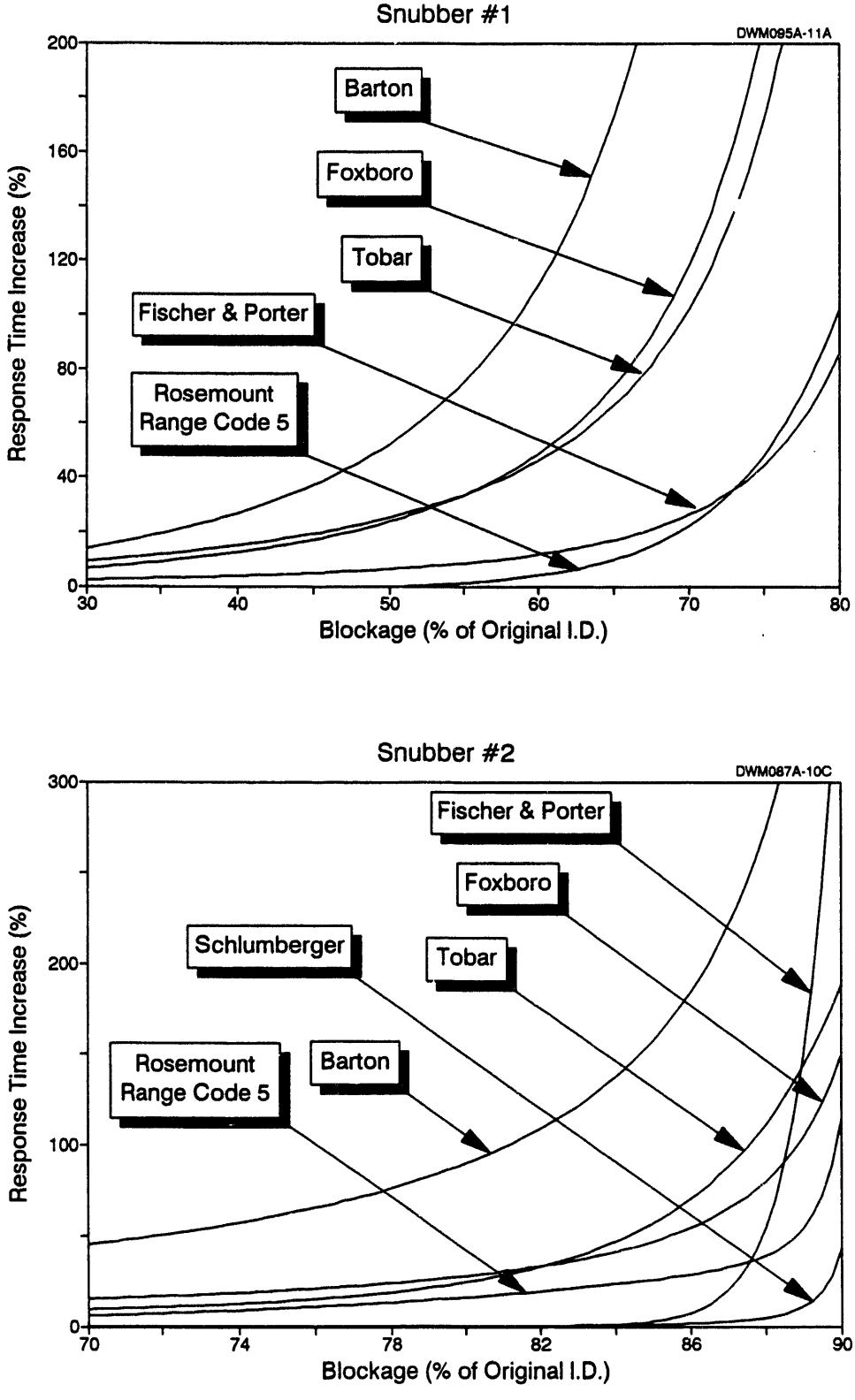


Figure 7. Percent Increase in Response Time as a Function of Sensing Line Blockages Simulated by Using Two Different Snubbers in Sensing Lines.

in the nuclear power industry. These results are from laboratory tests performed in this project using two different snubbers to simulate blockages. Note that due to a difference in the design of the two snubbers, the response time results for the same percentage of blockage is different for the two snubbers. More specifically, snubber number 1 has a piston that slides in and out in order to dampen the pressure fluctuations, while snubber number 2 only simulates a local reduction in the sensing line diameter.

The effects of sensing line blockages on the response time of pressure sensing systems depend predominantly on the compliance of the transmitter. If the transmitter has a large compliance value, then its response time will be greatly affected by any blockage in the sensing line that can restrict the flow of fluid to the transmitter. Otherwise, sensing line blockages are not a major concern unless they are advanced to more than 90 percent of the original diameter of the sensing line. A comprehensive overview of the effects of sensing lines on response time of pressure transmitters is given in Reference 4.

3.4 Conclusions on Aging of Pressure Transmitters

The aging test results presented in earlier sections of this paper have shown that the calibration and response time of pressure sensing systems in nuclear power plants are subject to degradation from normal aging, and must therefore be tested periodically to ensure acceptable performance. The question is how often the transmitters shall be tested or replaced and what is the useful life of the transmitters. These questions are addressed below.

3.4.1 Testing Intervals

Typical nuclear industry practices for the management of aging degradation of pressure sensing systems are as follows:

- Calibrate all safety-related transmitters once every fuel cycle.
- Response time test the transmitters in one safety-related channel once every fuel cycle.
- Blow down or purge the sensing lines as needed if there is reason to believe that blockages are present.

Discussions of whether or not the above practices are adequate for aging management of pressure transmitters are provided below.

Transmitter Calibration Intervals. The calibrations of about 60 percent of the transmitters investigated in various aspects of the project reported herein were found to be unaffected by normal aging. Of the remaining 40 percent, about 5 percent drifted out of tolerance and the rest were only moderately affected by the aging tests meaning that their calibrations were still acceptable. Other aging data included searches of the LER and NPRDS databases which showed about 1 to 3 percent calibration failures in a typical fuel cycle of two years, and a survey of the nuclear industry which showed that although up to about 20 percent of pressure, level, and flow transmitters experience some drift, less than 5 percent actually drift out of tolerance requiring a new calibration.[4] With this information, it is reasonable to conclude that the current

calibration interval of once every fuel cycle is adequate for the management of the effects of aging on calibration of pressure transmitters.

Response Time Testing Intervals. According to the results presented in Table 3, aging produced less degradation in the response times of pressure transmitters than in their calibrations. The response time of 84 percent of the transmitters tested in this study were unaffected by aging. Of the remaining 16 percent that suffered response time degradation, only about 4 percent failed from a response time standpoint. Furthermore, the search of the LER and NPRDS databases did not show much evidence of response time degradation except in the case of the oil loss problem in some models of Rosemount transmitters. The results of the survey of the nuclear power industry indicated that response time problems are not prevalent and pressure transmitters are only rarely replaced due to response time failures. Based on this information, response time testing intervals of once every fuel cycle are adequate if all safety-related transmitters are tested as opposed to testing only one channel.

Testing only one pressure transmitter channel (out of three or four) per fuel cycle leads to testing intervals of six to eight years. Although response time problems with pressure transmitters are not common in nuclear power plants, the safety importance of pressure transmitters and recently discovered problems such as the oil loss in Rosemount transmitters suggest that a testing interval of six to eight years is too long unless other means such as on-line monitoring techniques that can reveal response time degradations are implemented. Many plants have recognized the fact that testing one safety channel per fuel cycle is nonconservative and are therefore testing the response times of all their safety-related transmitters once every fuel cycle.

3.4.2 Replacement Schedules and Useful Life of Pressure Transmitters

The useful life of pressure transmitters depends on the conditions in which they are used. Transmitter manufacturers usually provide the useful life of their transmitters as a function of environmental conditions, especially temperature. Based on typical life versus temperature data published by manufacturers, the useful life of most pressure transmitters used in typical nuclear plant operating environments varies between ten and twenty years.

The life of the electronics in pressure transmitters is the dominating factor in determining how long a transmitter may be used in a plant. In most cases, a transmitter can be rejuvenated by replacing its electronics.

The test results in this project suggest that in light of the regular testing and maintenance activities in nuclear power plants, pressure transmitters can be used safely for as long as specified by the manufacturer. This is provided that the transmitter has not shown sustained drift, response time degradation, or other problems.

4. REFERENCES

1. Hashemian, H.M., et al., "Degradation of Nuclear Plant Temperature Sensors," U.S. Nuclear Regulatory Commission, Report Number NUREG/CR-4928, (June 1987).

2. Hashemian, H.M., et al., "Aging of Nuclear Plant Resistance Temperature Detectors," U.S. Nuclear Regulatory Commission, Report Number NUREG/CR-5560, (June 1990).

3. HASHEMIAN, H.M., et. al., Effect of Aging on Response Time of Nuclear Plant Pressure Sensors, NRC Report Number NUREG/CR-5383, U.S. Nuclear Regulatory Commission, Washington, D.C. (1989).

4. H. M. HASHEMIAN, et. al., Long Term Performance and Aging Characteristics of Nuclear Plant Pressure Transmitters, NRC Report Number NUREG/CR-5851, U.S. Nuclear Regulatory Commission, Washington, D.C. (1993).

FIGURES

Figure 1. Electric Resistances of an RTD.

Figure 2. A Typical RTD in Thermowell Installation.

Figure 3. Average Drift of the Test RTDs as a Function of Time in the Aging Furnace.

Figure 4. Summary of Aging Test Results.

Figure 5. Drift of Naturally Aged RTDs.

Figure 6. Overall Results of Aging Effects on Transmitter Calibration and Response Time.

Figure 7. Percent Increase in Response Time as a Function of Sensing Line Blockages Simulated by Using Two Different Snubbers in Sensing Lines.

ANALYSIS AND
MEASUREMENT SERVICES
CORPORATION

AMS 9111 CROSS PARK DRIVE / KNOXVILLE, TN 37923 USA (615) 691-1756

IAEA1-15

EFFECTS OF NORMAL AGING ON CALIBRATION AND RESPONSE TIME OF NUCLEAR PLANT RTDs AND PRESSURE SENSORS

H. M. Hashemian

Presented At

IAEA Specialists Meeting
Ramada Inn at Congressional Park
Rockville, Maryland
May 5-7, 1993

EFFECTS OF NORMAL AGING ON CALIBRATION AND RESPONSE TIME OF NUCLEAR PLANT RTDs AND PRESSURE SENSORS

H. M. Hashemian

Presented At

IAEA Specialists Meeting
Ramada Inn at Congressional Park
Rockville, Maryland
May 5-7, 1993

RESEARCH OBJECTIVE

Quantify the Effects of Normal Aging on Performance of RTDs and Pressure Transmitters.

- **Identify objective testing intervals and replacement frequencies**
- **Establish acceptable test methods**

PROCESS CONDITIONS THAT CAN AFFECT SENSOR PERFORMANCE

- Heat
- Humidity
- Vibration
- Mechanical Shock
- Overranging
- Cycling
- Radiation

EXAMPLES OF POTENTIAL CAUSES OF RTD DECALIBRATION

- **IR Failure Due to Seal Failure**
- **Changes in Resistivity of Platinum Sensing Element Due to:**

  Strain
  Interaction with support material
  Metallurgical changes

Temperature Cycling

- Expansion and contraction of sensor materials resulting in stress on the sensing element.

Heat

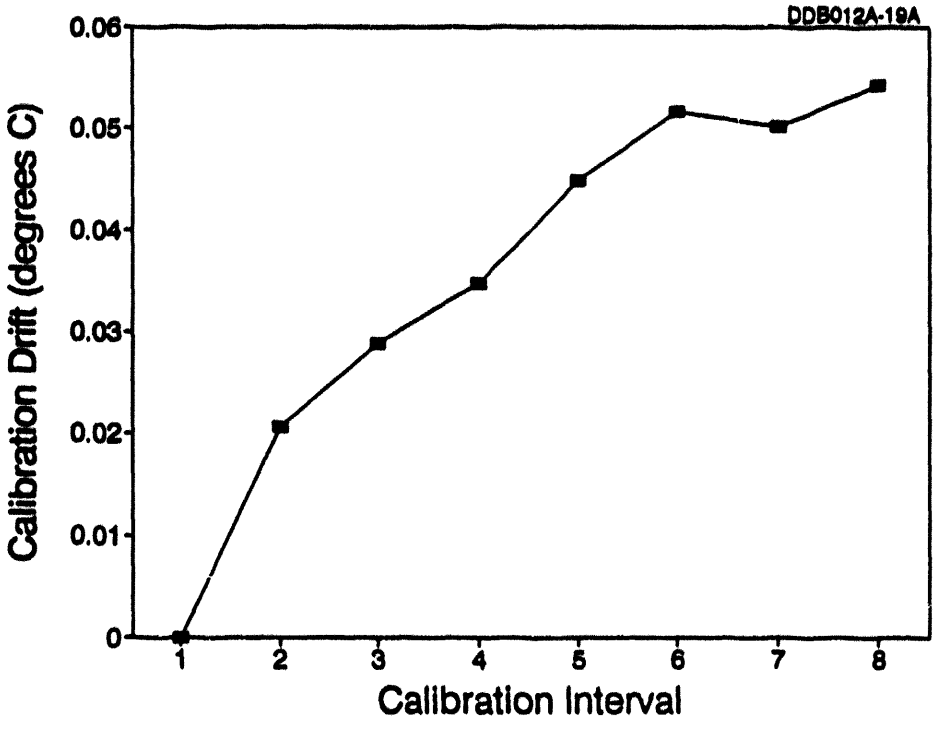
- Affects material properties. RTD seal may dry out, shrink, or crack and let moisture in.

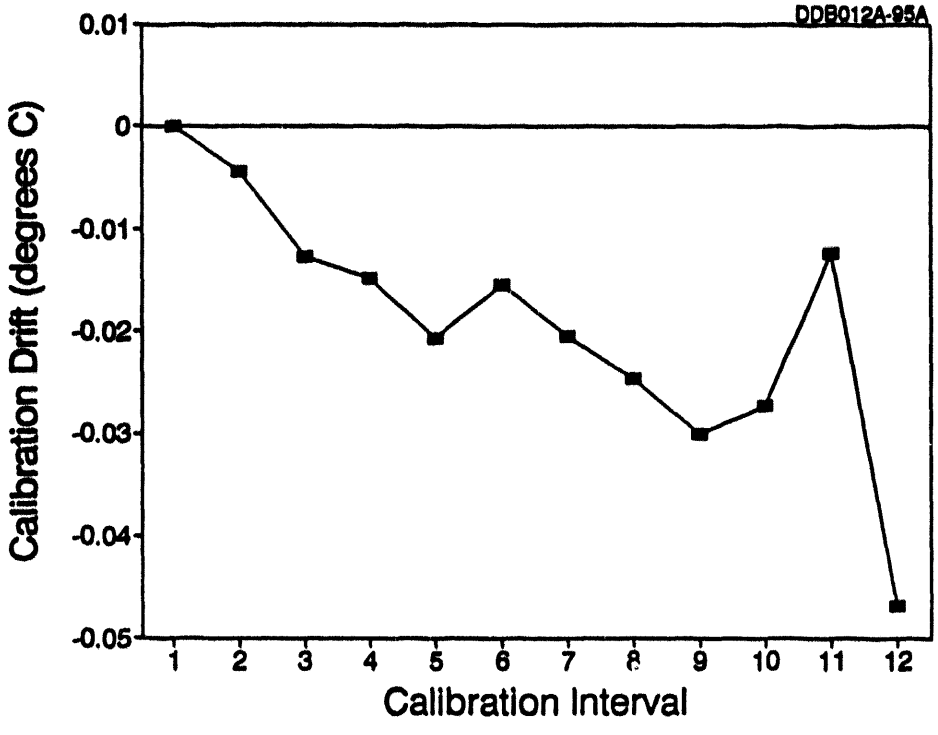
Humidity

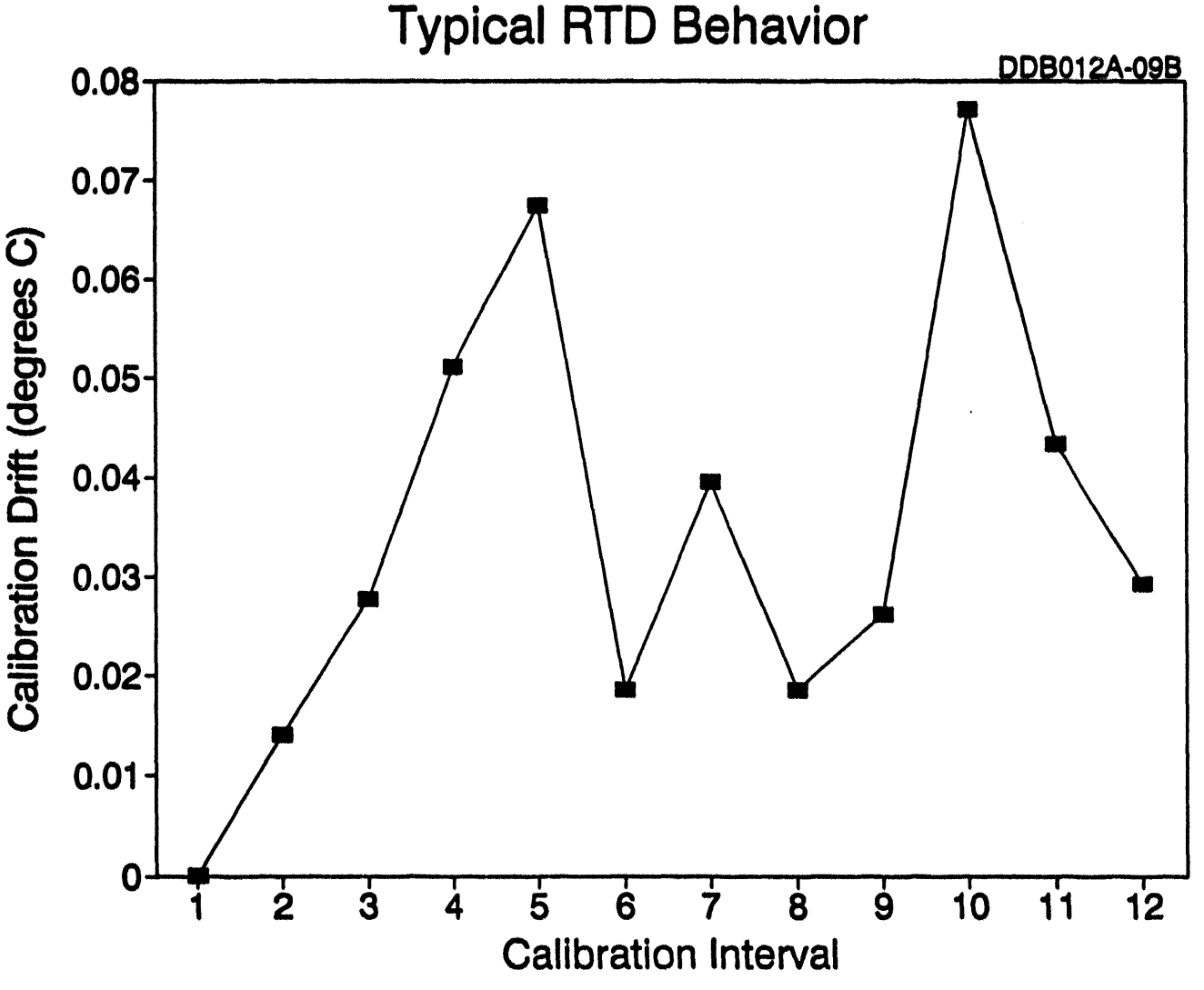
- Reduces the insulation resistance and causes calibration error and a noisy RTD output.

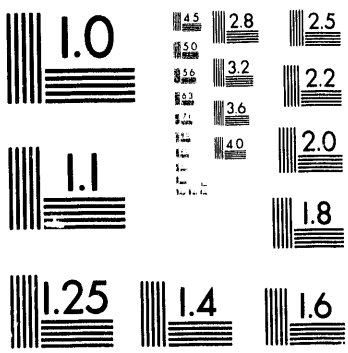
Vibration and Mechanical Shock

- Cold working of sensing element resulting in calibration shift.
- Gradual movement of RTD out of thermowell resulting in response time increase.
- Displacement or redistribution of insulation at high temperature resulting in response time degradation.

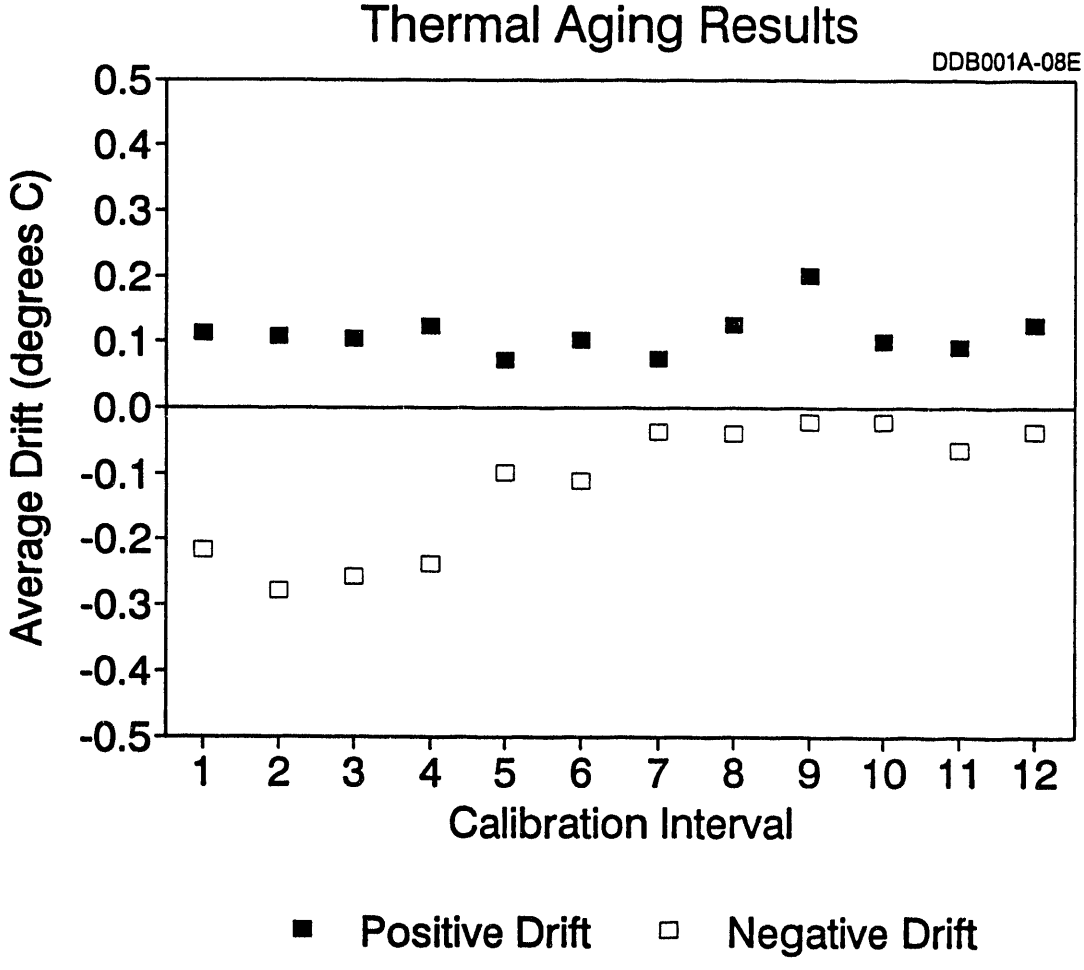

DDB012A-19A
0.06
0.05
0.04
0.03
0.02
0.01
0
Calibration Drift (degrees C)
1
2
3
4
5
6
7
8
Calibration Interval


DDB012A-95A
0.01
0
-0.01
-0.02
-0.03
-0.04
-0.05
Calibration Drift (degrees C)
1
2
3
4
5
6
7
8
9
10
11
12
Calibration Interval

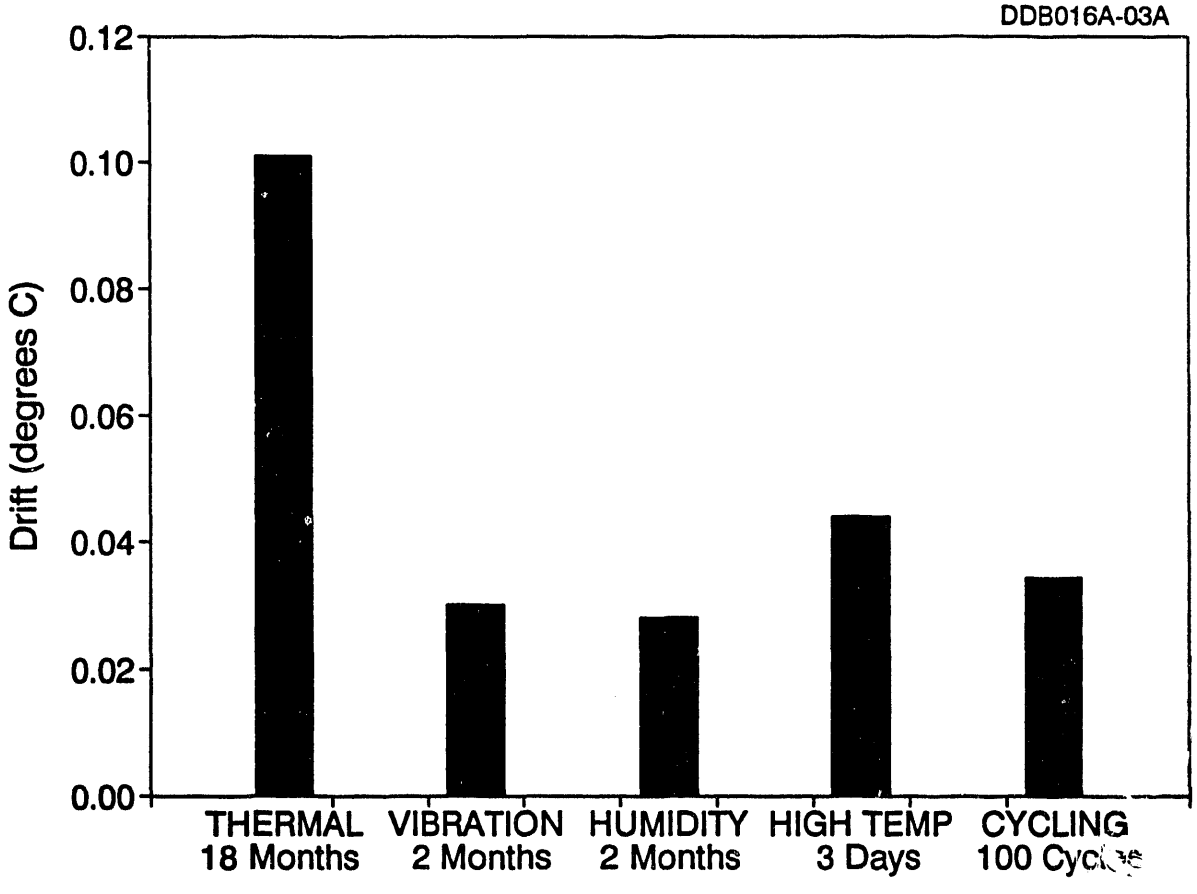

Typical RTD Behavior
DDB012A-09B
Calibration Drift (degrees C)
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0
1
2
3
4
5
6
7
8
9
10
11
12
Calibration Interval


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1

3 of 6


Thermal Aging Results
DDB001A-08E
Average Drift (degrees C)
0.5
0.4
0.3
0.2
0.1
0.0
-0.1
-0.2
-0.3
-0.4
-0.5
1
2
3
4
5
6
7
8
9
10
11
12
Calibration Interval
Positive Drift
Negative Drift

Summary of Aging Test Results



Drift of Naturally Aged RTDs

GROUP 1

Tag	Drift (°C)
1	-0.09
2	0.08
3	0.05
4	0.07
5	-0.38
6	0.01
7	0.02
8	0.08
9	-0.13
10	0.26
11	-0.21
Average	0.13

@ 300°C

Drift of Naturally Aged RTDs

GROUP 2

Tag	Drift (°C)
57	0.07
85	0.04
86	1.13
75A	0.02
76C	0.03
36	-0.01
37	0.09
38	0.12
Average	0.19

@ 300°C

Short-Term Storage Drift

Tag	Drift (°C) One Day	One Week
15A	0.009	0.06
15C	0.011	0.06
16A	0.004	0.06
16C	0.005	0.05
17A	0.008	0.02
17C	0.009	0.03
Average	0.008	0.05

@ 300°C

Response Time Degradation Mechanisms

- Deposits on sheath or well
- Embrittlement or cracking of fillers
- Relocation of fillers
- Relaxation of springs
- Wearing away of bushings
- Changes in RTD/Thermowell interface

ON-LINE TEST METHODS FOR RTDs

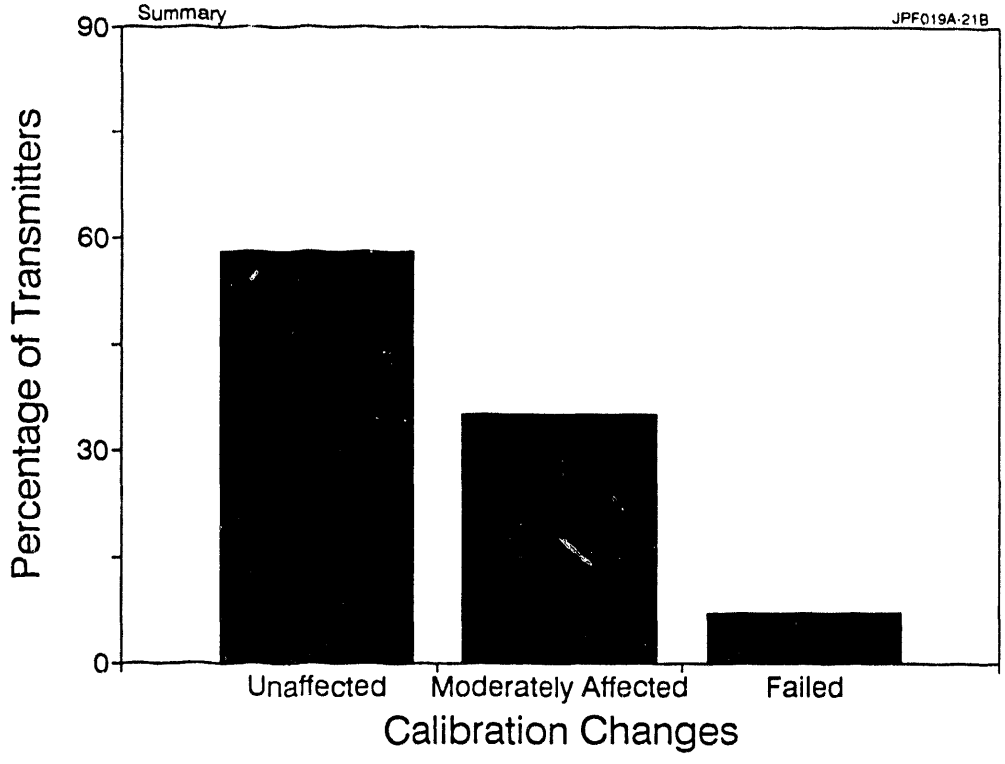
Response Time	LCSR Test
Calibration	Cross Calibration
Test Frequency	Once/Fuel Cycle

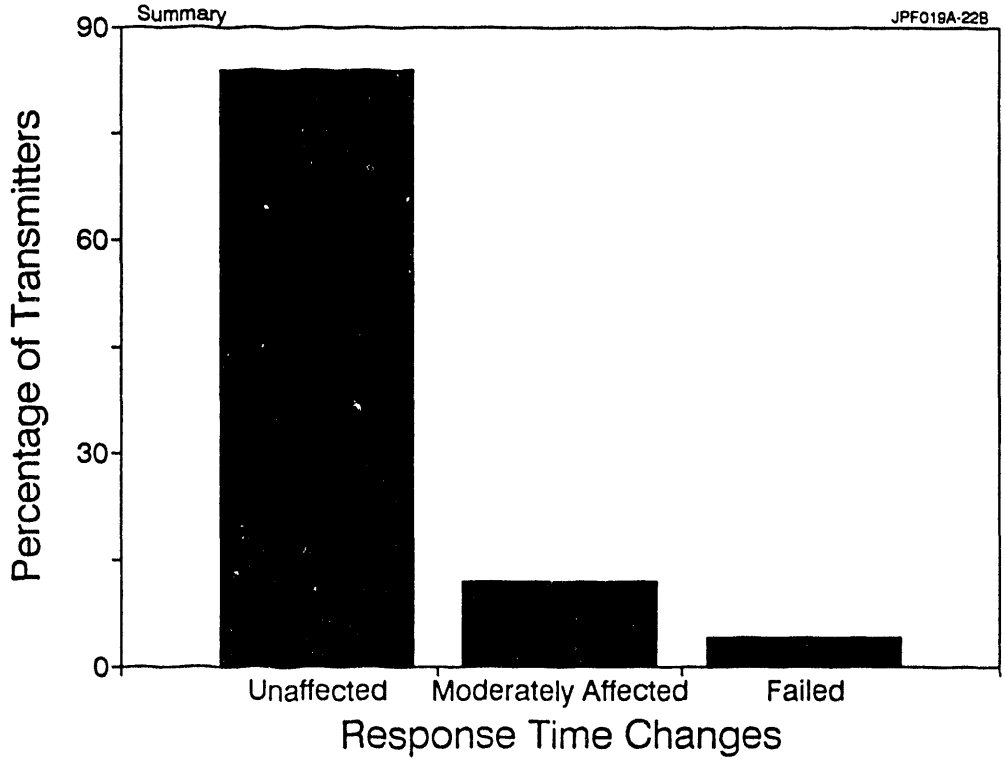
Aging Tests of Pressure Transmitters

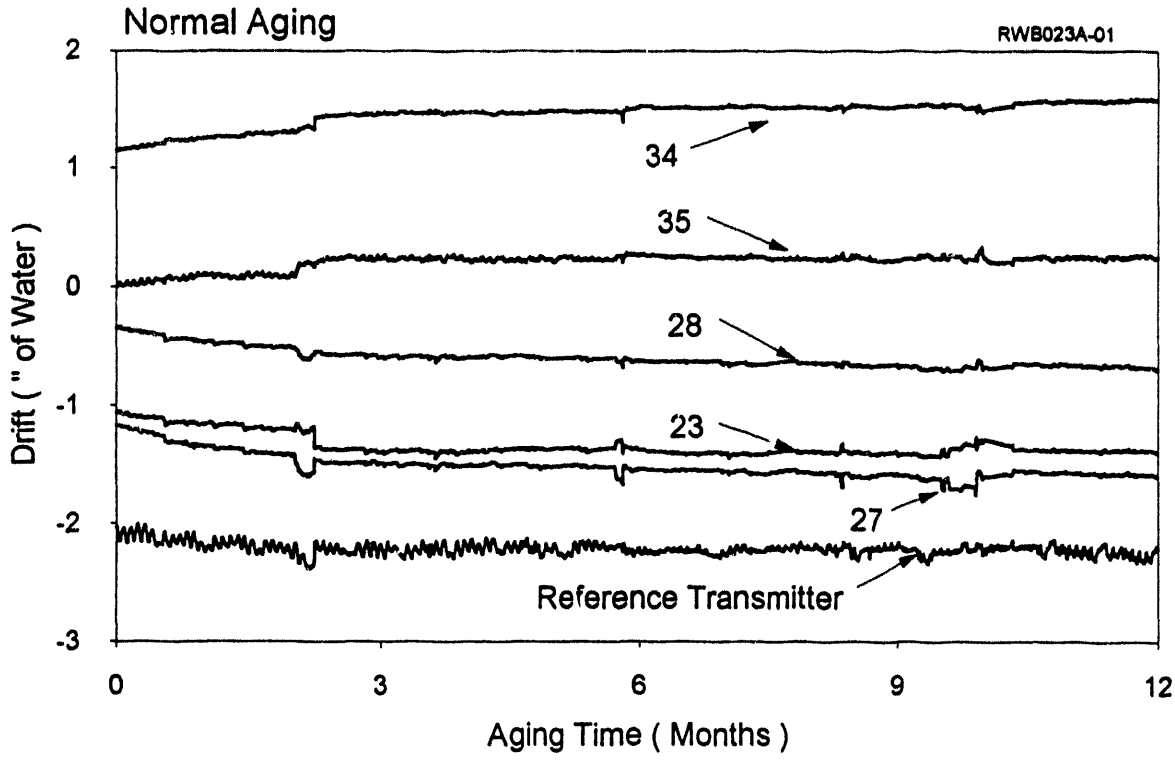
Stressor	Duration (Month)	Aging Conditions	Number of Transmitters Involved
Normal Heat & Humidity	6-12	110°F, 65% RH	23
Extremes of Normal Heat & Humidity	3	150°F, 90% RH	11
Vibration	2	3 mils at 20 Hz	7
Pressure Cycling	2	50% of Span: 100K to 500K Cycles	8
Overpressurization	0.5	1000 psi	8
Phase I Results			17

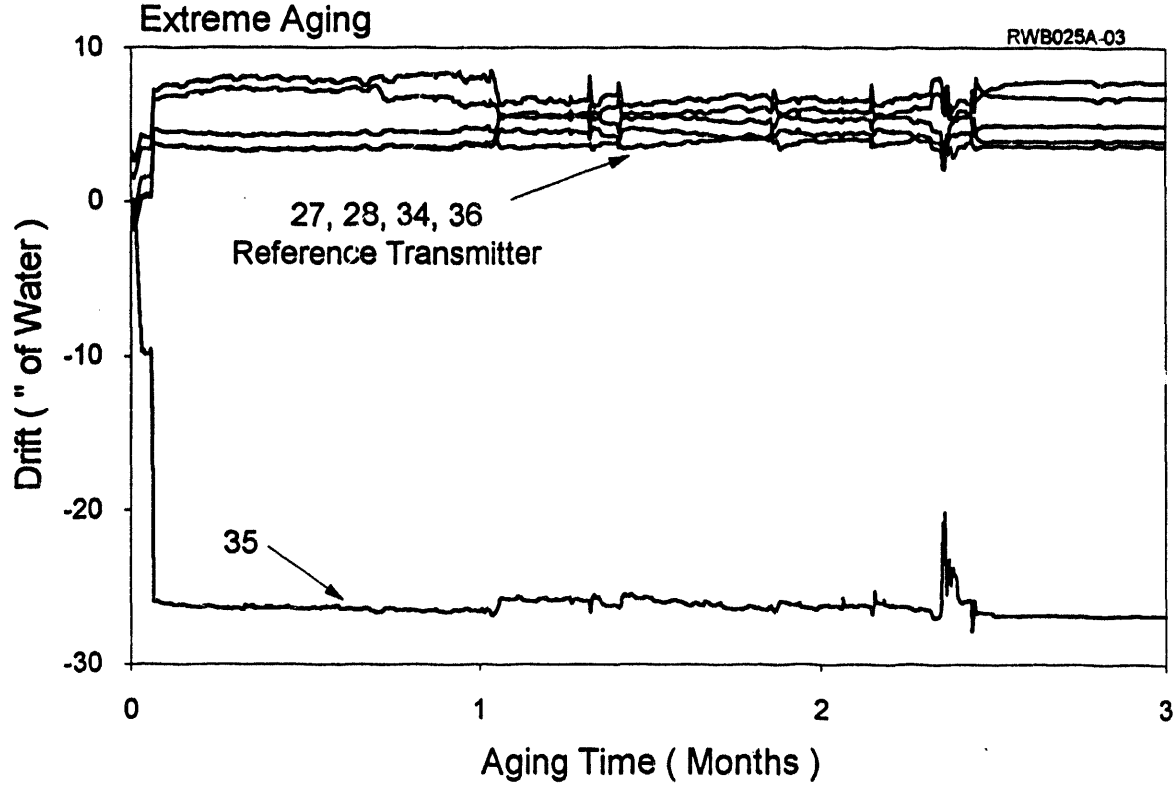
SUMMARY OF AGING TEST RESULTS

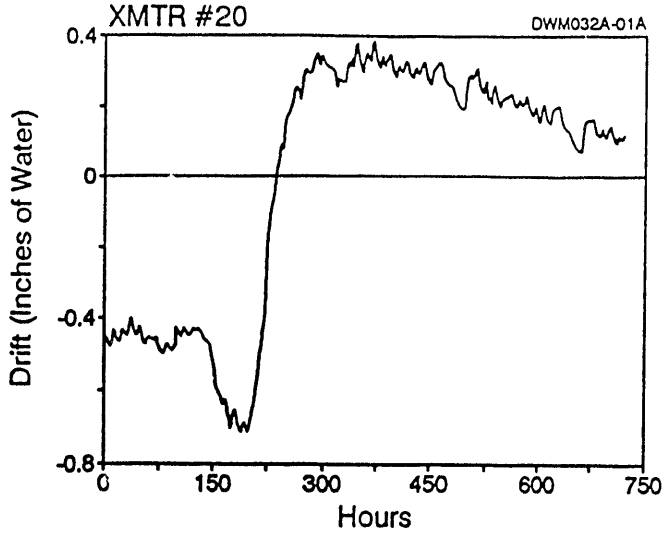
Stressor	Aging Test Results					
	Effect on Calibration			Effect on Response Time		
	Not Affected	Moderately Affected	Failed	Not Affected	Moderately Affected	Failed
Normal Heat & Humidity	61%	35%	4%	87%	4%	9%
Extreme Heat & Humidity	73%	18%	9%	64%	27%	9%
Vibration	0	100%	0	57%	43%	0
Pressure Cycling	63%	37%	0	100%	0	0
Overpressurization	75%	25%	0	100%	0	0
Phase I Results	59%	23%	18%	88%	12%	0
Averages	58%	35%	7%	84%	12%	4%

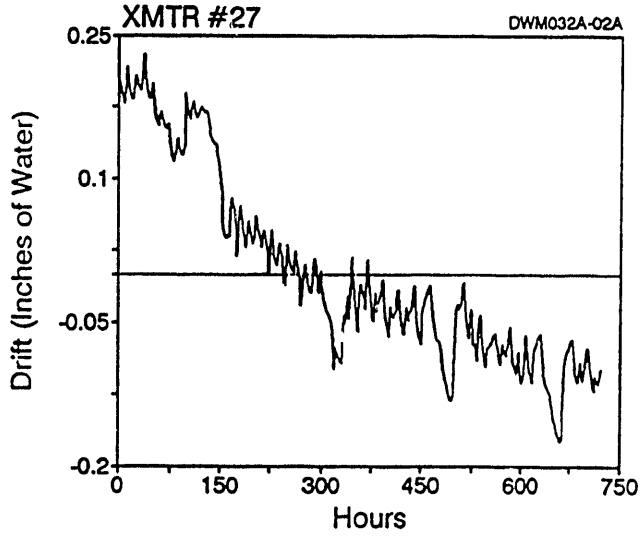

Summary
JPF019A-21B
90
60
30
0
Percentage of Transmitters
Unaffected
Moderately Affected
Failed
Calibration Changes

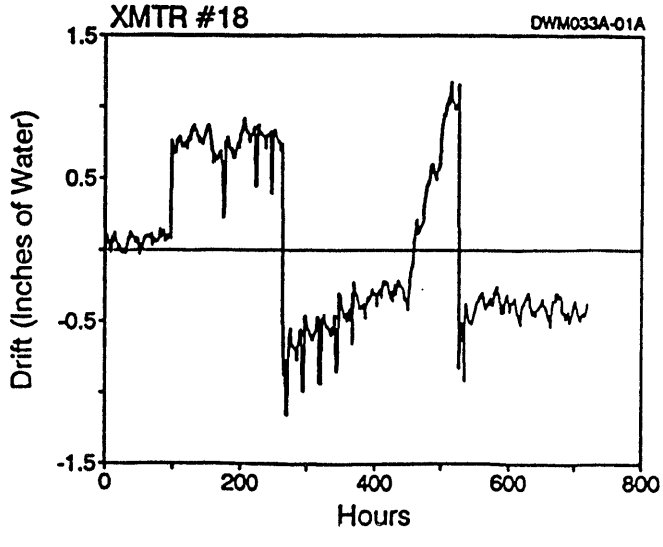

Summary
JPF019A-22B
90
60
30
0
Percentage of Transmitters
Unaffected
Moderately Affected
Failed
Response Time Changes


Normal Aging
RWB023A-01
Drift (" of Water)
2
1
0
-1
-2
-3
34
35
28
23
27
Reference Transmitter
0
3
6
9
12
Aging Time (Months)

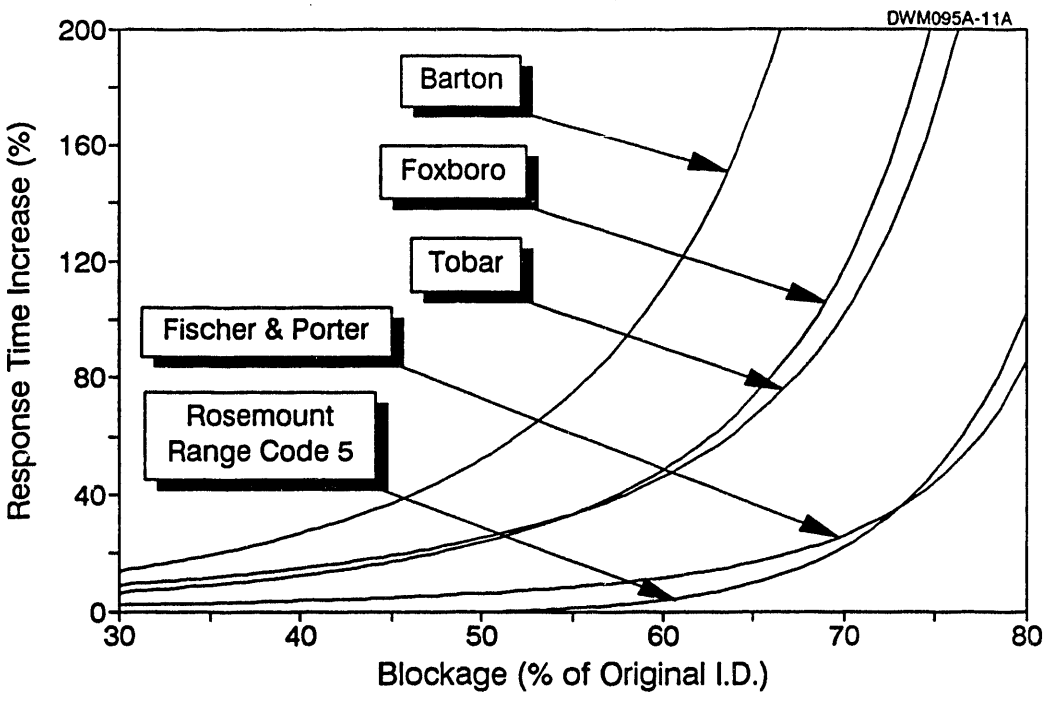

Extreme Aging
RWB025A-03
Drift (" of Water)
10
0
-10
-20
-30
27, 28, 34, 36
Reference Transmitter
35
0
1
2
3
Aging Time (Months)


XMTR #20
DWM032A-01A
Drift (Inches of Water)
0.4
0
-0.4
-0.8
0
150
300
450
600
750
Hours

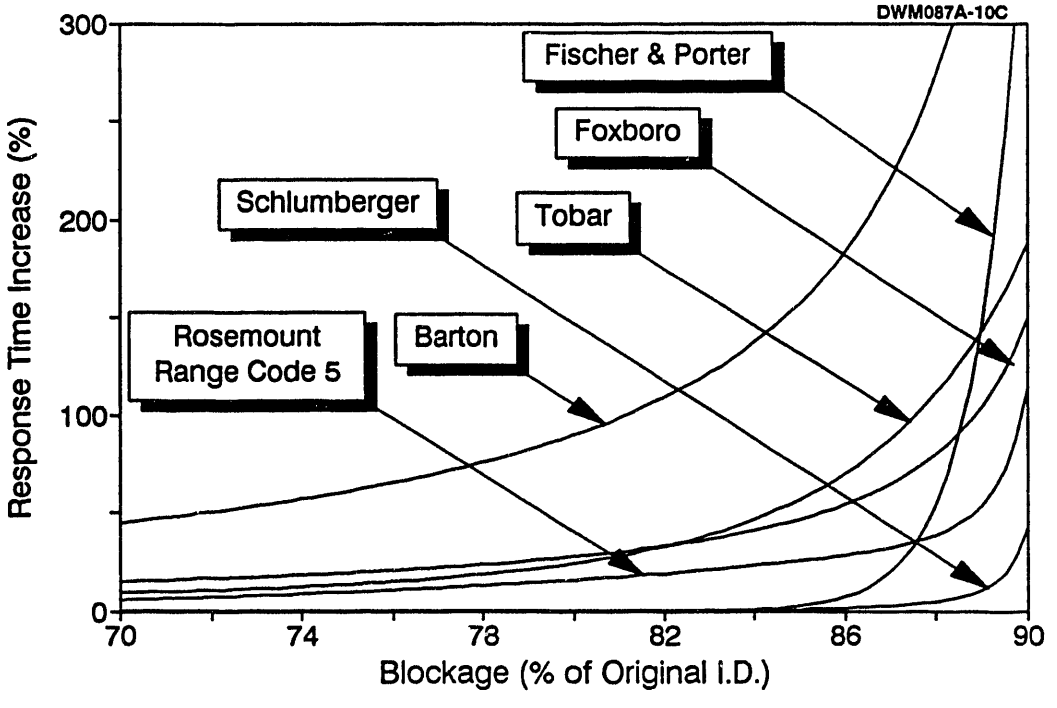

XMTR #27
DWM032A-02A
Drift (Inches of Water)
0.25
0.1
-0.05
-0.2
0
150
300
450
600
750
Hours


XMTR #18
DWM033A-01A
Drift (Inches of Water)
1.5
0.5
-0.5
-1.5
0
200
400
600
800
Hours

Snubber #1

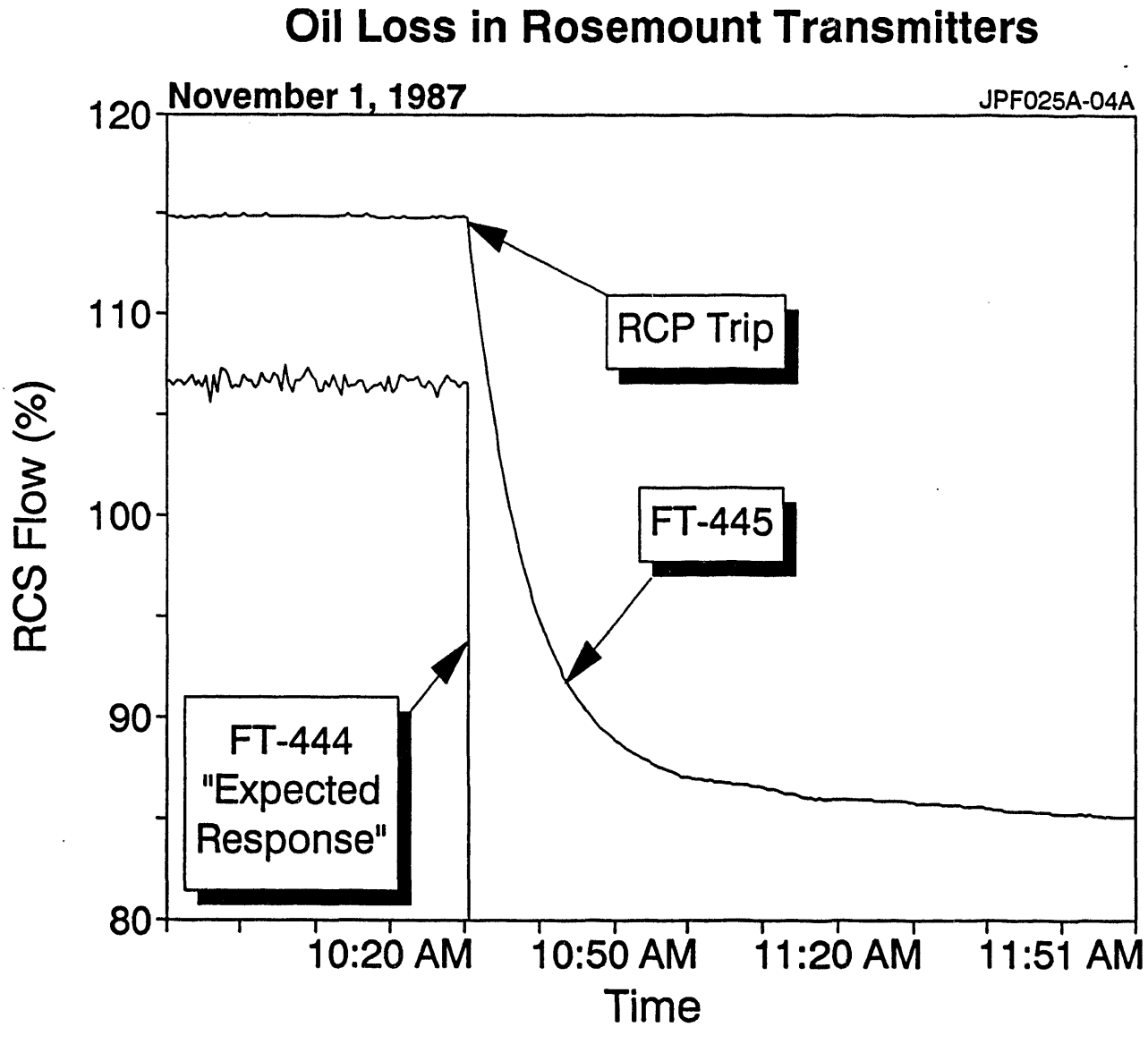


Snubber #2

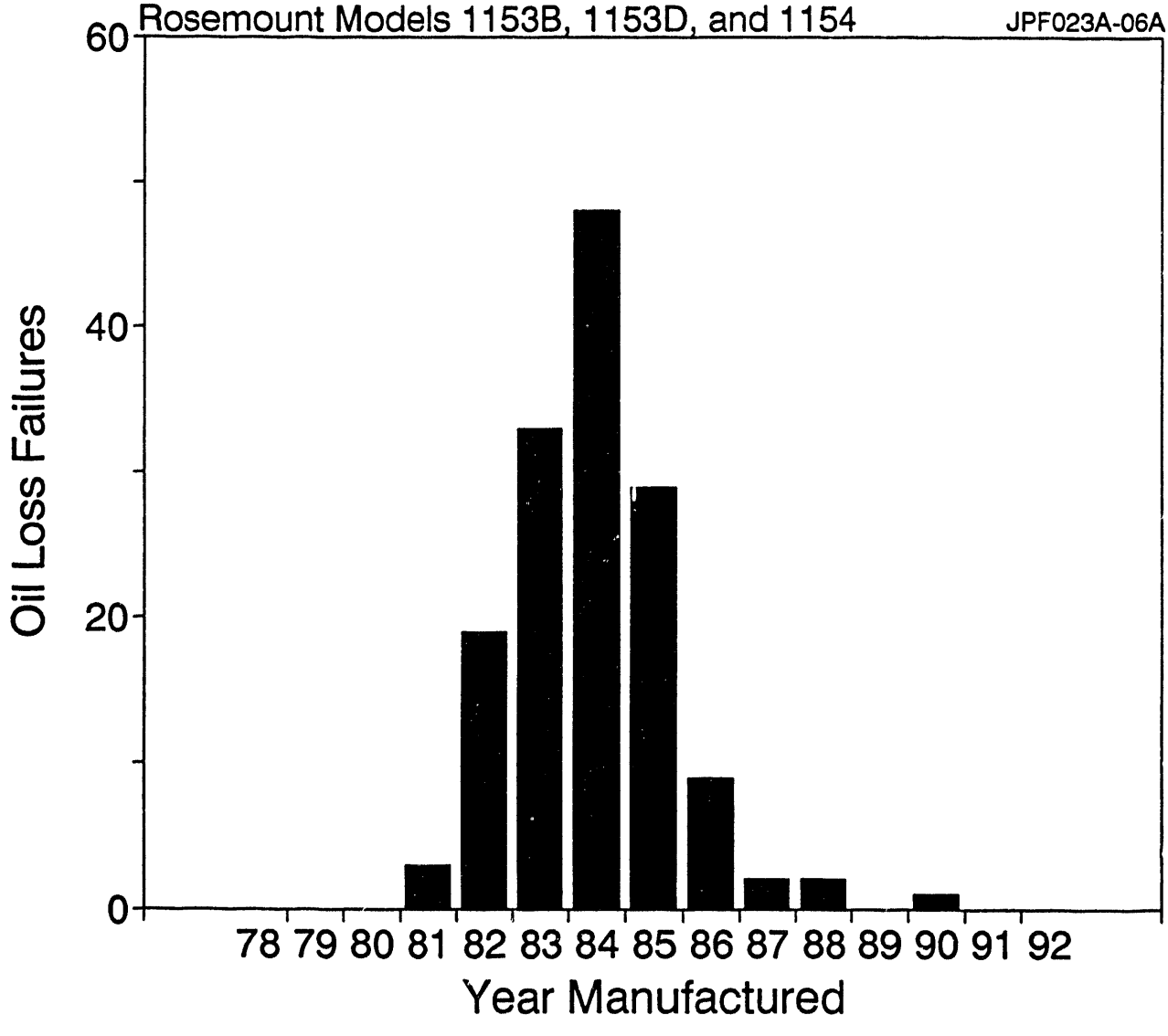


POTENTIAL EFFECTS OF AGING

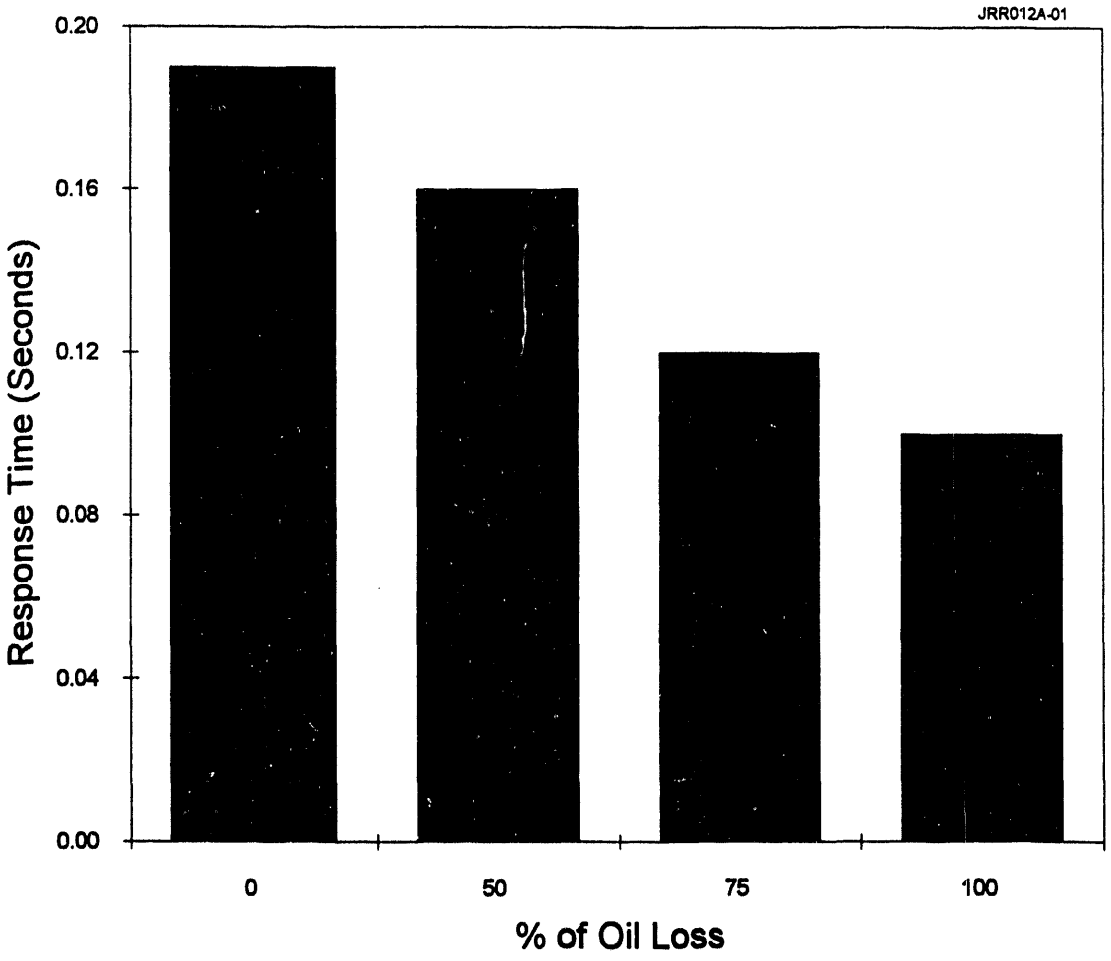
Degradation	Potential Cause	Calibration	Response Time
Partial or total loss of fill fluid	• Manufacturing flaws • High pressure	✓	✓
Degradation of fill fluid	• Viscosity changes due to radiation and heat		✓
Wear, friction, and sticking of mechanical linkages (especially in force balance transmitters)	• Pressure fluctuations and surges • Corrosion and oxidation		✓
Failure of seals allowing moisture into transmitter electronics	• Embrittlement and cracking of seals due to radiation and heat	✓	
Leakage of process fluid into cell fluid resulting in temperature changes in sensor, viscosity changes in fill fluid, etc.	• Failure of seals • Manufacturing flaws • Rupture of sensing elements	✓	✓
Deformation of sensing element resulting in changes in stiffness	• Pressure cycling • Overpressurization • Vibration	✓	✓
Changes in values of electronic components	• Heat, radiation, humidity • Changes in power supply voltages • Maintenance	✓	
Changes in spring constants of bellows and diaphragms	• Mechanical fatigue • Pressure cycling	✓	✓

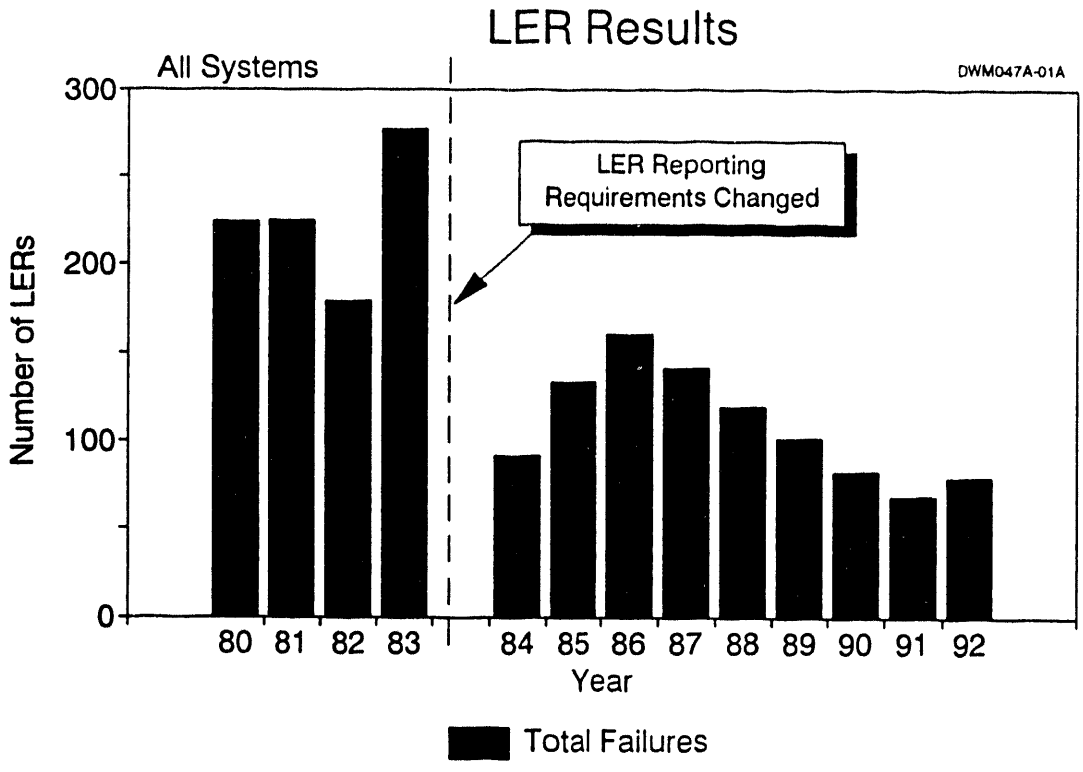

Oil Loss in Rosemount Transmitters
November 1, 1987
JPF025A-04A
120
110
100
90
80
RCS Flow (%)
RCP Trip
FT-445
FT-444
"Expected
Response"
10:20 AM
10:50 AM
11:20 AM
11:51 AM
Time

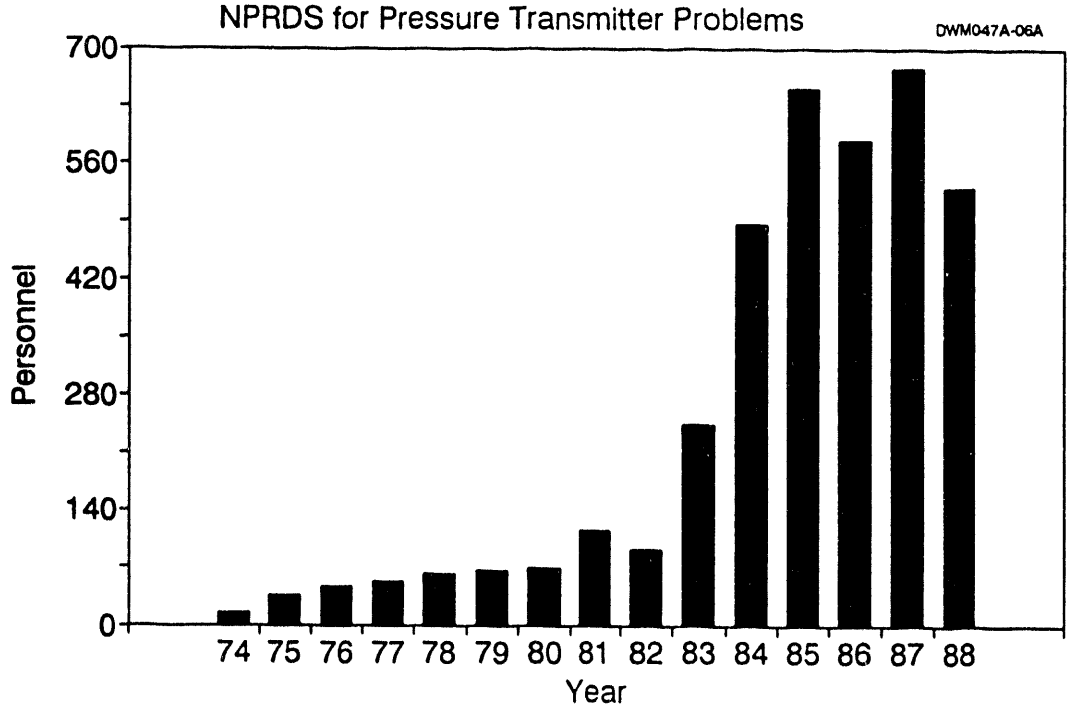
New Rosemount Information

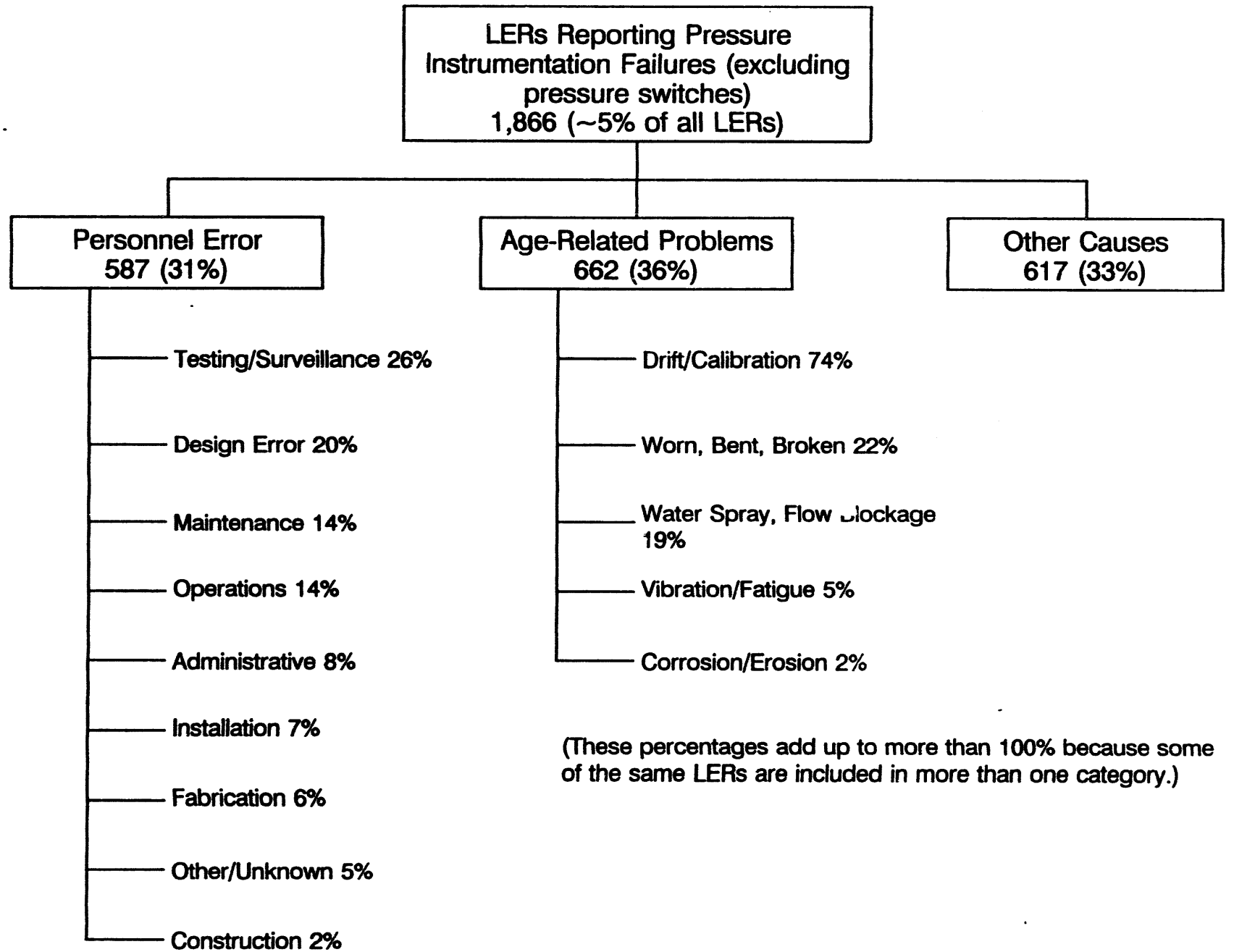


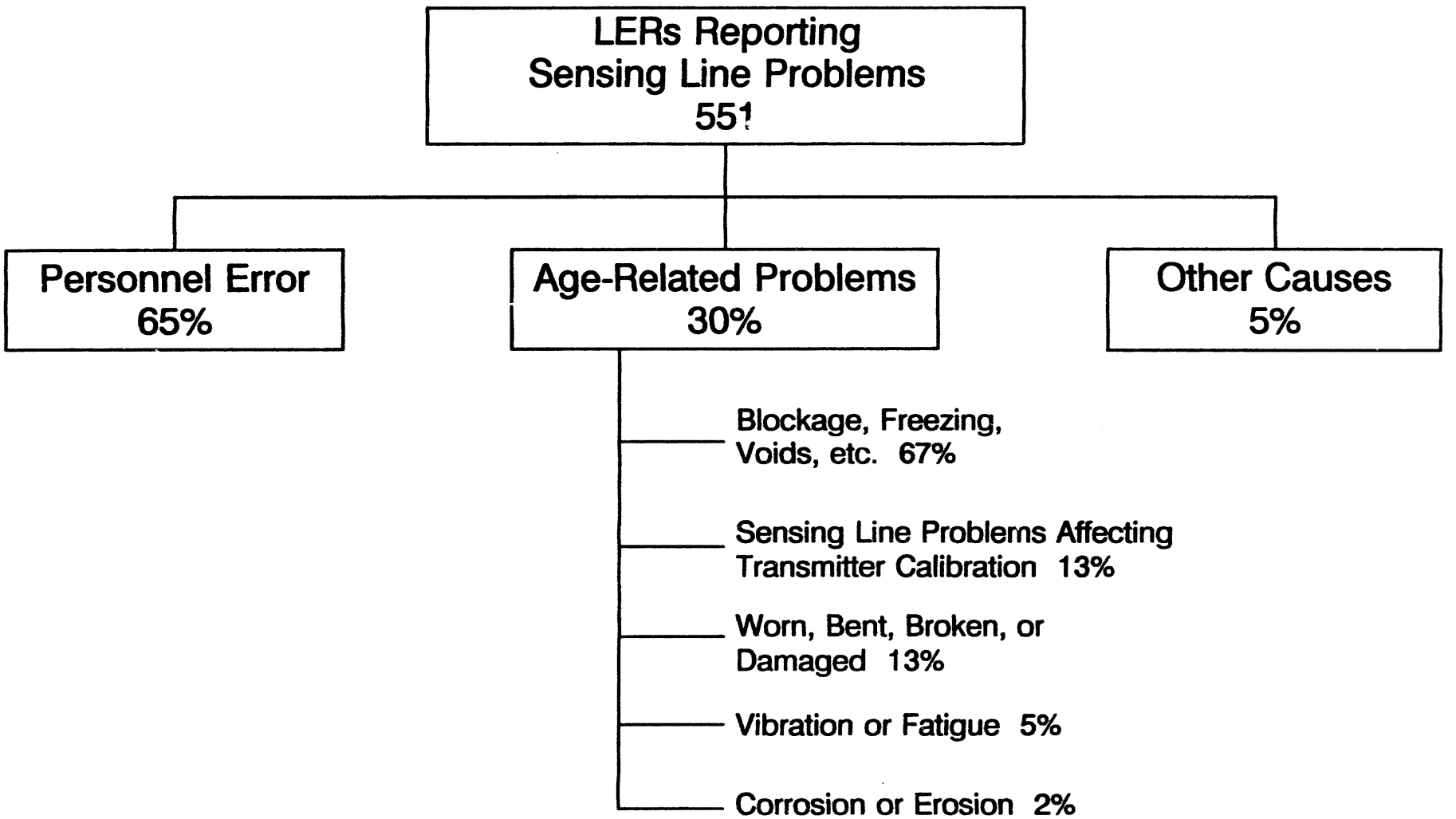
Oil Loss In Other Transmitters




LER Results
All Systems
DWM047A-01A
300
200
100
0
Number of LERs
LER Reporting
Requirements Changed
80 81 82 83 84 85 86 87 88 89 90 91 92
Year
Total Failures


NPRDS for Pressure Transmitter Problems
DWM047A-06A
700
560
420
280
140
0
Personnel
74 75 76 77 78 79 80 81 82 83 84 85 86 87 88
Year


LERs Reporting Pressure Instrumentation Failures (excluding pressure switches) 1,866 (~5% of all LERs)
Personnel Error 587 (31%)
Age-Related Problems 662 (36%)
Other Causes 617 (33%)
Testing/Surveillance 26%
Design Error 20%
Maintenance 14%
Operations 14%
Administrative 8%
Installation 7%
Fabrication 6%
Other/Unknown 5%
Construction 2%
Drift/Calibration 74%
Worn, Bent, Broken 22%
Water Spray, Flow Blockage 19%
Vibration/Fatigue 5%
Corrosion/Erosion 2%
(These percentages add up to more than 100% because some of the same LERs are included in more than one category.)


LERs Reporting
Sensing Line Problems
551
Personnel Error
65%
Age-Related Problems
30%
Other Causes
5%
Blockage, Freezing,
Voids, etc. 67%
Sensing Line Problems Affecting
Transmitter Calibration 13%
Worn, Bent, Broken, or
Damaged 13%
Vibration or Fatigue 5%
Corrosion or Erosion 2%

CONCLUSIONS

- Aging can Adversely Affect the Performance of Nuclear Plant RTDs and Pressure Transmitters
- Current Testing Interval of Once Every Fuel Cycle is Adequate for Aging Management
- In-Situ Response Time and Calibration Testing Methods have been Developed and Validated for Nuclear Plant RTDs and Pressure Transmitters

Validation of On-Line Monitoring Techniques for In-Situ Testing of Calibration Drift of Process Instrumentation Channels in Nuclear Power Plants

H. M. Hashemian
D. W. Mitchell

Analysis and Measurement Services Corporation
AMS 9111 Cross Park Drive
Knoxville, TN 37923 USA
Phone: (615) 691-1756
Fax: (615) 691-9344

C. E. Antonescu

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Division of Engineering
Electrical & Mechanical Engineering Branch
Washington, D.C. 20555
Phone: (301) 492-3824
Fax: (301) 492-3696

ABSTRACT

This paper reports on the progress of a research and development (R&D) project which is underway to provide an assessment of the validity of the on-line monitoring techniques for instrument calibration reduction in nuclear power plants.

Both laboratory and in-plant validation work on typical nuclear plant instrumentation channels are being conducted under this project. The laboratory validation tests are performed in a test loop in which a number of nuclear grade temperature and pressure sensors have been installed and connected to a Westinghouse Model 7300 instrumentation system of the type used in Pressurized Water Reactors (PWRs). The loop is used to determine if simulated drift in the sensors can be effectively detected by on-line monitoring methods. It is also used for verification and validation of on-line monitoring software packages being developed as a part of this project.

The in-plant validation work is being performed at the McGuire Nuclear Power Station where 170 process signals are being monitored under normal operating conditions. The signals are being recorded for an entire fuel cycle and analyzed to identify any channels that may have drifted out of tolerance during the fuel cycle. The results of this work will be compared with the results of the conventional hands-on calibrations that are normally performed at refueling outages. This comparison will help determine if on-line monitoring techniques can identify the same drift that is detected by conventional calibrations.

The results of the laboratory and in-plant research completed to date have shown that on-line drift monitoring should be a successful tool for isolating the instrument channels that must be calibrated. This will help limit the calibration activity to only those channels which need to be calibrated as opposed to calibrating all safety-related channels, as is presently being done.

1. INTRODUCTION

Process instrumentation channels in nuclear power plants are calibrated at every refueling outage and surveillance tested once every month or once every quarter depending on the plant. These activities usually employ hands-on procedures which involve extensive manpower and personnel radiation exposure, and have the potential of producing maintenance-induced errors, reactor trips, and wear and tear of the plant equipment. A search of the Licensee Event Report (LER) database has shown (Figure 1) that a notable number of instrumentation problems and plant trips have been caused by hands-on maintenance and testing activities. Furthermore, a review of historical calibration and surveillance data from nuclear power plants has revealed that less than five percent of instrument channels are normally found to drift out of tolerance over a typical fuel cycle of eighteen months. That is, a majority of the effort currently spent on calibration of instrument channels may not be necessary if a means can be established to identify those instrument channels which drift or otherwise need calibration or maintenance.

2. TECHNICAL BACKGROUND

Following the 1979 accident at the Three Mile Island Nuclear Power Station Unit 2, the U. S. Nuclear Regulatory Commission (NRC) implemented a number of new requirements to ensure that the reactor operators are provided with accurate, timely, and reliable information about the status of the plant under normal and accident conditions. In response, the nuclear industry began upgrading the control rooms of the plants using state-of-the-art computer technology, color monitors, and digital and analog display equipment to provide the operators with a great

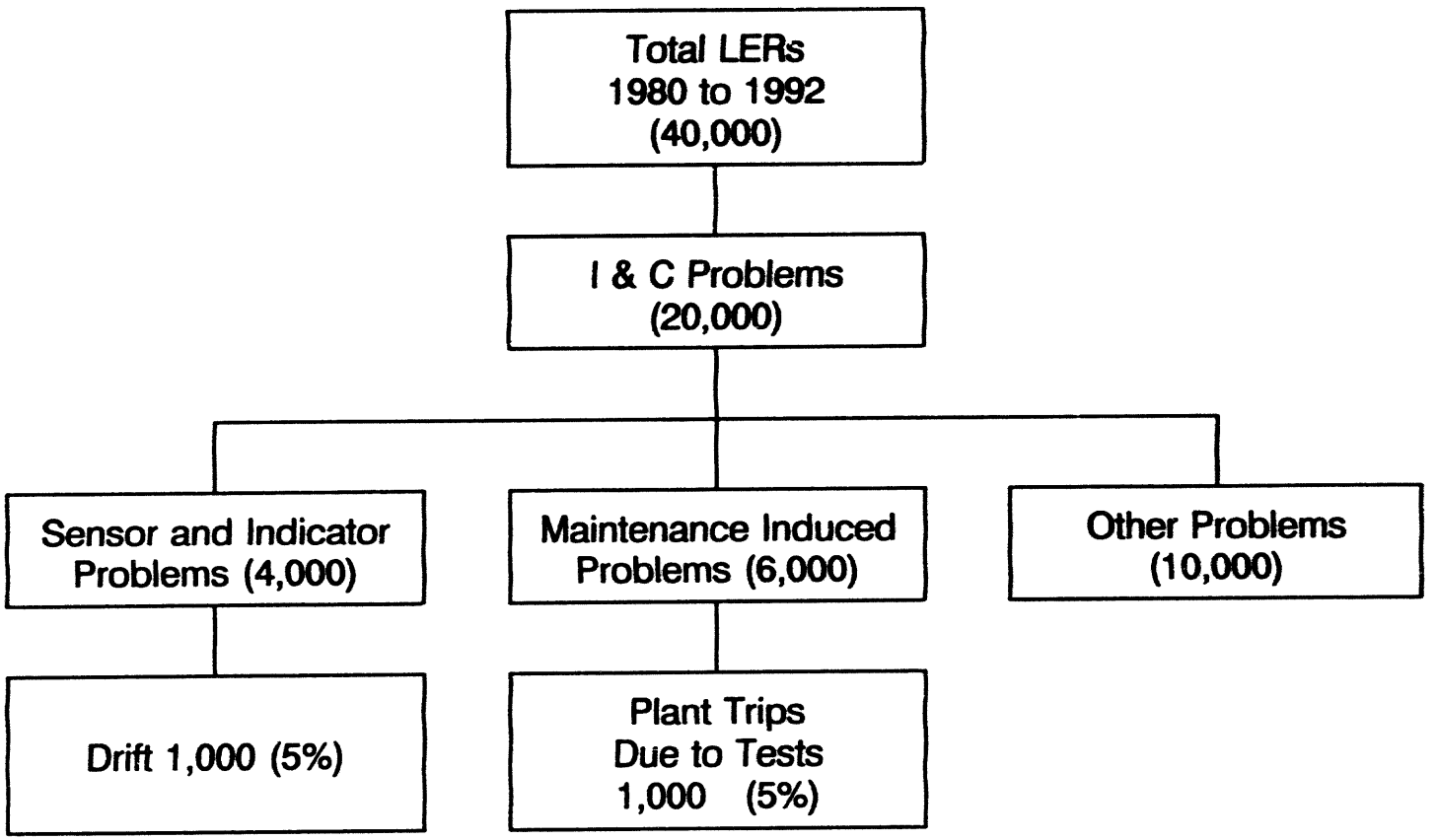


Figure 1. Results of Search of the LER Database (the LER Numbers in this Diagram are Rounded to Simplify the Presentation).

deal of qualitative and quantitative information at the touch of a few buttons. The displays were designed and located in the control room according to human factor principles to make it easy for the operators to determine the status of the plant at a glance. An example of an important operator aid that incorporates these new developments is the Safety Parameter Display System (SPDS) which is used to assess the safety status of the reactor and critical components of the plant. This system uses the existing signals from some of the process instrumentation channels to display the present and past status of the plant in terms of color graphs and simple charts.

To ensure that reliable signals are used in operator aids, the Electric Power Research Institute (EPRI) initiated research and development activities in the early 1980s in an area that is now known as "signal validation."[1] Signal validation techniques have been used previously in the aerospace and aviation industries for flight control and space vehicle applications.

Signal validation consists of a variety of signal processing techniques implemented in nuclear power plants to ensure that sensor drift, response time degradation, bias, noise, and other sensor or system anomalies do not mislead the reactor operators. Signal validation depends on the redundancy of sensors in nuclear power plants and the physical relationships between the process parameters to check the consistency of the measurements, predict the expected values of process variables, and detect, isolate, and characterize any significant anomaly in the instrument channel.

EPRI's efforts in the signal validation area have not only produced improvements in operator aids, but also have laid the foundation for the development of on-line methods for testing the calibration of instrument channels. In fact, the outgrowth of signal validation techniques for instrument calibration testing has overshadowed its application to SPDS and other operator aids. In addition to EPRI, a number of national and international research and development organizations, universities, national laboratories, and utilities have worked in the signal validation area. As a result, numerous techniques have been researched or developed and documented under a variety of names. A few examples of these techniques are described below.

2.1 Like Signal Comparison

This method is also referred to as cross calibration or DC signal comparison. It involves scanning the output of a number of instrument channels that are measuring the same process parameter and determining the deviation of each channel from the average of all channels (excluding the outliers). This method is popular in PWRs for on-line testing of calibration of temperature sensors at isothermal conditions. The principle of this method is illustrated in Figure 2. A problem with the like signal comparison technique is that it may not account for common mode drift unless a newly calibrated sensor is included in the comparison and/or a method such as analytical redundancy, as defined below, is used to provide an independent estimate of the process parameter.

2.2 Analytical Redundancy

This method is used when an adequate number of physically redundant channels is not available for intercomparison and when an independent measure of a process parameter is needed to account for common mode drift. As its name implies, analytical redundancy depends on theory to produce fictitious sensors or instrument channels to increase the redundancy. More specifically, it uses a group of diverse signals as the input to a physical or empirical model to produce a new signal that has a relationship with the group. Analytical redundancy is also referred to as diverse signal comparison. The principle of the method is illustrated in Figure 3.

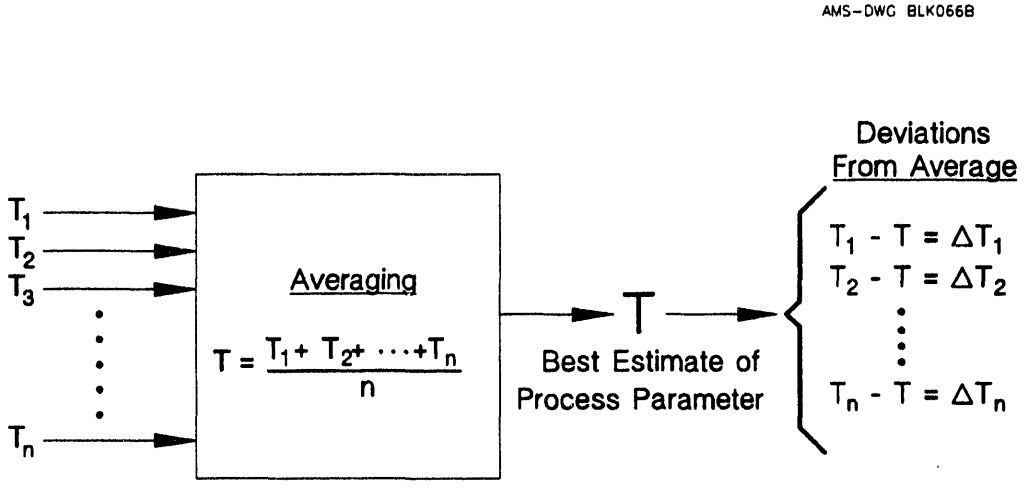


Figure 2. Illustration of Principle of Like Signal Comparison Technique.

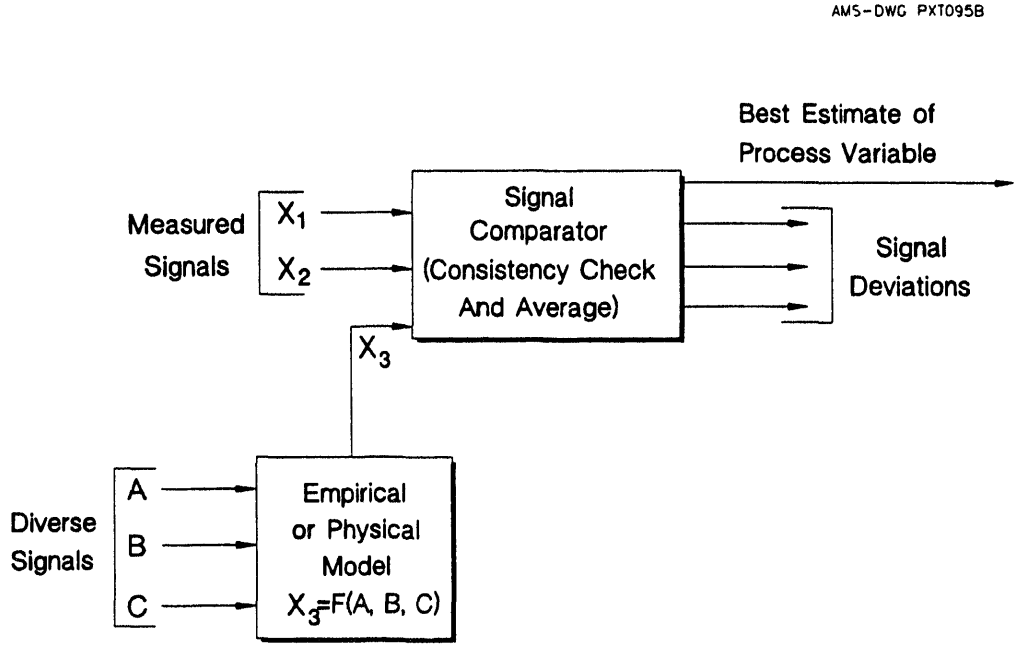


Figure 3. Principle of Analytical Redundancy.

2.3 Parity Space

This method is used to determine the consistency between a group of redundant signals. The common components of the signals are subtracted out and the remaining components are compared, two at a time. Based on the differences between the residual components in each pair, an inconsistency index is generated and used for diagnostics. This index is also used as a weighting factor in weighted averaging of redundant signals. Signals with low inconsistency indices are weighted more than signals with high inconsistency indices.

3. CURRENT NUCLEAR INDUSTRY PRACTICE

The nuclear power industry currently practices a very conservative approach with respect to performance testing of safety-related process instrumentation channels. In most plants, these channels are qualitatively checked three times a day, surveillance tested every month, and fully calibrated at every refueling outage and whenever a component is replaced.

There are some variations in testing practices throughout the nuclear power industry and some differences in the terminologies used for the tests. For example, the monthly or quarterly surveillance tests are referred to as functional tests in some plants and are performed according to a different set of procedures and acceptance criteria than the surveillance tests. These variations make it difficult to provide a general picture of the nuclear industry's practices. Nevertheless, we have attempted to present in the following sections a representative overview of the bulk of current practices.

3.1 Daily Channel Checks

The safety-related instrument channels in most plants are qualitatively checked by the plant operators once every shift. The operators look at the indicators in the control room to ensure that the redundant channels agree with one another within a certain tolerance. The resulting information is recorded in the plant's daily logs and any problem to be corrected is reported to the maintenance staff.

3.2 Surveillance Tests

Surveillance tests are usually performed on all safety-related instrument channels once every month while the plant is operating. The purpose of the surveillance tests is to either verify the trip setpoints or test the functionality of the instrument channels.

The surveillance tests are performed at the instrument racks, and include all the components of the instrument channel except for the sensor. The sensor is located in the field and is not usually tested during plant operation except for in-situ response time testing described in Reference 2. There is some concern as to whether or not it makes sense to test an instrument channel without the sensor. The sensor is the component of the channel that is most susceptible to performance problems because it is located in the harsh environments of the plant as opposed to the rest of the channel which is located in a mild environment. An on-line monitoring system as a substitute for the surveillance tests, as contemplated by the nuclear industry, has the advantage of testing the whole channel including the sensor. In addition, on-line monitoring is a completely passive approach in contrast with the surveillance tests which require physical interactions with the plant equipment.

3.3 Full-Channel Calibration

All safety-related instrument channels are fully calibrated during refueling outages. The calibration procedures are almost identical to the surveillance procedures except that they include the sensor. Furthermore, in executing calibration procedures, all instrument deviations are usually zeroed, if possible, whether or not a channel meets its acceptance criteria.

The full-channel calibration practice seems to be uniform throughout the nuclear industry except for what is done with the sensors. More specifically, the channels (excluding the sensors) are fully calibrated in all plants and all problems are usually resolved at every refueling outage. In addition, all safety-related pressure and differential pressure transmitters (including level and flow transmitters) are calibrated in all plants and all problems are resolved at every refueling outage. Thermocouples and neutron detectors are rarely calibrated, except for comparing neutron channel outputs to heat balance data, and the practice is sporadic with respect to resistance temperature detectors (RTDs). A few plants periodically remove and recalibrate their RTDs, some plants periodically install new RTDs with fresh calibrations, many plants perform cross calibration at hot standby conditions, and other plants do not calibrate their RTDs at all. The number of RTDs that are calibrated and the frequency of the calibration are also sporadic across the nuclear power industry.

4. VALIDATION OF ON-LINE MONITORING TECHNIQUES

The nuclear power industry has been interested in implementing on-line monitoring techniques to extend the frequency of calibration of process instrumentation channels in nuclear power plants. Although a lot of effort has been spent on development of on-line monitoring equipment and techniques in the last ten years, a systematic effort is yet to be completed on validation of these equipment and techniques. The research and development effort reported in this paper is the first systematic attempt in determining the feasibility and accuracy of on-line monitoring techniques for instrument calibration reduction in nuclear power plants. To date, a Phase I project has been completed by Analysis and Measurement Services Corporation (AMS) and a Phase II effort is underway. The Phase II effort is a two year R & D project to be completed by October 1994.

The results of the Phase I effort have been documented in the NUREG/CR-5903, which has been written by AMS under a contract with the NRC. [3] This report documents the initial efforts involving both laboratory and in-plant validation research conducted under a joint R & D effort between AMS, NRC, and Duke Power Company. The Duke Power Company is participating as the host utility for the project with its McGuire nuclear power plant as the site for the in-plant validation research. The NRC is providing partial funding for the project under a special U.S. government program that is intended to meet the government research needs and promote the commercialization of federally-funded R & D projects. The following sections provide examples of the results of the laboratory and in-plant tests performed in Phase I.

4.1 Laboratory Test Results

The feasibility of on-line monitoring techniques are being studied through a series of experiments performed on representative temperature and pressure sensors and associated signal conditioning equipment installed in a laboratory test loop. Figure 4 shows the type and location of the sensors as installed and tested in the loop. This includes pressure sensors designated as PT, flow sensors designated as FT, thermocouples designated as TC, and RTDs designated as TE.

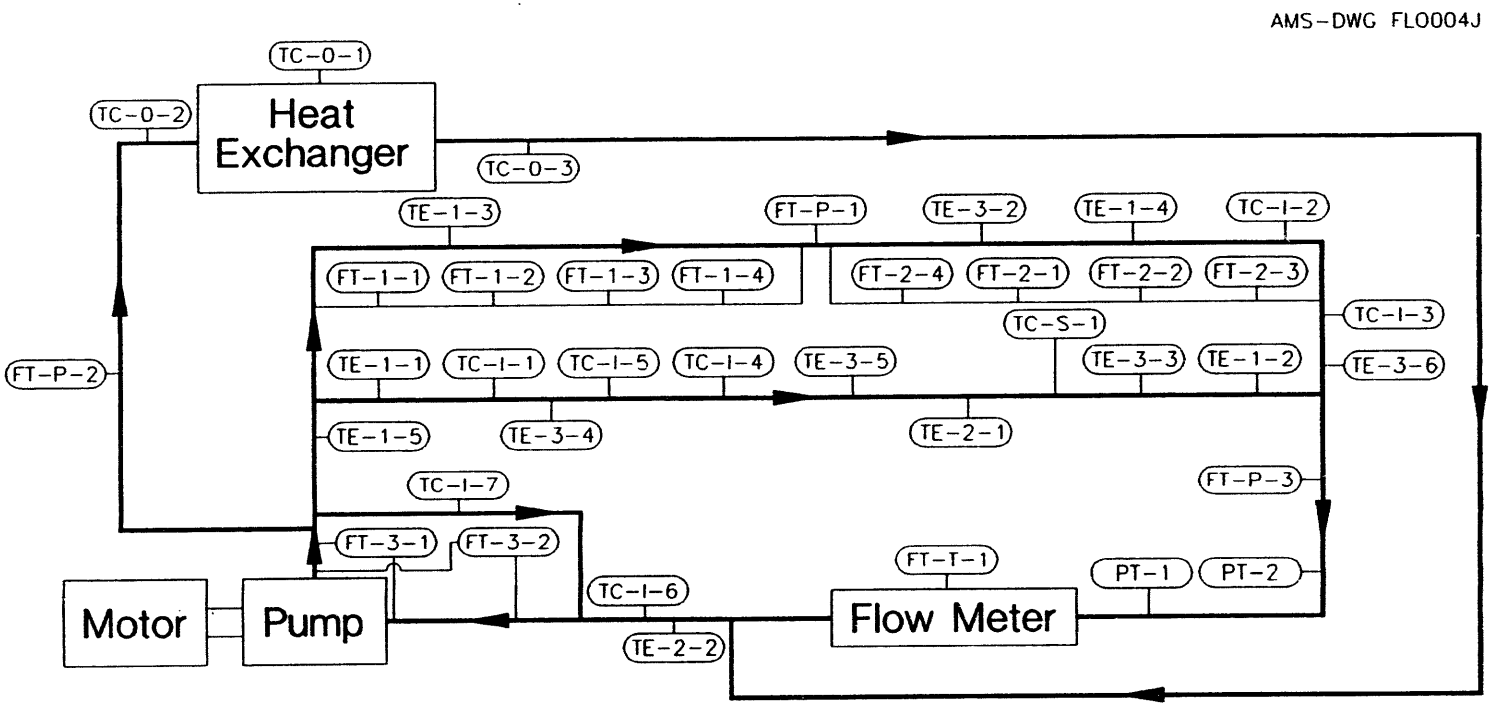


Figure 4. Temperature, Pressure, and Flow Sensors Installed in the Laboratory Test Loop.

An empirical model of the laboratory loop was developed and validated with data from the sensors in the loop. Representative results are shown in Figure 5 in terms of time history plots for a temperature signal. The plot shows the model prediction and the corresponding measured data. It is apparent that the model prediction agrees well with the measured data indicating the validity of the model. As shown in Figure 5, the signal level was changed several times during the tests to help identify the parameters of the model. The same type of comparison for a physical model is shown in Figure 6. This data represents a transient temperature signal induced by a cool down of the test loop. The difference between the model prediction and the actual temperature is also shown. The differences throughout the data are small (less than 1°F) indicating the validity of the physical model. Another example of transient temperature data is shown in Figure 7 for four thermocouples tested in the loop from start up through steady-state conditions. The model prediction is not shown in this figure but the actual loop temperature as measured with a calibrated RTD is shown. Following the initial transients during the loop start up, the thermocouples track the actual process temperature to within about 1°F as shown in the deviation plot of Figure 7. The deviation plot represents the difference between each signal and the average of all signals in the group. The significance of these plots is that they provide confirmation that the tests, data acquisition, and data analysis algorithms developed for this project are performing as expected.

Figure 8 shows time history traces for three flow transmitters, with a drift intentionally induced in FT-1-1 to show how the drift manifests itself in the deviation plot. Note that the drift in the FT-1-1 causes all three signals to exhibit drift behavior in the deviation plot at the beginning of the data. Also, note the sudden shift in the deviation traces at about 600 minutes into the data. This occurs because FT-1-1 is excluded from the average at this point in time when its deviation exceeds a preset criteria. This causes all three signals to exhibit a step change in the deviation plot.

It should be pointed out that the purpose of the project for generating the data and the plots of the types discussed above is to provide a database of information to serve as a learning tool in developing the experience that is necessary to interpret the drift behavior of various combinations of signals.

4.2 In-Plant Test Results

The in-plant validation of on-line monitoring techniques is the most important aspect of this project. The in-plant validation work is being conducted at the McGuire Nuclear Station Unit 2 where 170 signals from the primary and secondary systems of the plant are being monitored continuously, including when the plant is at cold shutdown. The monitoring began in March 1992 at the beginning of the plant's eighth fuel cycle and will continue for two complete fuel cycles. A listing of the signals being monitored is given in Table 1. This includes both safety-related and non-safety-related sensors. An attempt has been made to use all the redundant sensors from each service, but in some cases only two out of a group of three or four sensors were available for monitoring. It should be pointed out here before proceeding to present in-plant results that the work at the McGuire plant and the test results given here are of a preliminary research nature and should not be used as a basis for any conclusions without further investigation.

Figure 9 shows a block diagram of a typical instrument loop for a flow transmitter and how the flow signal is connected to the on-line monitoring system. It is clear that the monitoring includes not only the sensor, but also the instrument loop electronics. However the logic and trip circuitry are not included in the monitoring.

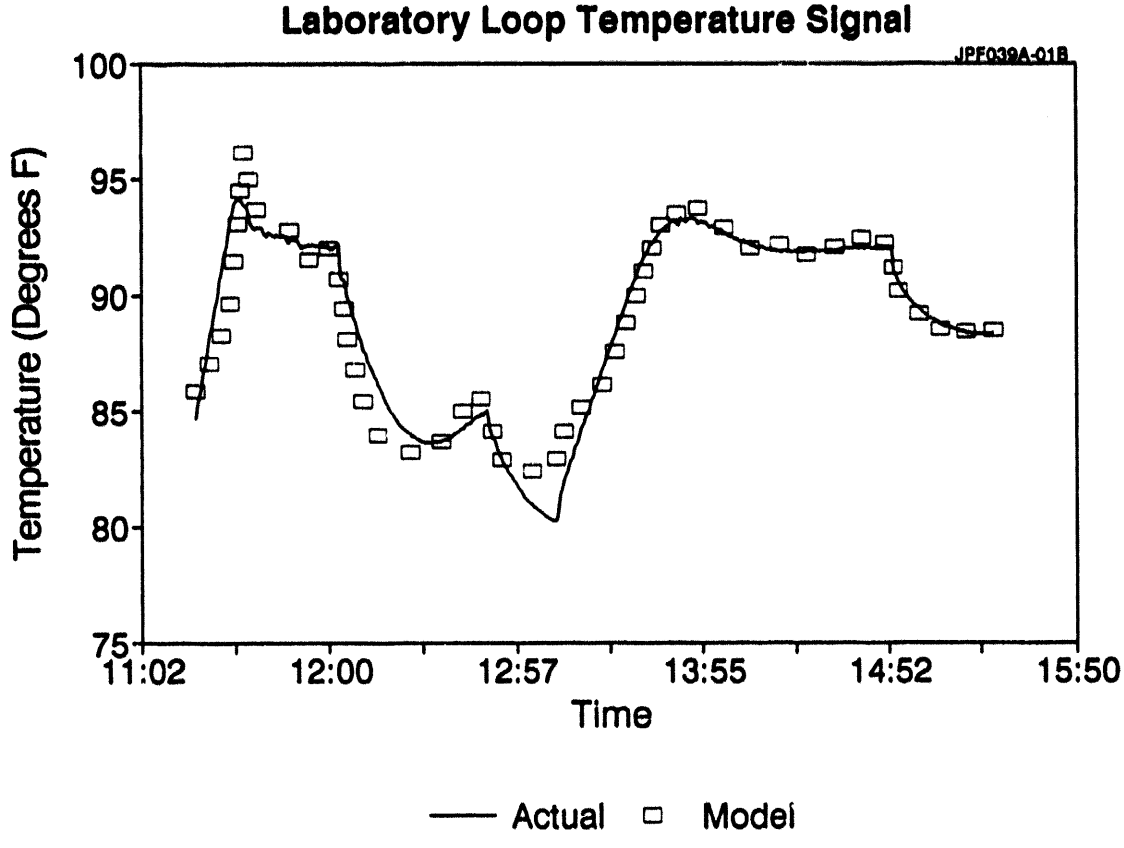


Figure 5. Agreement Between Results of Empirical Model and Actual Temperature Data.

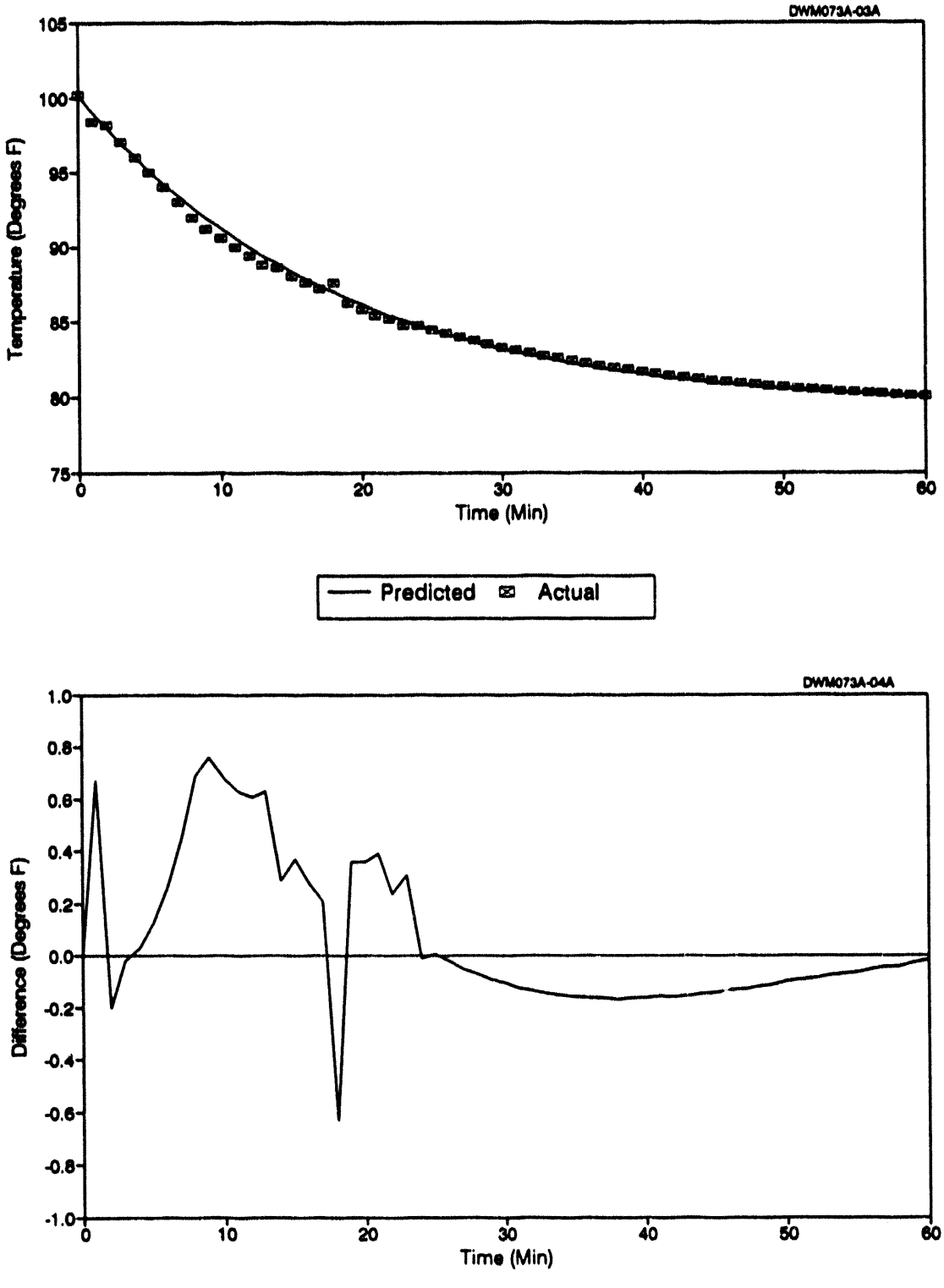


Figure 6. Agreement Between Results of Physical Model and Actual Temperature Data.

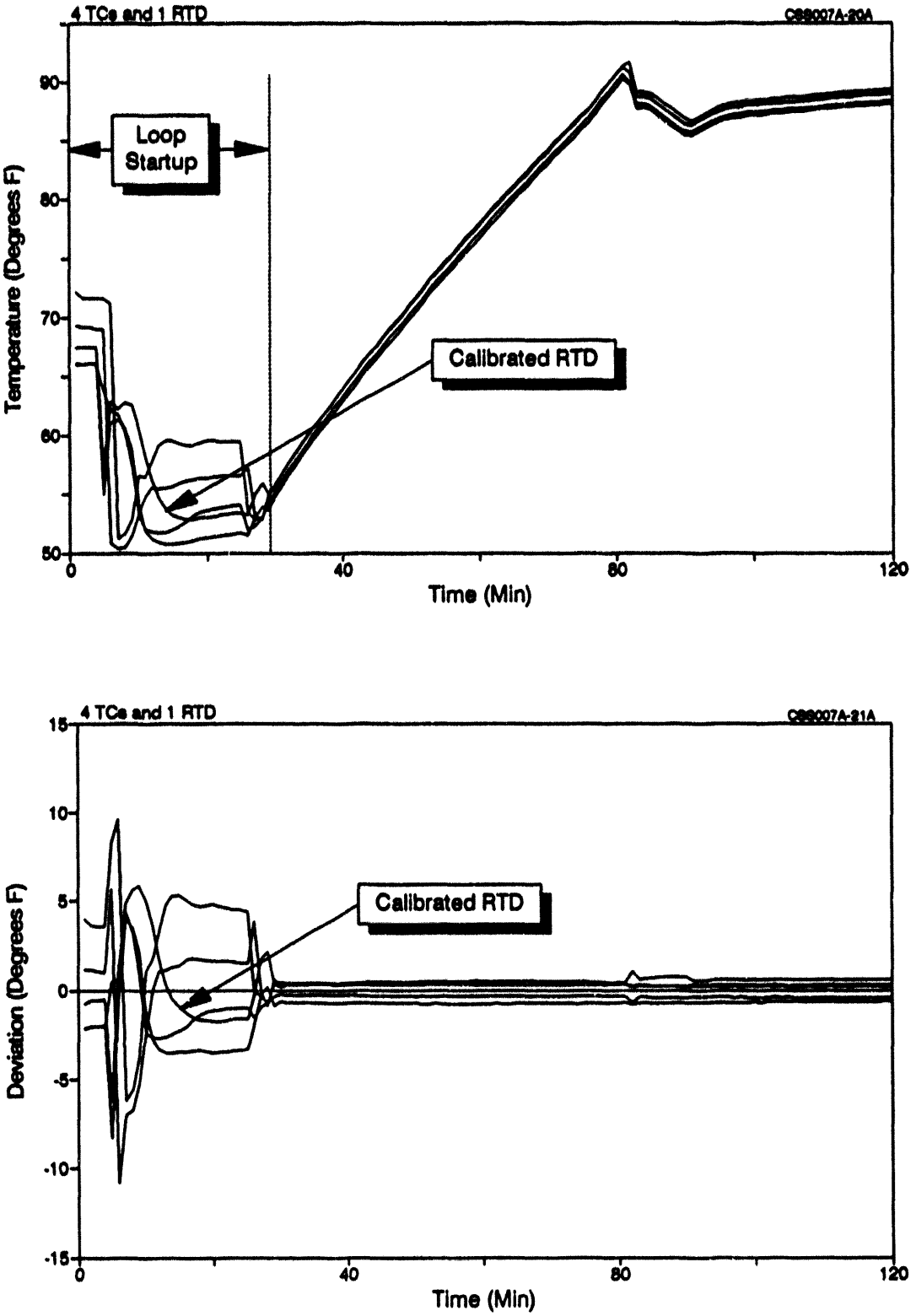


Figure 7. Agreement Between Five Temperature Sensors Monitoring the Loop Temperature from Start Up to Steady-State.

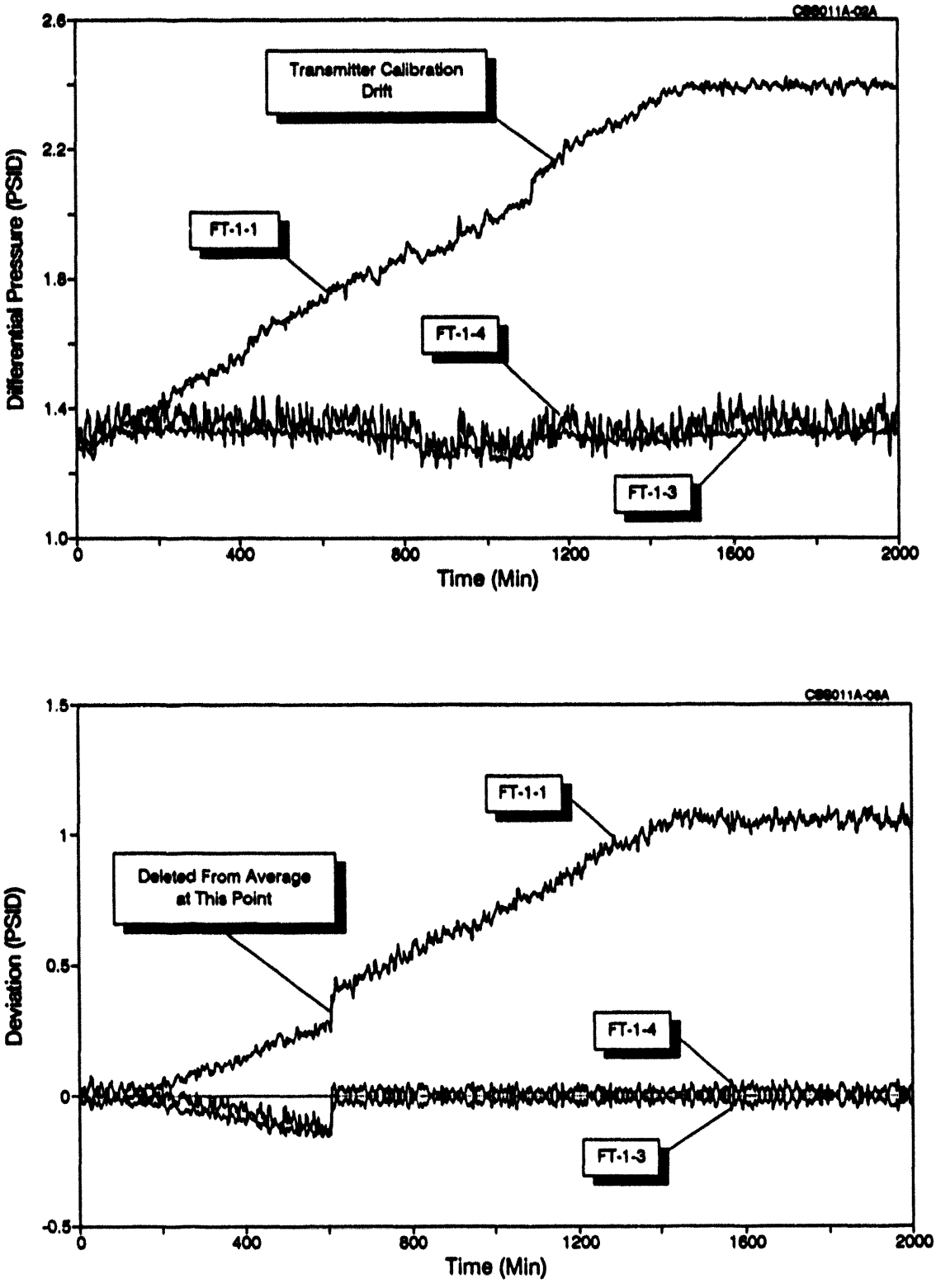


Figure 8. Bias and Drift in Transmitter Signals.

Table 1

Listing of Signals Monitored at McGuire Unit 2

Item	Description of Signal	Number of Signals
1	Steam Flow	8
2	Steam Pressure	12
3	Steam Generator Level	20
4	Feedwater Flow	8
5	Auxiliary Feedwater Flow	4
6	Reactor Coolant Flow	12
7	Pressurizer Level	3
8	Pressurizer Pressure	4
9	Wide Range Reactor Coolant Pressure	2
10	Containment Pressure	3
11	Reactor Vessel Level Indicating System (RVLIS)	6
12	Turbine Impulse Pressure	2
13	Neutron Flux Detectors (NI Channels)	12
14	Narrow Range RTDs	16
15	Wide Range RTDs	8
16	Core Exit Thermocouples	40
17	Miscellaneous	10
Total Signals		**170**

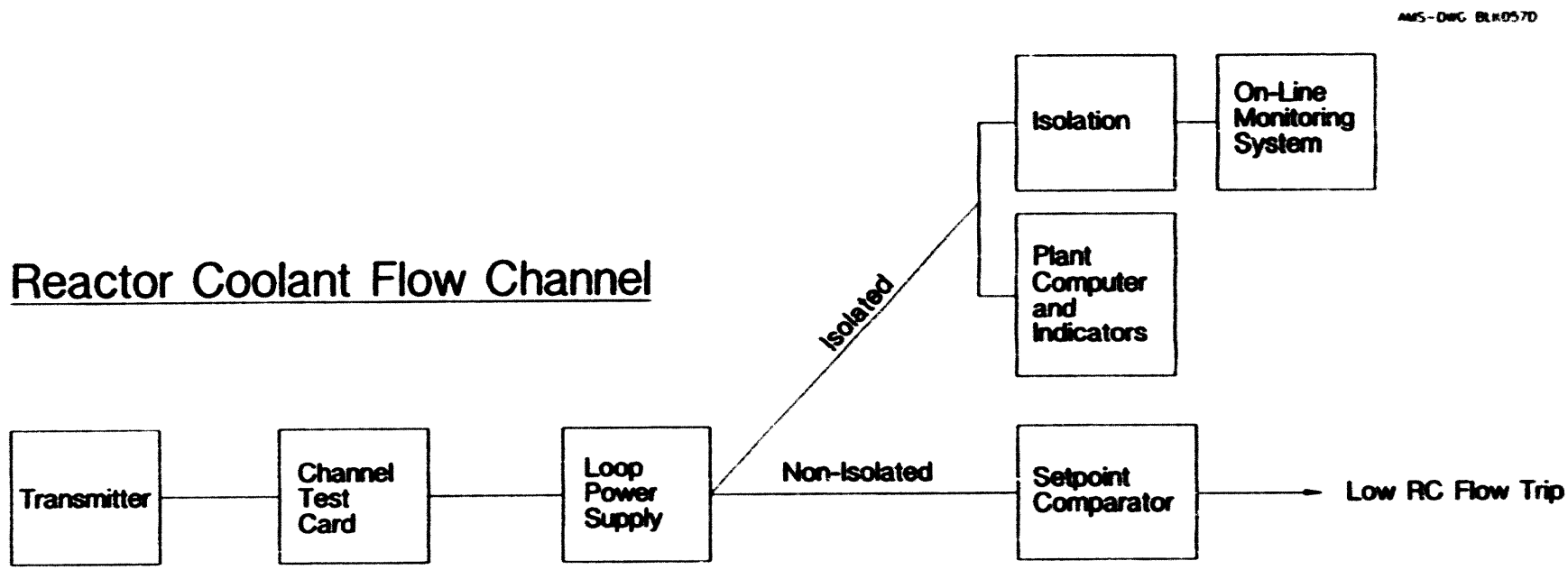


Figure 9. Placement of the On-Line Monitoring System in an Instrument Channel.

The main purpose of the in-plant validation effort is to determine if the on-line monitoring system is able to identify the faulty channels that are normally identified by regular surveillance tests and off-line calibrations. A fault could be due to an erratic behavior such as large spikes, noise, a sudden shift, or a calibration drift. An inherent problem (from a research point of view) with any in-plant validation of this type is that there are very few instrument channels in a nuclear power plant that show significant drift or degradation during a fuel cycle. More specifically, there are very few faults to be detected by the on-line monitoring system and used for the validation tests. Typically, of a hundred channels that are tested periodically in a nuclear power plant, less than ten are found to be out of tolerance or have any fault. As a matter of good practice, however, plant technicians often null any deviation observed during the surveillance and calibration tests even if the deviation is well within the acceptance band. This point is manifested in a comparison between the on-line monitoring results and the surveillance test records at McGuire (Figures 10 and 11). The data in Figures 10 and 11 show that the on-line monitoring system has been successful in revealing the channels that had drifted.

Comparisons of the types discussed above will be performed throughout the in-plant validation tests, especially with data from full channel calibrations performed during refueling outages to assess the feasibility of on-line drift monitoring as a substitute for some of the hands-on calibrations.

The next interesting point about the in-plant tests is related to the core exit thermocouples (CETs). These signals can be considered as redundant because they should be measuring the same temperature with the exception of any temperature streaming due to the water not being well mixed as it exits the core. We compared the thermocouples according to their locations above the core. Assuming that the water temperature around all thermocouples in each quadrant is the same, we obtained the results shown in Figure 12 for groups of thermocouples in each of the four quadrants.

The thermocouple monitoring tests included a period when the plant was shut down for a few weeks. During this shutdown period, the deviations of the outliers in each quadrant decreased to around zero indicating that the thermocouple errors are temperature dependent. This conclusion is consistent with temperature steaming effects and the common knowledge that faulty temperature sensors often show relatively small errors at low temperatures and larger errors at high temperatures. A plot of the deviations of four thermocouples as a function of temperature is shown in Figure 13. The group includes one good thermocouple (D07) and three bad thermocouples (J10, G12, and J02). Note that the deviation of the good thermocouple is independent of temperature, while that of the three bad thermocouples increase significantly as the temperature is increased.

The deviations of the McGuire hot leg RTDs are shown in Figure 14. These results represent the deviations of the individual RTDs from the average of all twelve hot leg RTDs; three in each of the plant's four loops. The same type of data is shown in Figure 15 for the four cold leg RTDs along with a plot of the temperature indication of the RTDs. No significant drift is apparent in the hot leg or cold leg RTD data during the monitoring period. The reason for the large spikes in the cold leg RTDs is not known. It appears that the spikes are not from the RTDs. They could be due to surveillance tests during which the RTDs were temporarily removed from service. Except for the spikes, the cold leg RTDs have normal behavior and agree well with each other to within 1°F. This compares with 4°F for the hot leg RTDs. The reason that the hot leg RTDs have larger deviations is probably due to the temperature stratification which is a more significant problem in the hot legs than the cold legs.

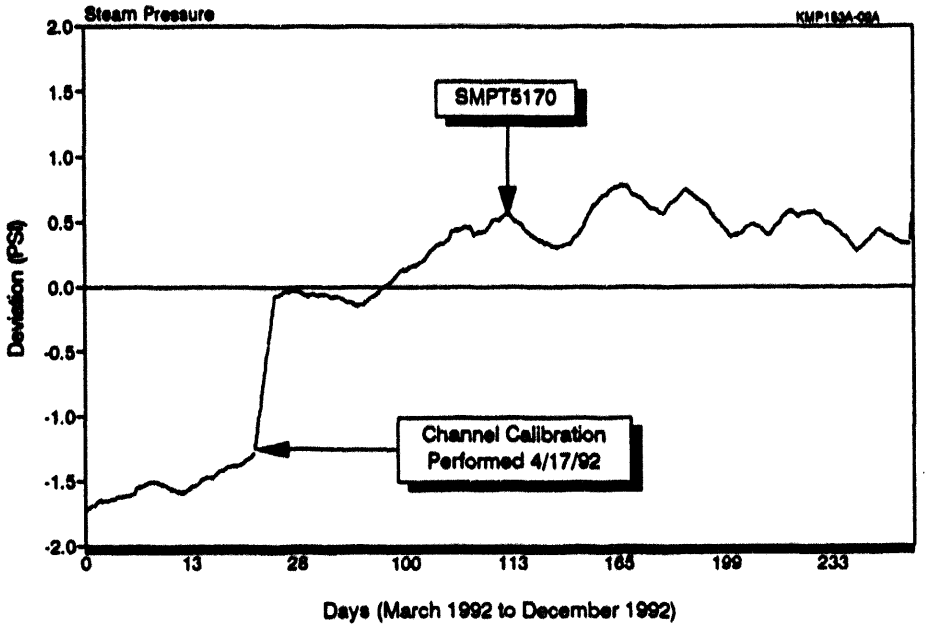


Figure 10. Detection of a Deviation in a Steam Pressure Signal that was Nulled During a Surveillance Test.

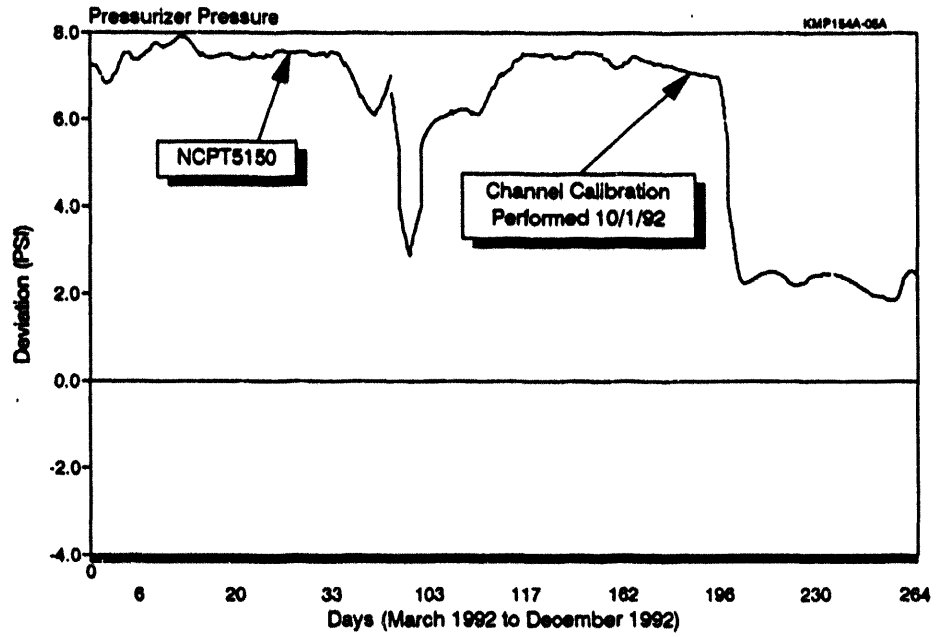


Figure 11. Detection of a Deviation in a Pressurizer Pressure Signal that was Nulled During a Surveillance Test.

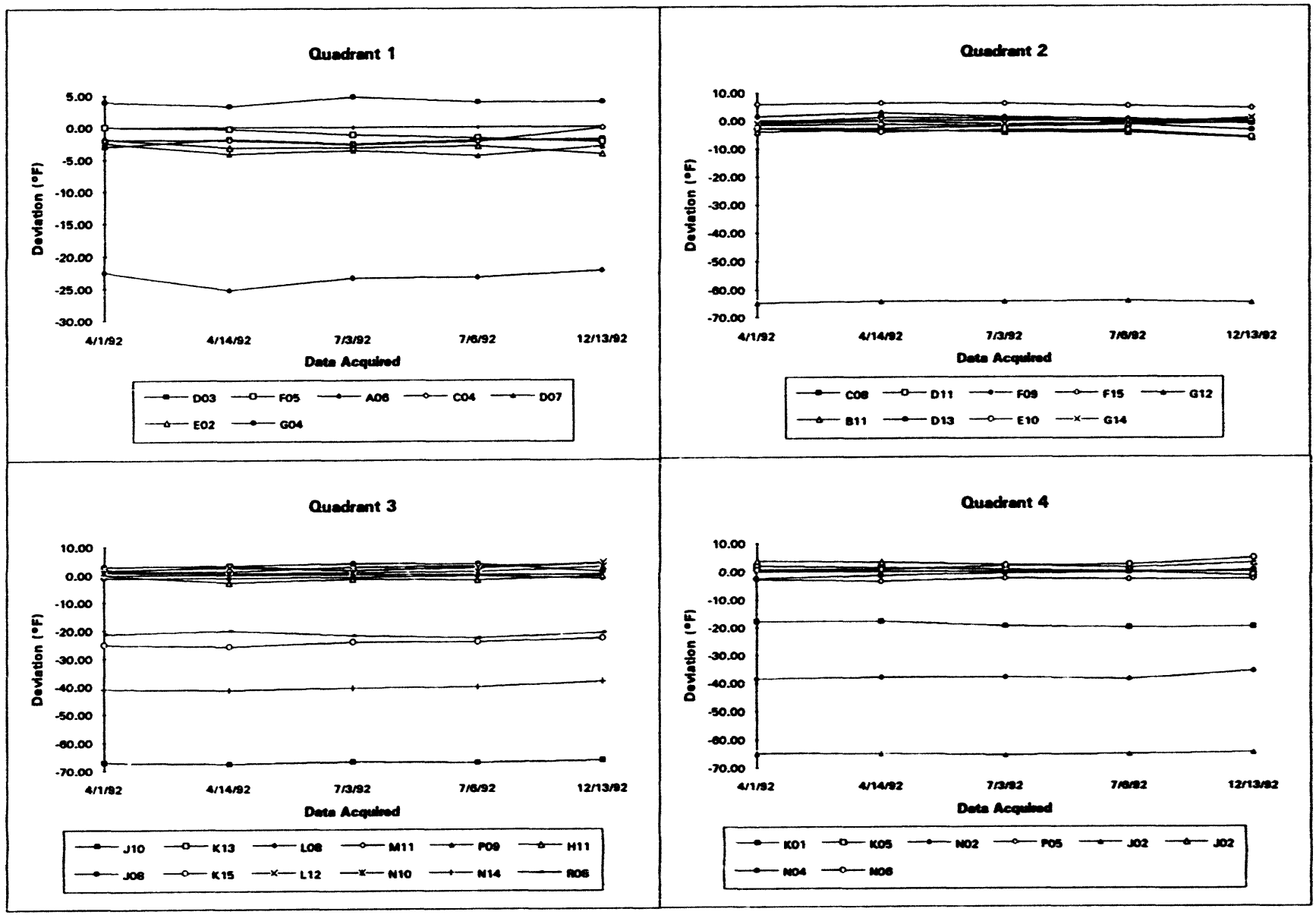


Figure 12. Cross Calibration Data Trending of Core Exit Thermocouples at Full Power.

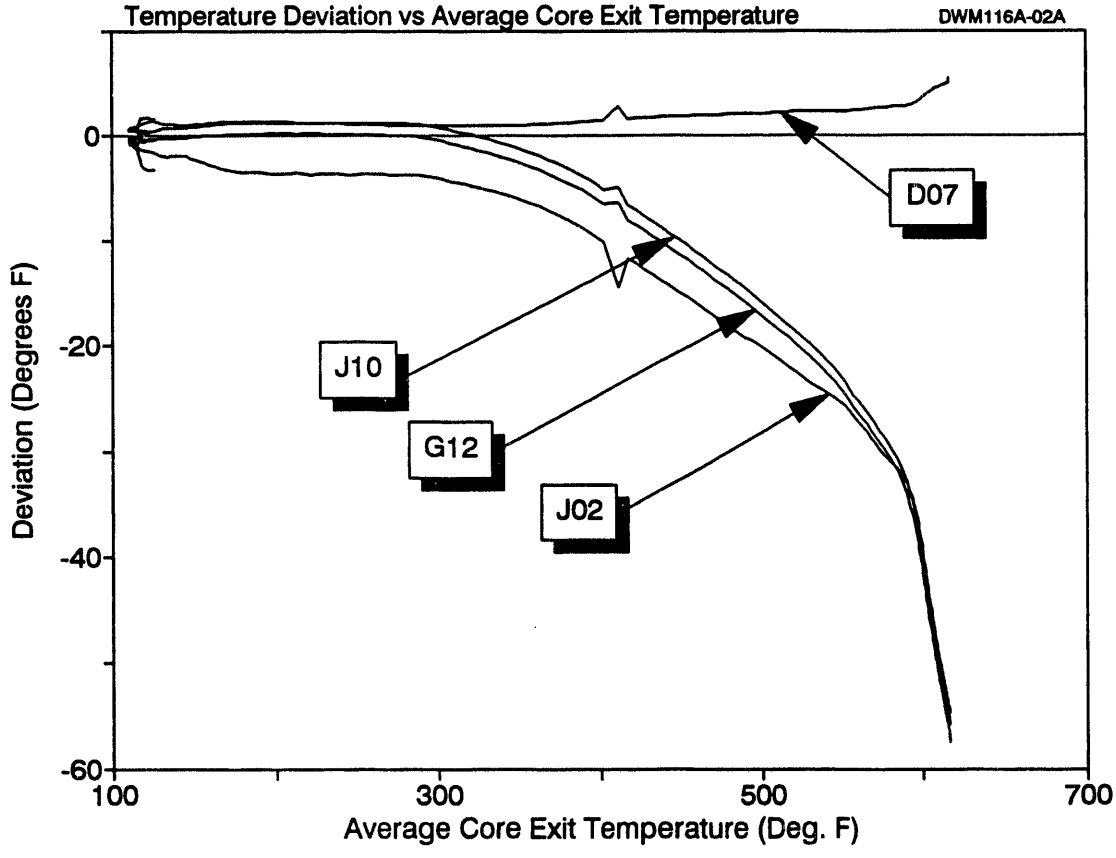


Figure 13. Deviation of Selected Thermocouples as a Function of Temperature.

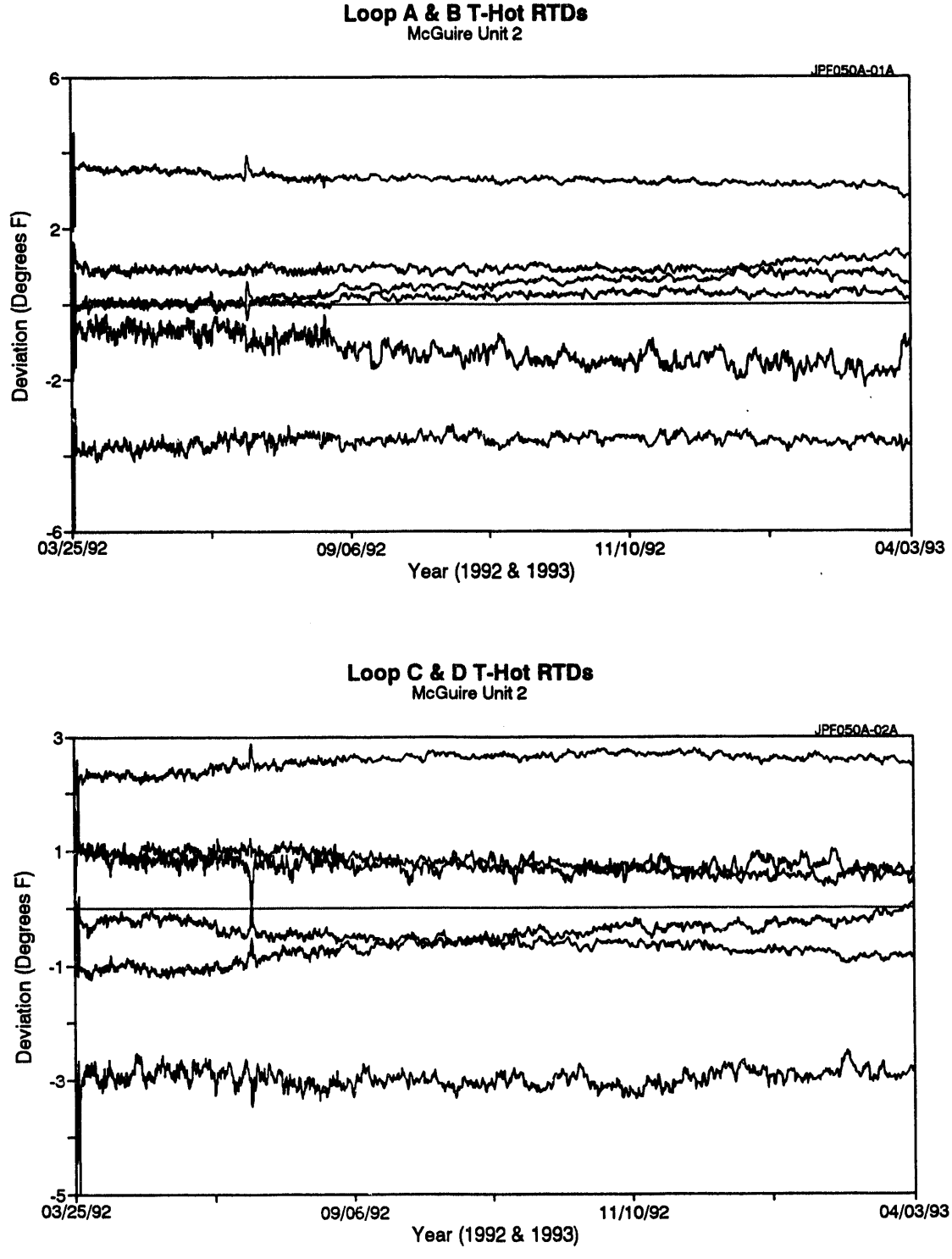
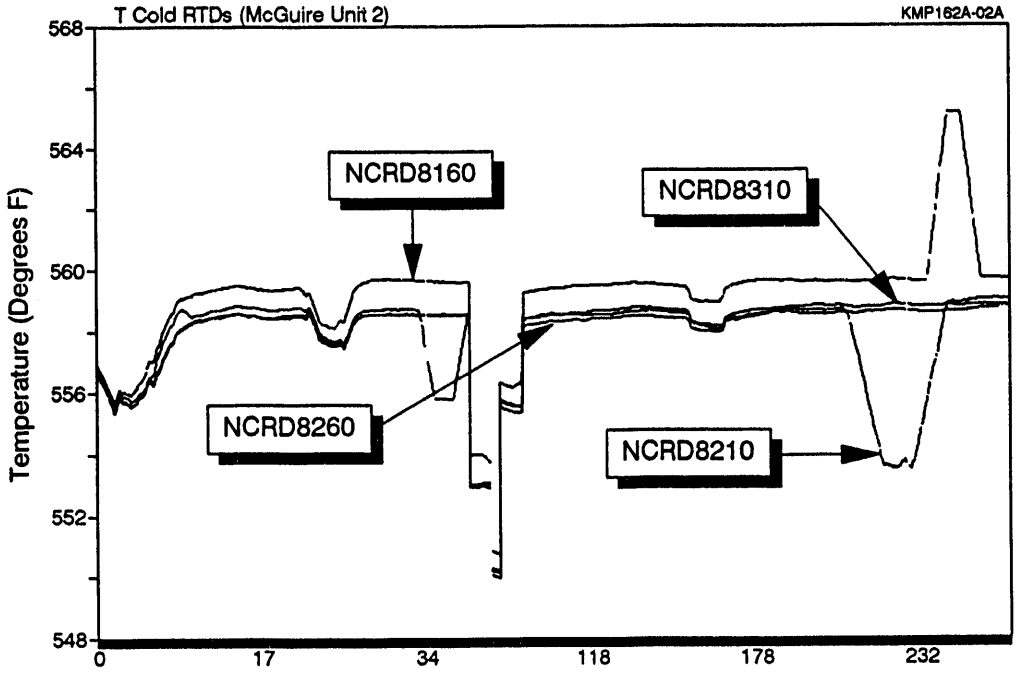


Figure 14. Hot Leg RTD Deviations in All Loops.



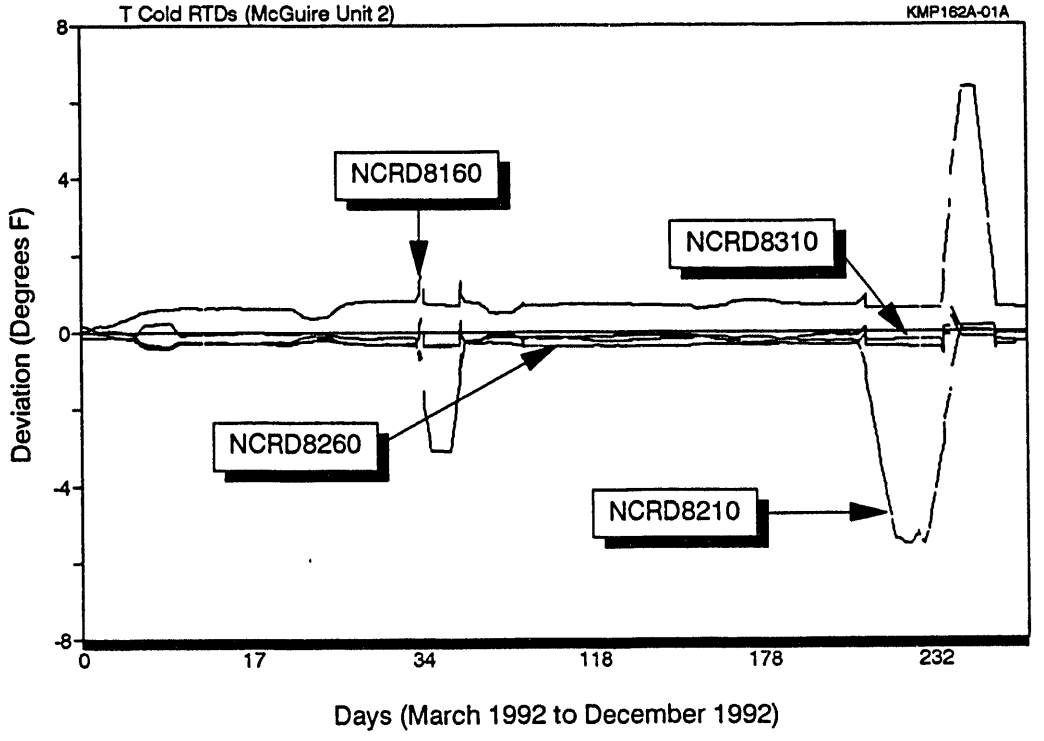


Figure 15. On-Line Monitoring Results for Cold Leg RTDs.

In addition to the use of drift and cross calibration analysis methods, empirical modeling techniques were used to model process conditions at the McGuire plant. In general, empirical modeling was performed using a fitting algorithm in which many data points were recorded from several independent process sensors and then analyzed to develop an equation describing the sensor output. These types of models are particularly effective in detecting common-cause or unidirectional drift within redundant signal groups. More specifically, if all the signals within a redundant group of sensors have experienced the same drift, modeling of the process condition provides the means to detect this error whereas other drift analysis or cross-checking methods may not. Several process conditions at McGuire have been modeled using the empirical techniques. Figures 16 and 17 illustrate the results of this modeling for reactor power and pressurizer level during a reactor power ascension transient. In each of these figures the model prediction and the actual measured values for the process conditions are shown. The empirical equations used to generate the model prediction are also given. As seen in these figures, there is close agreement between the model prediction and the actual measured values for these sensors.

5. CONCLUSION

A feasibility study was successfully completed on the validity of on-line monitoring techniques for remote testing of calibration of process instrumentation channels in nuclear power plants. This work involved research with temperature and pressure instrumentation in simulated reactor conditions in a laboratory, and in-plant validation work at the McGuire Nuclear Power Station, a four-loop PWR. Representative results of this work were summarized in this paper.

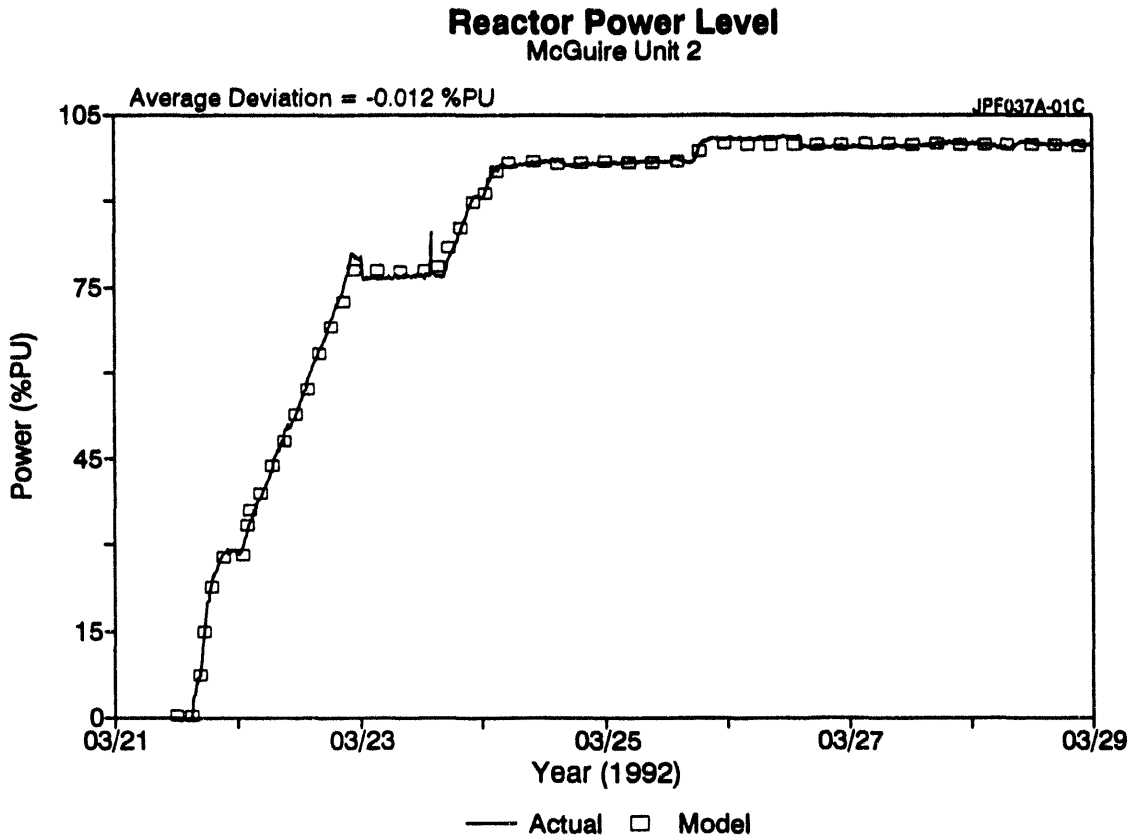
The effort described in this paper has successfully laid the foundation for an in-depth study that is underway to quantify the accuracy and reliability of the on-line monitoring techniques for instrument calibration reduction in nuclear power plants.

6. REFERENCES

1. C. H. MEIJER and J. P. PASQUENZA, On-Line Power Plant Signal Validation Technique Utilizing Parity-Space Representation and Analytical Redundancy, Electric Power Research Institute, EPRI NP-2110 Palo Alto, California, (1981).

2. H. M. HASHEMIAN, et al., Long Term Performance and Aging Characteristics of Nuclear Plant Pressure Transmitters, NRC Report Number NUREG/CR-5851, Nuclear Regulatory Commission, Washington, D.C. (1993).

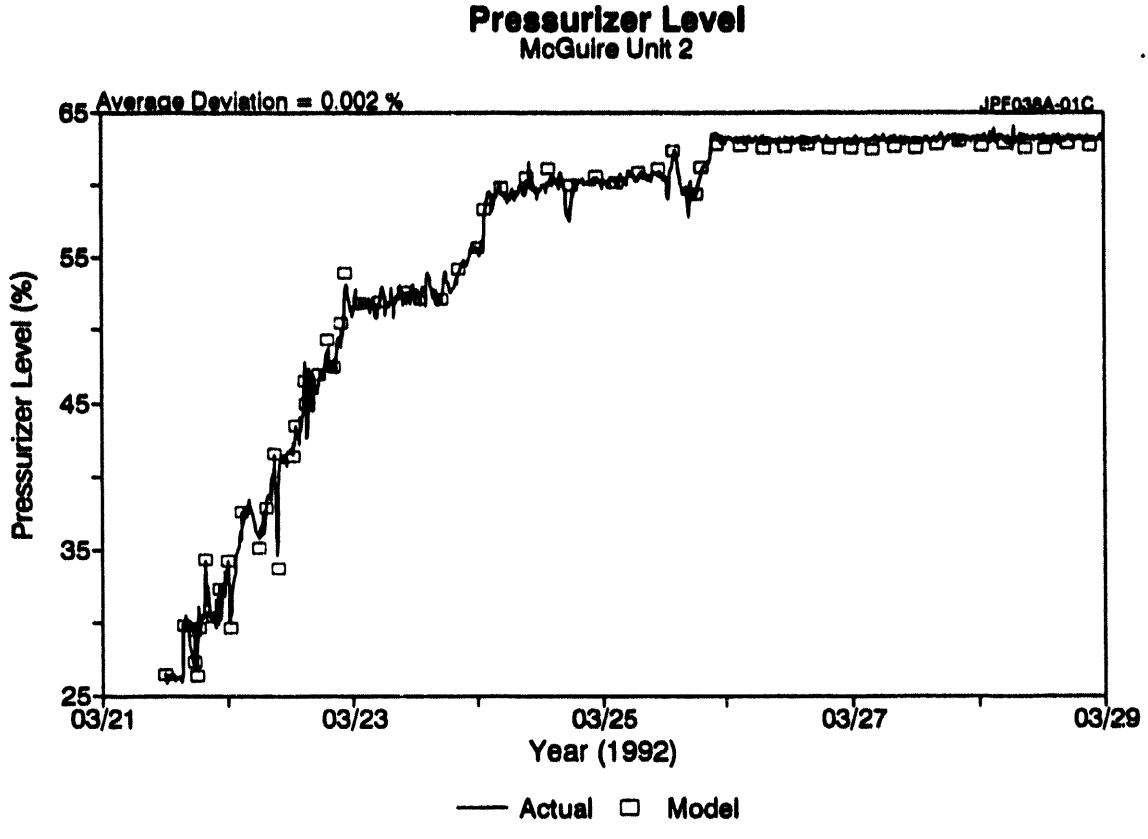
3. H. M. HASHEMIAN, et al., Validation of Smart Sensor Technologies for Instrument Calibration Reduction in Nuclear Power Plants, NRC Report Number NUREG/CR-5903, Nuclear Regulatory Commission, Washington, D.C. (1993).



$$RP = Ax_1^2 + Bx_1 + Cx_2 + D$$

RP	=	Reactor Power Level (N43 AVG)
x_1	=	Cold Leg Temperature (NCRD 5860)
x_2	=	Hot Leg Temperature (NCRD 5900)
A	=	0.00113412
B	=	0.27325183
C	=	-1.17652811
D	=	147.7985

Figure 16. Empirical Modeling Results for Reactor Power Level at McGuire During Power Ascension.



$$PL = Ax_4 + Bx_4 + Cx_2 + Dx_3 + E$$

PL	= Pressurizer Level (NCLT 5150)	A	= 0.12053496
x_1	= Pressurizer Pressure (NCPT 5160)	B	= 0.07323886
x_2	= Cold Leg Temperature (NCRD 5860)	C	= 0.94069032
x_3	= Hot Leg Temperature (NCRD 5900)	D	= 0.38394097
x_4	= Reactor Power Level (N43 AVG)	E	= -550.0212

Figure 17. Empirical Modeling Results for Pressurizer Level at McGuire.

FIGURES

Figure 1. Results of Search of the LER Database (the LER Numbers are in this Diagram are Rounded to Simplify the Presentation).

Figure 2. Illustration of Principle of Like Signal Comparison Technique.

Figure 3. Principle of Analytical Redundancy.

Figure 4. Temperature, Pressure, and Flow Sensors Installed in the Laboratory Test Loop.

Figure 5. Agreement Between Results of Empirical Model and Actual Temperature Data.

Figure 6. Agreement Between Results of Physical Model and Actual Temperature Data.

Figure 7. Agreement Between Five Temperature Sensors Monitoring the Loop Temperature from Start Up to Steady-State.

Figure 8. Bias and Drift in Transmitter Signals.

Figure 9. Placement of the On-Line Monitoring System in an Instrument Channel.

Figure 10. Detection of a Deviation in a Steam Pressure Signal that was Nulled During a Surveillance Test.

Figure 11. Detection of a Deviation in a Pressurizer Pressure Signal that was Nulled During a Surveillance Test.

Figure 12. Cross Calibration Data Trending of Core Exit Thermocouples at Full Power.

Figure 13. Deviation of Selected Thermocouples as a Function of Temperature.

Figure 14. Hot Leg RTD Deviations in All Loops.

Figure 15. On-Line Monitoring Results for Cold Leg RTDs.

Figure 16. Empirical Modeling Results for Reactor Power Level at McGuire During Power Ascension.

Figure 17. Empirical Modeling Results for Pressurizer Level at McGuire.

ANALYSIS AND
MEASUREMENT SERVICES
CORPORATION

AMS 9111 CROSS PARK DRIVE / KNOXVILLE, TN 37923 USA (615) 691-1756

IAEA1-1

VALIDATION OF ON-LINE MONITORING TECHNIQUES FOR IN-SITU TESTING OF CALIBRATION DRIFT OF PROCESS INSTRUMENTATION CHANNELS IN NUCLEAR POWER PLANTS

Presented At

IAEA Specialists Meeting
Ramada Inn at Congressional Park
Rockville, Maryland
May 5-7, 1993

VALIDATION OF ON-LINE MONITORING TECHNIQUES FOR IN-SITU TESTING OF CALIBRATION DRIFT OF PROCESS INSTRUMENTATION CHANNELS IN NUCLEAR POWER PLANTS

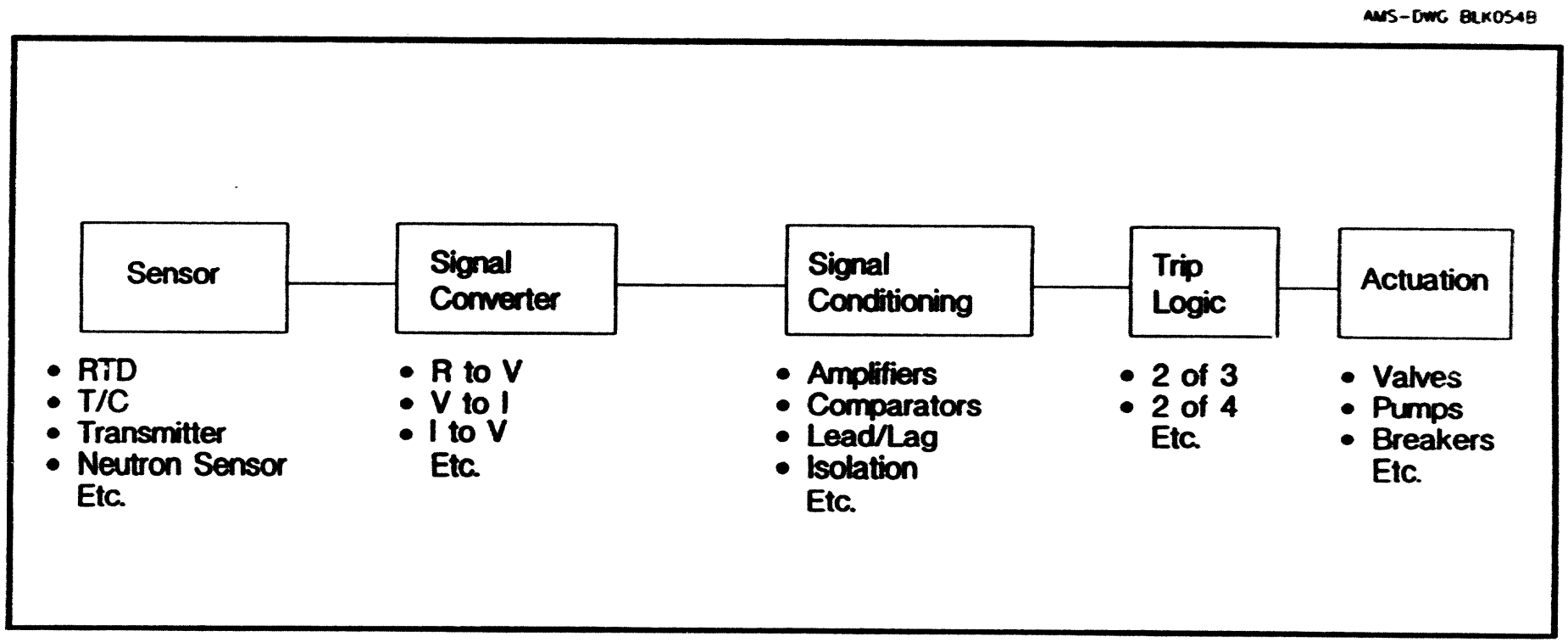
Jerry Mauck
NRC, NRR

Presented At

IAEA Specialists Meeting
Ramada Inn at Congressional Park
Rockville, Maryland
May 5-7, 1993

CURRENT PRACTICE

- Daily Channel Checks
- Monthly or Quarterly Surveillance Tests
- Full-Channel Calibration Performed Every Fuel Cycle

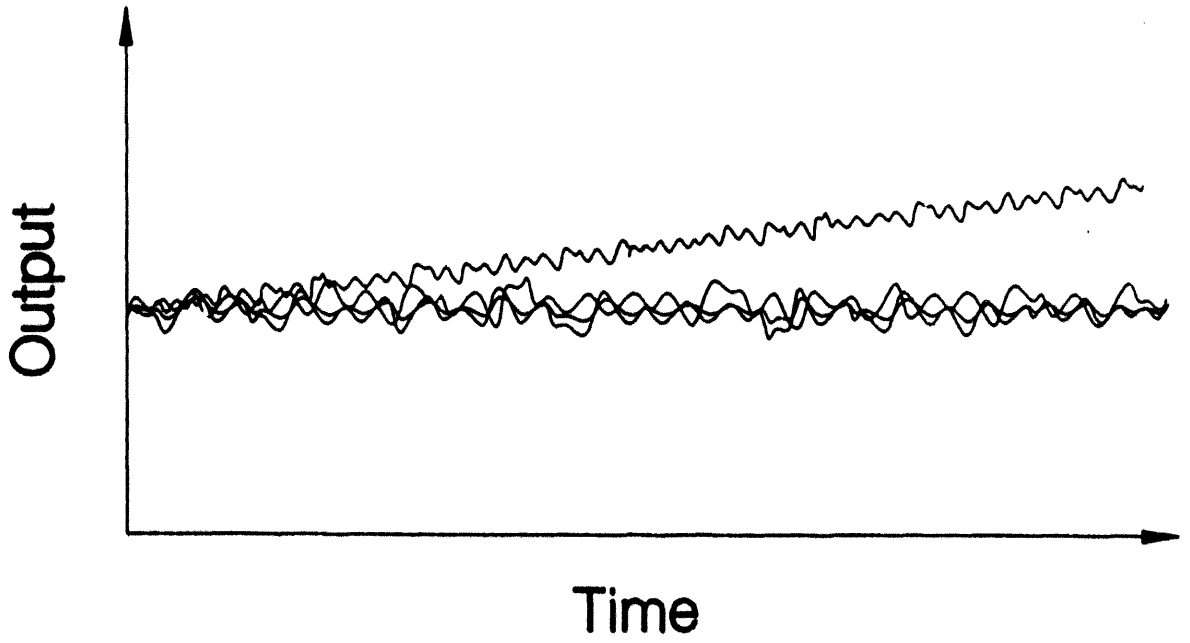


Typical Components of an Instrument Channel

PRINCIPLE OF ON-LINE MONITORING

- Sample DC Output of Redundant and Non-Redundant Instrument Channels During Plant Operation
- Identify the Channels that are Drifting or have Abnormal Behavior

AMS-DWG NO1010A



QUESTIONS

1. Does method have adequate resolution to replace conventional calibrations ?

2. What are its uncertainties ?

3. Will common mode problems be effectively detected ?

4. If not able to replace hands-on calibrations, can it be used to extend calibration intervals or as a substitute for surveillance tests ?

ADVANTAGES OF ON-LINE MONITORING TECHNIQUES

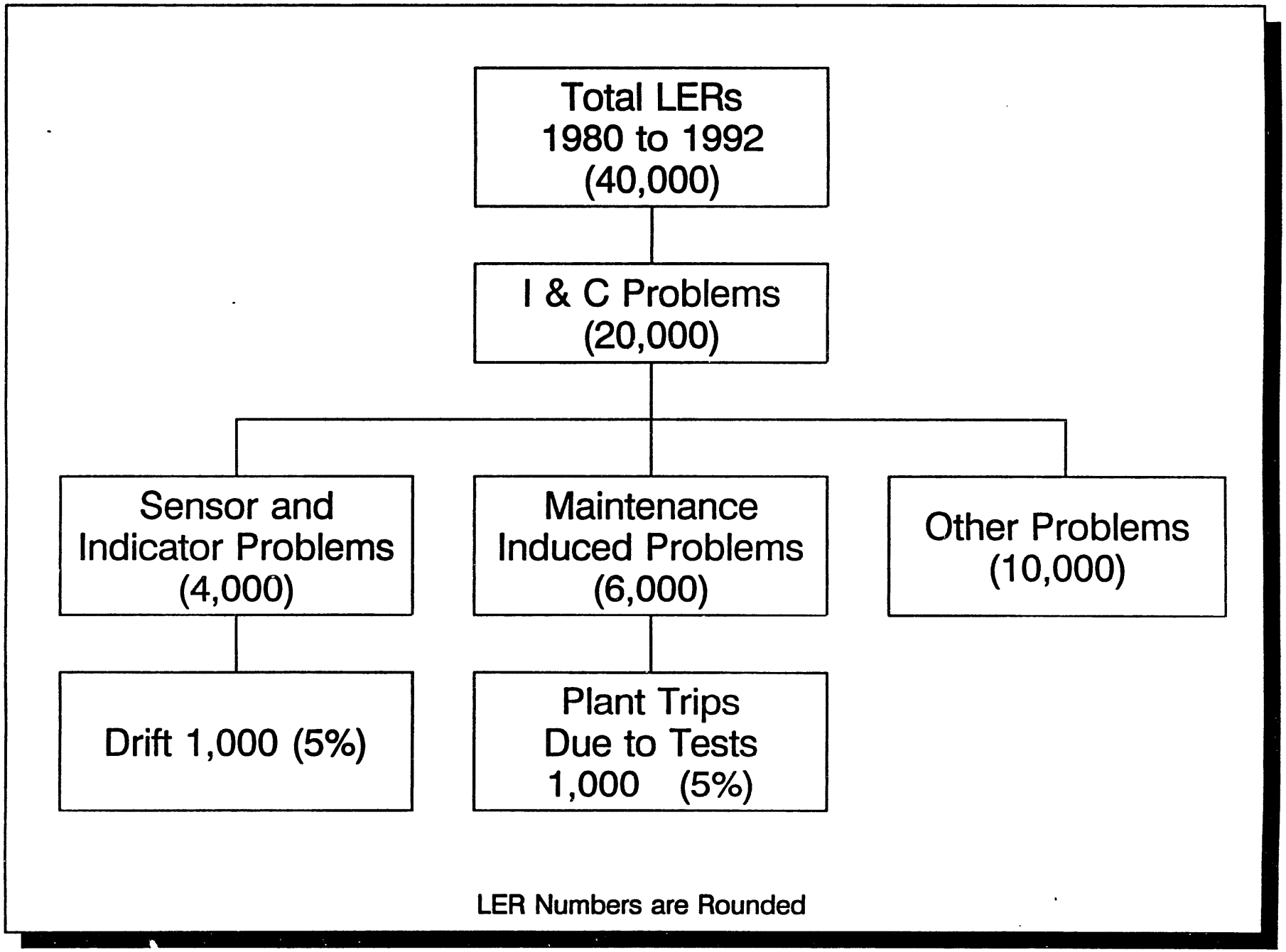
- Provides Early Warning of Drift and Incipient Failures
- Provides the In-Service Performance of Instruments
- Provides a Means to Include the Sensors in the Surveillance Tests
- Provides Diagnostic Capabilities Beyond that of Conventional Calibrations

VALIDATION OF ON-LINE MONITORING TECHNIQUES

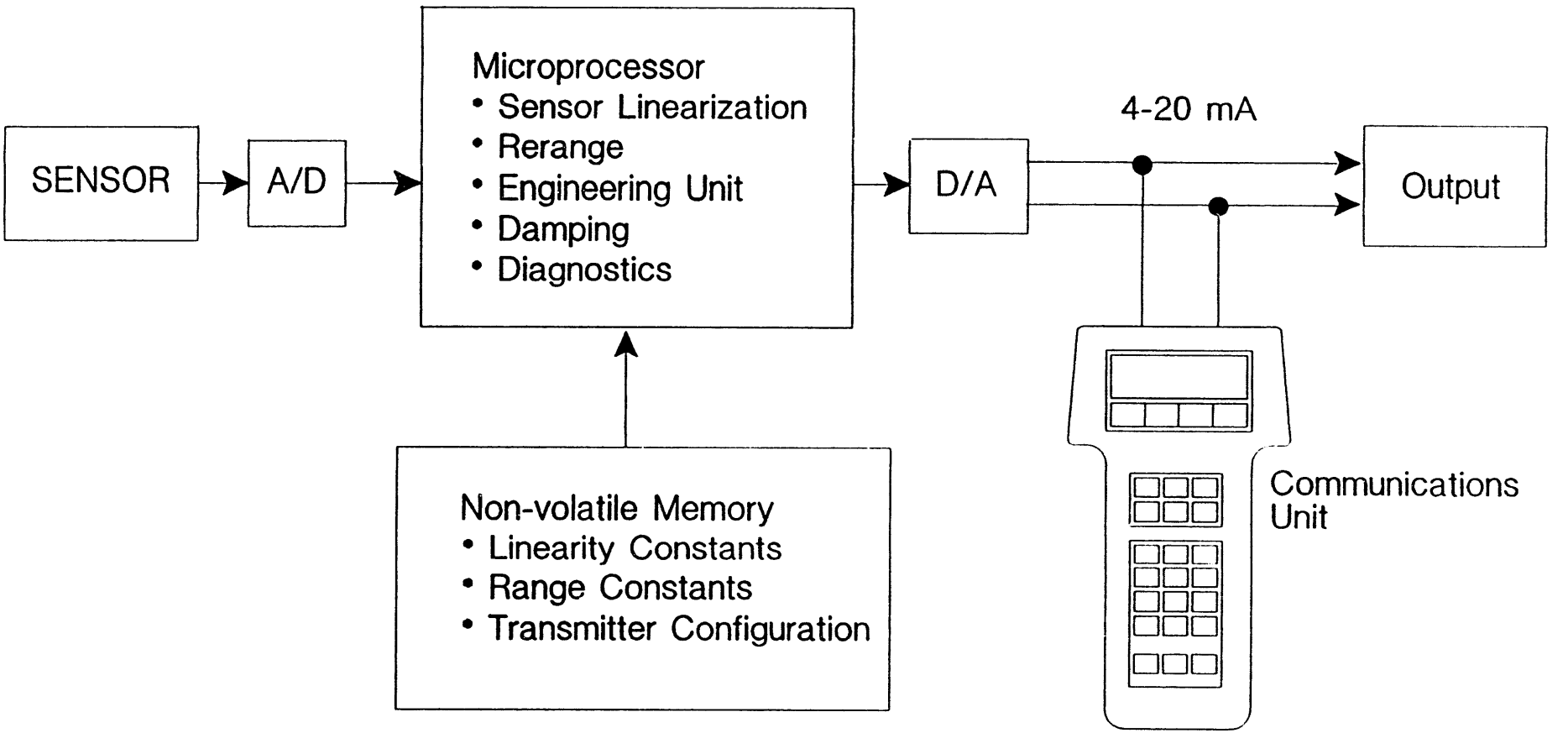
Joint Project Involving AMS, NRC, and Duke Power Company

- Laboratory Validation
- In-Plant Validation

Results are published in NUREG/CR-5903 entitled, "Validation of Smart Sensor Technologies for Instrument Calibration Reduction in Nuclear Power Plants," published January 1993.


Total LERs
1980 to 1992
(40,000)
I & C Problems
(20,000)
Sensor and
Indicator Problems
(4,000)
Maintenance
Induced Problems
(6,000)
Other Problems
(10,000)
Drift 1,000 (5%)
Plant Trips
Due to Tests
1,000 (5%)
LER Numbers are Rounded

AMS-DWG PXT124B



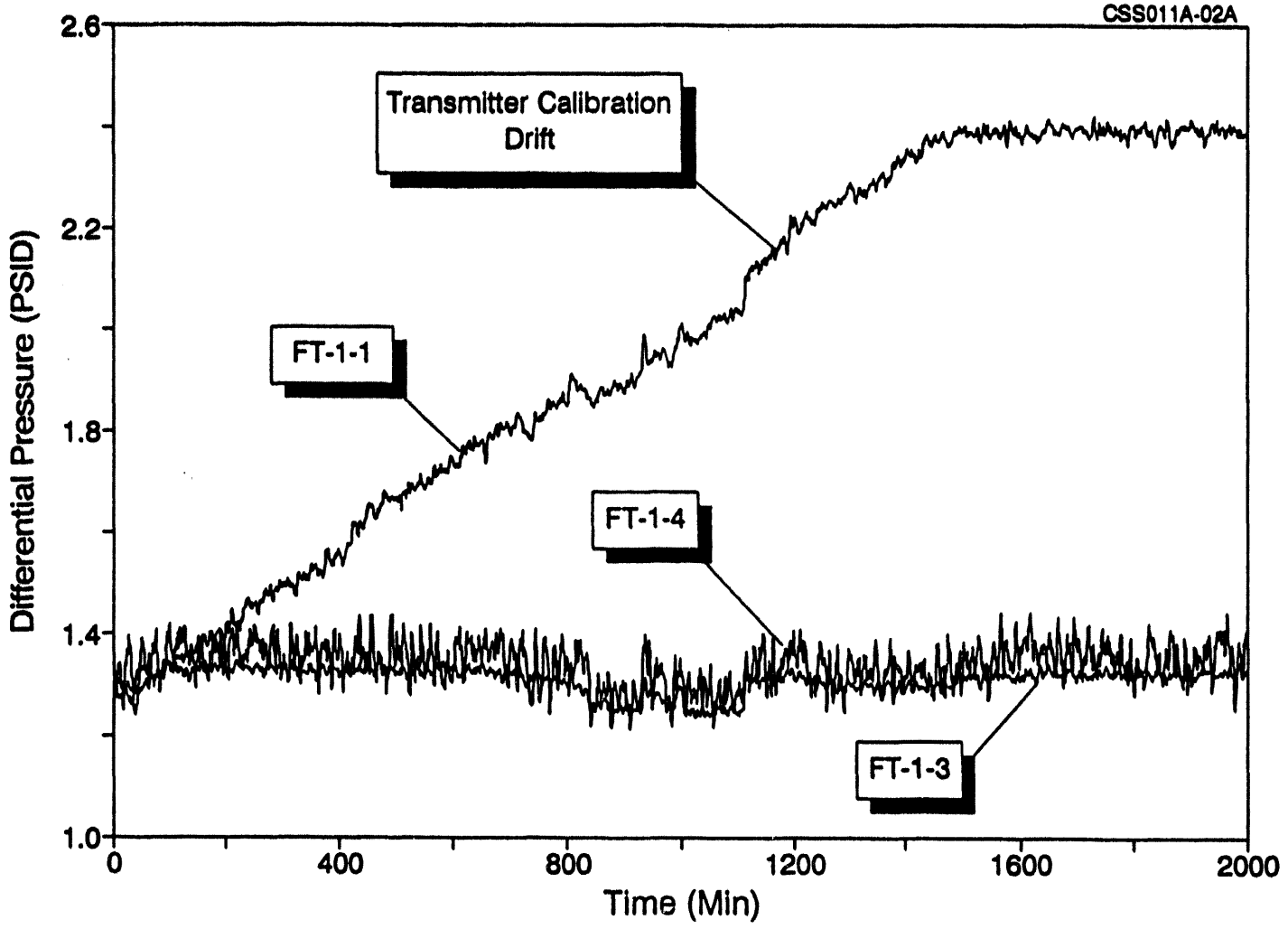
Block Diagram of a Smart Sensor

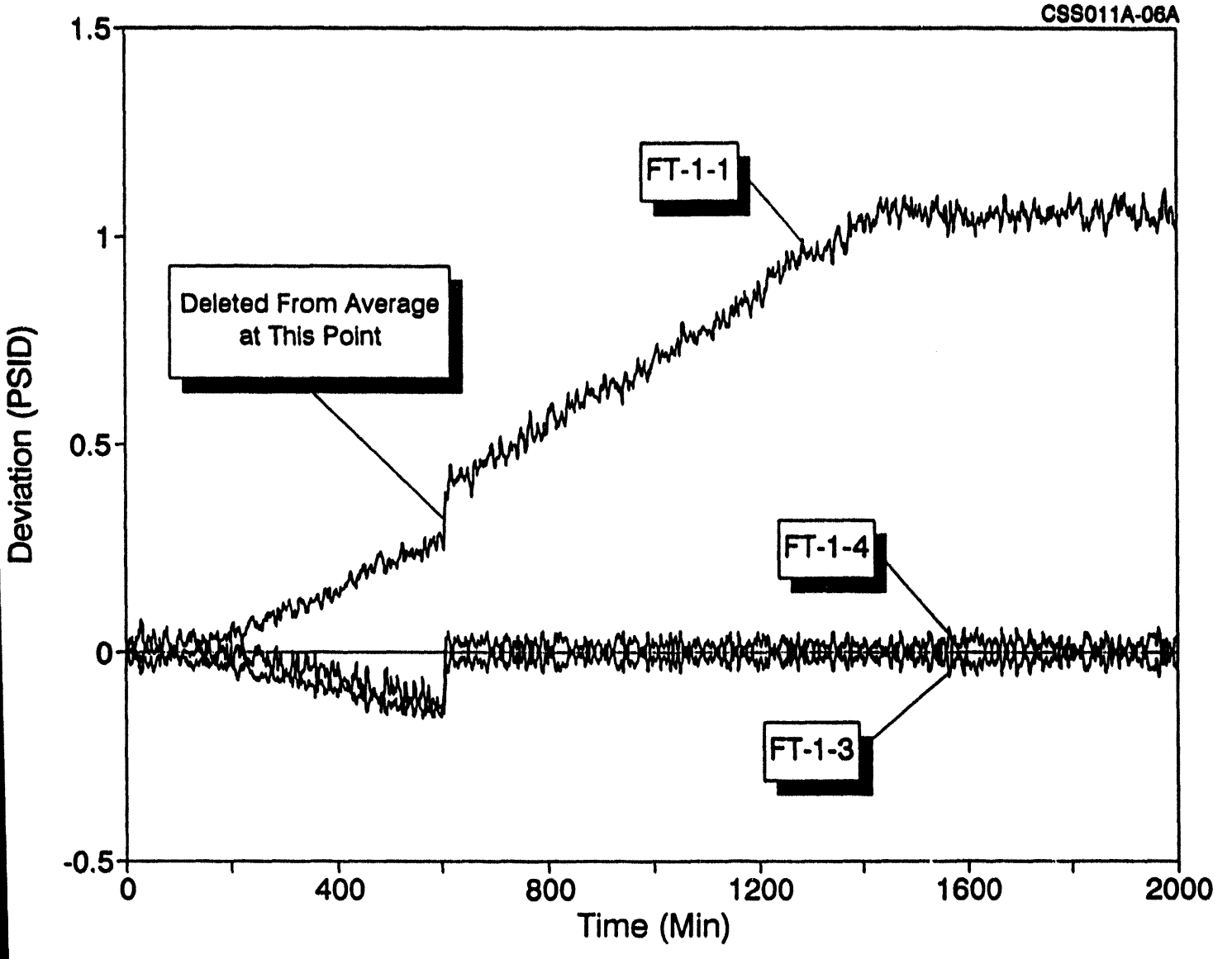
DESIRED DIAGNOSTIC CAPABILITIES

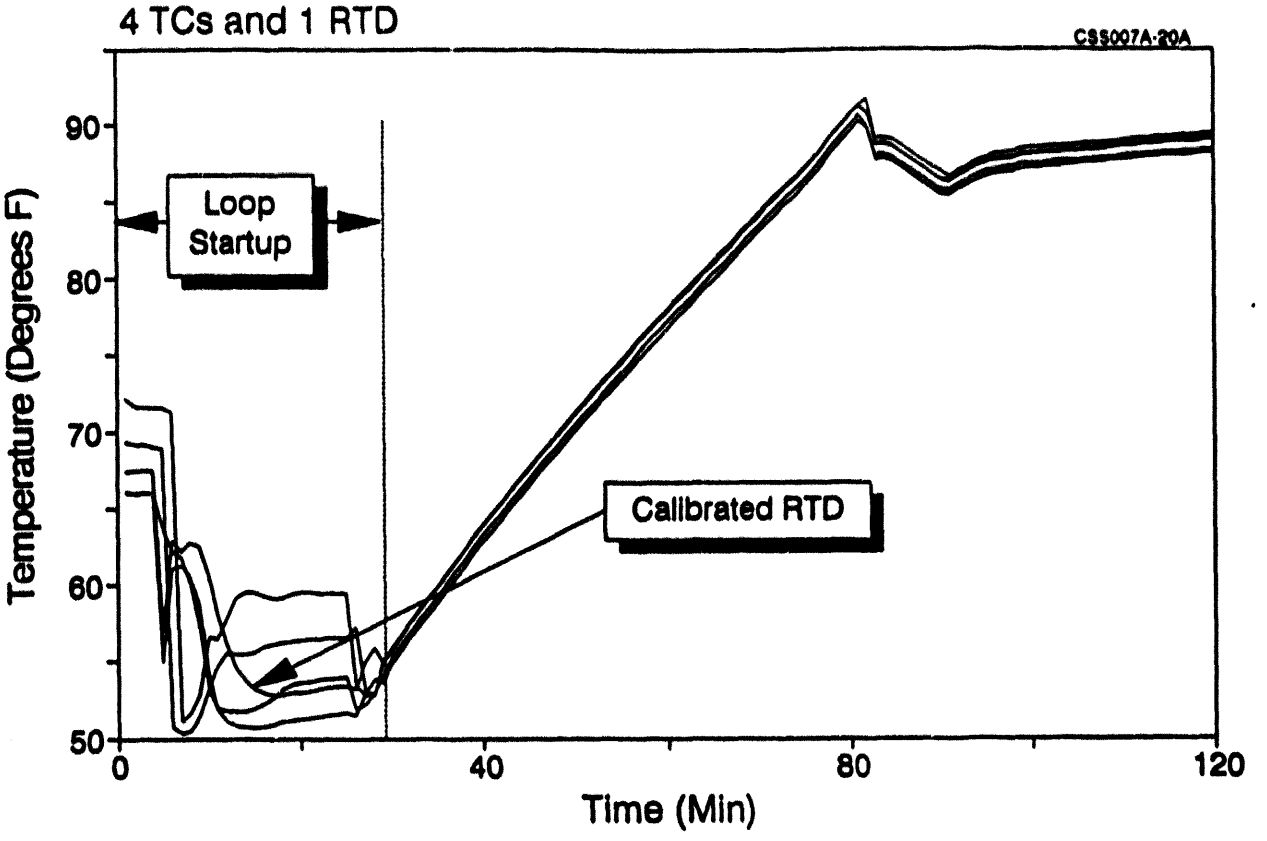
Diagnostics Measurement	Application
Loop Resistance	Circuit continuity test
Insulation Resistance Capacitance to Ground	Test of insulation breakdown and moisture ingress
TDR	Test of cables and connectors
Limit Checking and Auctioneering	Screening test of DC signals
Mean, Variance, Skewness, and Flatness	Qualify AC and DC signals
Like Signal Comparison	Drift Monitoring
Analytical Redundancy (Empirical and Physical Modeling)	Drift Monitoring for Non-Redundant Signals

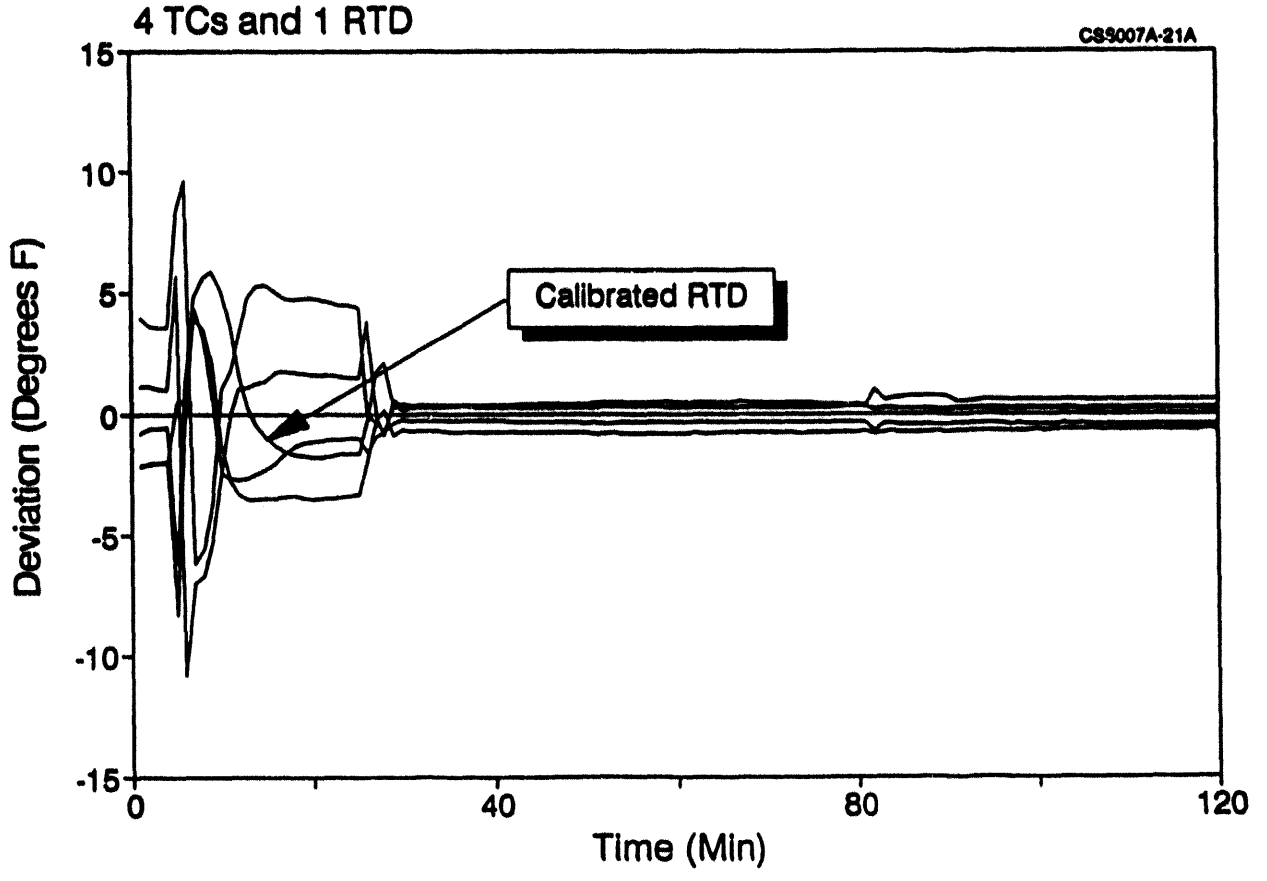
Survey Results (NUREG/CR-5851)

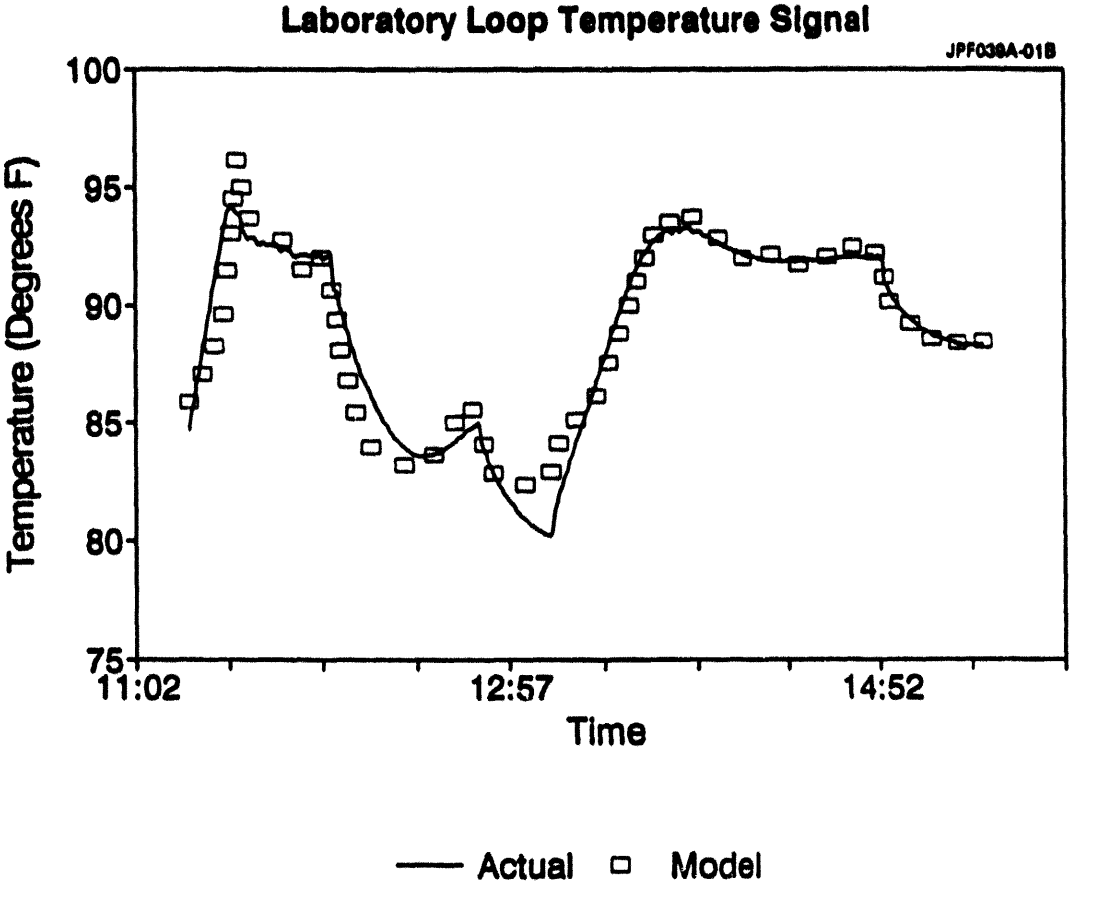
Question	Remarks
1. Should calibration intervals be extended?	50 % Yes 50 % No
2. During transmitter calibrations:	
a) % found out of tolerance ?	1 to 5%
b) % found to have drifted but are still in tolerance ?	10 to 20%
3. What are the most typical problems ?	Electronics Drift (~70%) Mechanical System Malfunctions (30%)
4. What is the most desirable improvement in transmitters?	Easier to calibrate, use smart or digital transmitters.


CSS011A-02A
Transmitter Calibration Drift
FT-1-1
FT-1-4
FT-1-3
Differential Pressure (PSID)
2.6
2.2
1.8
1.4
1.0
0
400
800
1200
1600
2000
Time (Min)


CSS011A-06A
1.5
1
0.5
0
-0.5
Deviation (PSID)
FT-1-1
Deleted From Average
at This Point
FT-1-4
FT-1-3
0
400
800
1200
1600
2000
Time (Min)

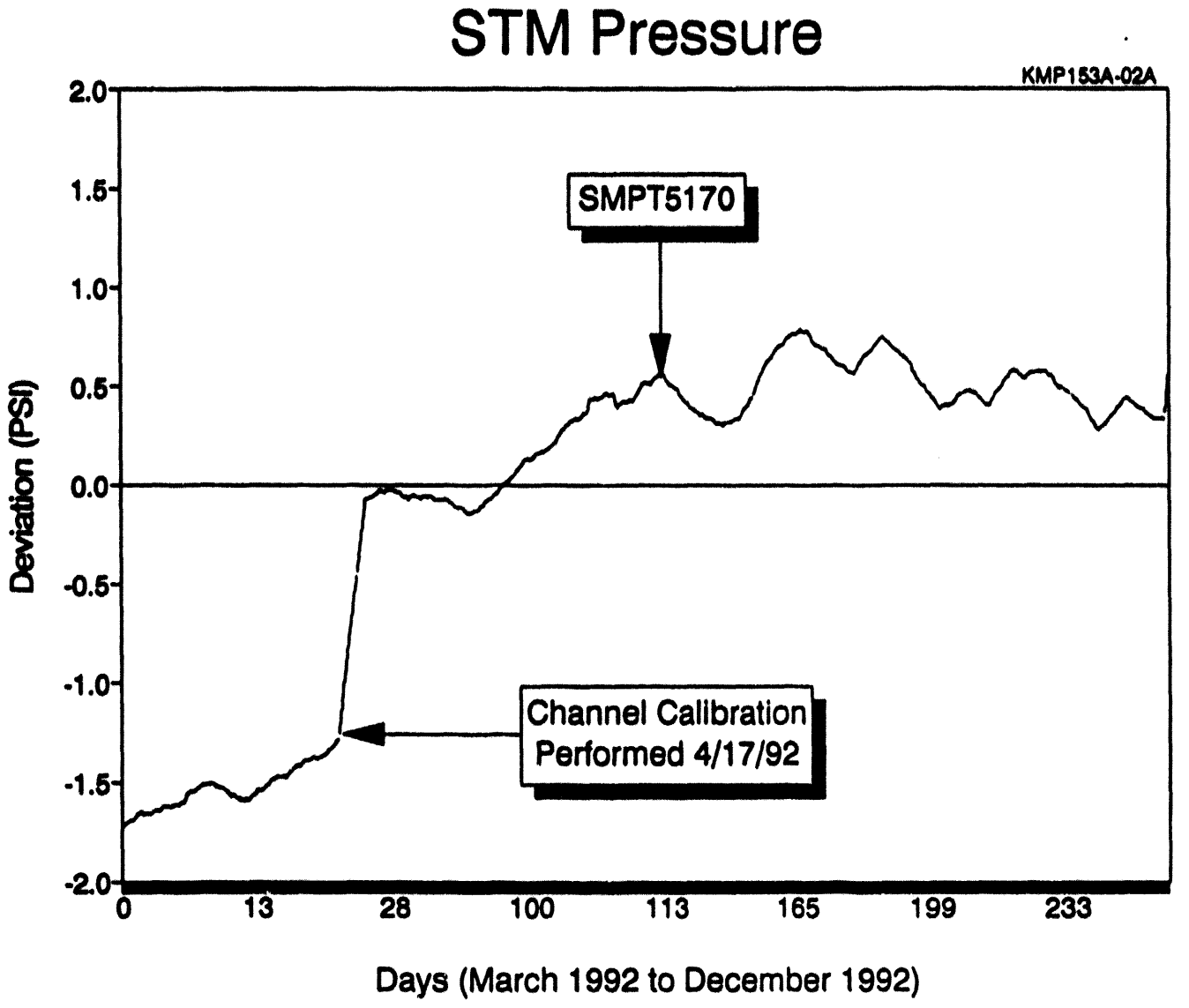

4 TCs and 1 RTD
CS9007A-20A
Loop Startup
Calibrated RTD
Temperature (Degrees F)
90
80
70
60
50
0
40
80
120
Time (Min)

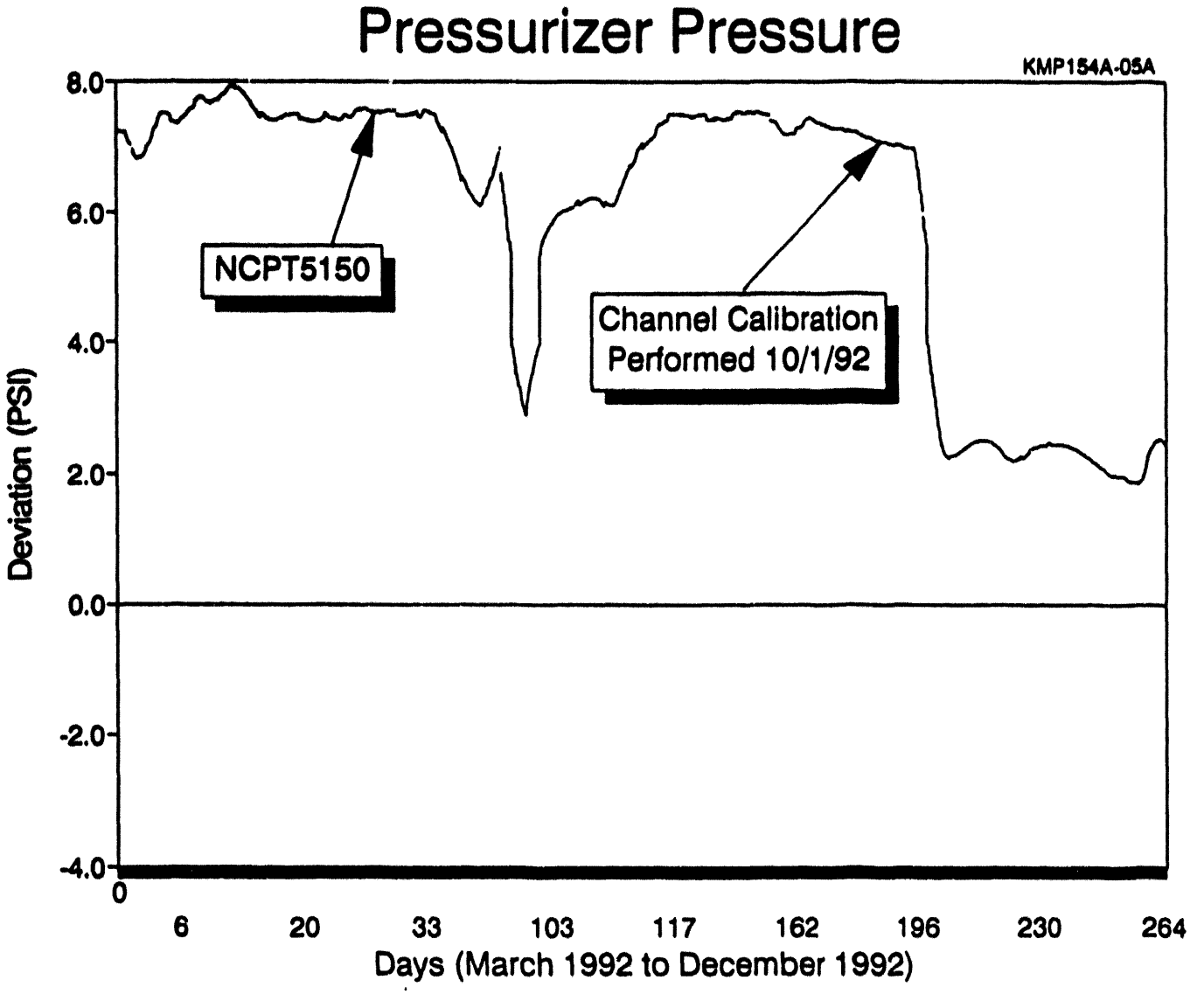

4 TCs and 1 RTD
CS9007A-21A
Calibrated RTD
Deviation (Degrees F)
15
10
5
0
-5
-10
-15
0
40
80
120
Time (Min)

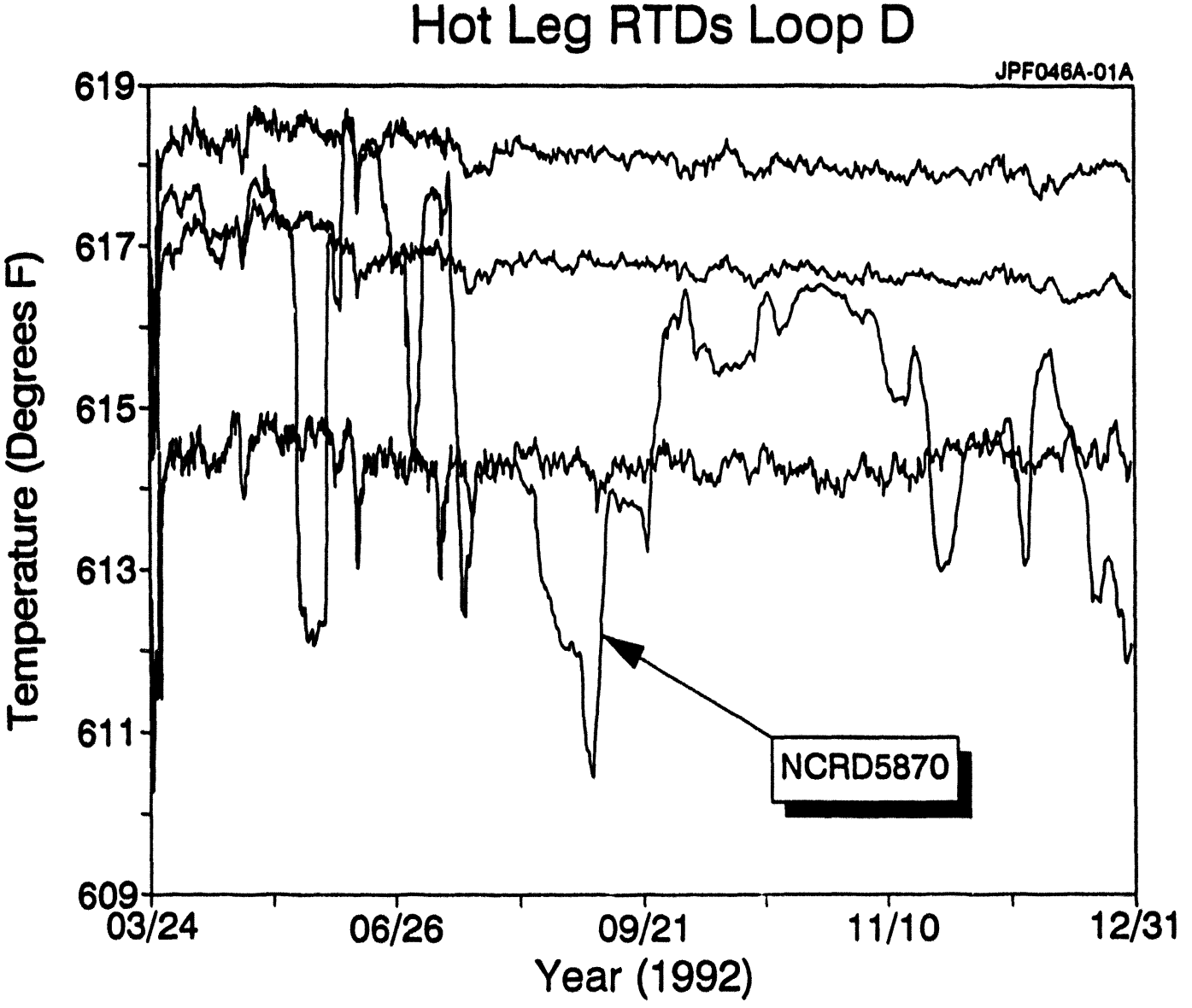


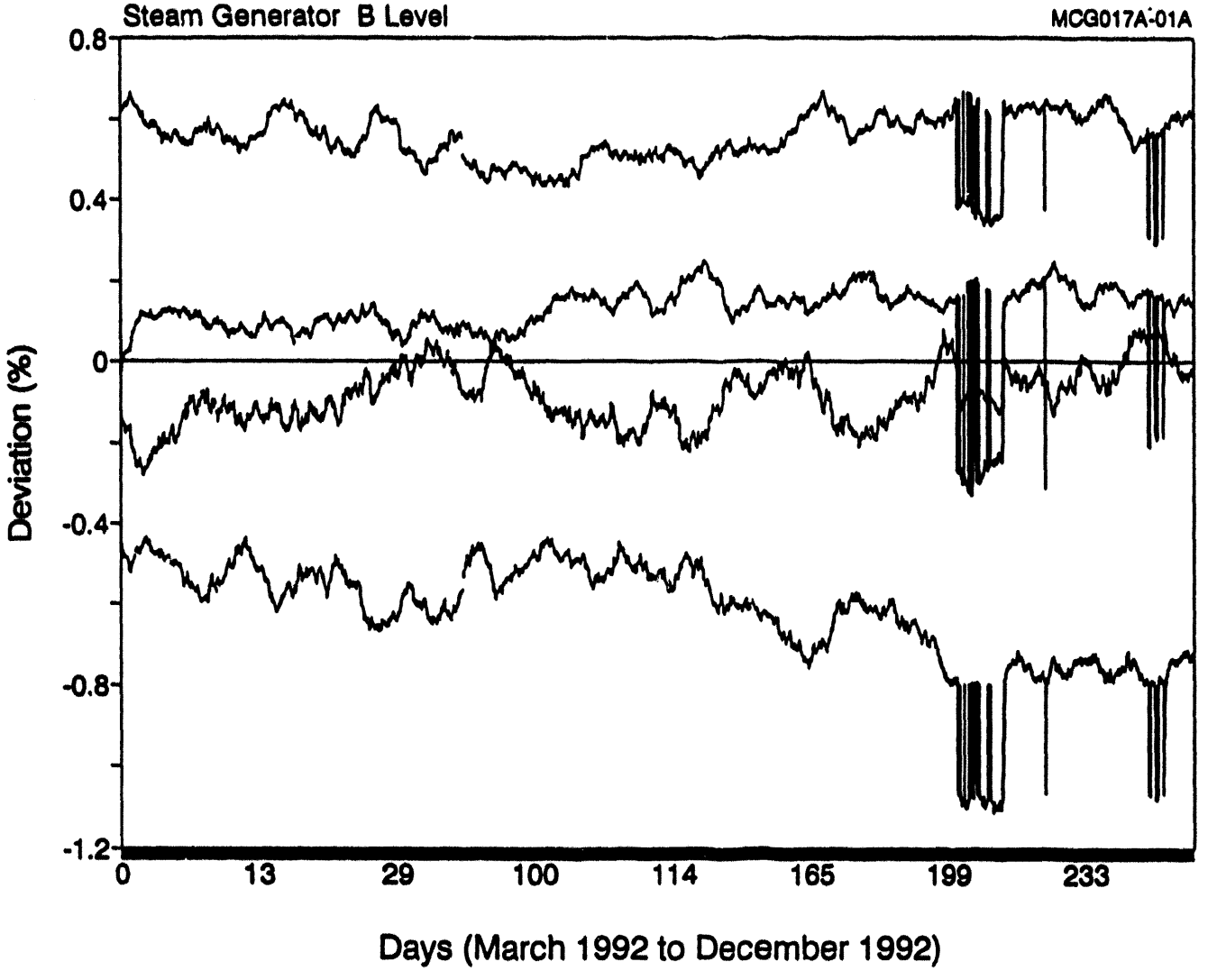
$$T = Ax_2 + Bx_2x_4 + Cx_1^2 + Dx_1 + Ex_2^2 + Fx_1x_3 + G$$

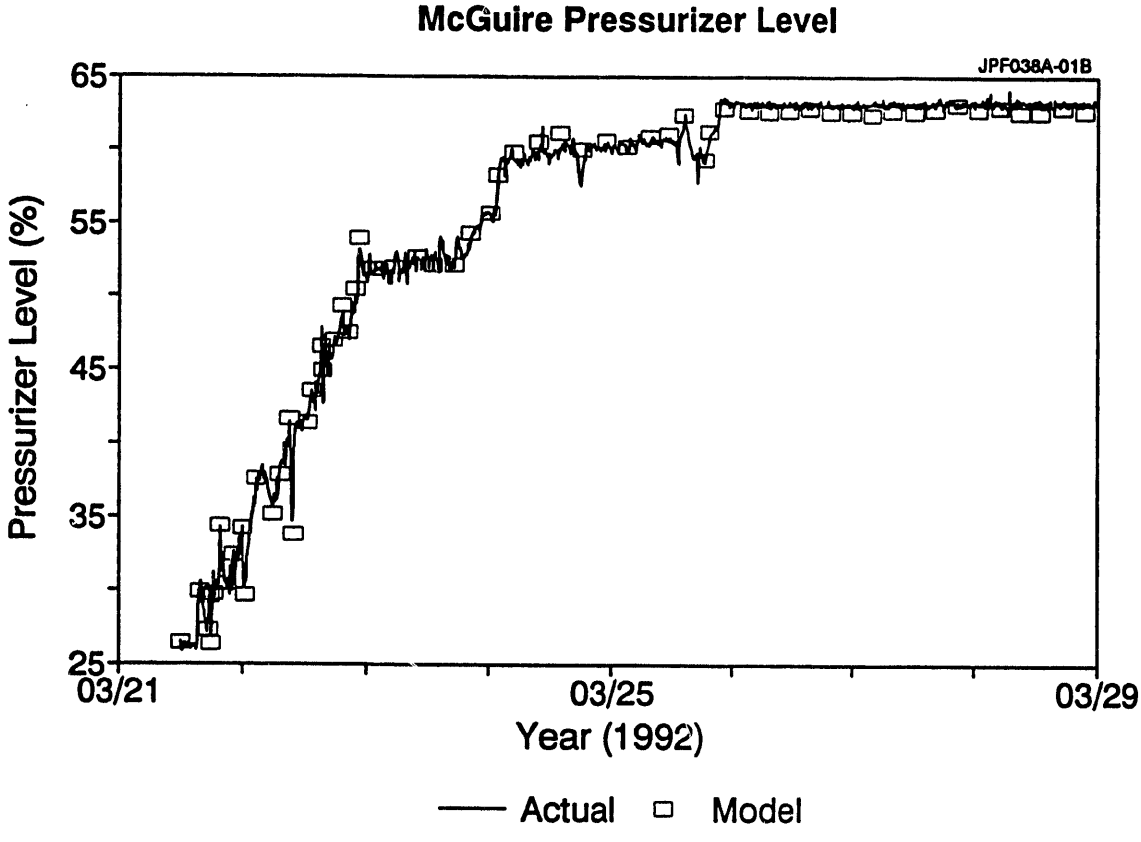
T	=	Low Velocity Leg Temperature	A	=	-9.53777622
x_1	=	Heat Exchanger Air Temperature	B	=	0.07970169
x_2	=	Heat Exchanger Inlet Temperature	C	=	0.03950938
x_3	=	Heat Exchanger Outlet Temperature	D	=	-5.41944437
x_4	=	Elbow #1 D/P	E	=	0.05727450
			F	=	-0.00188462
			G	=	667.1906


STM Pressure
KMP153A-02A
SMPT5170
Channel Calibration
Performed 4/17/92
Deviation (PSI)
2.0
1.5
1.0
0.5
0.0
-0.5
-1.0
-1.5
-2.0
0
13
28
100
113
165
199
233
Days (March 1992 to December 1992)


Pressurizer Pressure
KMP154A-05A
8.0
6.0
4.0
2.0
0.0
-2.0
-4.0
Deviation (PSI)
NCPT5150
Channel Calibration
Performed 10/1/92
0
6
20
33
103
117
162
196
230
264
Days (March 1992 to December 1992)


Hot Leg RTDs Loop D
JPF046A-01A
619
617
615
613
611
609
Temperature (Degrees F)
03/24
06/26
09/21
11/10
12/31
Year (1992)
NCRD5870

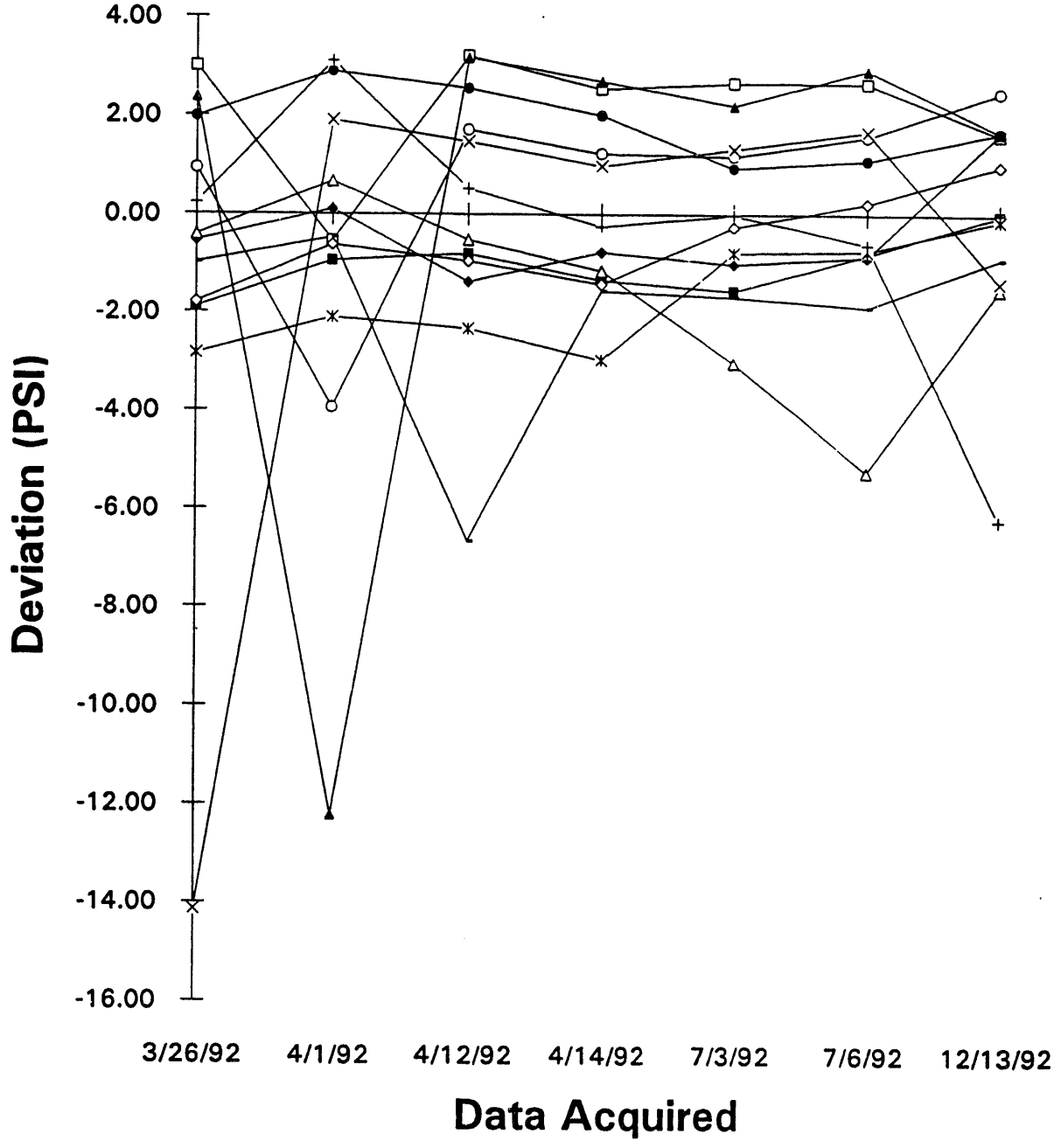

Steam Generator B Level
MCG017A-01A
0.8
0.4
0
-0.4
-0.8
-1.2
Deviation (%)
0
13
29
100
114
165
199
233
Days (March 1992 to December 1992)



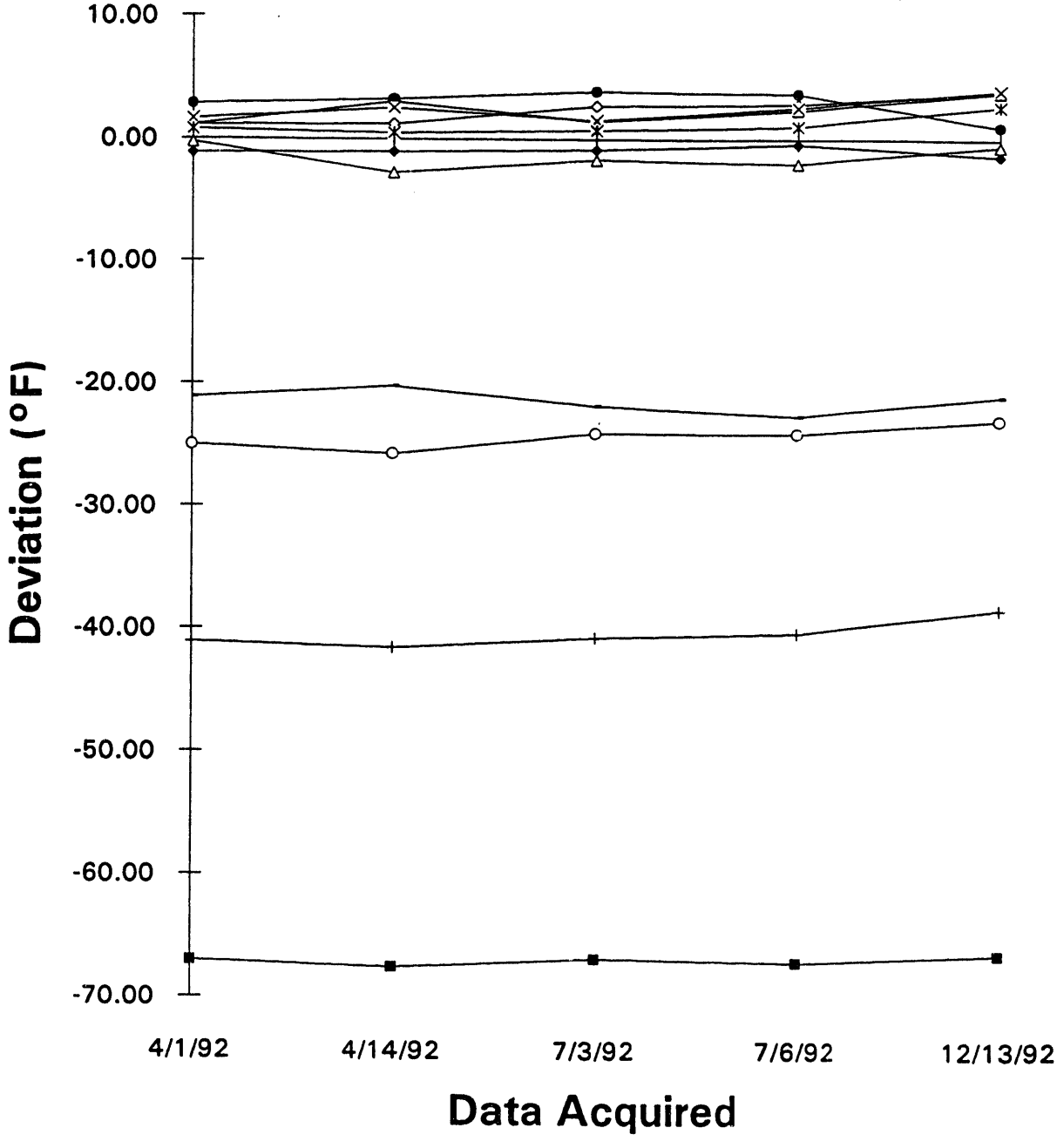
$$PL = Ax_4 + Bx_1 + Cx_2 + Dx_3 + E$$

PL	=	Pressurizer Level	A	=	0.12053496
x_1	=	Pressurizer Pressure	B	=	-0.07323886
x_2	=	Cold Leg Temperature	C	=	0.94069032
x_3	=	Hot Leg Temperature	D	=	0.38394097
x_4	=	Reactor Power Level	E	=	-550.0212

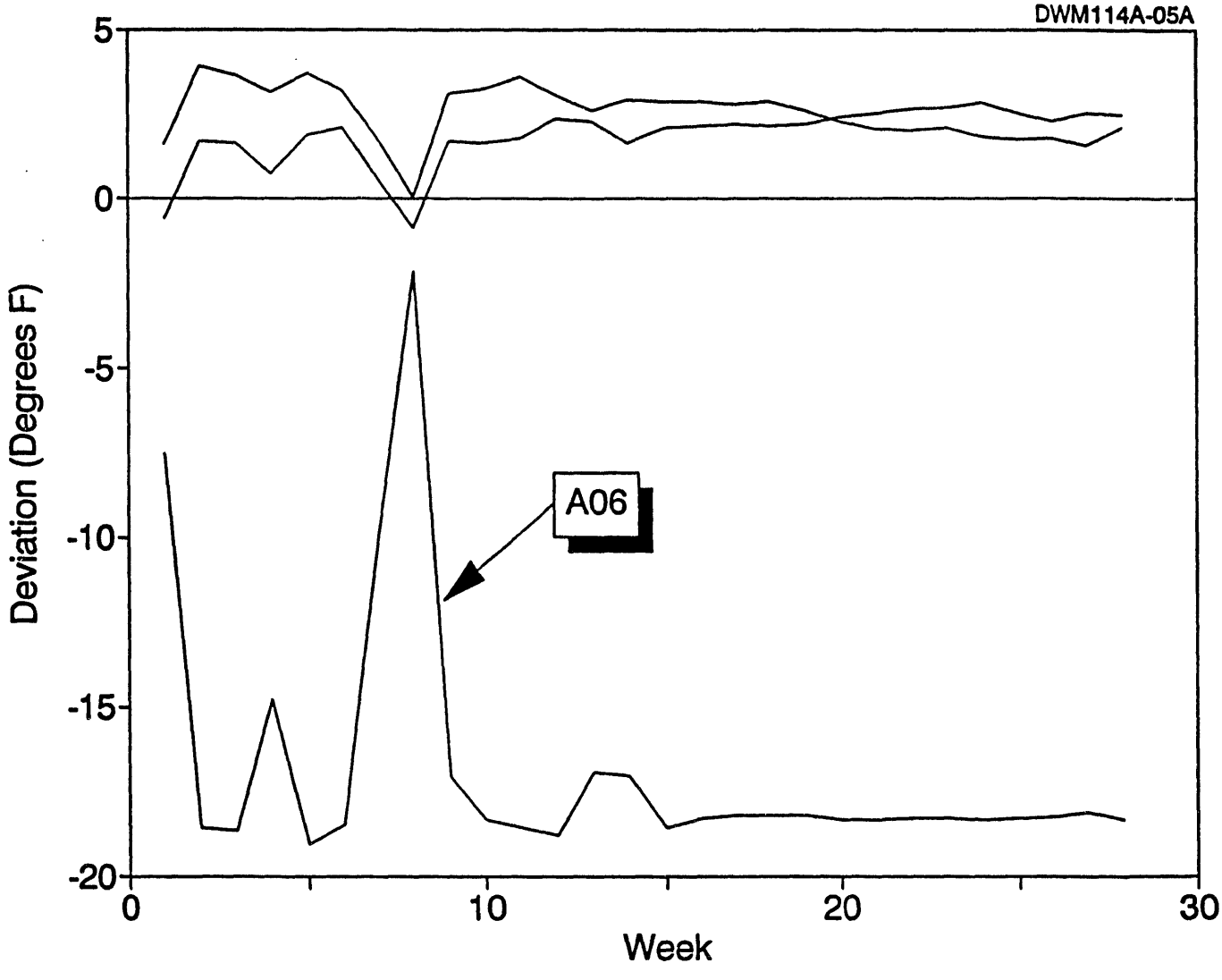
Steam Pressure Results at Power

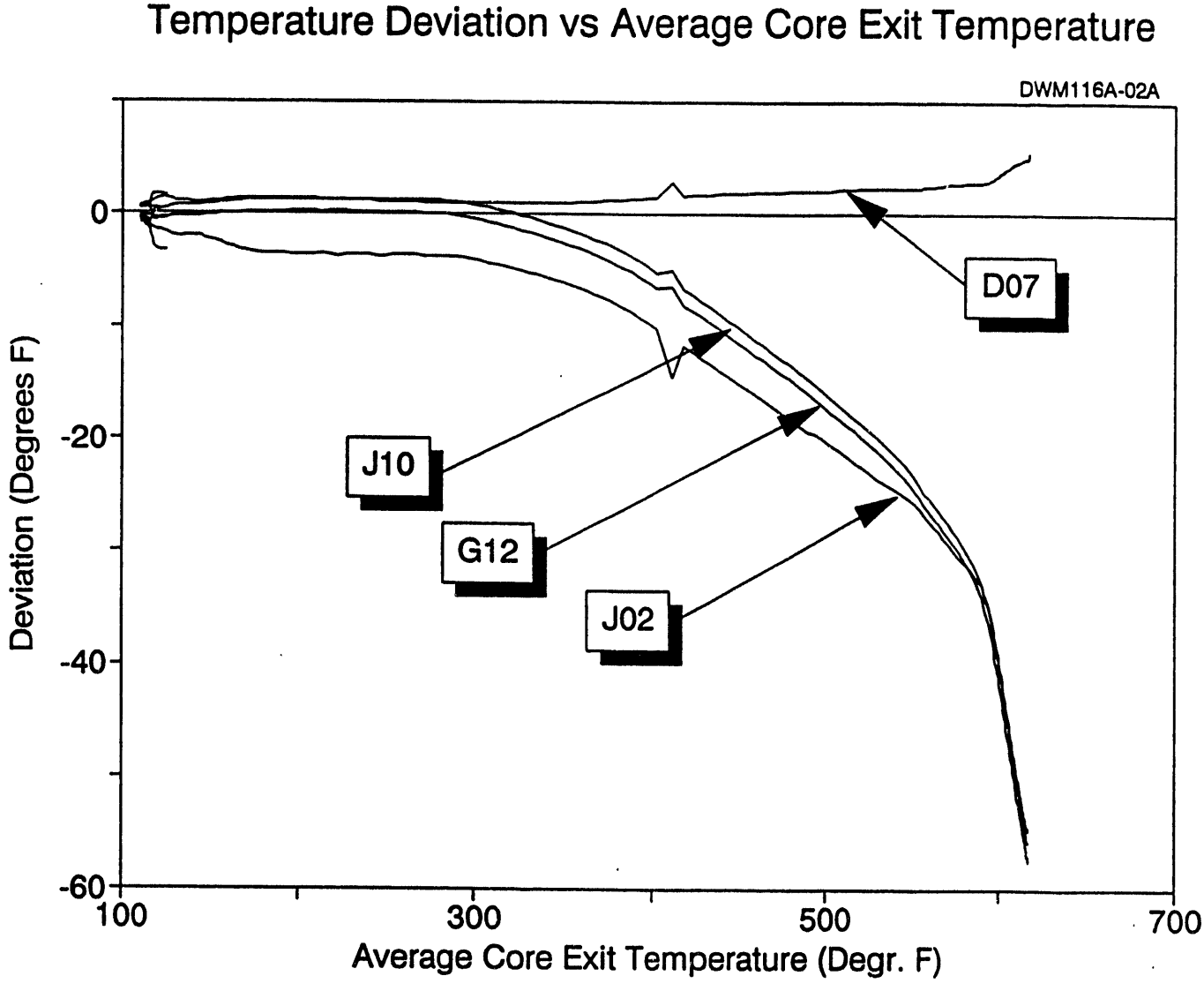


Thermocouple Monitoring Results
Quadrant 3 at Power



Core Exit Thermocouples




Temperature Deviation vs Average Core Exit Temperature
DWM116A-02A
0
-20
-40
-60
Deviation (Degrees F)
100
300
500
700
Average Core Exit Temperature (Degr. F)
D07
J10
G12
J02

CONCLUSIONS

- On-Line Monitoring can Help Segregate the Channels that Need Calibration from Those that Do Not
- Validation Tests are Underway to Establish the Uncertainties of On-Line Monitoring (NUREG/CR-5903)
- Benefits are: Reduces Radiation Exposure, Outage Manpower, and Maintenance-Induced Problems

SESSION 3

AGEING AND MAINTENANCE

Predictive Maintenance of Electrical Components Through Computer-Controlled Acquisition and Trending of Standard Circuit Parameters

The Effects of Aging on Electrical and I&C Components: Results of U.S. Nuclear Plant Aging Research

Rosemount Transmitters - Supplement to Bulletin 90-01

PREDICTIVE MAINTENANCE OF ELECTRICAL COMPONENTS THROUGH COMPUTER-CONTROLLED ACQUISITION AND TRENDING OF STANDARD CIRCUIT PARAMETERS

Gregory Allan and Thomas J. Weir
ECAD® Division of CM Technologies
1026 Fourth Avenue
Coraopolis, Pennsylvania 15108
U.S.A.

ABSTRACT

Condition monitoring techniques are finding greater acceptance within many power plant maintenance organizations as plant operators develop predictive maintenance programs. This paper describes a proven condition monitoring technique and it's application in an electrical circuit predictive maintenance program. The technique performs a series of standard electrical measurements, under computer control, using a pre-defined test methodology. The test data is evaluated by utilizing statistical analysis methods and by comparisons through graphical representations. These methods allow comparisons with data from similar circuits or with baseline measurements. Circuit and component degradation appears as a change in one or more of the measured electrical parameters. Trending these parameters over time provides for early identification of circuit degradation. Incorporating this technique into a plant predictive maintenance program will switch maintenance personnel from a reactive to proactive position.

1. INTRODUCTION

Condition monitoring techniques have been recently integrated into many power plant maintenance organizations as plants strive to develop efficient predictive maintenance programs. Nuclear and fossil plants alike are utilizing these techniques to maximize maintenance efficiency, increase overall plant availability and to extend operating life. The nuclear industry is also viewing these techniques necessary to improve overall plant safety and to provide data in support of operating license renewal.

In 1987, the ECAD System 1000 was introduced as a commercial condition monitoring system to address the need to monitor and trend the condition of an entire electrical circuit (including the cables, connectors, penetrations and instrumentation) from one location [1] [2] [3]. This paper describes the use of ECAD for predictive maintenance by presenting both the test and analytical methodologies used to monitor the condition of electrical circuits. Results from a laboratory circuit model and an actual power plant circuit are presented to demonstrate these methodologies. The paper concludes by discussing future directions for enhancement of the technique.

2. SYSTEM DESCRIPTION

ECAD's approach to condition monitoring of electrical circuits is to treat the circuit as a parallel wire transmission line connected to a load. These can be thought of as a distributed circuit element with a certain resistance, inductance, capacitance and conductance per unit length. Examples of parallel wire transmission lines include two wires in a multiconductor cable, a wire over a ground plane and a coaxial cable.

The ECAD System 1000 performs both lumped and distributed circuit measurements during each test. The lumped measurements are conducted by treating the circuit as a network of simple components (combinations of resistors, capacitors and inductors). Three basic types of measurements are performed to acquire the lumped data. The DC resistance, or loop resistance, is measured and represents the total resistance of the circuit. The AC resistance and reactance are measured at nine discrete frequencies between 100 Hz and 50 kHz; these are then converted to impedance and phase angle. From the impedance measurements, the circuit may be characterized as being either capacitive or inductive over the frequency range. The dissipation factor and quality factor are calculated and can be used as a "purity" factor, a measure of how close the circuit is to being a pure capacitor or inductor (no resistive losses). An insulation resistance test is performed to characterize the DC loss properties of the circuit's

insulating material. The lumped data measurements of the standard circuit parameters provide the best and earliest indication of degradation. Identifying a change in these measurements is important, however, it is also desirable to determine the location of the change. A technique known as Time-Domain Reflectometry (TDR) is used to accomplish this. TDR involves propagating an electromagnetic pulse between two wires and analyzing the reflected energy caused by discontinuities along the wires. By correlating the lumped and distributed measurement results, the nature and location of the change may be determined.

A key in any predictive maintenance program is to incorporate condition monitoring techniques that have the ability to acquire high quality data. The ECAD System 1000 relies on computer control to ensure both accuracy and repeatability. The computer and associated software controls each of the instruments through an IEEE-488 interface bus. The test sequence includes measuring AC and DC voltage, DC loop resistance, AC resistance and reactance, the TDR signature and insulation resistance. After the completion of each test, the results are automatically placed into a database. The manipulation and analysis of this database utilizing special methodologies extends the predictive capabilities of the ECAD technology.

Analysis of the ECAD data is based on establishing a reference by which all future aging, degradation, and changes can be compared. Any inconsistencies that are observed are the result of changing conditions and are not due to operator or equipment errors. Given the high level of confidence in the data, minimal acceptance criteria may be established through theoretical analysis or by using data acquired from similar circuits. Data analysis (by either direct comparison or statistical methods) is performed so that adverse trends may be observed.

3. LABORATORY EXAMPLE

This example is based on a model resistance temperature detector (RTD) circuit constructed in a laboratory. The purpose of this example is to demonstrate the ECAD System 1000 methodology and to present a sample of the data obtained. The circuit used for this example is shown in Figure 1.

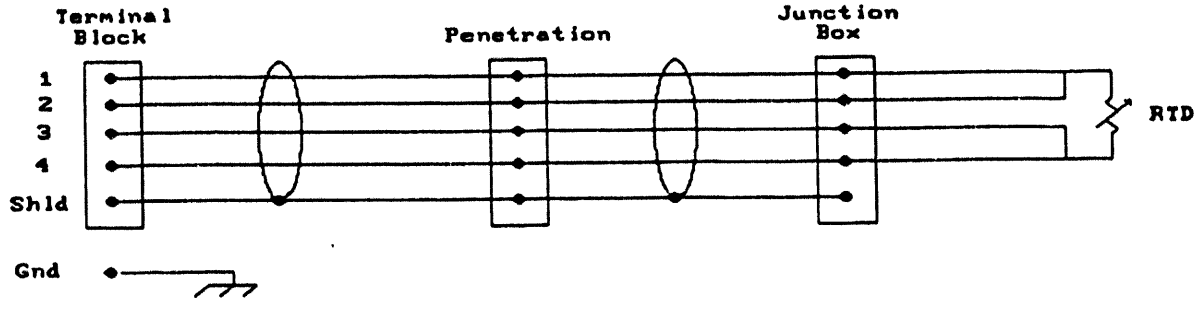


Figure 1. Diagram of RTD Circuit.

To completely characterize this circuit, a total of nine tests (or configurations) are required. Table I contains a brief description of each configuration.

Table I
Description of Tests for RTD

Configuration	Description
A	Across Compensating Leads (Pins 1 and 2)
B	Across Element (Pins 1 and 3)
C	Across Element (Pins 2 and 3)
D	Across Compensating Leads (Pins 3 and 4)
E	Lead to Shield (Pin 1 and Shd)
F	Lead to Shield (Pin 2 and Shd)
G	Lead to Shield (Pin 3 and Shd)
H	Lead to Shield (Pin 4 and Shd)
I	Shield to Ground (Shd and Gnd)

The model RTD circuit was tested twice as shown by the data in Table II. The first test obtained the baseline data (data which is dated 07/13/89). The circuit was then retested with a degraded connection inserted (data which is dated 2/24/92).

Table II
Comparison of Data from Model RTD circuit

CODE	CFG	DATE	LOOP RESISTANCE	AC RESISTANCE @ 1 kHz	REACTANCE @ 1 kHz
1TE101	A	07/13/89	1.84 Ω	1.86 Ω	110.00 mΩ
1TE101	A	02/24/92	11.78 Ω	12.63 Ω	152.83 mΩ
1TE101	B	07/13/89	195.76 Ω	196.42 Ω	-758.60 mΩ
1TE101	B	02/24/92	205.55 Ω	206.27 Ω	-794.48 mΩ
1TE101	C	07/13/89	195.82 Ω	196.50 Ω	-759.20 mΩ
1TE101	C	02/24/92	195.69 Ω	196.42 Ω	-759.03 mΩ
1TE101	D	07/13/89	1.82 Ω	1.83 Ω	112.00 mΩ
1TE101	D	02/24/92	1.85 Ω	1.85 Ω	112.00 mΩ

The baseline data (1989) shows results typical of a four wire RTD circuit. Both of the compensating lead configurations (Cfg A and D) have almost identical values of loop resistance, AC resistance and reactance. Additionally, configurations B and C, which test across the element, have similar results.

When the circuit was retested in 1992, and the results compared to the baseline data, some significant changes can be observed in the configuration A and B data. However, a comparison of configurations C and D does not show any appreciable differences. Based on these

comparisons, the affected lead can be determined. Table I shows that configuration A uses pins 1 and 2 and that configuration B uses pins 1 and 3 (pin 1 being common to both configurations). Since no changes were observed in the data from configurations C and D, the leads connected to p elimination, we conclude that a change has occurred in the lead connected to pin 1.

To further understand the nature of the change, a graphical comparison of the configuration A results was performed. Figure 2 presents a graph of AC resistance versus frequency for the 1989 and 1992 configuration A tests. It can easily be seen that the AC resistance values acquired in 1992 are approximately 11 ohms larger than the 1989 results. A change is also seen when the reactance values are examined as shown in Figure 3. From Figures 2 and 3, we conclude that the change is primarily resistive with only a small change in reactance.

Once the nature of the change is understood, the next step is to determine the location. From Table II, we deduced the change was present in the lead connected to pin 1. The TDR signatures are then used to determine the location. Figure 4 is an overlay of the 1989 and 1992 TDR signatures for the configuration A tests. The TDR signatures indicate the model circuit is approximately 90 feet in length. However, the 1992 configuration A TDR signature separates from the other signature approximately 10 feet from the end of the circuit. The fact that this signature separates and remains separated indicates a resistive change brought on by connector degradation.

4.0 CASE STUDY

This case study involves data obtained from a four wire RTD circuit in an operating power plant. The circuit was only tested once, however, during the analysis of the baseline data, an anomaly was discovered. The schematic of this circuit is the same as the circuit shown in Figure 1, except that no junction box is present. The configurations shown in Table I were used to characterize the circuit. A sample of the acquired data is shown in Table III.

Table III
Comparison of Data from Plant Circuit

CODE	CFG	DATE	LOOP RESISTANCE	AC RESISTANCE @ 1 kHz	REACTANCE @ 1 kHz
TE1328	A	11/08/91	7.96 Ω	8.88 Ω	812.53 mΩ
TE1328	B	11/08/91	117.27 Ω	118.30 Ω	-654.45 mΩ
TE1328	C	11/08/91	115.71 Ω	116.75 Ω	-664.71 mΩ
TE1328	D	11/08/91	5.27 Ω	5.28 Ω	768.00 mΩ
TE1328	E	11/08/91	1.06 GΩ	37.47 Ω	-1.88 kΩ
TE1328	F	11/08/91	1.08 GΩ	36.02 Ω	-1.88 kΩ
TE1328	G	11/08/91	1.15 GΩ	36.00 Ω	-1.88 kΩ
TE1328	H	11/08/91	1.27 GΩ	38.13 Ω	-1.88 kΩ
TE1328	I	11/08/91	9.18 MΩ	799.11 Ω	-3.59 kΩ

In this case, the baseline data indicates an imbalance between the two compensating lead configurations (Cfg A and D). A similar imbalance is observed when the tests across the element are compared (Cfg B and C). Expected data from a typical four wire RTD has balance between configurations A and D and between configurations B and C.

To determine the nature of the imbalance, the same analysis methodology, as described in the laboratory example, can be applied. Since both configurations A and D are essentially the same, a short circuit, the configuration with the smaller loop resistance will be used as a reference. Similarly, in comparing configurations B and C, the configuration with the smaller loop resistance will serve as the reference. By examining Table III, we determine that configurations A and B are suspect. As in the laboratory example and by using the process of elimination, we conclude the imbalance is on the line connected to pin 1.

To determine the nature of the imbalance, a graphical comparison of the data from configurations A and D is required. Figure 5 is a graph of the AC resistance versus frequency for configurations A and D. By examining Figure 5, it is apparent that the AC resistance values for configuration A are approximately 3 ohms larger than those from configuration D. Figure 6 contains a graph of reactance versus frequency for configurations A and D. The reactance values for these configurations vary slightly at the higher frequencies. From Figures 5 and 6, as in the model circuit, we conclude the imbalance is primarily resistive in nature.

With the nature of the imbalance understood, the TDR signatures for configuration A and D are used to determine the location. Figure 7 shows both of the TDR signatures. The signatures overlay until the end of the circuit (approximately 600 feet) and then begin to separate. This separation indicates a resistive change at approximately 600 feet from the beginning of the circuit (most likely at or near the RTD element).

5.0 CONCLUSIONS

The use of the ECAD System 1000 in an electrical circuit predictive maintenance program is straightforward. Critical plant components are selected based on plant safety and functionality criteria. Once plant procedures are established, the condition monitoring technique can be applied. Standard circuit parameters are monitored to determine if any changes due to degradation are occurring. When trends are identified using the data analysis methodologies, the surveillance interval may be increased or, if necessary, corrective maintenance performed.

The establishment of circuit functionality criteria based on the standard circuit parameters is providing the direction for further advancement. Over the past seven years, a large generic database has been developed containing test results from many power plants. This database is organized by circuit type which allows for detailed comparisons and determination of common trends between similar components.

As a parallel effort, several theoretical models are being considered for use in establishing acceptance criteria in terms of the standard circuit parameters. Development of these models will automate data analysis and provide improved failure prediction capabilities.

REFERENCES

[1] HUSLER, Robert O., WEIR, Thomas J., "Advanced Technologies for Maintenance of Electrical Systems and Equipment at the Savannah River Site Defense Waste Processing Facility (U)", Proceedings from the International Conference on Nuclear Plant Life Extension, Upgrading, Repair, Refurbishment, Uprating and Ageing (1991), 267-277.

[2] PENTECOST, Lloyd, and WEIR, Thomas J., "Electrical Condition Monitoring and Troubleshooting at San Onofre Nuclear Generating Station Using the ECAD Test System", Proceedings from the EPRI 4th Incipient Failure Detection Conference (1990).

[3] ST. ONGE, R.J., "Cable and Electrical Apparatus Monitoring Program at San Onofre Nuclear Generating Station (SONGS) Unit 1", Proceedings: EPRI Workshop on Power Plant Cable Condition Monitoring (1988).

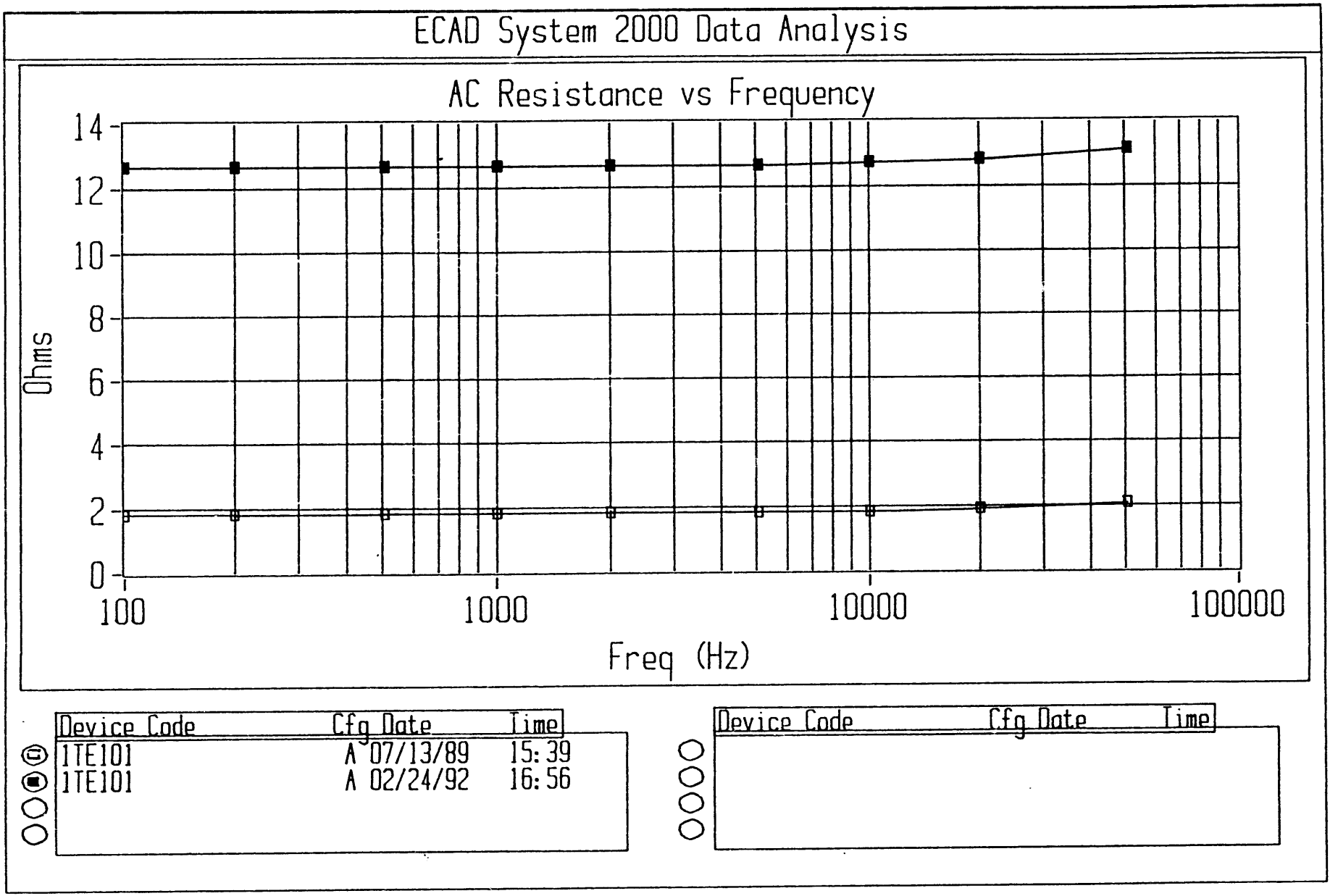


Figure 2. AC Resistance vs. Frequency for Model RTD Circuit

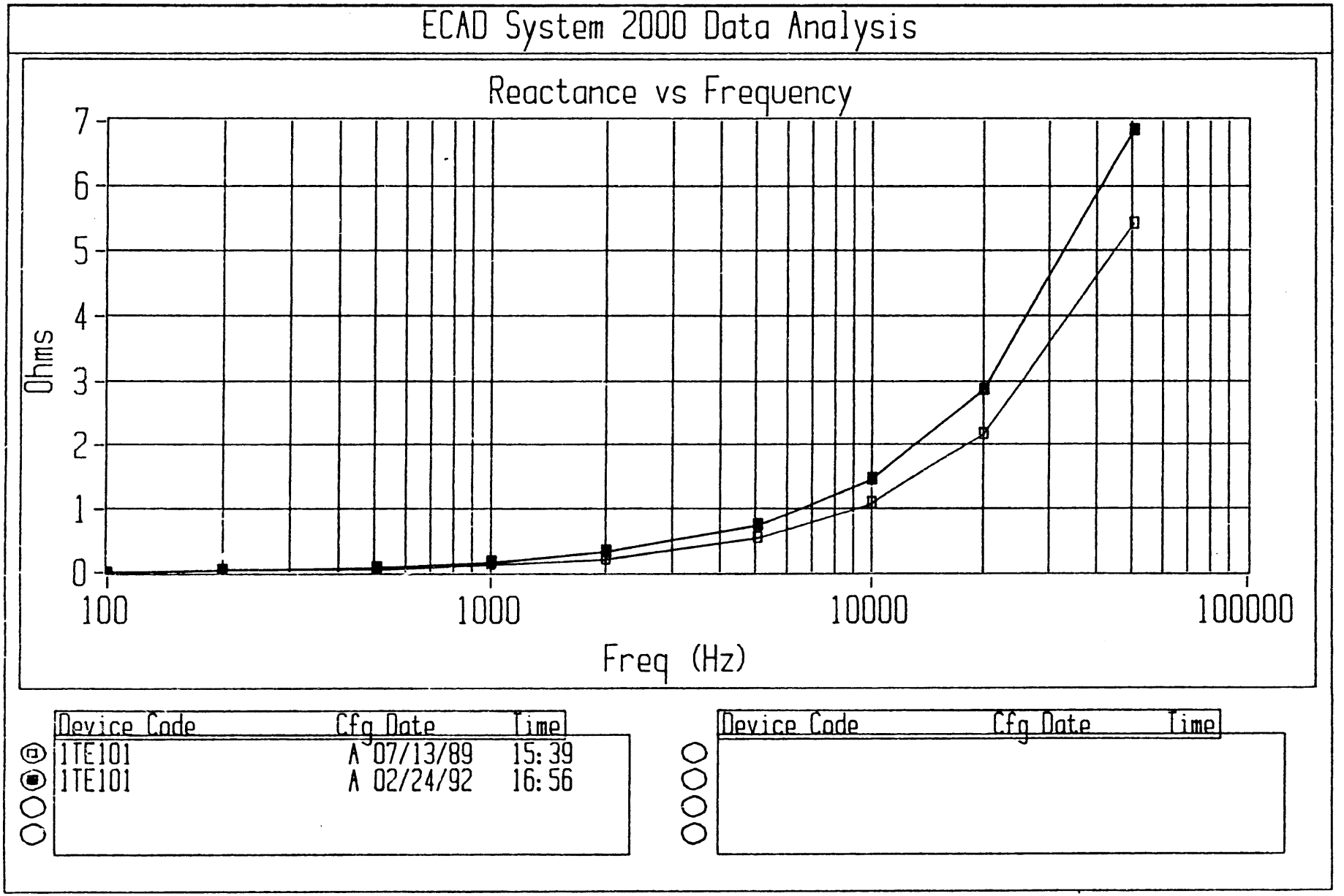


Figure 3. Reactance vs. Frequency for Model RTD Circuit

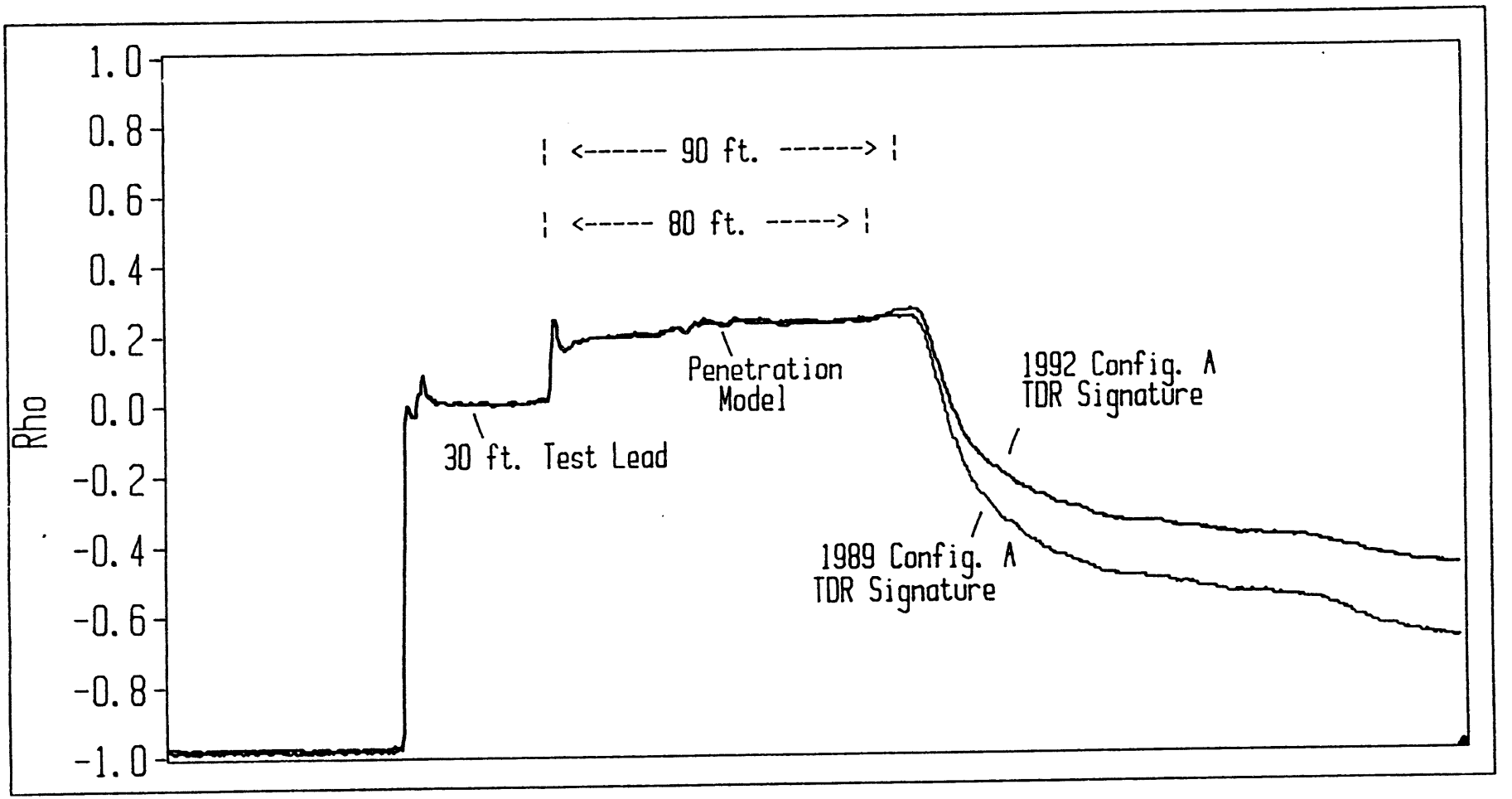


Figure 4. TDR Signatures for Model RTD Circuit

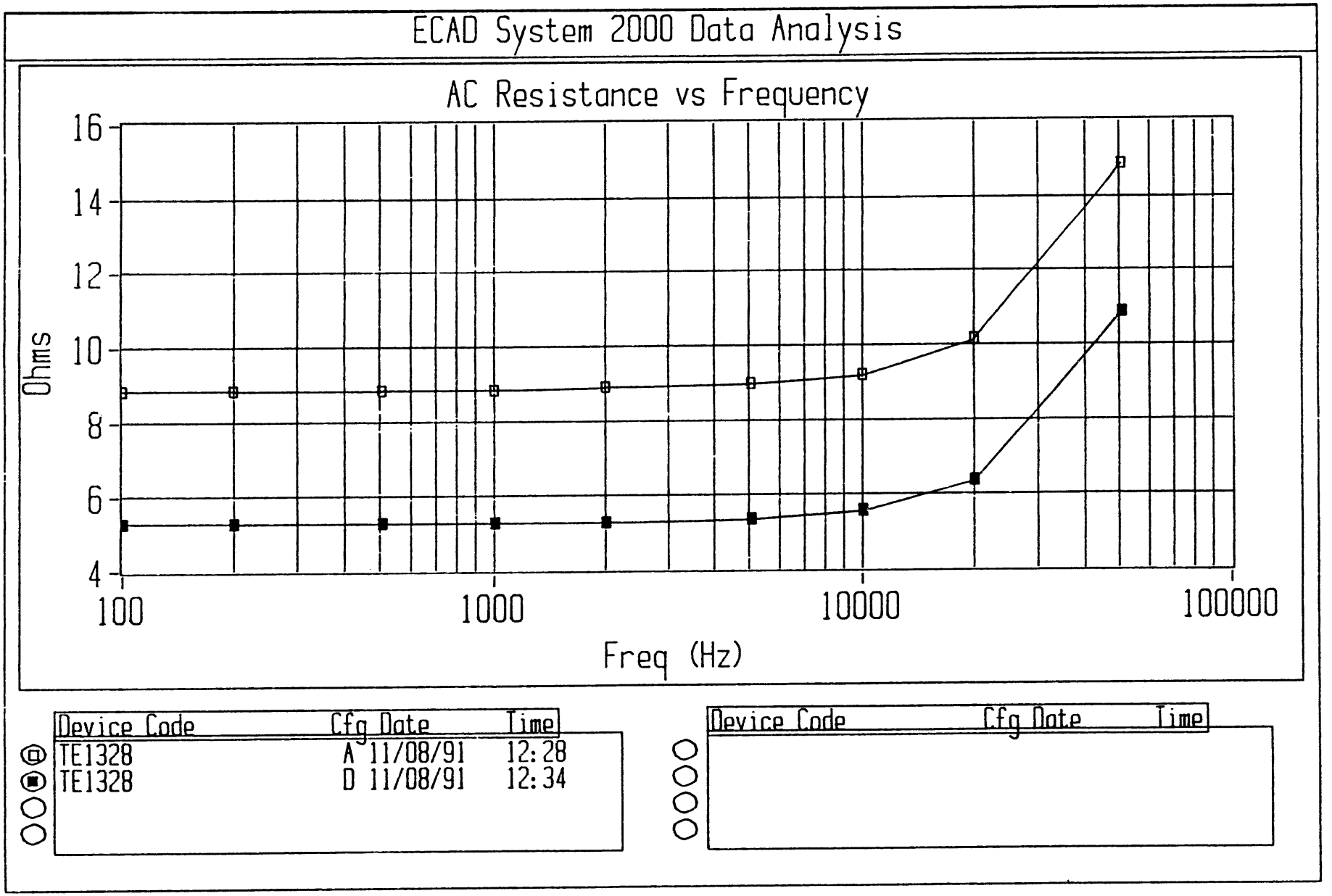


Figure 5. AC Resistance vs. Frequency for Plant RTD

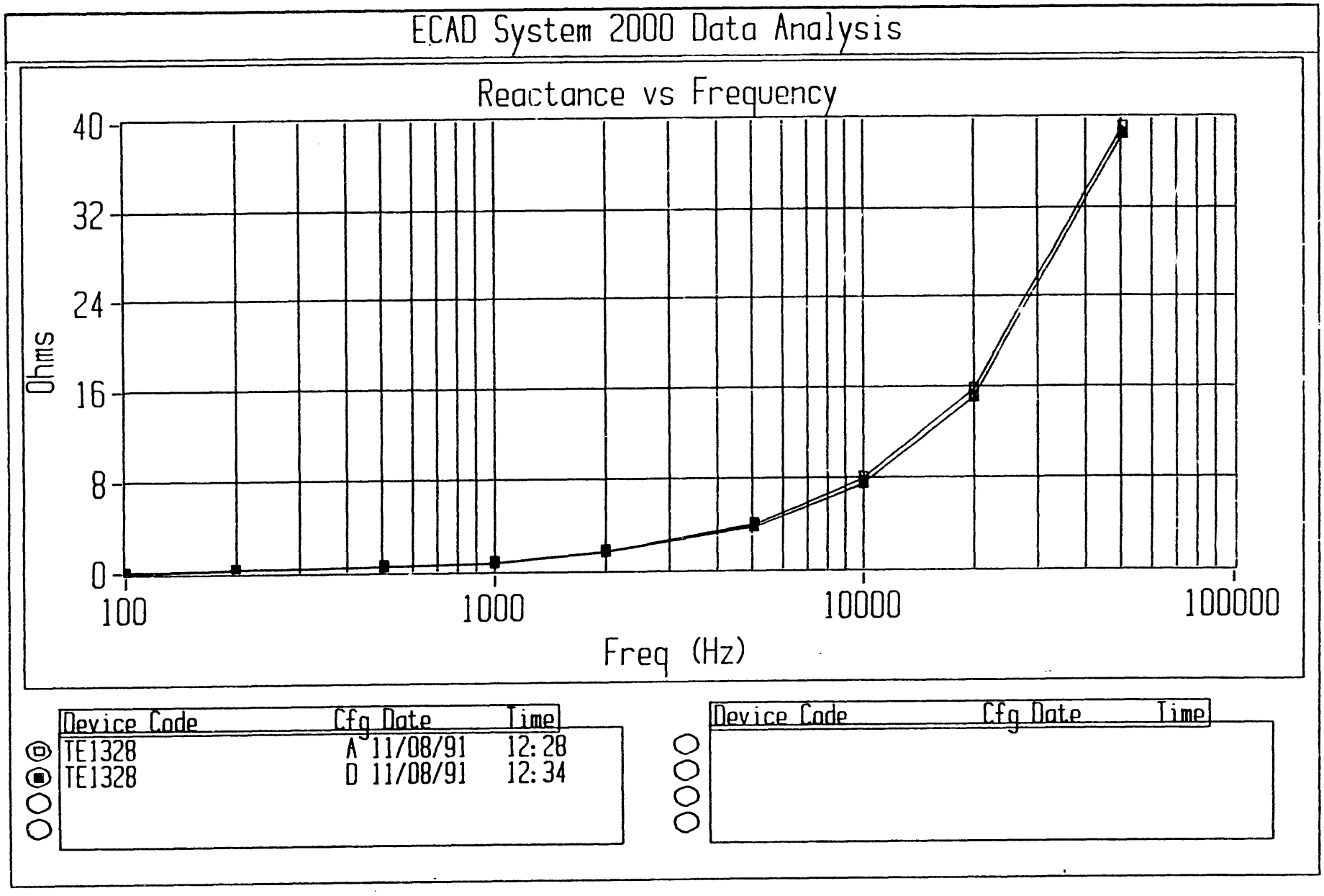


Figure 6. Reactance vs. Frequency for Plant RTD Circuit

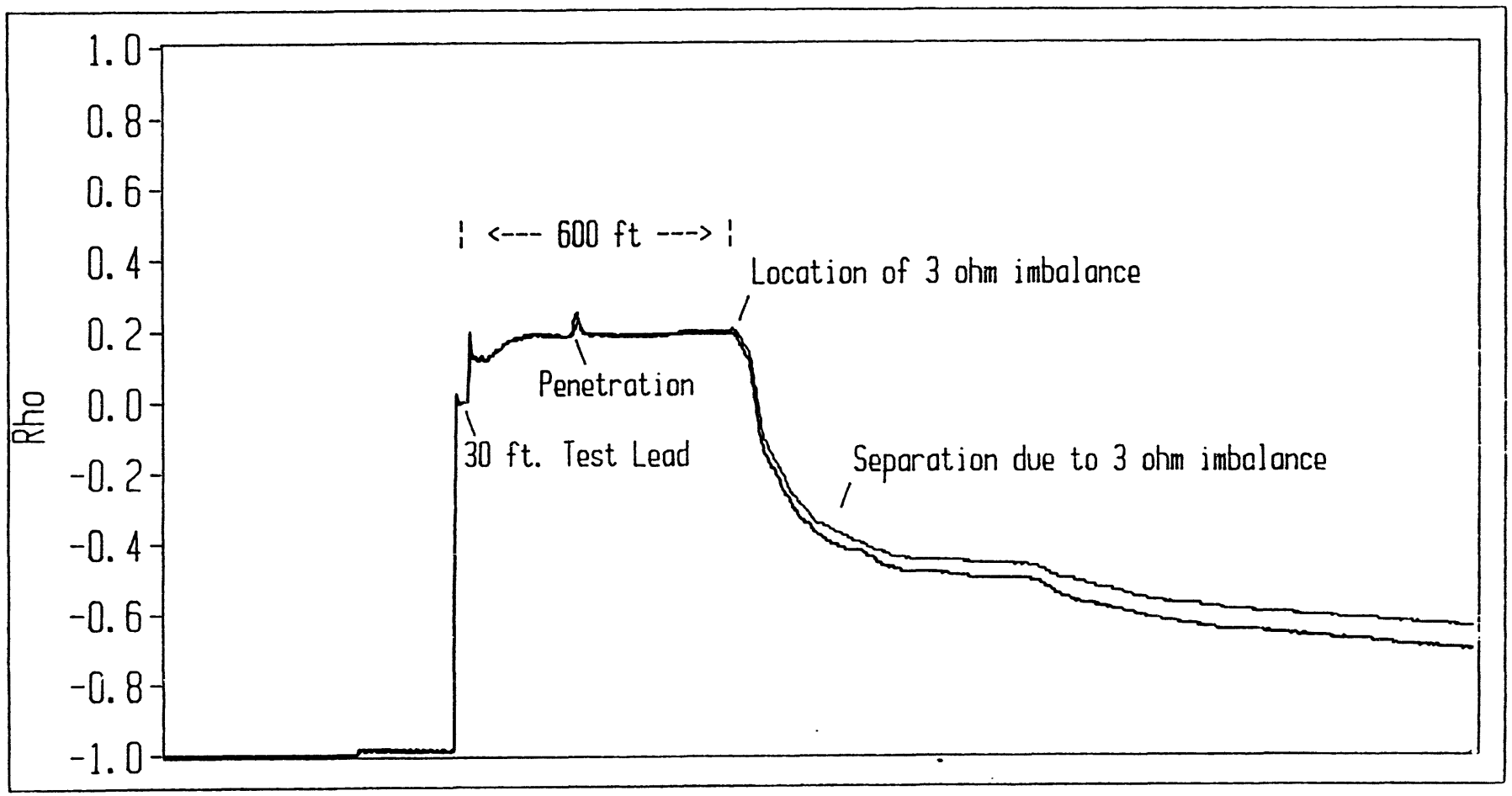


Figure 7. TDR Signatures From Plant RTD

THE EFFECTS OF AGING ON ELECTRICAL AND I&C COMPONENTS: RESULTS OF U.S. NUCLEAR PLANT AGING RESEARCH*

by
Satish K. Aggarwal
United States Nuclear Regulatory Commission
Washington, DC 20555

and
William E. Gunther
Brookhaven National Laboratory
Building 130
Upton, NY 11973

* This work done under the auspices of the U.S. Nuclear Regulatory Commission.

ABSTRACT

The U.S NRC's hardware oriented engineering research program for plant aging and degradation monitoring has achieved results in the area of electrical, control, and instrumentation (ECI) components used in nuclear power plants (NPPs). The principal goals of the program, known as the Nuclear Power Plant Aging Research (NPAR) Program, are to understand the effects of age-related degradation in NPPs and how to manage and mitigate them effectively. This paper describes how these goals have been achieved for key ECI components used in the safety systems of NPPs. The status of relevant on-going and planned research projects is also provided.

1. INTRODUCTION

The application of ECI components in NPPs requires that they be extremely reliable throughout the life of the plant. Studies of ECI components have revealed that degradation due to aging can detrimentally affect their life, and their ability to operate under normal and abnormal operating conditions. Through the U.S. NRC's NPAR Program, degradation mechanisms and aging management techniques are being or have been evaluated for bistables, switches, transmitters, inverters, I&C modules, and isolation devices. In addition, the ECI components associated with systems such as the Emergency Diesel Generators, Control Rod Drive Systems, and Emergency Core Cooling Systems have been assessed for their aging degradation with time. An evaluation of the operating experiences of these components and systems, coupled with a determination of the materials of construction, operating and environmental stresses, and failure modes, causes, and effects have provided the NRC with the technical basis required to assure the continued safe operation of present reactors. An additional benefit of our aging research program is the application of its lessons learned to the advanced reactors program to assure the longevity of these proposed new designs.

Examples of the specific research results applicable to the objectives of this meeting are provided in the paper. These results include a description of aging issues, as well as the recommended solutions for managing aging. As pointed out in this paper, degradation of certain subcomponents, such as electrolytic capacitors, fuses, or power semiconductors can effect the operation of various ECI equipment. Similarly, aging degradation associated with the mechanical properties of elastomers, connectors, and fuse holders can also result in ECI failures. To a large degree, the detection and mitigation of this degradation is accomplished through a comprehensive maintenance program which incorporates predictive and condition monitoring techniques, in addition to the testing and calibration procedures typically associated with instrumentation and controls. Current maintenance practices successfully employed by U.S. utilities are also summarized.

2. DISCUSSION

One of the initial tasks of the NPAR Program was to identify and prioritize components, systems, and structures whose degradation due to aging would have risk significance. NUREG/CR-3385 and NUREG/CR-4144 provided risk-based inputs to the selection process, and were instrumental in establishing various electrical and instrumentation and controls (ECI) components as topics for study in the NPAR Program. The importance of ECI components such as transmitters, switches, batteries, inverters, circuit breakers, and relays to the successful

operation of safety systems was clearly identified in these evaluations. Based on these early studies, work which focussed on the aging susceptibility of these components was completed in many of these areas. Table I identifies the reports related to ECI which have been published or will be published shortly. NUREG-1377, Rev. 2 is a complete listing and summary of all of the reports issued on plant aging through June 1991. The subsequent paragraphs describe some of the important findings related to this work which should be of interest to ECI designers, operators, and maintainers.

2.1 I&C Power Sources

In a nuclear power plant, power conditioning equipment such as battery chargers and inverters are the sources of power for the instrumentation buses, namely the vital ac bus (typically 120 Vac) and the essential dc bus (typically 125 Vdc). A high reliability for these components is important to assure that instrumentation and controls needed for the safe operation of the plant are available. An assessment of the operating experience, materials of construction, and application of battery chargers and inverters revealed that sixty-five percent of inverter failures are due to hardware degradation. NUREG/CR-4564 reported that components such as electrolytic capacitors, thyristors, and fuses are susceptible to aging and that their failure directly resulted in an outage of the inverter, and in many cases, a plant transient including a reactor scram. As illustrated in Figure 1, the analysis of the operating experience indicates that overheating, electrical transients, and errors by plant personnel are the leading causes of inverter failures.

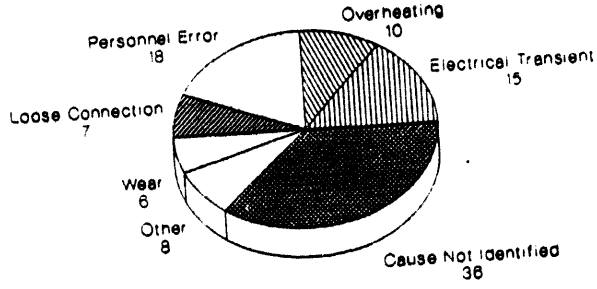


Figure 1 Percent of Failures (LERs 1984-1986)

Further study performed on inverters, including testing of a naturally aged inverter from the decommissioned Shippingport facility and completion of a comprehensive survey of U.S. utilities, revealed that means exist for detecting and managing the effects of aging on inverters. For example, the following improvements in the design have been demonstrated by some U.S. utilities to be effective means for managing inverter aging:

1. Installing forced air cooling rather than natural convection cooling tends to reduce the cabinet temperature, and protect those components vulnerable to overheating.

2. The introduction of higher voltage and temperature rated components, especially capacitors and semiconductors, makes these components less sensitive to operationally induced failures (electrical transients).

3. The use of an automatic transfer switch, which senses an inverter failure and switches to a backup power source, can be useful in mitigating the effects of an inverter failure.

Similarly, maintenance, inspection, and testing methods have been identified for use in managing the aging of inverters in nuclear power plants. Recommendations from NUREG/CR-5051 in this area follow:

1. Since overheating is an important cause of stress, it is prudent to periodically monitor the internal cabinet temperature.

2. Cleaning can also minimize the risk of overheating; the wiping of thyristor heat sinks and ventilation flow paths improves the heat transfer away from temperature sensitive components.

3. Capacity testing is recommended, especially for standby inverters. This verifies that the inverter can supply design loads, and permits inspection monitoring techniques to be applied at rated load.

The same reports, NUREG/CRs-4564 and 5051, contain similar evaluations and recommendations for battery chargers. In general, however, the failure of an inverter was more dramatic than a battery charger failure since the battery immediately picks up the dc loads, thereby minimizing the immediate plant impact resulting from the loss of the charger. On the other hand, degradation of the charger as indicated by an increased ac ripple on its output, could impair the instrumentation and controls supplied from the dc bus. Many of the findings associated with the study of battery charger and inverter aging apply to power supplies in general. Failures of electrolytic capacitors used for filtering, and overheating of electronic components are two examples of pertinent information related to ac and dc power sources used in instrumentation and controls.

2.2 Process Instrumentation

Research on aging has also been completed for process instrumentation used in nuclear power plants. NUREG/CR-4257 describes the types of pressure transmitters commonly used in nuclear power plants according to their application. The most common effects of the aging-related stresses on the transmitters are calibration shifts. The specific stresses that most often affect these transmitters are:

- ambient temperature
- humidity
- radiation
- process medium pressure and temperature

Based on the evaluation of operating experience and the assessment of the materials used, it is suggested that a combination of operability monitoring and condition monitoring be used to improve the probability of successfully mitigating the aging process. To this end, it is pointed

out that the evaluation of calibration data alone will not ensure that the transmitter is capable of operating under accident conditions. If, with time, steam or moisture penetrates the transmitter housing, the electronics may become inaccurate and fail. Therefore, the integrity of the housing seal must also be evaluated periodically to be able to predict continued performance capability.

A follow-up study on pressure sensors with an emphasis on the effects of aging on the instrument's response time was reported in NUREG/CR-5383. Laboratory testing was performed on the effects of various operating stresses on the dynamic response of pressure sensors. The significant findings from this work were:

1. The exposure of transmitters to heat, humidity, and vibration resulted in an increase in response time and a calibration shift, with the latter being the more pronounced problem.

2. Five effective methods are available for response time testing. Two of the methods (noise analysis and power interrupt test) have the advantage of providing on-line measurement capability at normal operating conditions.

A two phase study was also completed for temperature sensors, with the emphasis of the second phase placed on resistance temperature detectors (RTDs). The work involved laboratory testing of 72 nuclear grade RTD elements representing several from each of four U.S. manufacturers. Thirty were subjected to simulated reactor conditions which resulted in the failure of five and a calibration shift in six others. Two failures occurred during thermal aging, one in humidity aging, and one in thermal cycling. The remaining RTDs performed well during the aging tests, maintaining a drift band of 0.2 degrees C.

The results of the research showed that managing the aging of RTDs can be accomplished by periodically verifying their accuracy and response time, combined with a strong program for minimizing deficiencies due to design, fabrication, or installation. It was found that the average response time and stability of nuclear grade RTDs is about twice as good as that of commercial grade RTDs.

The NPAR Program has continued to devote research efforts to process instrumentation. A recent study, NUREG/CR-5700, discusses the aging susceptibility of six generic instrumentation modules: indicators, sensors, controllers, transmitters, annunciators, and recorders. Selected conclusions, observations, or recommendations derived from this study include:

1. Consideration should be given to methods that would be helpful in reducing the incidence of infant mortality, particularly for indicators and sensors, which dominate aging-related I&C module malfunctions and failures.

2. I&C modules make a modest contribution to safety-significant events. For example, 17% of the LERs issued during 1984-1988 dealt with malfunctions of the six I&C modules studied, of which 28% were aging related.

3. Systems that monitor voltages or waveforms internal to electronic devices may be useful in predicting imminent circuit failure.

2.3 Electrical Devices

The NPAR Program has also addressed the aging of circuit breakers, relays, terminal blocks, electrical penetrations, and solenoid valves. As indicated in Table I, reports have been issued on these devices in the same context as has been previously discussed for chargers, inverters, and I&C components. That is, the operating experience is reviewed to determine the types of failures being encountered; the failure mechanisms and modes are identified and evaluated; and the failure effects are assessed to determine their safety significance. From this structured approach, an understanding of aging is achieved, and the means to manage its effects are developed.

Examples of this include the following:

> NUREG/CR-4715: Normally energized relays suffer from more rapid deterioration than do deenergized relays. These failures were largely attributed to deterioration of the coil, changes in dimensions of certain organic components, and changes in the characteristics of timing diaphragms from thermal deterioration.
>
> NUREG/CR-5534: Cables, connections, and electrical penetrations are highly reliable devices under normal plant operating conditions with no evidence of significant increases in failure rate with aging. Further testing is being conducted to evaluate the effects of aging under postulated accident conditions.
>
> NUREG/CR-4819: Operating experience shows that SOV malfunctions have been caused both by electrical deterioration of the solenoid coil and its lead wires and by mechanical, chemical, and radiation degradation of certain valve internal parts. Several inspection activities have been identified as being useful in detecting and mitigating the effects of aging.
>
> NUREG/CR-5844: Commonly used instruments such as bellows, diaphragms and Bourdon Tubes are affected by similar aging mechanisms. These processes lead to loss of calibration, spurious signals, or false alarms, or eventually to complete loss of instrument function. These instruments are susceptible to damage from pressure surges or pulsations within the system they are monitoring and their overall service life is generally limited to a finite number of operating cycles, primarily due to fatigue.
>
> NUREG/CR-5762: The conclusions of this report state that while current nuclear plant inspection, surveillance, and monitoring methods are effective at detecting and mitigating some of the degraded conditions caused by aging, improved methods are available. For instance, for molded case circuit breakers, the methods of infrared temperature measurement and vibration testing are recommended. Additionally, it is recommended that the current practice of instantaneous trip testing be modified to assure that the instantaneous trip occurs within the instantaneous range by tests below and above the trip range.

Table I - NPAR Products Related to ECI

ECI Component	Reports
1. Battery Chargers and Inverters	NUREG/CR-4564 (Phase 1) NUREG/CR-5051 (Phase 2) NUREG/CR-5192 (Testing)
2. Circuit Breakers and Relays	NUREG/CR-4715 (Phase 1) NUREG/CR-5762 (Phase 2)
3. I&C Components	NUREG/CR-5700 (Phase 1)
4. Reactor Protection System	NUREG/CR-4740 (Phase 1)
5. Solenoid Operated Valves	NUREG/CR-4819, Vols. 1 & 2 (Phase 1) NUREG/CR-5141 (Phase 2)
6. Batteries	NUREG/CR-4457 (Phase 1) NUREG/CR-5448 (Seismic Testing)
7. Bistables/Switches	NUREG/CR-4992 (Multi-stage switches only) NUREG/CR-5844
8. Pressure Transmitters	NUREG/CR-4257, Vol. 2
9. Electrical Penetrations/Connectors, Cables	NUREG/CR-5334 (Testing) NUREG/CR-5461
10. Pressure Sensors	NUREG/CR-5383
11. RTDs/Temperature Sensors	NUREG/CR-4928 (Phase 1) NUREG/CR-5560 (Phase 2)

3. CONCLUSION

This paper has described the work that has been completed through the U.S. NRC's NPAR Program for electrical, control, and instrumentation (ECI) used in nuclear power plants. Examples of the specific research results applicable to this meeting have been provided, recognizing that each of the studies associated with the various ECI components contains a large amount of information. The results of this research, however, has indicated that the aging process is significant for ECI devices and must be aggressively managed in nuclear power plants to maintain its required high reliability. Means for detecting, monitoring, and mitigating the effects of aging are available and have been identified through this research program.

4. BIBLIOGRAPHY

1. VORA, J.P., "Nuclear Plant Aging Research (NPAR) Program Plan," NUREG-1144, Rev. 2, June, 1991.

2. DAVIS, T., et.al., "Importance Ranking Based on Aging Consideration of Components Included in Probabilistic Risk Assessments," NUREG/CR-4144. April, 1985.

3. KONDIC, N.N. AND HILL, E. L., "NRC Research Program on Plant Aging: Listing and Summaries of Reports Issued Through June 1991," NUREG-1377, Rev. 2, July, 1991.

4. GUNTHER, W., et.al.,"Operating Experience and Aging-Seismic Assessment of Battery Chargers and Inverters," NUREG/CR-4564, June, 1986.

5. GUNTHER, W. et.al., "Detecting and Mitigating Battery Charger and Inverter Aging," NUREG/CR-5051, August 1988.

6. TOMAN, G.J., "Inspection, Surveillance, and Monitoring of Electrical Equipment in Nuclear Power Plants. Vol. 2: Pressure Transmitters," NUREG/CR-4257, August 1986.

7. HASHEMIAN, H.M., et al, "Effect of Aging on Response Time of Nuclear Plant Pressure Sensors," NUREG/CR-5383. June 1989.

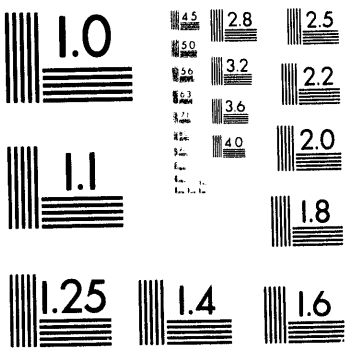
8. GEHL, A.C. AND HAGEN, E.W., "Aging Assessment of Reactor Instrumentation and Protection System Components, Phase 1," NUREG/CR-5700, July 1992.

9. JACOBUS, M.J., "Aging of Cables, Connections, and Electrical Penetration Assemblies Used in Nuclear Power Plants," NUREG/CR-5461, July, 1990.

10. HASHEMIAN, H.M., "Aging of Nuclear Plant Resistance Temperature Detectors," NUREG/CR-5560, June 1990.

11. LEE, B.S., et al., "Aging Assessment of Bistables and Switches in Nuclear Power Plants," NUREG/CR-5844, November 1992.

12. GLEASON, J.F., "Comprehensive Aging Assessment of Circuit Breakers and Relays, Phase II," February 1992.


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3

4 of 6

ROSEMOUNT TRANSMITTERS - SUPPLEMENT TO BULLETIN 90-01

Presented by Deirdre Spaulding, USNRC

May 5, 1993

IAEA Specialist's Meeting

Ageing, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability

HISTORY

In April 1989, the NRC issued Information Notice 89-42, "Failure of Rosemount Models 1153 and 1154 Transmitters," to alert the industry to a series of reported failures of these pressure and differential pressure transmitters manufactured by Rosemount Incorporated. Rosemount determined that the failure mode was due to a gradual loss of fill-oil from the sealed sensing module of the transmitter. On March 9, 1990, the NRC issued Bulletin 90-01, which requested that licensees promptly identify and take appropriate corrective action for Models 1153 series B and D, and Model 1154 transmitters manufactured by Rosemount that may be, or have the potential for leaking fill-oil. During the summer and fall of 1990, the Nuclear Management and Resources Council surveyed the industry to gather data on all installed Rosemount Model 1153 and 1154 transmitters and safety-related Model 1151 and 1152 transmitters at commercial nuclear facilities. NUMARC also requested data on all suspected or confirmed failures of Rosemount transmitters attributed to a loss of fill-oil from these same facilities. The NRC issued the Supplement to Bulletin 90-01 on December 22, 1992.

NRC STAFF ACTIONS

The NRC staff reviewed the Rosemount transmitter loss of fill-oil issue by analyzing data gathered from (1) licensee event reports, (2) the licensee's responses to NRC Bulletin 90-01, (3) technical information provided by Rosemount, (4) site visits, (5) NUMARC Report 91-02, "Summary Report of NUMARC Activities to Address Oil Loss in Rosemount Transmitters," and (6) numerous

meetings with representatives from the industry, NUMARC, and Rosemount. The NRC became concerned about this complex technical issue because the failure of the transmitter could occur and remain undetected while the transmitter was in service and could be a common mode failure. Documentation indicated that the transmitter failures resulted from a failure of a glass-to-metal seal inside the sensor which allowed fill fluid to leak out of the sensor at a very slow rate. When this condition occurs, the transmitter performance gradually deteriorates and may lead to failure.

The staff has reviewed licensee responses to NRC Bulletin 90-01 and concluded that the actions taken as a result of the bulletin helped to improve the safety of operating reactors by reducing the susceptibility to Rosemount transmitters due to a loss of fill-oil. This was accomplished mainly by prompting licensees to remove Rosemount transmitters that were installed in the reactor protection systems or engineered safety feature actuation systems that the manufacturer found to have a high failure fraction resulting from a susceptibility to a loss of fill-oil. The licensee also was to evaluate against appropriate operability acceptance criteria those transmitters that were suspected of exhibiting symptoms of a loss of fill-oil when reviewing the plant's historical records on the calibration of these transmitters. The licensees established enhanced surveillance programs by considering various diagnostic procedures including trending calibration data, trending operational data, reviewing transmitter performance for sluggish transient response, and conducting process noise analysis.

During the licensee response period to Bulletin 90-01, NUMARC surveyed all

utilities to collect data on all installed Rosemount Model 1153 and 1154 transmitters, and on Rosemount Model 1151 and 1152 transmitters installed in safety-related systems. The staff reviewed the data collected by NUMARC and two of the objectives were to evaluate surveillance issues regarding licensees responses in implementing the enhanced surveillance program requested by the staff in the bulletin, and to determine if any other insights could be drawn from this data. Brookhaven National Laboratory (BNL) assisted the staff in evaluating the data by assessing the failure rates for various types of transmitters by operating pressure, time in service, and suspect or nonsuspect lot classification. Brookhaven National Laboratory (BNL) provided the staff with the report, "Evaluation of Surveillance and Technical Issues Regarding Rosemount Pressure Transmitter Loss Fill-Oil Failures, "December 20, 1991. In addition, the staff considered the effects of the various failure rates on the potential for anticipated transients without scram (ATWS). The staff concluded that estimated unavailabilities and the associated impact on ATWS frequency could be very sensitive to changes in the transmitter failure rate.

In evaluating this issue, the staff confirmed a relationship between operating pressure, time-in-service, and failure rate. A high operating pressure was the most dominant factor leading to a loss of fill-oil.

With respect to time-in-service, it was seen that transmitters that had been in service for less than 60,000 psi-months, exhibited higher failure rates than transmitters that had been in service for more than 60,000 psi-months.

Transmitter lots were classified as suspect or nonsuspect. All suspect lots

as defined by Rosemount contained at least one confirmed failure and possibly more, depending on the size of the lot. If all other factors were assumed equal, suspect lots had higher failure rates than nonsuspect lots. However, when pressure application or time-in-service was considered, the classification by suspect or nonsuspect lot was of lesser importance.

Throughout this evaluation period, the staff found that the number of Model 1151 and Model 1152 transmitters which were confirmed as failing due to a loss of fill-oil, was very small given their operating experience, and therefore is sufficiently low to be of minimum concern.

The staff concern throughout the evaluation of this issue is the need to determine whether or not the Rosemount transmitter meets current criteria as a reliable component for which failures can be readily detected. General Design Criteria 21, "Protection System Reliability and Testability" in Appendix A to Part 50 of Title 10 of the Code of Federal Regulations requires the protection system to be designed with high functional reliability and with a capability to permit periodic testing of its functioning when the reactor is in operation. This requirement ensures that the licensee can readily detect failures of subcomponents and subsystems within the protection system and can readily detect loss of the subsystems within the protection system and can readily detect loss of the required protection system redundancy when it occurs.

In 10 CFR 50.55a(h), the NRC requires that protection systems meet the Institute of Electrical and Electronics Engineers Standard, "Criteria for

Protection Systems for Nuclear Power Generating Stations" , IEEE-279. In IEEE-279, the Standard states that means shall be provided for checking, with a high degree of confidence, the operational availability of each input sensor during operation. To achieve a high functional reliability, a transmitter must have a low probability of failure while it is operating. Furthermore, failures should be readily detectable, commensurate with the safety function while the transmitter is in operation.

Upon reviewing the analyses, evaluations, and historical data on the loss of fill-oil, the staff concludes that actions requested by the previous bulletin, 90-01 were not extensive enough to ensure compliance with the regulations requiring that the transmitters achieve the desired high functional reliability. Hence, the promulgation of the Supplement to Bulletin 90-01, putting forth the following licensee requested actions.

REQUESTED LICENSEE ACTIONS

All holders of operating licenses for nuclear power reactors have been requested to act upon two major action items.

The first action item requires that the licensee: review plant records and identify any Rosemount Model 1153 Series B, Model 1153 Series D, and Model 1154 transmitters manufactured before July 11, 1989, that are used or may be used in the future in either safety related systems or systems installed in accordance with 10 CFR 50.62 (the ATWS rule). Associated with this action is the responsibilty to:

a. Expeditiously replace, or monitor for the life of the transmitter on a monthly basis using an enhanced surveillance monitoring program for transmitters that have a normal operating pressure greater than 1500 psi and that are installed in reactor protection trip systems, ESF actuation systems or ATWS systems.

b. Replace or monitor for the life on a quarterly basis using an enhanced surveillance monitoring program, any transmitters that have a normal operating pressure greater than 1500 psi and that are used in safety related applications but are not installed in reactor protection trip systems, ESF actuation systems, or ATWS systems.

c. Replace or monitor using an enhanced surveillance monitoring program, until the transmitter reaches the appropriate psi-month threshold criterion, any transmitters that have a normal operating pressure greater than 500 psi and less than or equal to 1500 psi, that are installed in reactor protection trip systems, Esf actuation systems or ATWS systems.

The threshold criterion is 60,000 psi-months or 130,000 psi-months depending on the range code of the transmitter.

d. Replace or monitor, using an enhanced surveillance program until the transmitter reaches the appropriate psi-month threshold criterion recommended by Rosemount, any transmitters that have a normal operating pressure greater than 500 psi and less than or equal to 1500 psi and that are not installed in reactor protection trip systems, ESF actuation systems, or ATWS systems.

e. At licensee discretion, exclude from the enhanced surveillance program any transmitters that have a normal operating pressure greater than 500 psi and less than or equal to 1500 psi that have reached the appropriate psi-month threshold criterion recommended by Rosemount.

f. At licensee discretion, exclude from the enhanced surveillance program any transmitters that have a normal operating pressure less than or equal to 500 psi.

The second action item requires the licensee to; evaluate the enhanced surveillance monitoring program to ensure that the program provides measurement data with an accuracy range consistent with that needed for comparison with manufacturer drift data criteria for determining degradation caused by a loss of fill oil.

Additionally, the following reporting requirements are required from the licensees.

Reporting Requirements

Within 60 days following receipt of the Supplement to Bulletin 90-01, a response from the licensee containing the following information was required:

1. A statement as to whether or not the licensee will take the actions requested.
2. A list of the specific actions that the licensee will complete for

operating reactors, including justifications as appropriate, to meet action item one, as previously discussed in the the requested actions section.

3. The schedule for completing licensee actions to meet action item one of requested actions.

4. When completed, a statement confirming that the requested actions for operating reactors have been completed.

5. A statement identifying those actions requested by the NRC that the licensee is not taking and an evaluation which provides the bases for not taking the requested actions.

The NRC staff is engaged in an on-going process of reviewing the responses from the licensees as they are received.



ROSEMOUNT TRANSMITTERS SUPPLEMENT TO BULLETIN 90–01

Date: May 5, 1993
Presenter: D. Spaulding

SUPPLEMENT TO BULLETIN 90-01

- HISTORY
- NRC STAFF ACTIONS
- REQUESTED LICENSEE ACTIONS
- REPORTING REQUIREMENTS

HISTORY

April 21, 1989 - Information Notice (IN) 89-42, "Failure of Rosemount Models 1153 and 1154 Transmitters"

March 9, 1990 - Bulletin 90-01

Summer 1990 - NUMARC Surveyed the industry to gather data on all installed 1153 and 1154 transmitters and safety-related 1151 and 1152 transmitters

December 20, 1991 - BNL report "Evaluation of Surveillance and Technical Issues Regarding Rosemount Pressure Transmitter Loss of Fill-Oil Failures"

December 22, 1992 - Supplement to Bulletin 90-01

ACTIONS

Analyzed Data Gathered From Various Sources

- Licensee Event Reports

- Licensee Responses to NRC Bulletin 90-01

- Information Provided by Rosemount

- Nuclear Management and Resources Council (NUMARC) survey

- Brookhaven National Laboratory (BNL) data evaluation

Relationship Between:

Operating Pressure

Time-In-Service

Failure Rate

STAFF CONCERN

Need to determine whether or not transmitter meets current criteria as a reliable component for which failures can be readily detected

- General Design Criteria 21

- IEEE 279

REQUESTED ACTIONS

Non-Mature RPS/ESF/ATWS	**Replace or monitor with an enhanced surveillance program on a monthly basis**
Non-Mature Non-RPS/Non-ESF Non-ATWS	**Replace or monitor with an enhanced surveillance program on a quarterly basis**
Mature RPS/ESF/ATWS	**Replace or monitor with an enhanced surveillance program on a monthly basis**
Mature Non-RPS/Non-ESF Non-ATWS	**Replace or monitor with an enhanced surveillance program on a quarterly basis**

For operating pressure greater than 1500 psi

REQUESTED ACTIONS

Non-Mature RPS/ESF/ATWS	**(BWR) Replace or monitor with an enhanced surveillance program on a monthly basis (PWR) Replace or monitor with an enhanced surveillance program at intervals no greater than 24 months**
Non-Mature Non-RPS/Non-ESF/Non-ATWS	**Replace or monitor with an enhanced surveillance program at intervals no greater than 24 months**
Mature RPS/ESF/ATWS	**Enhanced surveillance program discretionary Maintain ability to detect failures**
Mature Non-RPS/Non-ESF/Non-ATWS	**Enhanced surveillance program discretionary Maintain ability to detect failures**

For operating pressure greater than 500 and less than or equal to 1500 psi

REQUESTED ACTIONS

Non-Mature	**Enhanced surveillance program discretionary**
RPS/ESF/ATWS	**Maintain ability to detect failures**
Non-Mature	**Enhanced surveillance program discretionary**
Non-RPS/Non-ESF	**Maintain ability to detect failures**
Non/ATWS	
Mature	**Enhanced surveillance program discretionary**
RPS/ESF/ATWS	**Maintain ability to detect failures**
Mature	**Enhanced surveillance program discretionary**
Non-RPS/Non-ESF/Non-ATWS	**Maintain ability to detect failures**

For operating pressure less than or equal to 500 psi

REPORTING REQUIREMENTS

Within 60 days:

A statement indicating whether licensee will take requested actions

A list of specific actions that licensee will complete

The schedule for completing licensee actions

A statement confirming that Requested Actions have been completed

SESSION 4

MODERNIZATION

Account of Requirements for Modernization in VPBER-600 Enhanced Safety Reactor Instrumentation and Control System Development

Regulatory Requirements for Replacement of Analog Systems With Digital Upgrades

Account of Requirements for Modernization in VPBER-600 Enhanced Safety Reactor Instrumentation and Control System Development

Shashkin S.L., Pobedonostsev A.B., Drumov V.V.,
OKBMechanical Engineering, Nizhny Novgorod,
Russia
Chudin A.G.
Ministry of Nuclear Energy of Russian Federation,
Moscow, Russia

IAEA Specialists Meeting
"Experience in Ageing, Maintenance and Modernization of
Instrumentation and Control Systems
for Improving NPP Availability"
May 5-7, 1993, Rockville, Maryland, U.S.A.

Account of Requirements for Modernization in VPBER-600 Enhanced Safety Reactor Instrumentation and Control System Development

Shashkin S.L., Pobedonostsev A.B., Drumov V.V.,
OKBMechanical Engineering, Nizhny Novgorod, Russia
Chudin A.G.
Ministry of Nuclear Energy of Russian Federation, Moscow, Russia

Abstract

Nuclear power plant (NPP) with VPBER-600 reactor is a station of new generation. The specified term of reactor plant operation is 60 years and taking into account that the proposed term of starting the first power unit is on the turn of centuries one can definitely state that for Russia conditions VPBER-600 is a plant of 21.century. Such far removed term for NPP now in the stage of development as it can seem does not not put the problems of modernization as first order tasks. But "...who does not think about future lives in the past". It is that NPP instrumentation and control (I&C) systems are in the most degree subjected to the influence of factors which favor their modifications. These factors can be arbitrarily divided into two groups:

- inner factors, i.e.changes (failures, aging, etc) in I&C components as well as changes dictated by technologial reasons (change of equipment composition, control algorithms, operation modes);

- outer factors, i.e.intensive development of information technologies and rapid improvement of electronic components.

Arbitrarily,in the capacity of some stabilizing factors,a constant of its kind, the requirements can be accepted for I&Cs with account of safety codes.

The project of I&C for NPP with VPBER-600 is developed with account of above circumstances. Such approach somewhat enlarges the definition "modernization" which is conventionally interpreted as change, improvement meeting modern requirements, as of something obsolete and/or failured.

For new projects of NPP I&C systems to which number, without doubt, VPBER-600 refers it is proposed to extend the term "modernization" to project stage also. This is actual with account of real terms of designing new generation plants requiring large volume of R&D.

Besides, with account of NPPs operation and age factors of I&C components it is necessary to account also tor conventional (traditional) interpretation of the term "modernization".

In combination, I&C system modernization tasks for VPBER-600 are determined as specifications for the system which were formulated already on initial conceptual studies of the project (See Fig.1). Let us consider them in more detail.

1. Requirements to Modernization of I&C on Design Stage

A set of requirements to modernization of VPBER-600 new generation plant during design stage forsees the possibility of the system change and making improvements - control algorithms which should be intoduced into the project subsequent to the results of development of equipment, specifying the composition and operation modes of NPP. These requirements are oriented, in general, on the desingers of the system, on software - hardware, means and technology of I&C designing "Simultaneously, these requirements and their realization already on initial stages of the project have real influence on solutions which are accepted and laid into the basis of the project.

The main engineering solutions assuring the possibility of realization of improvements on design stages are connected with formulation of requirements for wide use of digital control means, principles of block-module hardeware shaping, use of universal (non-standard) interfaces and high level languages. These are traditional requirements to I&C. The main task which is solved by the set of requirements is the assurance of possibility of realization of improvements by changing software without changing hardware in combination with capabilities offered by decentralized I&C grid structures.

Another set of requirements is oriented to the choice of I&C system structure connected with decomposition of the system into control complexes oriented on control object technological system.

Together with requirements concerning the possibility of partial change of I&C system structure in the framework of hierarchical and decentralized system architecture and "autonomy" of controlling safety systems in the requirements are formulated in the project for realization of reserves on computing capabilities, number of in-outputs, and arrangement of additional hardware and cables. Not less than 10% reserve is envisaged for the enumerated components.

For facilitating the changes in the system on the design stage the task is set to use on different stages of control and monitoring technical means' lines unified in respect to software and hardware.

Among the requirements to I&C in NPP incorporating VPBER-600 the task is formulated for compilation and realization of a kind of "standard" of software independent I&C functioning description. Simultaneously, for the stages of detailed desinging in the framework of the project an attempt is made to realize such approach for designing which would allow to assure the unity of software-hardware means of desinging and operation, an ideal result of which would be the transfer of carrier information about software means - from designer to NPP without recompilation, debugging and other procedures concerning the software.

The corresponding requirements envisage obligatory on plant verification of main solutions concering I&C.

As already noted, a set of requirements enumerated in this Section is assigned to ensure making inprovements in I&C project on design and commissioning stages before putting NPP with VPBER-600 into commercial operation.

2. Requirements to I&C Modernization on Operation Stage

The requirements to modernization of I&C system are directed towards assuring the possibility of the system change during operation for realization of the following tasks:

- replenishment and replacement of technical means having limited lifetime;

- improvement of I&C due to change in operation procedures, modernization of operation and control technology;

- replacement of failed and outdated equipment and electronic components of I&C.

Reqirements to modernization of I&C for the time of NPP with VPBER-600 operation are directed towards the alleviation of operation conditions, planning of running replacements, repairs and reconstruction of separate elements and replacement of entire system as well.

For assuring replenishment of technical means having limited lifetime the following is envisaged:

* choice of I&C equipment resources to the cycles of I&C object functioning ; for example, divisible by the transitions between reactor refuellings; this circumstance is specially actual for control system sensors placed inside containment and quard vessel;

* changing non-detachable cable connections for detachable ones; unification of signals' input/output of sensors and secondary apparaturs;

* realization of metrological service by NPP operating personnel in operating plant or in rigs and fixtures.

For realization of improvements due to change of operation procedures and equipment composition with the aim of optimization of technico-economical indexes and introduction into the operation praxis of novations the approach is envisaged analogous to the approach considered in Section 1.

Besides, it is envisaged that I&C system program and technical complex, its technical and structural realization must provide for stage-by-stage realization by:

* changing separate instruments and blocks in cabinets for new ones having large functional capabilities without variation of cabinet design, inside wiring and external interfaces;

* development (addition) of the systems composition, modernization of its structure, arrangement of additional equipment rooms reserved for this end.

For realization of basic I&C systems structure necessitated by failures and aging processes technical requirements are developed which take into account many years unique experience of successful operation of control systems in nuclear power plants of "Russia", "Arctica" and other ice-breakers, where total operation time of the control systems exceeds 100 reactor years.

It is envisaged that calculation for spares should be done according to techniques having experimental verification and taking into account statistical data concerning aging and failures.

The ordering of spares should be done for the entire service life and taking into account that element base of I&C has limited production time a stock of spares should be provoded.

It is envisaged also that aiming at lowering the possibility of undetected failures the hardware diagnostics must be done including interchangeable typical replacement element.

For planning future reconstruction and doing statistical records the maintenance of automated data bases for hardware failures and replacements is envisaged.

3. Conclusions

The questions of I&C system of NPP with new generation VPBER-600 are defined as specifications and cover both design stage and period of coming operation.

These requirements are formulated with account of positive operation experience of analogous and prototype systems and are called to account for the peculiarities of creation and operation of I&C systems for NPP.

All requirements accounting for the problems of modernization in enlarged wording with covering design phase find steady and purposeful realization in the project of NPP I&C for enhanced safety VPBER-600 reactor.

Proposals for Future

In many aspects the tasks of modernization which the I&C designer must solve are determined by correct and error-free choice of software-hardware having steady line of development, succession of various generations of the means. This problem in turn, is closely associated with multi-profileness of supplier and availability of wide I&C realization markets what is absolute stimulus for "suscessive" modernization and facilitating introduction of innovations concerning I&C for NPP

Thus, the task of formulating technical requirements accounting for I&C modernization already on the stage of NPP with VPBER-600 control system designing in its complexity and importance is near to the tasks which one has to solve at scientific-engineering prognostication.

Therefore, in conclusion of the report for generalization of I&C development experience, consideration of promising solutions and prognostic estimation concerning I&C development for NPP it is possible to recommend a series of specialists' meeting under IAEA auspicies for prognostication of I&C development for NPP. The following questions are proposed for discussion:

- procedures for compilation prognoses, generalization of experience and statistics, promissing development trends, international standards applicability estimation, international cooperation.

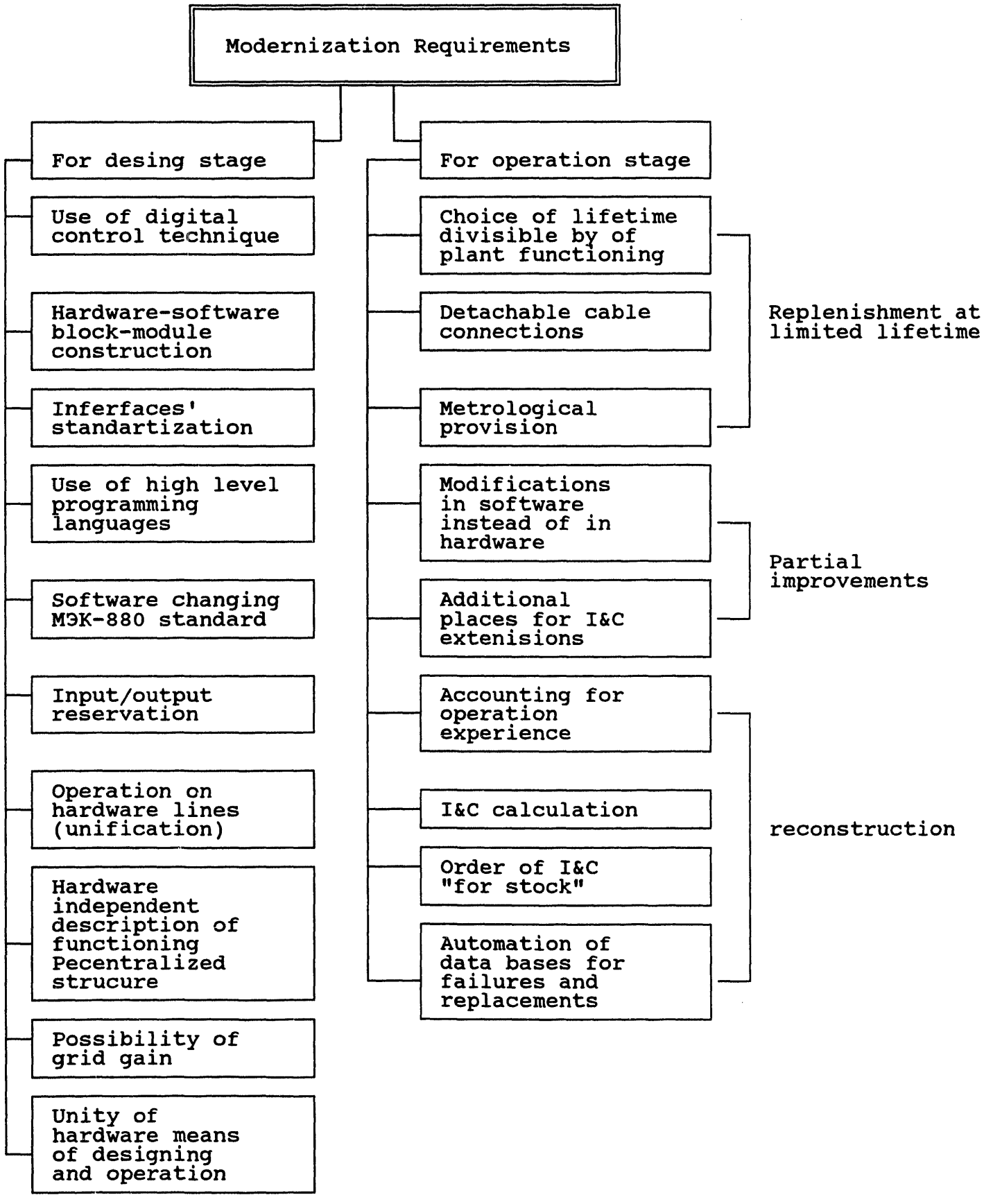


Fig.1 Structure of Requirements for Modernization of I&C system for New Generation NPP with VPBER-600

REGULATORY REQUIREMENTS FOR REPLACEMENT OF ANALOG SYSTEMS WITH DIGITAL UPGRADES

Paul J. Loeser

NRC, USA

OPERATING PLANTS ANALOG TO DIGITAL RETROFITS

- The following is a sample of plants which have implemented analog to digital replacement under 10 CFR 50.59:

Haddam Neck	-	full RPS/ESF changeout
Peach Bottom	-	Signal conditioning (processing) portion of the RPS
Zion	-	Signal conditioning (processing) portion of the RPS/ESF

- We believe a number of other plants are performing similar modifications of varying magnitudes under 10 CFR 50.59

- The following is a sample of plants that have performed analog to digital modifications and requested staff review:

Watts Bar	-	RTD Bypass
Sequoyah	-	RPS/ESF signal conditioning (processing)
Turkey Point	-	EDG sequencer and RTD bypass
Haddam Neck	-	Aux. Feed controller
South Texas	-	Qualified Safety Parameter Display System
ANO2	-	Core Protection Calculator
Prairie Island	-	EDG sequencer

WHY ARE PLANTS CONVERTING FROM ANALOG TO DIGITAL SYSTEMS

- Analog systems are experiencing excessive drift because of aging
- Vendors are discontinuing analog product lines
- Difficulty in obtaining product support for existing systems, i.e., replacement components and service
- Some plants want to take advantage of digital system flexibility

ADVANTAGES OF DIGITAL I&C UPGRADES

- Replace Aging I&C Systems
- Improve Surveillance Capabilities
- Improve Information for the Operator

SAFETY CONCERNS

THE PRINCIPAL SAFETY CONCERN IS THE POTENTIAL FOR UNDESIRABLE AND UNPREDICTABLE EFFECTS ON DIGITAL SAFETY EQUIPMENT PERFORMANCE AS A RESULT OF:

- **PLANT ENVIRONMENT DURING NORMAL OPERATION, ACCIDENTS, AND POST-ACCIDENT CONDITIONS**

- **SUSCEPTIBILITY TO THE AMBIENT EMI/RF ENVIRONMENT, OR BY EMISSIONS FROM INSTALLED EQUIPMENT**

10 C.F.R. 50.59

(1) The holder of a license authorizing operation of a production of utilizing facility may

(i) make changes in the facility as described in the safety analysis report,
(ii) make changes in the procedures as described in the safety analysis report, and
(iii) conduct tests or experiments not described in the safety analysis report,

without prior Commission approval, unless the proposed change, test or experiment involves a change in the technical specifications incorporated in the license of an unreviewed safety question.

(2) A proposed change, test or experiment shall be deemed to involve an unreviewed safety question

(i) if the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report may be increased; or
(ii) if a possibility for an accident of malfunction of a different type than any evaluated previously in the safety analysis may be created; or
(iii) if the margin of safety as defined in the basis for any technical specification is reduced.

PROBLEMS INHERENT IN DIGITAL SYSTEMS

- Due to the increased complexity of computer system tasks it is much more difficult to verify correct task performance under all possible circumstances.

- Due to the increased complexity of computer system software it is much more difficult to verify freedom from programming error.

- Computer systems hardware uses a large variety of very small but rather complex components whose failure behavior is difficult to detect and localize.

- Computers normally take advantage of some standard tools such as their operating systems or compilers, both during on-line operation or during development; it is more or less impossible to get such tools error free.

- Due to the complexity of computer system software it is virtually impossible to demonstrate high reliability of a software system.

TECHNICAL CONCERNS WITH DIGITAL SYSTEMS

- Common Mode Failure by Software: Similar or Identical software running on identical hardware in multiple trains of redundant instrumentation.

- Sensitivity of digital based systems to plant Environments:
  - EMI
  - RFI
  - Temperature
  - Power quality
  - Grounding

- Effect on Safety Margins through input consolidation.

- Possible lack of On-site experience
  - troubleshooting
  - problem recognition
  - assimilation in plant

- Commercial Dedication

PROPOSED STAFF POSITION

- All Digital Upgrades will require an 10CFR 50.59 Evaluation.

- Staff expects that items above the threshold will fail the 50.59 evaluation, except in unusual circumstances.

- Items below the threshold may or may not pass 50.59 evaluation, based upon merits of case.

THRESHOLD SAMPLES

Above:
(Prior NRC Approval probably required)

- Reactor Trip System
- ESF Actuation/Control System
- PAM's (CAT 1)

- Staff Review Process Streamlined
  - Topical Report Approval
  - Previously Approved System

Below:
(Standard 50.59 procedure. Approval may or may not be required.)

- Non-Safety Systems
- Reactor Building Ventilation System with Analog Backup
- Modification to previously approved Digital system
- PAM's (CAT 3)
- Balance of Plant Control Channels (e.g.) water tank level and Feedwater Control

NRC STAFF REVIEW APPROACH

- Detailed review of system design and Verification and Validation Program.
- Review of information on the software and hardware history.
- Review of the specific nuclear plant applications.
- Specific and detailed review of specific V&V performed on software, including comparison to ANSI/IEEE-ANS-7-4.3.2-1982.
- Thread audit of sample plant parameters.
- Software and Hardware systems review for timing or Software/Hardware interface problems.

FUTURE ACTIVITIES

- Staff is reviewing NUMARC Proposal which states all upgrades should be done via 50.59 methodology

- Staff is preparing response to NUMARC proposal with threshold

- Meetings with NUMARC and EPRI will continue through 1993.

TECHNICAL CONCERNS WITH DIGITAL SYSTEMS

- Common Mode Failure by Software: Similar or Identical software running on identical hardware in multiple trains of redundant instrumentation.

- Sensitivity of digital based systems to plant Environments:
  - EMI
  - RFI
  - Temperature
  - Power quality
  - Grounding

- Effect on Safety Margins through input consolidation.

- Possible lack of On-site experience
  - troubleshooting
  - problem recognition
  - assimilation in plant

- Commercial Dedication

PROPOSED STAFF POSITION

- All Digital Upgrades will require an 10CFR 50.59 Evaluation.

- Staff expects that items above the threshold will fail the 50.59 evaluation, except in unusual circumstances.

- Items below the threshold may or may not pass 50.59 evaluation, based upon merits of case.

THRESHOLD SAMPLES

Above:
(Prior NRC Approval probably required)

- Reactor Trip System
- ESF Actuation/Control System
- PAM's (CAT 1)

- Staff Review Process Streamlined
  - Topical Report Approval
  - Previously Approved System

Below:
(Standard 50.59 procedure. Approval may or may not be required.)

- Non-Safety Systems
- Reactor Building Ventilation System with Analog Backup
- Modification to previously approved Digital system
- PAM's (CAT 3)
- Balance of Plant Control Channels (e.g.) water tank level and Feedwater Control

NRC STAFF REVIEW APPROACH

- Detailed review of system design and Verification and Validation Program.

- Review of information on the software and hardware history.

- Review of the specific nuclear plant applications.

- Specific and detailed review of specific V&V performed on software, including comparison to ANSI/IEEE-ANS-7-4.3.2-1982.

- Thread audit of sample plant parameters.

- Software and Hardware systems review for timing or Software/Hardware interface problems.

FUTURE ACTIVITIES

- Staff is reviewing NUMARC Proposal which states all upgrades should be done via 50.59 methodology

- Staff is preparing response to NUMARC proposal with threshold

- Meetings with NUMARC and EPRI will continue through 1993.

SESSION 5

MODERNIZATION

Addressing the Susceptibility of Digital Systems to Electromagnetic Interference

Life Extension Activities and Modernization Strategies for Instrumentation and Control Systems of Research and Power Reactors in India

Regulatory Perspective on Digital Instrumentation and Control Systems for Future Advanced Nuclear Power Plants

Instrumentation and Controls Division

ADDRESSING THE SUSCEPTIBILITY OF DIGITAL SYSTEMS TO ELECTROMAGNETIC INTERFERENCE

Paul D. Ewing and Kofi Korsah

Christina Antonescu*

Submitted for presentation at the
IAEA Specialists Meeting
on
Experience in Ageing, Maintenance
and Modernization of Instrumentation
and Control Systems for Improving
Nuclear Power Plant Availability
May 5-7, 1993
Ramada Inn at Congressional Park
Rockville, Maryland

Prepared for
U.S. Nuclear Regulatory Commission
Washington, DC 20555
under Interagency Agreement No. DOE 1886-8195-1L

NRC FIN L1951

"The submitted manuscript has been authored by a contractor of the U.S. Government under contract No. DE-AC05-84OR21400. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes."

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6285
managed by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-84OR21400

*Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Rockville, Maryland.

ADDRESSING THE SUSCEPTIBILITY OF DIGITAL SYSTEMS TO ELECTROMAGNETIC INTERFERENCE[1]

Paul D. Ewing and Kofi Korsah
Instrumentation and Controls Division
Oak Ridge National Laboratory
Oak Ridge, Tennessee

Christina Antonescu
Office of Nuclear Regulatory Research
Nuclear Regulatory Commission
Rockville, Maryland

"The submitted manuscript has been authored by a contractor of the U.S. Government under contract No. DE-AC05-84OR21400. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes."

[1]Research sponsored by the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, under Interagency Agreement No. 1886-8195-1L, and performed at Oak Ridge National Laboratory, managed by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under contract DE-AC05-84OR21400.

The submitted manuscript has been authored by a contractor of the U.S. Government under contract No. DE-AC05-84OR21400. Accordingly the U.S. Government retains a nonexclusive royalty-free license to publish or reproduce the published form of this contribution or allow others to do so, for U.S. Government purposes.

ABSTRACT

This paper discusses the development of the technical basis for acceptance criteria applicable to the immunization of digital systems against electromagnetic interference (EMI). The work is sponsored by the U.S. Nuclear Regulatory Commission and stems from the safety-related issues that need to be addressed as a result of the application of digital instrumentation and control systems in nuclear power plants. Designers of digital circuits are incorporating increasingly higher clock frequencies and lower logic level voltages, thereby leading to potentially greater susceptibility of spurious interference being misinterpreted as legitimate logic. Development of the technical basis for acceptance criteria to apply to these digital systems centers around establishing good engineering practices to ensure that sufficient levels of electromagnetic compatibility (EMC) are maintained between the nuclear power plant's electronic and electromechanical systems. First, good EMC design and installation practices are needed to control the emissions from interference sources and thereby their impact on other nearby circuits and systems. Second, a verification and validation (V&V) program is needed to outline the EMI tests to be performed, the associated test methods to be followed, and adequate acceptance criteria to ensure that the circuit or system under test meets the recommended guidelines. V&V should be followed by periodic maintenance to assess whether the recommended EMI control practices continue to be adhered to as part of the routine operation of the nuclear power plant. By following these steps, the probability of encountering safety-related instrumentation susceptibility attributable to EMI will be greatly reduced.

1. INTRODUCTION

Instrumentation and control (I&C) systems in advanced nuclear reactors are expected to make extensive use of digital equipment and will be significantly different from the current analog-based designs. Digital signals can carry an increased amount of information as opposed to analog signals, and digital equipment generally has a much faster information processing capability than its analog counterpart. Thus, the widespread use of digital I&C systems in the design of monitoring, control, and protection systems is inevitable and, when properly used, can be expected to improve both safety and performance in nuclear power plants.

Several U.S. nuclear power plants have replaced selected analog systems with digital systems; however, the complete replacement of all analog systems in a plant has not been performed. With the limited operational experience of the nuclear industry with digital technology, the full extent of the susceptibility of digital I&C systems to electromagnetic interference (EMI) is unknown and hence of concern to the U.S. Nuclear Regulatory Commission (NRC). This concern is safety-related and, therefore, is consistent with the issues cited in Subpart B of Part 52 of Title 10 of the Code of Federal Regulations (10 CFR Part 52). This issue has led the NRC Office of Nuclear Regulatory Research to sponsor a research program for developing the technical basis for acceptance criteria specific to the electromagnetic compatibility (EMC) of digital I&C systems.

2. OVERVIEW OF TECHNICAL BASIS

Digital technology is constantly evolving, and manufacturers of digital systems are incorporating increasingly higher clock frequencies, faster operating speeds, and lower logic-level voltages into their designs. Recent experiences (Hyne 1984; Oranchak et al. 1980; Hanson 1989) have shown that industrial systems using the faster digital 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. This issue has led NRC to the conclusion that acceptance criteria are needed to ensure that EMI problems are minimized in nuclear power plants. The need for research was cited in Section 9.d of Enclosure 1 (List of Research Needs that Require Early Attention) to the NRC Policy Issue SECY-91-273, "Review of Vendors' Test Programs to Support the Design Certification of Passive Light Water Reactors."

Oak Ridge National Laboratory's (ORNL's) assistance in establishing the technical basis for acceptance criteria to address the susceptibility of digital systems against EMI has thus far focused on two primary areas: EMC practices and EMI verification and validation (V&V) techniques. The development effort first concentrated on EMC design and installation practices to ensure operational safety in equipment and then on EMI verification techniques to verify that the EMC practices do indeed achieve their intended purpose. A third area, surge-withstand capability (SWC), is also being investigated to ensure that digital I&C systems can withstand the transients typically encountered in the nuclear power plant environment. However, the SWC investigation is still in the preliminary stage and so will not be discussed in this paper. The end result will be recommendations for acceptance criteria intended to help the NRC staff establish the practices and techniques acceptable for complying with NRC regulations.

For maximum benefit, acceptance criteria should first concentrate on the establishment of good engineering practices that will ensure that sufficient levels of EMC are maintained between the nuclear power plant's electronic and electromechanical systems. The goal here is to reduce the impact of interference sources on nearby circuits and systems. Second, acceptance criteria should emphasize the importance of implementing well-founded V&V techniques to demonstrate that the engineering practices used are adequate to meet the desired design criteria. These techniques should center around an EMI V&V program consisting of test criteria, their associated test methods, and adequate acceptance criteria. With nuclear power plants' incorporation of good EMC practices, followed up by EMI V&V, the probability of encountering safety-related problems associated with EMI should be greatly reduced.

The research effort began with reviewing the EMI-related guides and standards currently in widespread use for their applicability to digital systems. Also, a literature search was conducted to ensure that all relevant information was included in the process. The ORNL investigators found that the Institute of Electrical and Electronics Engineers, Inc. (IEEE) Standard 1050-1989, *Guide for Instrumentation and Control Equipment Grounding in Generating Stations*—for the most part—does an adequate job of specifying EMC design and installation practices that are applicable to the nuclear power plant environment. However, after uncovering some anomalies, exceptions were taken to portions of IEEE Std. 1050-1989. Because the U.S. military branches regularly incorporate digital systems into their hardware, Military Standard (MIL-STD)-461C, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*, and MIL-STD-462, *Measurement of Electromagnetic Interference Characteristics*, were found to be reasonable points from which to begin an evaluation of relevant test criteria and methods.

3. EMC DESIGN AND INSTALLATION PRACTICES

It is the opinion of the authors that the technical basis for EMC design and installation practices should be founded on those practices outlined in IEEE Std. 1050-1989. This standard was developed to provide guidance specific to a power generating plant for the design of grounding systems for I&C equipment. This standard was sponsored by the Energy Development and Power Generation Committee of the IEEE Power Engineering Society and approved by the IEEE Standards Board on February 2, 1989. It should be noted that the terms *standard* and *guide* are used interchangeably in IEEE Std. 1050-1989 and *standard* does not imply that the practices are to be required, as in its usual connotation.

3.1 Review of IEEE Std. 1050-1989

IEEE Std. 1050-1989 comprises eight sections, and the applicable technical content is contained primarily in Section 4 (**Design Considerations for Electrical Noise Minimization**), Section 5 (**Grounding**), and Section 6 (**Typical Grounding Requirements for Generating Station Applications**). Ancillary information is contained in Sections 1 and 2 (**Scope and Introduction**), Section 3 (**Definitions**), Section 7 (**Testing**), and Section 8 (**Bibliography**). IEEE Std. 1050-1989 is comprehensive in that it covers both the theoretical and practical aspects of grounding and EMC. Consequently, it can provide useful guidance to design engineers who lack an extensive background in grounding and noise-minimization techniques. The authors of the guide do a thorough job of describing EMI in the power generating plant environment.

IEEE Std. 1050-1989 is directed specifically toward grounding and noise-minimization techniques for I&C systems in a generating station environment. Section 4 covers the gamut of possible interference sources and the mechanisms by which noise can couple into equipment and systems. Section 5 gives the reader background information on the fundamentals of a grounding system, and Section 6 outlines the problems associated with designing typical grounding systems for the power plant environment. Also included are references to practices specific to the treatment of digital systems, which is of special concern to NRC. In particular, Section 6.6 addresses the grounding of control circuits on the basis of their susceptibility to EMI. The grounding and shielding practices for digital systems are described, along with the rationale used in their selection.

3.2 Complementary Documents

IEEE Std. 1050-1989 is intended to be complementary to and complemented by IEEE Std. 518-1982, *IEEE Guide for the Installation of Electrical Equipment to Minimize Noise Inputs to Controllers from External Sources*, and IEEE Std. 665-1987, *IEEE Guide for Generating Station Grounding*. These guides are referenced throughout IEEE Std. 1050-1989. Like IEEE Std. 1050-1989, IEEE Std. 665-1987 was also sponsored by the Power Generation Committee of the IEEE Power Engineering Society and identifies the grounding practices that have been generally accepted by the electric utility industry and provides guidance in designing a safe and effective grounding system. It is particularly thorough in its treatment of electrical bonding. Sponsored by the Industrial Control Committee of the IEEE Industrial Applications Society, IEEE Std. 518-1982 provides guidance for installing controllers and control systems to ensure proper operation in their intended environment. In addition, the guide thoroughly covers shielding, grounding, and bonding techniques used to minimize noise on signal cables.

IEEE Std. 518-1982 and IEEE Std. 665-1987 offer even greater detail and more effective explanations than does IEEE Std. 1050-1989 on some topics. For example, Sections 4.3.3 and 5.4 of IEEE Std. 1050-1989 describe the grounding requirements for signal cable shields in a somewhat incomplete style, whereas Section 4.4 on page 64 of IEEE Std. 518-1982 explains this subject matter more effectively. Also, the treatment of bonding (i.e., the interconnection of conductive parts so as to maintain a common electrical potential) is not concise in IEEE Std. 1050-1989; references to bonding in the discussions on grounding systems are vague and lack sufficient detail. Fortunately, Section 5.2 of IEEE Std. 665-1987 covers the subject in considerably greater detail.

3.3 Findings on IEEE Std. 1050-1989

The ORNL investigators found that IEEE Std. 1050-1989—for the most part—is accurate in its treatment of EMC design and installation practices and applicable to the nuclear power plant environment. Some exceptions have been taken, and these will be reviewed thoroughly before final recommendations are made. Several enhancements have also been suggested to improve the understanding and usefulness of IEEE Std. 1050-1989. The enhancements are meant to be helpful but are by no means necessary. The particulars of the exceptions and enhancements will be discussed in NUREG/CR-5941 (Ewing and Korsah), which will cover the activities of the entire development effort and is scheduled to be published in June 1993. Associated guides, like IEEE Std. 518-1982 and IEEE Std. 665-1987, may also be helpful but should be used only in a manner consistent with acceptance criteria based on IEEE Std.1050-1989.

4. EMI VERIFICATION AND VALIDATION

It is the opinion of the authors that MIL-STD-461C, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*, and MIL-STD-462, *Measurement of Electromagnetic Interference Characteristics*, are applicable to the needs of the nuclear industry. MIL-STD-461C and -462 were developed for use by U.S. Department of Defense agencies to evaluate electromagnetic compatibility. Applying to both equipment designs and procurement specifications, the purpose of the standards is to ensure that equipment and subsystems are compatible with their intended electromagnetic operating environment and that EMI effects are considered early in the design process.

4.1 Review of MIL-STDS

MIL-STD-461 and -462, first issued in 1967, were intended to consolidate the requirements and test methods for the Army, the Navy, and the Air Force. The tri-services have since revised MIL-STD-461 such that it has become three separate documents under a single cover. The first two revisions, MIL-STD-461A and MIL-STD-461B, were issued on August 1, 1968, and April 1, 1980, respectively. They focus on establishing separate test requirements for each military service branch. The third and most recent revision was released on August 4, 1986, as MIL-STD-461C. This revision updated the standard to include electromagnetic pulse (EMP) requirements and changed the test limits for some existing requirements.

MIL-STD-462 has also been updated. Because each of the service branches adopted separate test requirements, modifications of the MIL-STD-462 test methods soon followed. To date, the

original version has been superseded by six "Notices" designed to modify MIL-STD-462 to the unique requirements of the Army, the Navy, and the Air Force. Notices 1 and 2 were released by the Air Force on August 1, 1968, and May 1, 1970, respectively. Notice 1 corrected grammatical errors and modified the structure of the document. Notice 2 made changes to some of the test procedures and redefined the applicability of others. Notice 3 was released on February 9, 1971, by the Army as a complete, stand-alone document to meet their requirements. Notice 4 was released by the Navy on April 1, 1980, to add a test method for evaluating the susceptibility of equipment to common-mode currents. The most recent releases were issued as Notice 5 on August 4, 1986, for the Navy and Notice 6 on October 15, 1987, for the Air Force. Notices 5 and 6 include the new EMP test methods, along with changes to existing test methods.

MIL-STD-461C establishes the emission and susceptibility requirements for electronic, electrical, and electromechanical equipment and subsystems. The standard ensures that control of both conducted and radiated interference are addressed over the frequency range 30 Hz to 40 GHz. It also provides a basis for evaluating the electromagnetic characteristics of equipment and subsystems by setting operational test limits. The requirements of MIL-STD-461C are typically applicable only as specified in the contracting agreement between a private enterprise and the government. MIL-STD-462 establishes the procedures to be followed in making test measurements to determine the electromagnetic characteristics of the equipment or subsystem under test. MIL-STD-462 also specifies the test equipment, setup, and grounding configuration requirements to ensure meaningful and repeatable test data.

Unless explicitly stated otherwise, the applicability of the MIL-STD-461C test requirements depends on the class designation assigned to the equipment or subsystem under review. MIL-STD-461C consists of 10 parts that describe the requirements for different classes of equipment and subsystems according to their mission, platform, and intended environment. Part 1 of MIL-STD-461C establishes the general documentation and design requirements, and Parts 2 through 6 cover the requirements for equipment and subsystems installed in critical areas. Parts 7 through 10 cover support and miscellaneous general-purpose equipment. The equipment and subsystem class designations and their applicable parts in MIL-STD-461C are shown in Table I.

The MIL-STD-461C test requirements are specified by alpha-numeric codes, as shown in Table II. The first designation declares the requirement as either radiated (R) or conducted (C) and the second designation specifies whether it covers emissions (E) or susceptibility (S). A unique method (UM) assignment is given to requirements that do not fall into these predefined designations. The alphabetic notation is followed by a numbering system that is specific to the particular test requirement. The test methods corresponding to the MIL-STD-461C requirements are described in MIL-STD-462 and are designated by the same alpha-numeric codes.

4.2 Findings on Test Requirements and Test Methods

MIL-STD-461C and -462 were developed as measures to rate the required electromagnetic compatibility of equipment and subsystems according to their intended electromagnetic environments. The standards have been used successfully by the military for many years and are commonly referenced in commercial applications as well. As related to the needs of NRC, the scope of the ORNL development effort has focused on only the *susceptibility* test requirements in MIL-STD-461C and their associated MIL-STD-462 test methods, shown in Table III.

Table I. MIL-STD-461C equipment and subsystem classes vs applicable parts

Class	Description	Applicable parts
A	Equipment and subsystems which must operate compatibly when installed in critical areas, such as the following platforms and installations:	
	A1 Aircraft (including associated ground support equipment)	2
	A2 Spacecraft and launch vehicles (including associated ground equipment)	3
	A3 Ground facilities (fixed and mobile including tracked and wheeled vehicles)	4
	A4 Surface ships	5
	A5 Submarines	6
B	Equipment and subsystems which support the Class A equipment and subsystems but will not be physically located in critical ground areas. Examples are electronic shop maintenance and test equipment used in noncritical areas, theodolites, navaids, and similar equipment used in isolated areas.	7
C	Miscellaneous general purpose equipment and subsystems not usually associated with a specific platform or installation, such as the following specific items:	
	C1 Tactical and special purpose vehicles and engine-driven equipment	8
	C2 Engine generators and associated components, uninterruptible power sets and mobile electric power equipment supplying power to or used in critical areas	9
	C3 Commercial electrical and electromechanical equipment	10

Some of the MIL-STD-461C susceptibility test requirements were found to be directly applicable to digital equipment. Tabular information characterizing the applicability of the MIL-STD-461C test requirements versus equipment and subsystems is available in two formats, according to the different classes of equipment and subsystems. Data entries are sometimes presented in tables that compare the applicability of the test requirements to an entire class of equipment or subsystems. Conversely, the data are sometimes tabulated in a manner that compares the applicability of the test requirements to specific types of equipment within a class. For the sake of this research effort, the second format proved to be the more useful because "digital equipment" was one of the types of equipment being compared to the requirements.

The information in MIL-STD-461C specifically pertinent to the susceptibility test requirements for digital equipment can be extracted and compiled for four classes of equipment and subsystems: platforms for aircraft (A1), ground facilities (A3), surface ships (A4), and submarines (A5). Although the resemblance of these platforms to a nuclear power plant is not immediately apparent, a comparison of their test requirements gives some insight into the commonality of specific test requirements for digital equipment.

Table IV summarizes the susceptibility requirements in MIL-STD-461C that apply to particular classes of digital equipment. The entries in the table denote the relationship between the classes and the requirements. Depending on the type of entry, the extent to which any given

Table II. MIL-STD-461C emission and susceptibility requirements

Requirement*	Description
CE01	Conducted emissions, power and interconnecting leads, <15 kHz
CE03	Conducted emissions, power and interconnecting leads, 0.015 to 50 MHz
CE06	Conducted emissions, antenna terminals, 10 kHz to 26 GHz
CE07	Conducted emissions, power leads, spikes, time domain
CS01	Conducted susceptibility, power leads, 30 Hz to 50 kHz
CS02	Conducted susceptibility, power and control leads, 0.05 to 400 MHz
CS03	Intermodulation, 15 kHz to 10 GHz
CS04	Rejection of undesired signals, 30 Hz to 20 GHz
CS05	Cross-modulation, 30 Hz to 20 GHz
CS06	Conducted susceptibility, spikes, power leads
CS07	Conducted susceptibility, squelch circuits
CS09	Conducted susceptibility, structure (common mode) current, 60 Hz to 100 kHz
CS10	Conducted susceptibility, damped sinusoidal transients, pins and terminals, 10 kHz to 100 MHz
CS11	Conducted susceptibility, damped sinusoidal transients, cables, 10 kHz to 100 MHz
RE01	Radiated emissions, magnetic field, 0.03 to 50 kHz
RE02	Radiated emissions, electric field, 14 kHz to 10 GHz
RE03	Radiated emissions, spurious and harmonics, radiated technique
RS01	Radiated susceptibility, magnetic field, 0.03 to 50 kHz
RS02	Radiated susceptibility, magnetic and electric fields, spikes and power frequencies
RS03	Radiated susceptibility, electric field, 14 kHz to 10 GHz
RS05	Radiated susceptibility, electromagnetic pulse field transient
UM03	Radiated emissions and susceptibility, tactical and special purpose vehicles and engine-driven equipment
UM04	Conducted emissions and radiated emissions and susceptibility, engine generators and associated components, uninterruptible power sets and mobile electric power equipment
UM05	Conducted and radiated emissions, commercial electrical and electromechanical equipment

*C = conducted, E = emission, R = radiated, S = susceptibility, and UM = unique method.

Table III. MIL-STD-461C susceptibility requirements

Requirement*	Description
CS01	Conducted susceptibility, power leads, 30 Hz to 50 kHz
CS02	Conducted susceptibility, power and interconnecting control leads, 0.05 to 400 MHz
CS03	Intermodulation, 15 kHz to 10 GHz
CS04	Rejection of undesired signals, 30 Hz to 20 GHz
CS05	Cross-modulation, 30 Hz to 20 GHz
CS06	Conducted susceptibility, spikes, power leads
CS07	Conducted susceptibility, squelch circuits
CS09	Conducted susceptibility, structure (common mode) current, 60 Hz to 100 kHz
CS10	Conducted susceptibility, damped sinusoidal transients, pins and terminals, 10 kHz to 100 MHz
CS11	Conducted susceptibility, damped sinusoidal transients, cables, 10 kHz to 100 MHz
RS01	Radiated susceptibility, magnetic field, 0.03 to 50 kHz
RS02	Radiated susceptibility, magnetic and electric fields, spikes and power frequencies
RS03	Radiated susceptibility, electric field, 14 kHz to 10 GHz
RS05	Radiated susceptibility, electromagnetic pulse field transient
UM03	Radiated emissions and susceptibility, tactical and special purpose vehicles and engine-driven equipment
UM04	Conducted emissions and radiated emissions and susceptibility, engine generators and associated components, uninterruptible power sets and mobile electric power equipment

*C = conducted, R = radiated, S = susceptibility, and UM = unique method.

Table IV. MIL-STD-461C requirements vs classes for digital equipment*

Susceptibility requirement**	Aircraft	Ground facilities	Surface ships	Submarines
CS01	Y_L	Y_L	Y	Y
CS02	Y	Y	Y	T
CS03				
CS04				
CS05				
CS06	Y	Y	Y	Y
CS07				
CS09		Y_L	Y_L	Y_L
CS10		T	T	T
CS11		Y_L	Y_L	
RS01		Y_L	Y	Y
RS02		Y_L	Y	Y
RS03	Y	Y	Y	Y
RS05		Y_L	Y_L	

*Y = applicable, Y_L = applicable with limitations, and T = tailored on a case-by-case basis.

**C = conducted, R = radiated, and S = susceptibility.

requirement is applicable and the level to which the associated test limit will be imposed can vary. A **Y** entry denotes that the requirement is applicable and the limit shall be met by using the test method described in MIL-STD-462. A $\mathbf{Y_L}$ entry denotes that there are limitations in the applicability of the test requirement, and a T entry denotes that the applicability of the requirement will be determined on a case-by-case basis. *Absence of an entry means that the test requirement is not applicable.*

With the evaluation criterion that a requirement must be applicable to multiple classes of equipment before it can be termed generally applicable, the susceptibility requirements in Table IV can be narrowed. The test requirements listed in Table V meet this evaluation criterion and are suggested for consideration as test criteria to evaluate the susceptibility of digital equipment in nuclear power plants. The rationale for the selection of the susceptibility criteria in Table V is that NRC can take advantage of the tri-services' experience in evaluating digital equipment. A critique of the test criteria indicates that they are applicable to a nuclear power plant environment and also address the specific concerns of NRC. These susceptibility criteria cover conducted and radiated interference, transients, exposure to both electric and magnetic fields, and noise entry through the power and control leads. By specifying these susceptibility criteria and their associated test methods, a conclusion can be reached as to whether equipment and subsystems can be expected to function properly in their intended electromagnetic operating environments.

The test methods specified in MIL-STD-462 are applicable to the evaluation of the susceptibility of digital systems in nuclear power plants only to the extent that they follow the test requirements; they are just the means by which compliance can be demonstrated. The MIL-STD-462 test methods have become well developed through the years and are generally accepted in industry. This acceptance would make their adaptability to a V&V program relatively easy and inexpensive because many laboratories already have the necessary test equipment and are familiar with the test procedures.

4.3 Findings on Acceptance Criteria

The acceptance criteria in MIL-STD-461C are specified according to the particular application and the expected electromagnetic environment in which equipment and subsystems must operate. This environment may vary from low-interference levels at ground-based locations to extremely

Table V. Applicable C susceptibility criteria for digital equipment

Requirement*	Description
CS01	Conducted susceptibility, power leads, 30 Hz to 50 kHz
CS02	Conducted susceptibility, power and interconnecting control leads, 0.05 to 400 MHz
CS06	Conducted susceptibility, spikes, power leads
RS01	Radiated susceptibility, magnetic field, 0.03 to 50 kHz
RS02	Radiated susceptibility, magnetic and electric fields, spikes and power frequencies
RS03	Radiated susceptibility, electric field, 14 kHz to 10 GHz

*C = conducted, R = radiated, and S = susceptibility.

harsh levels on the decks of aircraft carriers. In past surveys of nuclear power plant environments (Cirillo and Prussel 1986), the levels of radiated emissions from most equipment were found to be moderate or below. Nevertheless, equipment was identified that could not operate reliably in its intended environment. From the results of these surveys, it is reasonable to assume that a nuclear power plant can be categorized as an industrial environment, with its electromagnetic ambient being considerably less harsh than a typical military environment.

In areas where digital systems will be installed, the radiated and conducted emission levels should be measured and the susceptibility criteria established accordingly. Acceptance criteria that are less stringent than those specified in MIL-STD-461C will allow the avoidance of unnecessary test costs and modifications in equipment designs. The acceptance criteria for the nuclear power plant environment should be based on susceptibility levels developed from radiated and conducted emission profiles anticipated at various sites. The profiles will provide an assessment of the ambient electromagnetic environment; a safety margin can then be added to ensure the operability of the equipment and subsystems. This type of approach will help in establishing acceptance criteria that are both appropriate and realistic.

Of the environments described for the classes of military equipment and subsystems, the noncombat ground facilities environment most closely resembles that of a nuclear power plant. Thus, the MIL-STD-461C acceptance criteria specified for noncombat ground facilities (or some variation thereof) could be used in the interim for nuclear power plant environments until acceptance criteria based on actual nuclear power plant profiles can be established. These acceptance criteria were found to be representative of the criteria already informally accepted in the nuclear industry, and are at least equal to or slightly more stringent than the proposed American National Standards Institute (ANSI) C63.12 (ANSI 1987) immunity criteria in the areas common between the ANSI standard and the MIL-STDs.

5. SUMMARY

This paper has detailed the effort to date to develop the technical basis for evaluating the susceptibility of digital I&C systems to EMI. To summarize, IEEE Std. 1050-1989, with minor exceptions, was found to provide good EMC design and installation practices. As an added precaution, periodic maintenance checks would ensure that the EMC design and installation practices continue to perform their intended function. Specific MIL-STD-461C test criteria and their associated MIL-STD-462 test methods were found to form the basis for an EMI V&V program. Also, interim acceptance criteria based on the MIL-STD-461C criteria for noncombat ground facilities could be established for the test criteria until adequate measurement data can be compiled to profile the electromagnetic ambient environment in nuclear power plants. By following this approach, we believe that a greatly reduced probability of encountering EMI-associated problems with upgrades to digital I&C systems could be realized.

6. REFERENCES

[1] "American National Standard for Electromagnetic Compatibility Limits-Recommended Practice," (ANSI 1987) ANSI C63.12, American National Standards Institute, New York.

[2] CIRILLO, J., PRUSSEL, M., "Electromagnetic Compatibility in Nuclear Power Plants," (WATTec Conf., Knox., TN, 1986).

[3] EWING, P. D., KORSAH, K., Recommended Guidelines and Technical Bases for Installation, Testing, and Acceptance Criteria for EMI/RFI in Digital Systems for Nuclear Power Plant Applications, NUREG/CR-5941, Oak Ridge Natl Lab, TN (to be published in June 1993).

[4] HANSON, R. J., Interference effects on microprocessor and subsystem performance, Eval. Eng. (1989) 155-57.

[5] HYNE, J., "Electromagnetic compatibility in instrumentation," (Conf. Measur. Instrum./Digital Technol. Australia, 1984) 127-30.

[6] ORANCHAK, J. R., et. al., RFI effects on power plant I&C equipment, IEEE Trans. Nucl. Sci., NS-27 (1980) 863-65.

LIFE EXTENSION ACTIVITIES AND MODERNIZATION STRATEGIES FOR INSTRUMENTATION & CONTROL SYSTEMS OF RESEARCH AND POWER REACTORS IN INDIA

S.P. Chaganty, B.R. Bairi

Bhabha Atomic Research Centre
Electronics Division, Trombay,
Bombay-400 085.
INDIA

ABSTRACT

Based on three and half decades of experience gained in the operation and maintenance of Instrumentation and Control Systems of nuclear reactors in India, specific investigations were made to understand various aspects of aging. The analysis of the failure rates of various instruments,plant outage figures and obsolescence of components have necessitated the replacement of instrumentation to improve the reliabilty and performance.The aging models available were used to determine the extent of performance degradation and to formulate maintenance strategies.The nuclear instrumentation of the aging research reactors at Bhabha Atomic Research Centre (BARC) has been replaced with high reliability equipment using modern integrated circuits. This has resulted in an improvement in the mean time between failure (MTBF) by a factor of five. The neutronic instrumentation of Fast Breeder Test Reactor (FBTR) at Madras is currently being upgraded with the introduction of microprocessor based safety units for reactvity computation and online testing of safety logic with Fine Impulse Technique. The operating experience has also indicated the necessity of developing online surveillance methods and status monitoring of various systems to detect aging. Online cable insulation measurement technique and noise analysis methods for vibration monitoring have been developed. Campbell method of signal processing has been successfully used in extending the useful life of Local Power Range monitors in the Boiling Water Reactor at Tarapur. In order to improve reliability, accuracy and provide efficient man machine interface, microprocessor based systems with online testing features have been installed in power reactors. These include the high performance reactor regulating system and centralised radiation monitoring systems commissioned at Kakrapara power station. The paper describes the above systems and the modernisation strategies for nuclear instrumentation and control.

1 AGING DETECTION :

1.1 Assessment

The aging assessment and modelling are done by :

a) Analysis of the operating experience regarding the failure rate and performance degradation of components.

b) Reviewing the design features of an aging component in terms of the construction material used, the quality control measures adopted during fabrication, impact of the stresses to which it is exposed under normal and accidental conditions and investigation of the usage of the component as per its specifications.

c) Conducting accelerated aging tests to predict, identify and characterize the failure.

d) Implementation of online diagnostic methods to monitor degradation in performance.

In addition to studying aging effects on naturally aged instrumentation, accelerated life tests with respect to stress factors such as temperature, humidity and radiation determine the vulnerability of equipment to aging stresses. The accelerated life tests only confirm the near time reliability and provide comparative analysis of alternative materials and designs. Arrhenius model has been most widely used for thermal aging studies.Many statistical failure models are available for life predictions[1]. Some of them being gamma, exponential, normal, log normal and weibull. These failure models are not based on the physical mechanisms of degradation but provide consistent mathematical structure to predict the system reliability.

Constant failure rate model was used for analyzing the reliability of electronic equipment which has undergone initial burn-in and can be theoretically estimated by using various data bases available. The failure rate of the components used in the radiation monitoring instrments of research reactor Dhruva at Bombay was calculated using the data available from MIL-HDBK-217E [2] and compared with the practically observed failure rate. Table 1. shows these results.

Table 1 : Failure rates of the components

Component	observed failure rate/10^6hrs	*calculated failure rate/10^6hrs
Linear I.C	0.20	0.60
Transistors	0.078	0.067
Electrolytic capacitors		
Tantalum	0.007	0.012
Aluminium	1.6	0.75

* Quality factor assumed was on higher side in view of different grades of components used.

This data has been extremely useful in certain component replacements with high quality MIL-883 B screened components for integrated circuits and JAN screened for semiconductor components. In view of high failure rate of Aluminium dielectric electrolytic capacitors, these are being replaced every 5 years.

The time dependent increase in failure rate characterized by linear rate failure model is applicable to components such as relays, Motor Operated Valves, Generators, and certain electronic components which are sensitive to humidity and radiation. Accelerated tests[3,4] with exposure of components to thermal cycling, radiation, humidity and vibration have been conducted at BARC for components such as electrolytic capacitors, multi-pin connectors, reed switches, rubber insulated cables, cross linked polyethylene cables, mineral insulated cables etc. These aging studies helped in qualifying the components for use in class 1E equipment at reactors.

1.2 Detection

In order to detect aging and predict failure many on-line diagnostic methods were developed. Some of them are Insulation Resistance monitoring of incore neutron detectors and associated cables, power spectral density measurement of noise signal from incore neutron detectors for vibration monitoring.

The technique developed for monitoring insulation resistance (IR) of Self Powered Neutron Detectors (SPND) with integral Mineral Insulated Cable assembly was primarily necessitated as large number of Local Power Range Monitors (LPRM) were showing low IR value at Boiling Water Reactor at Tarapur. The investigation on these detectors indicated fall of IR due to failing of ceramic to metal seal at the cold end of the Mineral Insulated cable and ingress of moisture which resulted in lowering of insulation resistance. An amplifier is developed for measurement of incore neutron flux for the future 500 MW reactors for the purpose of flux mapping, zonal power control and reactor protection system and provides online mesurement of IR value. The block diagram is shown in fig. 1.

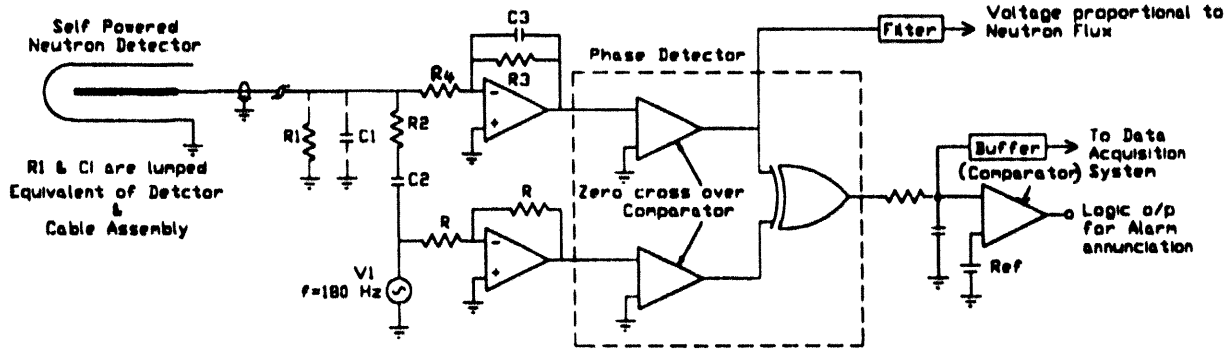


Fig. 1 Simplified scheme for on-line insulation monitoring of SPND & cable assembly

The principle consists of superimposing a sinusoidal signal V1 at the input of amplifier and detecting its phase shift at the output of amplifier which is a function of detector IR and capacitance. The frequency of sinusoid was optimized to 180 Hz and at this frequency, the detector and cable can be

lumped as R1 (representing the IR value) in parallel with C1(total capacitance of cable and detector). The phase detector output is converted into a d.c. value which is a function of R1, C1, frequency and other components in the circuit and is fed to a comparator with a set threshold value corresponding to the normal detector. This dc signal is also given to a computer for monitoring the changes in the IR value and cable capacitance with respect to time, temperature and absorbed radiation dose.

2. REPLACEMENT & PREVENTIVE MAINTENANCE STRATEGIES & EXPERIENCES

2. 1 Replacement strategies

The replacement strategies were based on the following factors:

a) Effect on the availability and safety of reactor due to observed failure rates.
b) Obsolescence, non availability of spare parts and difficulty of maintenance.
c) Availability of latest technology with higher reliability and enhanced safety features with cost benefit.

Unreliability (fraction of time an instrument is not capable of performing the function required by it) figure of 10^{-3} was aimed for safety system[5]. With a 2 out of 3 coincidence logic and frequency of testing of once in a month, the acceptable unsafe failure rate of overall system demanded a MTBF of greater than five years.

Neutronic instrumentation of APSARA and CIRUS reactors (commissioned in 1956 and 1960 respectively) showed increase in failure rates in the early seventies and table 2 shows the overall failure rates (unsafe and safe) observed:

Table 2 : Failure rates of CIRUS & APSARA instrumentation

System	MTBF (in hours)
Reactor start up instrumentation	2800
Over power trip (linear channel)	47000
Period trip channel	2300
Servo channel (power regulating channel)	2250

This instrumentation was of obsolete vacuum tube design and spare parts were not available. In view of above factors decision was taken for complete replacement of the neutronic channels and new systems with improved safety features based on solid state technology were commissioned in 1985. The failure data of the new equipment indicated and improvement by a factor of 5 during the first three years and subsequently no failures have been reported. The new designs incorporate MIL screened components and extensive quality control tests, thermal and seismic aging tests were conducted at different stages of fabrication prior to commissioning.

2.2 Surveillance instrumentation :

In order to reduce the unsafe failure rate to a value much less than 0.2/year, additional features have been incorporated to detect and annunciate unsafe failures in the neutronic instrumentation. Some of them are:

1) Scanning of the outputs and threshold values of the triplicated safety channels and genarate discordance trip or alarm by surveillance computer.

2) On line fine impulse testing (FIT): This method has been used to detect anomalies in the performance of safety logic of reactor protection system. The trip circuits and the solid state safety logic are continuously checked by super imposing two millisecond wide test pulses over the analog signals from different safety systems connected to the trip circuit. These test pulses are generated by a micro computer in a sequential manner every 3 seconds and output of power gates for actuating the shutdown system are verified against the normal expected values. Industrial grade personal computer connected to the micro computer logs the data and aids in identifying the faulty component. The block diagram of the system is shown in fig. 2.

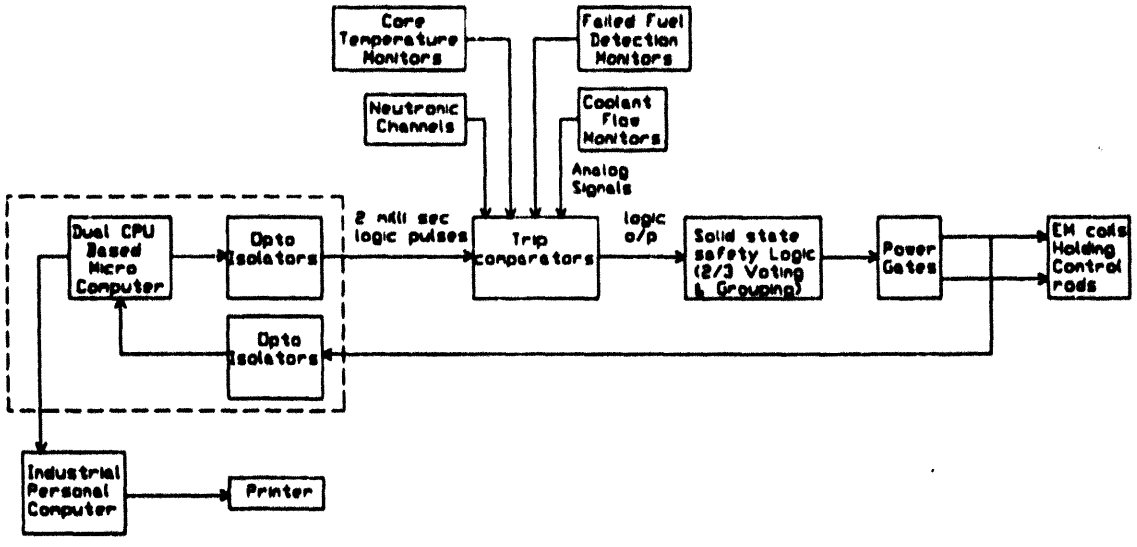


Fig. 2 Fine Impulse Test System

3) Detection of discontinuity between the detector, cable and the instrument: Fig.3 shows the principle of operation for over power trip generating channel using Boron Coated Ion chamber for measuring neutron flux.

A sinusoidal signal of 4 KHz is superimposed over high voltage supply. This a.c. signal gets coupled to the signal elctrode of the detector due to inter-electrode capacitance C and is converted into d.c. voltage and fed to a comparator. Comparator output level indicates discontinuity between detector, cable and instrument.

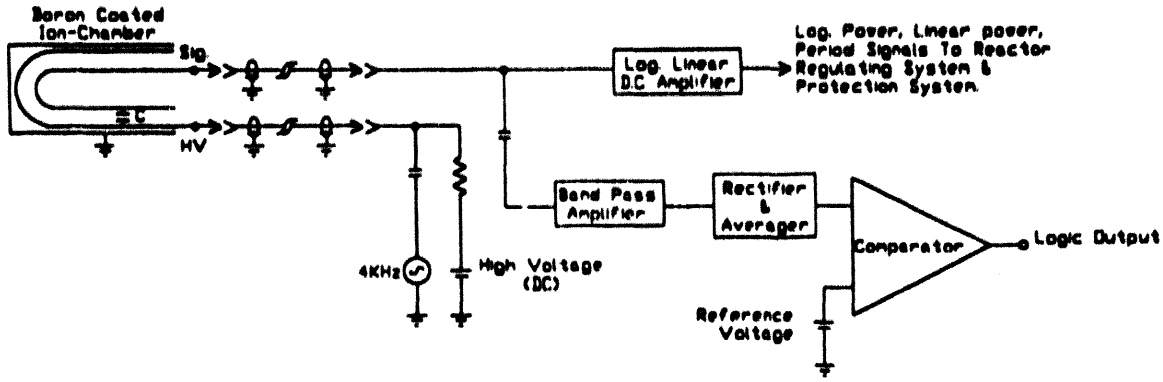


Fig. 3 Cable Discontinuity Monitoring Technique

2.3 Upgradation activities:

The aging neutronic instrumentation of Fast Breeder Test Reactor (FBTR) at Madras designed in 1970 is currently being upgraded with designs based on technological advances in the field. Industry standard components screened to MIL-883 and supported by multiple manufacturers and vendors are chosen. Microprocessor based safety systems such as reactivity monitors, stand alone Fine Impulse Test systems with self test facilities are introduced for improving reliabilty. The aging cables are also being replaced with super screened radiation resistant cables to reduce Electro Magnetic Interference.

The ion chamber amplifiers used for reactor power regulation and protection system of Rajasthan Atomic Power Station (RAPS) exhibited high failure rate due to inadequate input protection and complex temperature compensation methods incorporated. These have been replaced with improved design having low component count and simplified temperature compensation.

Some of the other issues considered for performance upgradation are:

a) Review and approval of new designs at the system level and circuitry level to ensure
   i) Fail safe operation
   ii) Low stress factor for individual component
   iii) Fool proof input and output protection
   iv) Ease of maintenance and testing.

b) Software Validation and verification to ensure safety and reliability. Validation tests are performed by an independent group from regulatory team to avoid any common mode (systematic) errors in implementation.

3. PREVENTIVE MAINTENANCE STRATEGIES :

With primary goal of increasing plant reliability and availability, the preventive maintenance activity was based on:

a) Observed failures and performance degradation
b) Systematic analysis of the failure data, identification of "weak components" and replacement of these on regular basis at intervals determined by operational experience.
c) Developing control methods for reducing stress factors causing performance degradation.

Elaborate record keeping methodology is introduced to determine cause of failure and its influence on the plant reliability. The information to be recorded is:

Reactor status prior to fault and after fault, Systems affected, Problem description,
Details of the component failed, Mode of failure, Type of failure,
Date and time of occurrence of fault, Date and time of detection of fault,
Date and time of normalization of system, Details of corrective action,
Probable cause of failure.

The different categories for failure cause investigated are :

A) Design:

Not designed to the operating conditions.
Often goes out of tolerance.
Inadequate margin

B) Fabrication:

Inadequate Quality control
Inadequate standards
Inadequate Testing

C) Operation & maintenance:

Operation beyond stipulated life
Imperfect procedures
Failure to follow procedures
Imperfect calibration
Imperfect test/repair

D) Environmental:

Corrosion
Temparature
Humidity
Vibration
Radiation

4. MODERNIZATION STRATEGIES

With the operating experiences and upgradation work carried the need for development work to improve instrumentation reliability and safety of reactor with reduced down time has been taken as a primary thrust area. Availability of low cost microprocessors, microcontrollers and fault tolerant hardware architectures has given great impetus for development of automated control systems. The primary goals for the modernization programme attempted are to :

a) Enhance plant safety margins.
b) Increase measurement accuracy and implement complex calculations.
c) Perform more effective testing and surveillance to detect any performance degradation and aging.
d) Elimination of manual data logging, performance analysis by expert system.

f) Minimize the mean time to detect and repair a fault and increased ease of maintenance.
g) Improving availability factor using fault tolerant architecture.
h) Address obsolescence and spare part inventory control problems.
i) Establish techniques to increase life of the equipment.

The modernization work carried out at BARC has been successfully applied to support the nuclear power programme of India and many computer based systems have been commissioned at Pressurized Heavy Water Reactors at Narora and Kakrapara. These have been subjected to extensive software validation and verification tests prior to installation and have been functioning smoothly since past two years. These include Reactor Power Regulating System, Centralised Radiation Data Acquisition System,Stack activity monitoring system. Microprocessor based Reactivity computation unit which forms a part of reactor protection system has been developed on similar lines for FBTR.

4.1 Reactor Power Regulating System:

The micro computer based reactor power regulating system generates regulating signals to drive the adjuster rods and control actual power equal to the demand power in the range of 10^{-8} to 100 % of full power. The overall transfer function of the regulating system has been theoretically analyzed and the digital computation has resulted in excellent closed loop stability with fast response.
Block diagram of the system is shown in fig. 4.

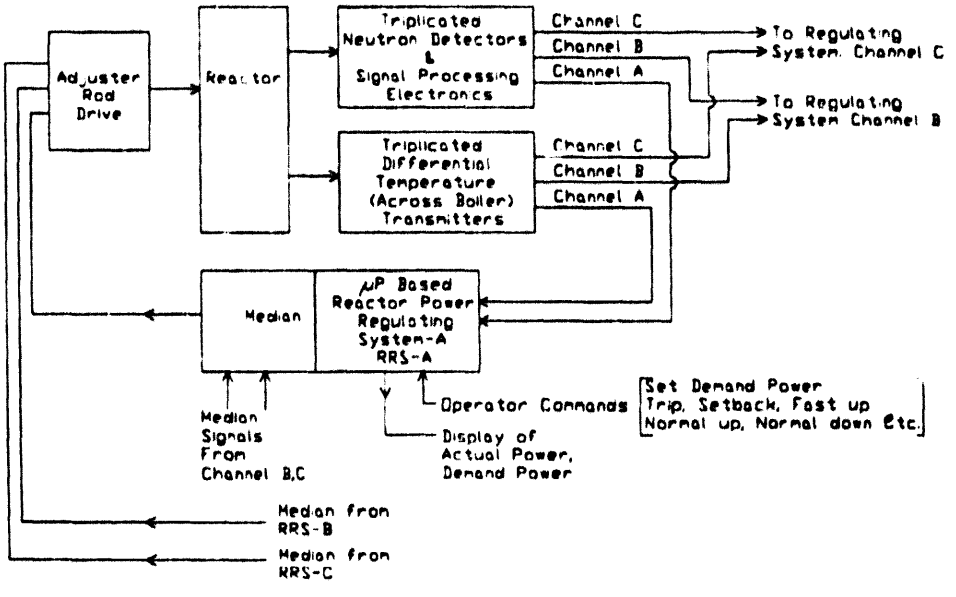


Fig. 4 Reactor power regulating system

Actual power is calculated from the out of core neutron detector signals and differential temperature signals across the boiler. The actual power signal is compared with demand power set through console and the error signal after compensation for feed back stability is used for driving groups of adjuster rods. The regulating system are triplicated and each channel generates regulating signal and

also compares it with regulating signals generated by other two channels and a median is selected in participating in control action. The design employs the novel technique of reactor power control based on the linear neutron flux signal which is corrected continuously by the boiler differential temperature signal in order eliminate the unintended power changes due to disturbances in the secondary system and achieve better transient response.

The micro processor based system installed at Narora and Kakrapara offers following features :

1. Accurate implementation of transfer function through digital computation eliminating the drifts associated in conventional analog systems.
2. Enhanced flexibility to modify and tune the system performance to meet field requirements.
3. Improved man machine interface and guidance to the operator for effecting any power change.
4. Self check and diagnostic features to ensure reliable performance and fault isolation.
5. Ease of maintanance and minimum calibration requirements.
6. Fault tolerance due to triplicated systems with median selection.

4.2 Reactivity Monitor

Reactivity monitor computes reactivity from neutron flux signals by solving inverse kinetic equations and is configured around Intel's 8088 CPU with numeric co-processor 8087. These channels are triplicated and generate a reactor trip signal after 2 out of 3 voting when reactivity computed exceeds a preset value. The software has been developed in accordance with IEC-880 document. The block diagram is shown in fig. 5.

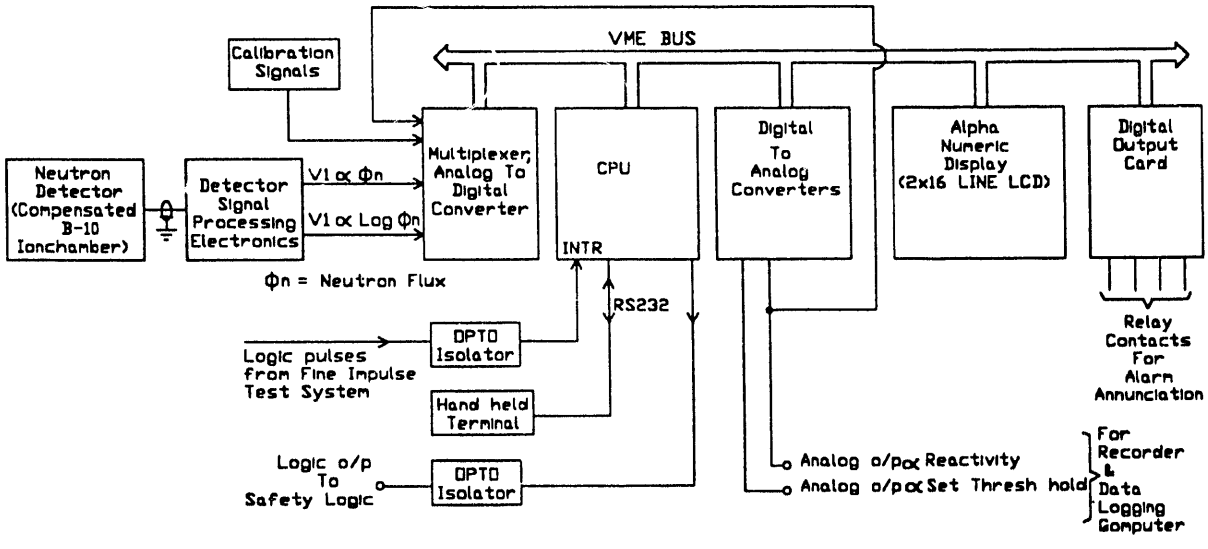


Fig. 5 Reactivity monitor

4.3 Centralized Radiation Data Acquisition System

Fig. 6 shows the block diagram of the distributed data acquisition system developed to monitor the different radiation levels in the reactor containment building, alarm any excessive radiation levels and perform certain dedicated control actions such as switching solenoid valves for sampling air to measure tritium concentration.

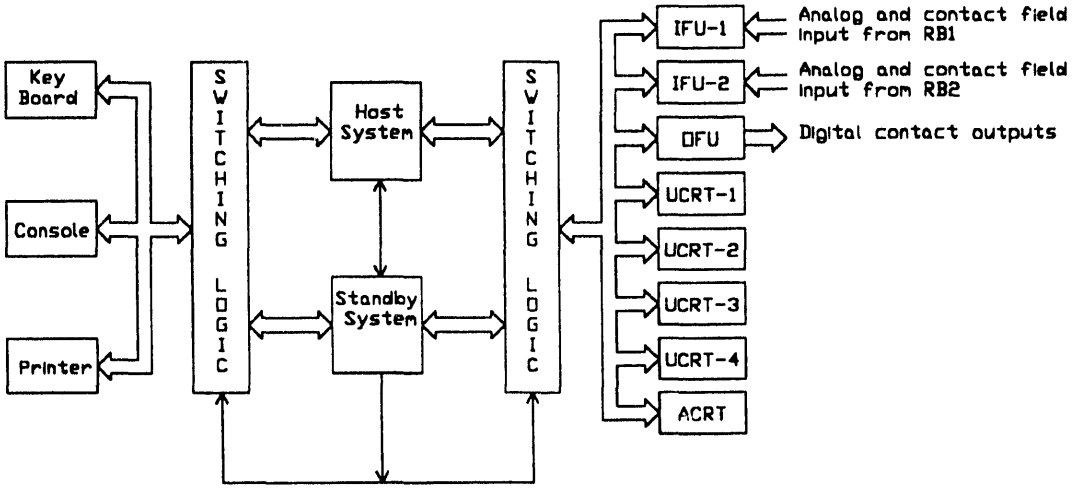


Fig. 6 Radiation Data Acqusition System

The system is built around ruggedised industrial Personal Computers(PC) with fault tolerant features. The system is connected to external units via eight RS422 serial links. Two of the serial links are used for acquiring pre-processed field instrument data from intelligent field units (IFU-1 & IFU-2) scanning the analog signals and system status contacts of the radiation monitors. One link is used for field alarm actuation through an Output Interface Unit (OFU). The remaining five serial links are used for providing the information regarding the radiation levels (formatted as trend display, history display and current radiation levels in engineering units) and alarm status to various intelligent interactive user terminals (UCRT) located in the different places outside the containment building. Some of the features are :

1. Dual computer architecture for fault tolerance.
2. Diskless PC with ROM and battery backed RAM for improving reliability.
3. PC based terminals to fight obsolescence and facilitate ease of maintenance
4. Reduced cabling and error free data transmission.
5. Multitasking real time kernel for supervising tasks such as data acquisition and processing, alarm generation, report generation and console commands.
6. VME based modular hardware architecture for field interface units for future expandability.
7. Menu driven, user friendly interactions with terminals for improved man-machine communication.

4.4 Stack release monitoring system

Microprocessor based stack gas monitoring system measures the release rate and cumulative

release of radioactive isotopes such as Iodine-131, Argon-41, Strontium-90, and other gaseous fission products through stack of the nuclear reactor. The salient features are:

- Use of multichannel analyzer technique
- Spectrum analysis incorporating smoothing, peak validation, tracking in the region of interest, background subtraction, online change of acquisition interval to optimize on standard deviation and fast response.
- User friendly operator interface

Fig. 7 shows the pictorial view of the standardised radiation monitor which can be reconfigured for measuring different types of radiation through software change. With suitable detectors it can be used as a) neutron flux monitor for reactor power regulation regulation,flux mapping, failed fuel detection system, b) alpha and beta contamination monitor, c) area gamma monitor, stack activity release monitor

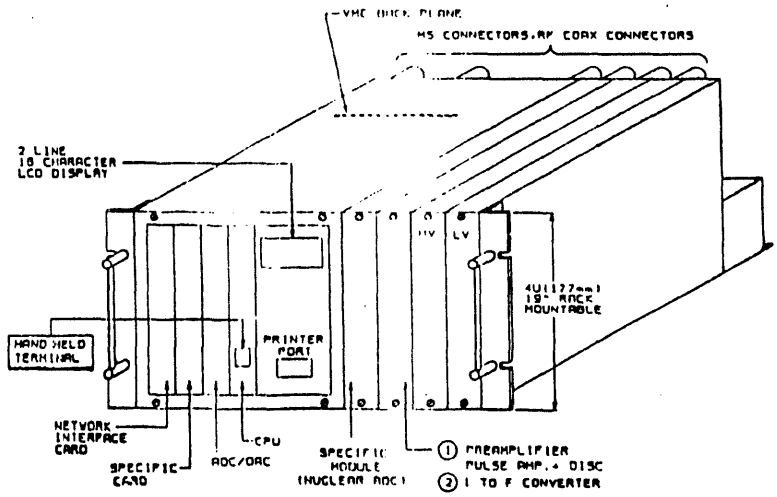


Fig. 7 Standardised radiation monitor

This system has network interface card to connect to a proprietary Local Area Network(LAN) and can perform dedicated control actions and self test operations on command either locally through a hand held terminal or from host computer located in control room connected through the LAN.

5. LIFE EXTENSION ACTIVITIES

As a part of development of techniques to extend life of instrumentation system inclusive of the sensors, Campbell method of signal processing has been applied to extend the useful life of in-core miniature fission chambers for measuring neutron flux of the order of 10^{13}nv in presence of gamma of 10^{9} R/hr. The Local Power Range Monitors (LPRM) at Boiling Water Reactor at Tarapur are used for measuring neutron flux by measuring the d.c. signal from the detector. The prolonged exposure to high neutron flux results in the burn-up of U-235 atoms in the detector and sensitivity reduction.The detector

is replaced (normally once in two years) when the neutron induced current falls to a value comparable to current produced by gamma. The neutron to gamma current ratio of the order of 40 for a new detector and is replaced at a time when the ratio falls to 5. By processing the signal in mean square voltage (MSV) mode based on Campbell technique the initial neutron to gamma signal ratio is enhanced to 20000 as signal is proportional to square of charge produced in the detector and the time required for this ratio to fall to 5 is of the order of 6 years. Thus the useful life is extended by 4 years resulting in cost effective benefit and reduced radiation exposure due to lower frequency of LPRM replacement. The new method is also advantageous in operating the detectors with lower insulation resistance (up to 1 Mega ohms) as the d.c. leakage current does not contribute significant error in the a.c. signal. Though regenerative type detectors with coatings of Uranium-234 and 235 are currently are employed[6] for longer life,the MSV technique extends the useful life of the old detectors with marginal extra expenditure due to replacement of electronics.The Detailed testing of the new system has established the feasibility of this technique and about 12 nos of detectors are being operated with the new instrumentation at TARAPUR and performance is found to be very satisfactory. Fig. 8 shows the block diagram of the amplifier developed :

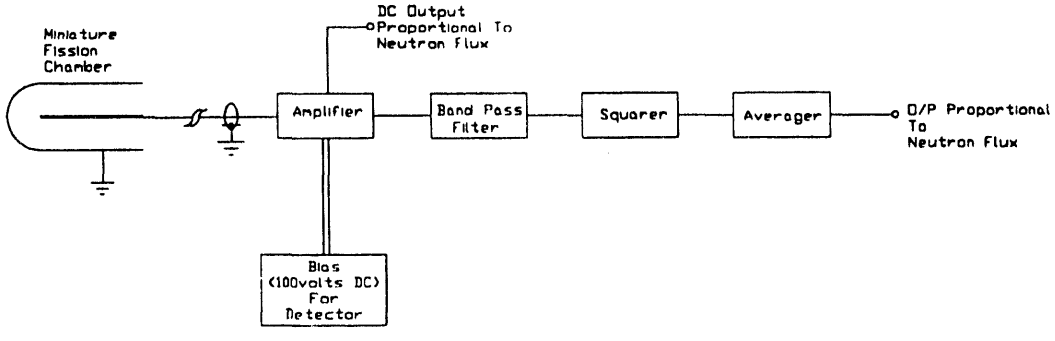


Fig. 8 LPRM amplifier

The fluctuating component of the signal from the detector has a constant power spectral density for frequencies above 500 Hz and its mean square value (MSV) is proportional to the neutron flux. This noise signal is fed to a band pass filter (1 KHz to 2 KHz) and output is squared and averaged as an indication of mean neutron flux. The card developed has provision of both MSV & d.c. signal processing simultaneously and can be easily retrofitted in the existing General Electric make chassis for LPRM system with minor modifications.

6. CONCLUSION

Many techniques have been developed to detect aging of electronic instrumentation for nuclear power plants. Failure data analysis and accelerated life test programs are continuing for estimating performance degradation and effect on plant reliability. The introduction of micro processor based systems has resulted in enhanced system performance, reduction in operator errors due to human engineered interface and enhanced self testing capabilities. Distributed Digital Control systems with token bus networking architecture are being planned for the future I&C systems of power reactors.

REFERENCES :

1. JOHNSON,R.T.Jr., THOME,F.V., CRAFT,C.M., Survey of state of art in aging of electronics, Rep.NUREG/CR-3156, Sandia National Labs, NM,USA(1983)

2. (b) Reliability Prediction of Electronic Equipment, Military Handbook, MIL-HDBK-217E, Department of Defense, Washington (1986)

3. BORA, J.S., BABAR, A.K., " Reliability improvement and import substitution through ageing research" (Proceedings of national symposium on advanced instrumentation for nuclear research, BARC,Bombay, 1993),Department of Atomic Energy, INDIA,E8

4. GLEASON, J.F., "Aging and seismic performance for safety related equipment in a mild environment" IEEE Transactions on Nuclear Science., 31 1 (1984) 837

5. PEARSON.A.,LENNOXC.G.,"Sensing and Control Instrumentation" The Technology Of Nuclear Reactor Safety, Vol.1(THOMSON.T.J., BECKERLEY.J.G.) The MIT Press,MA(1964) 285.

6. GLESIUS.F.L.,KROON.J.C.,MYRABO.A.L.,HAMMER.M.F.,"Development of an Extended Range Start-up Monitor"IEEE Transactions on Nuclear Science.,31 1 (1984) 738.

REGULATORY PERSPECTIVE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS FOR FUTURE ADVANCED NUCLEAR POWER PLANTS

MATTHEW CHIRAMAL
INSTRUMENTAION AND CONTROLS BRANCH
U.S. NUCLEAR REGULATORY COMMISSION

+ THE CONSENSUS OPINION OF THE NUCLEAR INDUSTRY AND U.S. NRC STAFF IS THAT THE USE OF DIGITAL TECHNOLOGY IN I&C SYSTEMS PROVIDES THE POTENTIAL FOR IMPROVEMENTS IN THE SAFE AND RELIABLE OPERATION OF NUCLEAR POWER PLANTS. THIS POTENTIAL IS ACHIEVABLE THROUGH THE IMPLEMENTATION OF HIGHLY RELIABLE DIGITAL EQUIPMENT.

+ DIGITAL COMPUTER-BASED I&C SYSTEMS DIFFER SIGNIFICANTLY FROM ANALOG SYSTEMS - THE DIGITAL SYSTEM HAS A GREATER DEGREE OF SHARING OF DATA TRANSMISSION, FUNCTIONS, AND PROCESS EQUIPMENT.
  - o ALSO RELIANCE ON SOFTWARE

+ SECY-91-292 IDENTIFIES THE GENERAL REGULATORY APPROACH FOR APPLICATION OF DIGITAL COMPUTER TECHNOLOGY FOR ALWRS

  - o USE EXISTING REGULATORY REQUIREMENTS
  - o STAFF PARTICIPATION IN NATIONAL AND INTERNATIONAL CODES AND STANDARDS COMMITTEES. DEVELOPMENT OF NEW REQUIREMENTS AND USE OF NEW STANDARDS
  - o LESSONS LEARNED IN THE U.S. AND OTHER COUNTRIES THROUGH TECHNICAL INFORMATION EXCHANGES, CONFERENCES AND MEETINGS
  - o INPUT FROM RESEARCH EFFORTS AND FROM EXPERTS
  - o USE THE GUIDELINES PROVIDED IN THE EPRI UTILITY REQUIREMENTS DOCUMENT

+ THE STAFF HAS THE SUPPORT OF A MULTI-DISCIPLINARY CONTRACTOR TEAM WITH THE REQUISITE TECHNICAL EXPERTISE TO ASSIST IN THE IDENTIFICATION AND RESOLUTION OF DIGITAL SYSTEM ISSUES

ISSUE OF COMMON-MODE FAILURE IN DIGITAL SYSTEMS

- DIGITAL SYSTEMS USE IDENTICAL PROGRAMS AND DATA BASES (SOFTWARE) AND PROCESS EQUIPMENT (HARDWARE) IN REDUNDANT CHANNELS
- QUANTITATIVE ESTIMATE OF RELIABILITY OF I&C SYSTEMS BASED ON SOFTWARE SYSTEMS CANNOT BE EASILY DETERMINED
- A HARDWARE DESIGN ERROR, A SOFTWARE DESIGN ERROR, OR SOFTWARE PROGRAMMING ERROR MAY RESULT IN A COMMON MODE OR COMMON CAUSE FAILURE OF REDUNDANT EQUIPMENT
- CURRENT REGULATORY REQUIREMENTS DO NOT SUFFICIENTLY ADDRESS THE POTENTIAL SAFETY CONCERNS ASSOCIATED WITH DIGITAL I&C SYSTEMS - PARTICULARLY THE SOFTWARE QUALITY AND COMMON MODE FAILURE CONCERN, AND THERE ARE NO CONSENSUS STANDARDS FOR CERTIFYING THE DESIGN OF DIGITAL I&C SYSTEMS FOR APPLICATION IN NUCLEAR POWER PLANTS

DEFENSE AGAINST COMMON MODE FAILURES

- DEFENSE AGAINST COMMON MODE FAILURES:

  QUALITY AND DIVERSITY

- QUALITY

  - FOR SPECIFIC ALWR PROGRAMMABLE DIGITAL I&C SYSTEM DESIGNS, THE STAFF HAS PROPOSED A PLANNED SOFTWARE-HARDWARE INTEGRATED DEVELOPMENT METHOD TO ENSURE QUALITY OF SOFTWARE AND HARDWARE THROUGHOUT THE LIFE CYCLE. THE PLANS SHALL ALSO DEFINE METHODS FOR AUDITING AND TESTING SOFTWARE AND HARDWARE DURING THE DESIGN, IMPLEMENTATION, INTEGRATION, INSTALLATION, OPERATION, AND MAINTENANCE PHASES. THE PLANS COMPRISES OF:
    - MANAGEMENT PLAN
    - CONFIGURATION MANAGEMENT PLAN
    - VERIFICATION AND VALIDATION PLAN
    - SOFTWARE QUALITY ASSURANCE PLAN
    - SAFETY PLAN

- DIVERSITY

  - BASED ON (1) RECENT ASSESSMENTS OF INTEGRITY OF SOFTWARE APPLIED TO VARIOUS SAFETY-CRITICAL FUNCTIONS COVERING A BROAD RANGE OF APPLICATIONS WHICH INCLUDE COMPUTER-BASED MEDICAL TREATMENT FACILITIES, COMPUTER-BASED FLY-BY-WIRE AIRCRAFT CONTROL SYSTEMS, AND NUCLEAR POWER PLANT PROTECTION SYSTEMS, AND (2) OPINIONS AMONG EXPERTS, THE STAFF RECOMMENDED THE POSITION THAT APPLICANTS ASSESS THE DEFENSE-IN-DEPTH AND DIVERSITY OF I&C SYSTEMS, DEMONSTRATE ADEQUATE DEFENSE AGAINST CMF, AND PROVIDE INDEPENDENT BACKUP MANUAL CONTROLS AND DISPLAYS FOR CRITICAL SAFETY FUNCTIONS

THE POSITION ON DEFENSE-IN-DEPTH AND DIVERSITY

1. THE APPLICANT SHALL ASSESS THE DEFENSE-IN-DEPTH AND DIVERSITY OF THE PROPOSED INSTRUMENTATION AND CONTROL SYSTEM TO DEMONSTRATE THAT VULNERABILITIES TO COMMON-MODE FAILURES HAVE BEEN ADEQUATELY ADDRESSED. THE STAFF CONSIDERS SOFTWARE DESIGN ERRORS TO BE CREDIBLE COMMON-MODE FAILURES THAT MUST SPECIFICALLY BE INCLUDED IN THE EVALUATION. AN ACCEPTABLE METHOD OF PERFORMING ANALYSES IS DESCRIBED IN NUREG-0493, "A DEFENSE-IN-DEPTH AND DIVERSITY ASSESSMENT OF THE RESAR-414 INTEGRATED PROTECTION SYSTEM," MARCH 1979. OTHER METHODS PROPOSED BY AN APPLICANT WILL BE REVIEWED INDIVIDUALLY.

2. IN PERFORMING THE ASSESSMENT, THE VENDOR OR APPLICANT SHALL ANALYZE EACH POSTULATED COMMON-MODE FAILURE FOR EACH EVENT THAT IS EVALUATED IN THE ACCIDENT ANALYSIS SECTION OF THE SAFETY ANALYSIS REPORT (SAR). THE VENDOR OR APPLICANT SHALL DEMONSTRATE ADEQUATE DIVERSITY WITHIN THE DESIGN FOR EACH OF THESE EVENTS. FOR EVENTS POSTULATED IN THE PLANT SAR, AN ACCEPTABLE PLANT RESPONSE SHOULD NOT RESULT IN A NON-COOLABLE GEOMETRY OF THE CORE, VIOLATION OF THE INTEGRITY OF THE PRIMARY COOLANT PRESSURE BOUNDARY, OR VIOLATION OF THE INTEGRITY OF THE CONTAINMENT.

3. IF A POSTULATED COMMON-MODE FAILURE COULD DISABLE A SAFETY FUNCTION, THEN A DIVERSE MEANS, WITH A DOCUMENTED BASES THAT THE DIVERSE MEANS IS UNLIKELY TO BE SUBJECT TO THE SAME COMMON-MODE FAILURE, SHALL BE REQUIRED TO PERFORM EITHER THE SAME FUNCTION OR A DIFFERENT FUNCTION. THE DIVERSE OR DIFFERENT FUNCTION MAY BE PERFORMED BY A NON-SAFETY SYSTEM IF THE SYSTEM IS OF SUFFICIENT QUALITY TO PERFORM THE NECESSARY FUNCTION UNDER THE ASSOCIATED EVENT CONDITIONS. DIVERSE DIGITAL OR NON-DIGITAL SYSTEMS ARE CONSIDERED TO BE ACCEPTABLE MEANS. MANUAL ACTIONS FROM THE CONTROL ROOM ARE ACCEPTABLE IF TIME AND INFORMATION ARE AVAILABLE TO THE OPERATORS. THE AMOUNT AND TYPES OF DIVERSITY MAY VARY AMONG DESIGNS AND WILL BE EVALUATED INDIVIDUALLY.

4. A SET OF SAFETY-GRADE DISPLAYS AND CONTROLS LOCATED IN THE MAIN CONTROL ROOM SHALL BE PROVIDED FOR MANUAL, SYSTEM-LEVEL ACTUATION OF CRITICAL SAFETY FUNCTIONS AND MONITORING OF PARAMETERS THAT SUPPORT THE SAFETY FUNCTIONS. THE DISPLAYS AND CONTROLS SHALL BE INDEPENDENT AND DIVERSE FROM THE SAFETY COMPUTER SYSTEM IDENTIFIED IN ITEMS 1 AND 3 ABOVE. THE SPECIFIC SET OF EQUIPMENT SHALL BE EVALUATED INDIVIDUALLY, BUT SHALL BE SUFFICIENT TO MONITOR THE PLANT STATES AND ACTUATE SYSTEMS REQUIRED BY THE CONTROL ROOM OPERATORS TO PLACE THE NUCLEAR PLANT IN A HOT SHUTDOWN CONDITION AND INTENDED TO CONTROL THE FOLLOWING CRITICAL SAFETY FUNCTIONS: REACTIVITY CONTROL, CORE HEAT REMOVAL, REACTOR COOLANT INVENTORY, CONTAINMENT ISOLATION, AND CONTAINMENT INTEGRITY.

THE DISPLAYS AND CONTROLS SHALL BE HARDWIRED IN THE SAFETY COMPUTER SYSTEM ARCHITECTURE TO THE LOWEST LEVEL PRACTICAL. TO ACHIEVE SYSTEM-LEVEL ACTUATION AT THE LOWEST LEVEL IN THE SAFETY COMPUTER SYSTEM ARCHITECTURE, THE CONTROLS MAY BE HARDWIRED EITHER TO ANALOG COMPONENTS OR TO SIMPLE, DEDICATED, AND DIVERSE SOFTWARE-BASED DIGITAL EQUIPMENT THAT PERFORMS THE SYSTEM-LEVEL ACTUATION LOGIC. THE SAFETY PARAMETER DISPLAYS MAY INCLUDE DIGITAL COMPONENTS EXCLUSIVELY DEDICATED TO DISPLAYS. THIS REQUIREMENT WOULD PROVIDE FOR AN INDEPENDENT AND DIVERSE CONTROL LOGIC FOR MANUAL SYSTEM-LEVEL ACTUATION OF THE SAFETY FUNCTION THAT WOULD BE CONNECTED DOWNSTREAM OF THE LOWEST LEVEL SAFETY SOFTWARE-BASED COMPONENT WITHOUT AFFECTING THE HARDWARE (INTERCONNECTING CABLES AND INTERFACES) BETWEEN THE LOWEST LEVEL ELECTRONIC CABINETS AND THE PLANT'S ELECTRO-MECHANICAL EQUIPMENT.

HUMAN ENGINEERING PRINCIPLES AND CRITERIA SHALL BE APPLIED TO THE SELECTION AND DESIGN OF THE PARTICULAR DISPLAYS AND CONTROLS. THE DESIGN OF THE DISPLAYS AND CONTROLS SHALL ENSURE THAT THE HUMAN SYSTEM INTERFACE SHALL BE ADEQUATE TO SUPPORT THE HUMAN PERFORMANCE REQUIREMENTS.

THE HARDWIRED SYSTEM-LEVEL CONTROLS AND DISPLAYS PROVIDE THE PLANT OPERATORS UNAMBIGUOUS INFORMATION AND CONTROL CAPABILITIES. THESE CONTROLS AND DISPLAYS ARE REQUIRED TO BE IN THE MAIN CONTROL ROOM TO ENABLE THE OPERATORS TO EXPEDITIOUSLY MITIGATE THE EFFECTS OF THE POSTULATED SOFTWARE COMMON MODE FAILURE OF THE DIGITAL SAFETY I&C SYSTEM. THE CONTROL ROOM WOULD BE THE CENTER OF ACTIVITIES TO SAFELY COPE WITH THE EVENT WHICH COULD ALSO INVOLVE THE INITIATION AND IMPLEMENTATION OF THE PLANT EMERGENCY PLAN. THE DESIGN OF THE PLANT SHOULD NOT REQUIRE OPERATORS TO LEAVE THE CONTROL ROOM FOR SUCH AN EVENT. FOR THE LONGER TERM RECOVERY OPERATIONS, CREDIT MAY BE TAKEN FOR ACTIONS FROM OUTSIDE THE MAIN CONTROL ROOM, WHEN THE EMERGENCY RESPONSE ORGANIZATION IS FULLY BRIEFED AND IN PLACE TO TAKE SUCH ACTIONS.

CONCLUSION

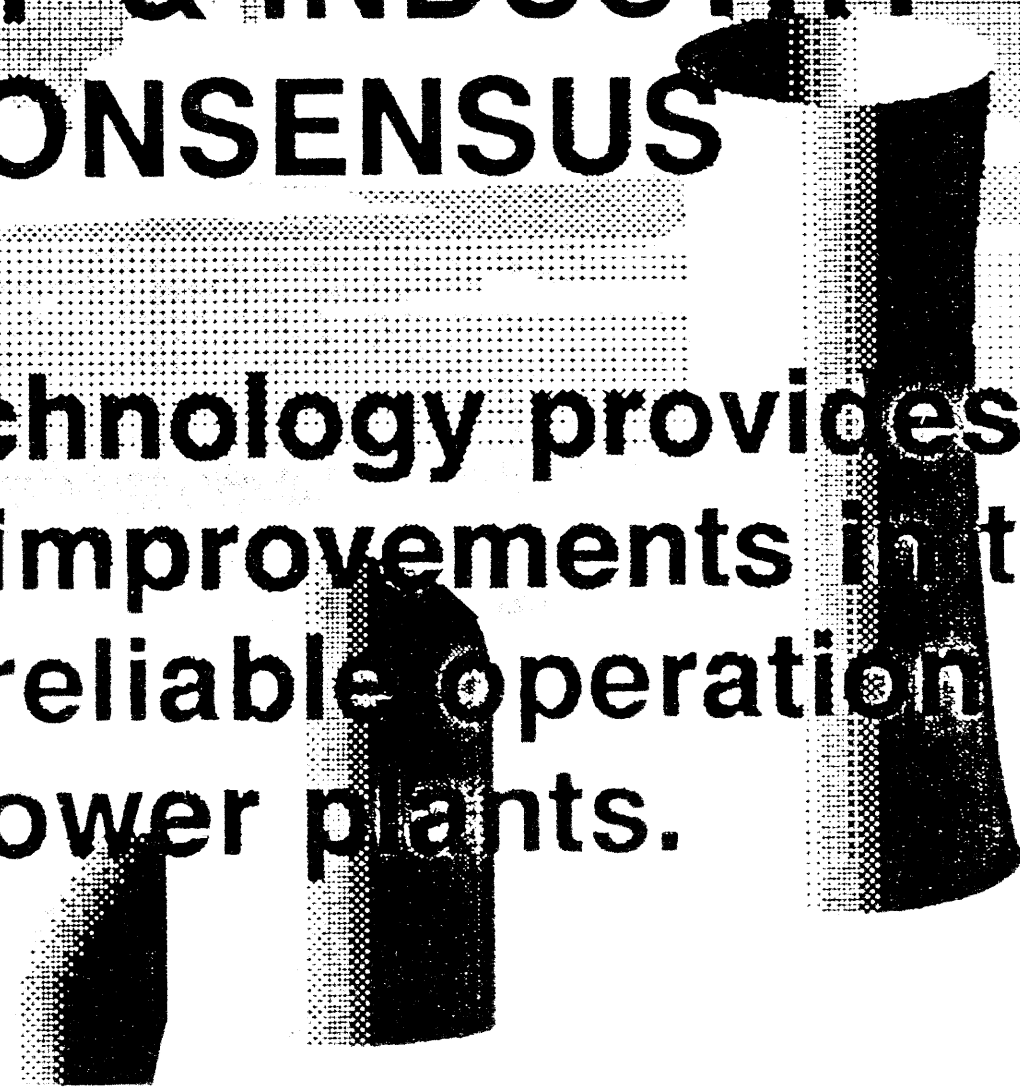
THE NRC STAFF RECOGNIZES THE POTENTIAL FOR ENHANCED SAFETY AND RELIABILITY THAT DIGITAL COMPUTER SYSTEMS BRING TO THE NUCLEAR POWER INDUSTRY.

THE NRC STAFF ALSO RECOGNIZES THE CHALLENGES TO SAFETY THAT ARE UNIQUE TO DIGITAL SYSTEMS, AND HAS PROPOSED PRUDENT MEASURES FOR THEIR APPLICATIONS IN FUTURE ADVANCED NUCLEAR POWER PLANTS.

REGULATORY PERSPECTIVE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS FOR FUTURE ADVANCED NUCLEAR POWER PLANTS

Matthew Chiramal
Instrumentation & Controls Branch
Division of Reactor Controls & Human Factors

STAFF & INDUSTRY CONSENSUS



Digital technology provides potential improvements in the safe and reliable operation of nuclear power plants.

DIGITAL COMPUTER-BASED SYSTEMS DIFFER SIGNIFICANTLY FROM ANALOG SYSTEMS

- Data transmission, functions, and process equipment are shared to a greater degree
- Digital systems rely on software

REGULATORY APPROACH FOR DIGITAL APPLICATIONS IN ALWRS

Identifed in SECY 91-292

Use existing regulatory requirements

Participate in national and international code and standards committees

Use information exchanges, conferences, meetings, research efforts, experts

Use EPRI Utility Requirements Document guidelines

CONTRACTOR SUPPORT

A multi-disciplinary team of technical experts assist the NRC staff in identifying and resolving digital systems issues

- ISSUE -

DIGITAL SYSTEM VULNERABILITIES TO COMMON MODE FAILURES

DIGITAL SYSTEM COMMON MODE FAILURE IS AN NRC ISSUE

- Digital systems use identical hardware and software in redundant channels
- Quantitative estimates of software reliability cannot be determined
- Hardware design errors and software errors may result in a common mode failure
- Regulatory requirements do not address software quality and CMF
- No concensus standards for certifying digital system I&C designs in nuclear power plants

IAEA07/MEW

QUALITY AND DIVERSITY PROVIDE SOME ASSURANCE OF DEFENSE AGAINST COMMON MODE FAILURES

THE NRC STAFF PROPOSES USING A PLANNED HARDWARE-SOFTWARE INTEGRATED DEVELOPMENT PROCESS

THE SOFTWARE DEVELOPMENT PLAN CONSISTS OF:

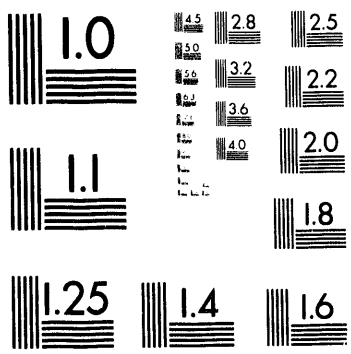
- Software Management Plan
- Configuration Management Plan
- Verification and Validation Plan
- Software Quality Assurance Plan
- Software Safety Plan

THE REQUIREMENT FOR DIVERSITY IS BASED UPON THE OPINIONS OF EXPERTS, AND ASSESSMENTS OF DIGITAL SYSTEM PERFORMANCE IN SAFETY-CRITICAL MEDICAL TREATMENT FACILITIES, FLY-BY-WIRE AIRCRAFT, AND NUCLEAR POWER PLANT PROTECTION SYSTEMS

NRC STAFF POSITION

- Applicants must assess the defense in depth and diversity of the digital system
- Applicants must provide independent backup manual controls
- Applicants must provide independent backup displays of safety-critical functions

NRC POSITION ON DEFENSE-IN-DEPTH AND DIVERSITY


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6

5 of 6

Position 1

The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common mode failures have been adequately addressed.

Position 2

In performing the assessment, the vendor or applicant shall analyze each postulated event that is in the analysis section of the safety analysis report (SAR). The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

Position 3

If a postulated common-mode failure could disable a safety function, then a diverse means, with documented bases that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function.

Position 4

A set of safety-grade displays and controls shall be provided in the main control room for system-level actuation of critical safety functions. The displays and controls shall be diverse and independent from the safety computer system identified in Positions 1 and 3.

The NRC staff recogriize the potential for enhanced safety and reliability that digital systems bring to the nuclear industry.

The NRC staff a so recog ize the challenges to safety that are unique to digital systems implementations.

SESSION 6

MODERNIZATION

Experience in Installing a Microprocessor-based Protection System on a UK Nuclear Power Plant

Reactor Safety Instrumentation of Paks NPP (Experience and Perspective)

Strategy to Safety Grade Systems Replacements

EXPERIENCE IN INSTALLING A MICROPROCESSOR-BASED PROTECTION SYSTEM ON A UK NUCLEAR POWER PLANT

by

C D JONES* and I C SMITH**

* Nuclear Electric plc, Dungeness 'B' Power Station, Romney Marsh, Kent TN29 9PX, England

** AEA Technology, Winfrith, Dorchester, Dorset DT2 8DH, England

ABSTRACT

This paper describes a recently completed project to install a microprocessor-based reactor protection system on a twin reactor station in the United Kingdom. This represented the first application of digital technology as part of such a system in the UK. The background of the application and details of the chosen solution are provided. The experience gained during the installation, commissioning and early operation of the equipment is reviewed by the operator. Interactions between the utility and the regulatory body are outlined and the impact of the regulatory process on the utility's resources and the project timescales are discussed.

1. BACKGROUND

Dungeness 'B' was the first of the Advanced Gas-Cooled Reactor stations to be ordered by the Central Electricity Generating Board (now Nuclear Electric plc). Construction was started in the late 1960s but suffered delays during construction. The station was designed to have an output of 660 MWe from each of the graphite-moderated CO_2 gas-cooled reactors. Each reactor has 408 fuel channels containing 7 fuel elements. The fuel elements consist of graphite sleeves holding 36 stainless steel clad uranium dioxide fuel pins. The fuel in each channel is attached to a plug unit which acts as a closure to the reactor pressure boundary. When in operation coolant gas flows up through the fuel and the lower section of the plug unit. Gas flow in each channel is controlled by the action of a motor driven sleeve valve (referred to as a "gag"). The flows are adjusted to maintain constant channel gas outlet temperature across the core.

In the original design assessment it was considered that the integrity of the plug units and associated gag mechanisms was sufficiently high to support claims of very low probability of gag failure or spurious closure. In the mid-1980s it became apparent that the integrity of the gag mechanism could no longer be justified. Fault studies conducted at the time indicated that closure of a gag at full power (CGOT of 675°C) could result in an unacceptable release of activity. The studies indicated that for gag failure a system providing rapid shutdown initiation, of the order of ten seconds, would be required. Until this could be implemented operation was limited to a temperature of 590°C, representing a limitation to around 400 MWe. Compliance with the temperature limit was based on alarm indication from the existing data processing system, the reactor protection system and a temporary data logger. The Safety Case during this period was based on operator action to shutdown the reactor within 30 minutes of a gag failure in response to high temperature alarms. The financial penalty of this limitation provided considerable pressure on the installation of the protection system.

2. SYSTEM REQUIREMENTS

The requirements of the system were determined to be as follows:

- To monitor the installed pair of thermocouples in each of the 408 fuel channels.

- To compare the signals from the thermocouples to a preset high trip level.

- To initiate a reactor trip demand via the existing four channel reactor protection system in the event of a high temperature in any single channel.

- To have a reliability of the order of 10^{-3} failures per demand whilst maintaining a low spurious trip rate (the initiating failure rate being 10^{-4} per annum).

The above requirements were interpreted as requiring a four channel protection system monitoring the two existing thermocouples. The trip system logic required was to trip the reactor if the four protection channels provided a majority (any two channels) demand for trip with respect to any single fuel channel, the required system was thus to be effectively 408 parallel sets of 2-out-of-4 tripping logic.

At an early stage it was determined that buffering would be required between the channels sharing the same thermocouple and also between the existing equipment that used these thermocouples. Such an arrangement represented a departure from general UK practice for a protection system but was supported by detailed examination of the possible failure modes coupled to the impracticality of providing additional sensors.

Whilst not written into the contract requirements, an important feature of the project was the perception of the maintenance burden that would have to be accepted by the station. This would always have been a secondary concern with respect to the considerable financial benefits of installing the system, however the requirement to minimise maintenance costs deeply influenced the station staff's view of the system.

3. THE CHOSEN SYSTEM

Having determined the overall requirements of the project the job of designing, installing and commissioning the system was placed out to tender to several companies.

In the end two options were considered; one essentially analogue, the other digital. The contract was awarded to AEA Technology to provide a system based on their ISAT™[1] digital technology.

The choice of a digital system for use in a reactor protection role was a significant step for Nuclear Electric. The system represented the first application of digital technology for reactor protection and there was considerable concern over the problems to be faced both in assessing the system within Nuclear Electric and in convincing the regulator, the Nuclear Installations Inspectorate (NII), of the adequacy of such a system.

---

1. ISAT is a trademark of AEA Technology

4. SYSTEM ARRANGEMENT

The Single Channel Tripping System (SCTS) installed on the two Dungeness 'B' reactors is a fail-safe computer-based protection system supplied by AEA Technology and based on their ISAT™ digital technology.

The SCTS monitors two thermocouples from each of the 408 fuel channels in each reactor. The protection system is sub-divided into two (north and south) sets of four identical safety channels. Each set operates on a two-out-of-four basis with each thermocouple being duplicated to two channels. Hence, whilst any single thermocouple recording out of range will invoke a trip, failure of any electronic module, such as the isolation amplifier, will not generate a trip. A schematic diagram of the system is shown in Figure 1.

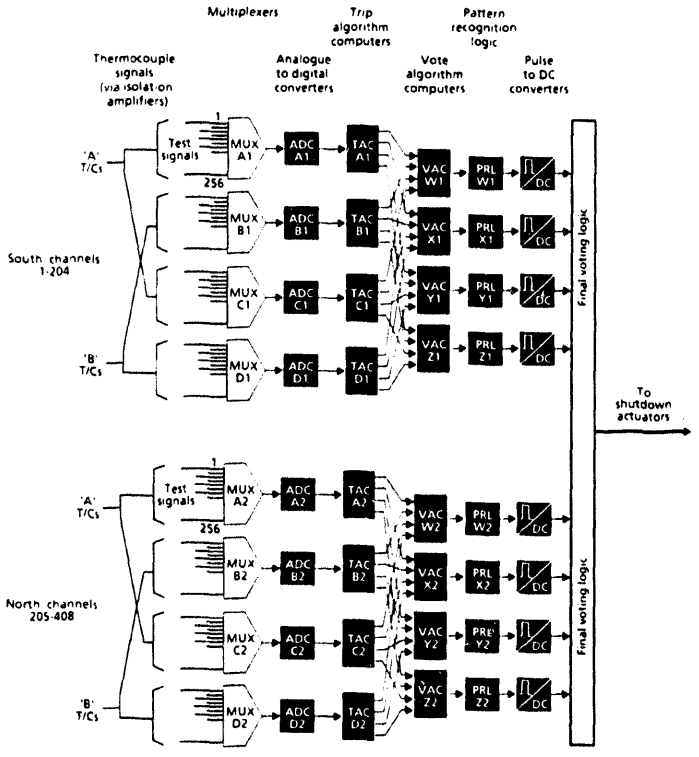


Figure 1

Schematic Diagram of the SCTS

The key element of the ISAT™ system is the use of interleaved test signals. These are generated as simulated thermocouples, which are scanned in exactly the same way as real signals. If these test signals are correctly scanned, they will generate a trip demand in the Trip Algorithm Computers which is passed via the vote computers to present a unique pattern of trip and healthy

signals to the Pattern Recognition Logic. This unit checks the voted output data stream for the correctness of the pattern. Any failure to match with built-in reference patterns collapses the square output provided by the PRL. Thus a healthy signal is an alternating square wave while a genuine reactor trip condition or a failure of a PRL board produces a static output.

The output square wave from each of the four safety channels is cabled as an alternating signal to the reactor safety trip system. At that point the alternating signal is passed through a pulse to d.c. converter to provide the necessary d.c. excitation current to the existing magnetic logic circuits. If and when the alternating output from the PRL goes static, the d.c. output current from the pulse to d.c. converter collapses initiating a reactor trip.

An administratively-controlled key system is included to permit a by-pass (veto) on selected channels where a failed thermocouple exists.

An important feature of the ISAT™ dynamic protection system is the provision of powerful diagnostics. A second output data stream is taken from the DCS and this, together with data supplied from the VAC computer, is passed to two ring buffers. Each holds 20 seconds worth of data. This data is then transmitted via Industry standard Ethernet to a monitor computer in the Control Room. This computer monitors the state of the equipment, alarms if an instrument fault occurs and indicates which module is faulty. A printer logs all faults giving time of occurrence and time of return to full service. The system also logs all by-passes put on and taken off, the plant data and the state of the RPS. Following a genuine reactor trip the 20 seconds leading up to the trip is available for analysis via the monitor computer. This can greatly speed up determination of the cause of the trip and hasten the return to power process.

5. PROJECT MANAGEMENT

The task of managing the provision of the new system was allocated to the Projects Division of the CEGB. Generation of the Safety Case was provided by the utility's Technology Division.

AEA Technology were given the contract to design, install and commission the new system. A condition of the AEA contract was to provide all supporting material required to allow the utility to assess the performance and safety aspects of the system and thus generate the Safety Case.

6. THE ASSESSMENT PROCESS

6.1 Background

In the UK nuclear utilities operate within a regulatory regime that devolves considerable regulation to the utility itself. This regime of self-regulation has two important implications. The regulator largely places the onus for assessment and approval of modifications to the plant onto the utility itself, with the regulator retaining a role of carrying out

independent assessment to a breadth and depth dependent on the significance of the perceived hazards. Secondly, the regulator generally acts in a non-prescriptive manner. Guidelines describing overall targets for attaining a satisfactory level of safety are provided but details on how to design or assess plant are not.

In all cases, the individual Station Manager has the prime responsibility for maintaining safety. Changes to the plant that have a significant impact on nuclear safety or involve changes to the principles on which safety arguments have been based have first to be approved by HSD, then by the Nuclear Safety Committee, a body formed of suitably competent individuals (some independent of the utility). Finally, this level of change is assessed independently by the regulator.

For this type of project the normal practice would have been for the design of the system to be verified by the contractor under the appropriate QA procedures. The system design and the other wider safety implications would have been assessed by the utility personnel creating the Safety Case. On completion the Safety Case would have been assessed within the company and, when considered satisfactory, passed to the regulator. Both the design assessment and the Safety Case arguments would normally be closely based on previous experience on similar systems.

6.2 Assessment of this Project

For this project the financial pressures warranted commencement of system design and manufacture prior to completion of the Safety Case. Early contact was made with the regulator and the project aims and general safety arguments were outlined. Agreement was reached on the level of preparatory site works that could be allowed.

The initial safety arguments were based on the approach that the self-checking nature of the system and the very small quantities of safety-critical software involved would allow a Safety Case to be generated without reliance on formal assessment of the software. This approach was supported by AEA and an independent assessment of the reliability of the system was commissioned with the Safety and Reliability Directorate of AEA. This assessment was based on Failure Mode and Effects Analysis (FMEA) of the hardware, the software being judged to be of sufficient integrity when coupled to the self-testing hardware configuration as to not significantly degrade the hardware reliability.

As a result of the complexity, novelty and overall time constraints a decision was taken that the Safety Case assessment within the utility would be supported by an assessment to be undertaken by an independent contractor.

As the production and assessment of the Safety Case progressed, it became clear that the original concept of not formally assessing the software would create problems when attempting to present the safety and reliability arguments to the regulator. To overcome this the software of the TAC, VAC and HIDAC scanners was assessed using the static analysis tool MALPAS. This assessment showed the system to be free from any significant problems and

formed an essential feature in convincing the regulator, however, the late decision to undertake this work did affect the project programme.

7. INSTALLATION AND COMMISSIONING

7.1 Installation

Installation was carefully planned to be integrated within the planned duration of the first available statutory outage on each reactor. Wherever possible, preparatory work was completed prior to commencement of the outage. In this way significant amounts of cabling and termination work was completed early.

On the first reactor the equipment was installed in advance of completion of the assessment of the Safety Case. This philosophy was agreed with the regulator in the clear knowledge that if the equipment had not completed its safety assessment by the end of the outage, then it would not be connected into the existing protection system.

By the end of the outage the assessment had progressed to the point of acceptance of the system as a replacement of the existing high temperature alarm system, but not as a qualified protection system. The reactor was returned to power with the SCTS operational but driving an alarm rather than the protection system. This allowed a period of trial operation to generate confidence in the system whilst the assessment process came to a conclusion. Following a period of almost 6 months of passive operation the system was connected to the reactor protection system. Completion of this stage allowed reactor temperatures to be increased from 590 to 650°C.

On the second reactor the system had gained approval of the regulatory body. Installation was completed within the planned timescale with no significant problems.

7.2 Commissioning

Careful consideration was given to the principles to be applied during the on-site commissioning. Given the very large number of analogue measurement channels with the associated voting provided by the computers, simplistic channel by channel testing of both the analogue measurement accuracy and the majority voting was seen as a considerable threat to the timely completion of the project.

Each system was built within the factory and comprehensively tested. The testing demonstrated accuracy of all analogue channels and the functionality of the trip and vote computers.

Following installation at site the system was powered up and test run with no thermocouples connected. This had the benefit of allowing the system to run for some time during the outage. The self-testing nature of the design demonstrated that the system components had been successfully interconnected on site.

Given the arrangement of the system, with a trip demand being generated by any two signals with the same input address being found to be above the trip level, it was essential to demonstrate that the analogue signal paths were correctly connected from the pre-existing thermocouple wiring through to the input to the SCTS scanners. Many potential faults were considered where these potentially threatened the correctness of the signal paths. For example, the individual isolation amplifier chassis could be installed in the wrong order, however, this would be revealed by the system tripping from displacement of the test signals. These self-testing features of the ISAT™ design were invaluable in reducing on-site testing time.

In order to achieve the required functionality great care was taken to ensure correct connection of the plant signals. The procedure adopted was to take each signal one at a time and carry out an injection test. This would then result in the high temperature being indicated by the two SCTS channels sharing that signal, with the signal being checked to ensure that it was seen by the same input address on the two SCTS channels. The plant wiring was then connected to the existing thermocouple signal and the correct reactor temperature confirmed. This procedure was repeated for each and every signal.

8. OPERATIONAL EXPERIENCE

Following the successful conclusion of the assessment of the Safety Case by the NII, the system was commissioned on both reactors.

The first reactor was connected into the guardlines in March 1992. The second has run with the SCTS in service since the beginning of September 1992.

8.1 System Operation

To date, two spurious trips have occurred due to the SCTS. The first resulted from an open circuit thermocouple signal, eventually traced to a suspect crimp termination. The second trip occurred due to a human error in carrying out fault investigation on other protection equipment connected in parallel to one of the CGOT thermocouples. Both of these types of trips were expected. Early in the project it was decided to modify the design of the trip system software to introduce a delay of several hours into the low trip algorithm and thus ameliorate the effects of such faults. This work was postponed in preference to early completion of the equipment in its original configuration. This work has now been completed satisfactorily on both reactors.

8.2 Maintenance Aspects

Maintenance of the system centres around the monitoring system. The monitor provides alarms to warn of system component failure and also allows the operator to examine all analogue and trip demand signals within the system.

The maintenance requirements were expected to be dominated by the random failure rate of the large number (1700+ per reactor) of isolation amplifiers and the 400+ buffer amplifiers used on the shared signals. Whilst a number

of these have been changed, some have since proved to be healthy, the fault actually being traced to a suspect connection or faulty scanner. Failure rates of the isolation amplifiers has remained lower than predicted.

Some problems have been experienced with the HIDAC scanners. A high turnover of scanners has been traced to very infrequent intermittent faults on two individual units. The diagnosis of these failures occupied an extended period due to the very infrequent nature of the fault. These have now been satisfactorily repaired and the failure rate has dropped to a very low level. Even with the above faults included, the scanner performance has so far exceeded that predicted by the manufacturers.

The Intel single board computers have proven to be highly reliable; to date only one board has been changed.

Given the quantity of equipment involved the maintenance burden has so far proved to be surprisingly low.

The extent of routine in-service testing required to confirm system functionality and accuracy is comparatively low. Testing of the trip function from the VAC through to the existing guardlines is accomplished using push buttons that enable the serial input links to the VAC to be interrupted. The cessation of any single serial line should not initiate a trip on the VAC if the remainder of the system is healthy. The operation of any two push buttons causes the VAC to trip. This is confirmed on each channel for every 2 out of 4 combination every 3 months, this interval is in line with the routine proof-testing of all existing protection equipment.

Testing of the analogue measurement channels is performed by regular and routine comparison of the four available measurements of the two thermocouples in each fuel channel. This comparison is performed by a PC-based system that monitors the data available on the Ethernet link to the main system monitor. This task is undertaken weekly to satisfy the Safety Case, although more regular checks are currently performed in order to gain experience of both system and thermocouple performance.

The comparison check is proving to be an essential tool in monitoring the operation of the system. The comparison system provides a printout of the total spread in the readings of the four measurements associated with each fuel channel. These four readings come from the two thermocouples and thus it is possible to discern both drift in the measurement accuracy of each SCTS channel and the potential drift of one thermocouple with respect to the other.

At present the comparison only provides a measurement for the single scan of data at the instant the comparison programme is run. Originally it was expected that small channel to channel variations would be masked by the random variations of several bits due to system noise (approximately 0.5°C per bit). Experience shows that it is proving possible to discern very small deviations between either the SCTS channels or between thermocouples. Figure 2 shows a typical graph of the overall measurements from a single fuel channel with no apparent problems. Figure 3 shows a larger overall spread which in Figure 4 is seen to be due to a varying deviation between the two

sensors. Evaluation of this data is providing confidence that incipient faults will be revealed before they compromise system operation.

It is now intended that the monitoring function described above should be provided as a continuous on-line monitoring function. This "Health Monitoring" system will be connected to a spare port on the installed Ethernet. The configuration of the trip system with uni-directional fibre optic links to the Ethernet allows such additional monitoring facilities to be added without risk of compromising the trip system reliability.

9. CONCLUSIONS

The use of the novel ISAT™ digital technology has allowed Nuclear Electric to successfully implement a majority voting trip system of unusually large size. The provision of this system has allowed a significant increase in the availability of the affected plant.

The system architecture has allowed the in-service test burden to be minimised whilst maintaining system reliability.

The use of a programmable system has allowed changes to the system functionality without significant changes to the hardware.

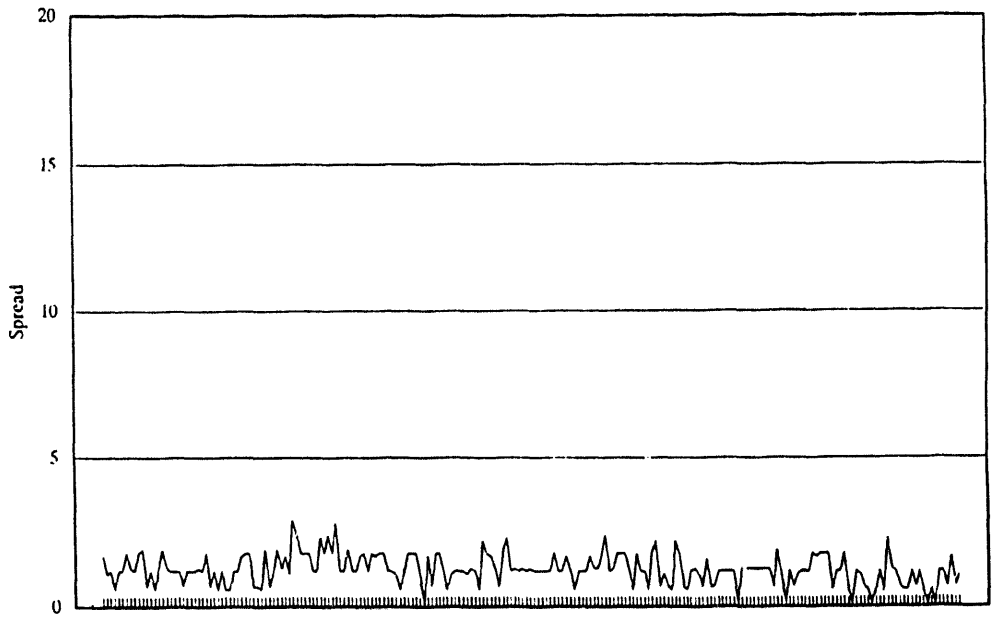


Figure 2

Variation in Spread for Thermocouples A and B
R21 - fuel channel B14

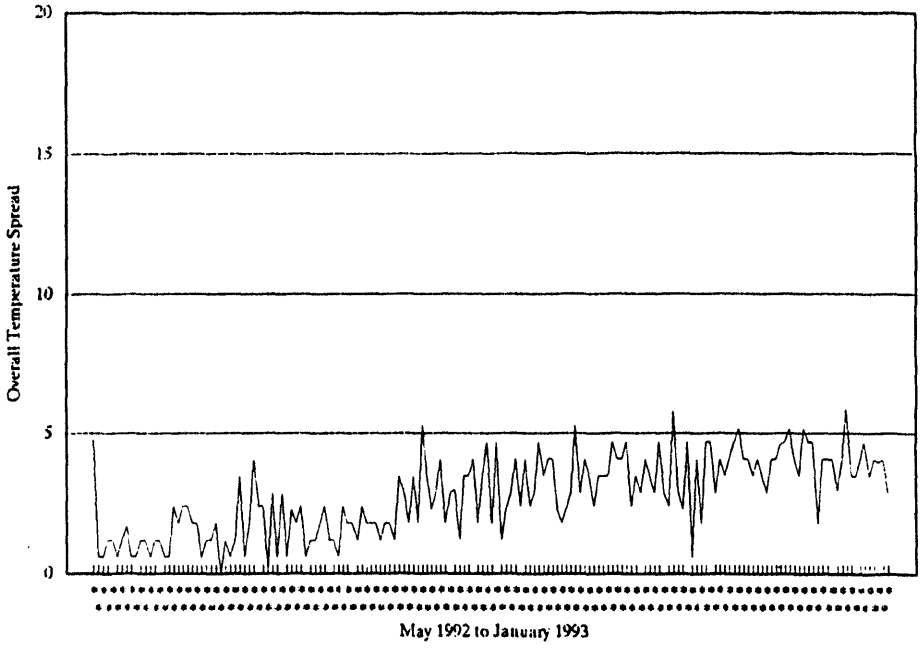


Figure 3

Spread of CGO Thermocouple Readings for R21 - fuel channel S12

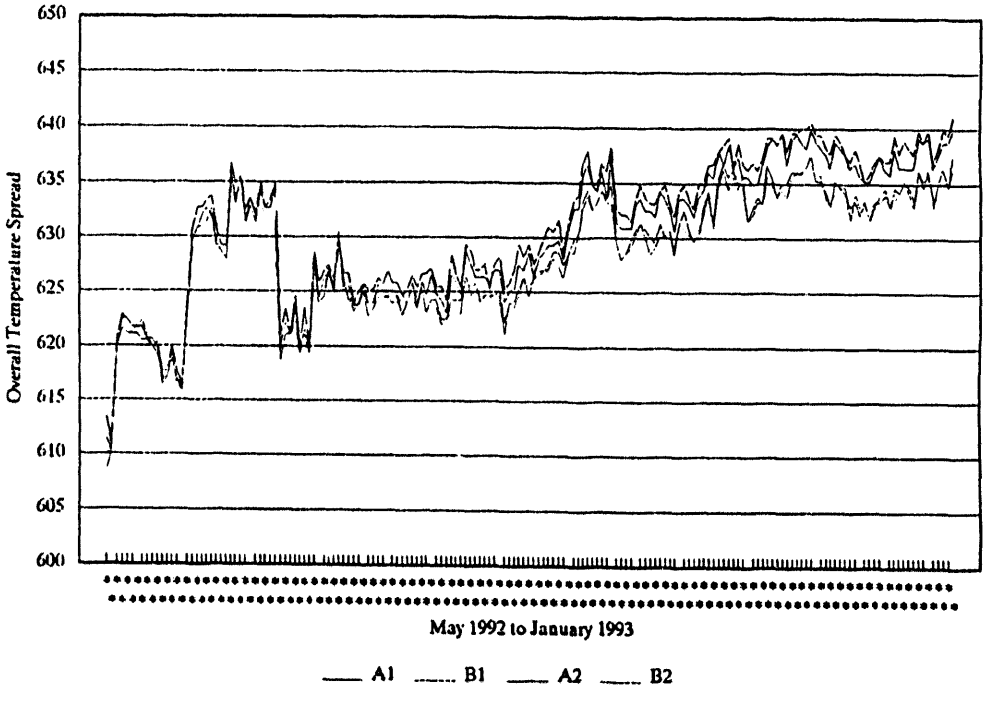


Figure 4

Spread of CGO Thermocouple Readings for R21 - fuel channel S12

LIST OF CAPTIONS

Figure 1. Schematic Diagram of the SCTS

Figure 2. Variation in Spread for Thermocouples A and B R21 - fuel channel B14

Figure 3. Spread of CGO Thermocouple Readings for R21 - fuel channel S12

Figure 4. Spread of CGO Thermocouple Readings for R21 - fuel channel S12

Reactor Safety Instrumentation of Paks NPP

(Experience and Perspective)

Presented

by

Sándor ÉLŐ and Károly HAMAR
Hungarian Atomic Energy Commission

at

the Specialists Meeting on
Experience in Ageing, Maintenance and Modernization of I&C Systems for Improving Nuclear Power Plant Availability

5 - 7 May, 1993
Rockville, Maryland, U.S.A

INTRODUCTION

The majority of the existing control and protection systems in nuclear power plants use old analog technology and design philosophy. Maintenance and the procurement of spare parts is becoming increasingly difficult. In general there is an age degradation concern.
Ageing degradation in nuclear power plants must be effectively managed to avoid a loss of vital safety function, shutdown of the station, a reduced power generation, or any failure leading to expensive repair.

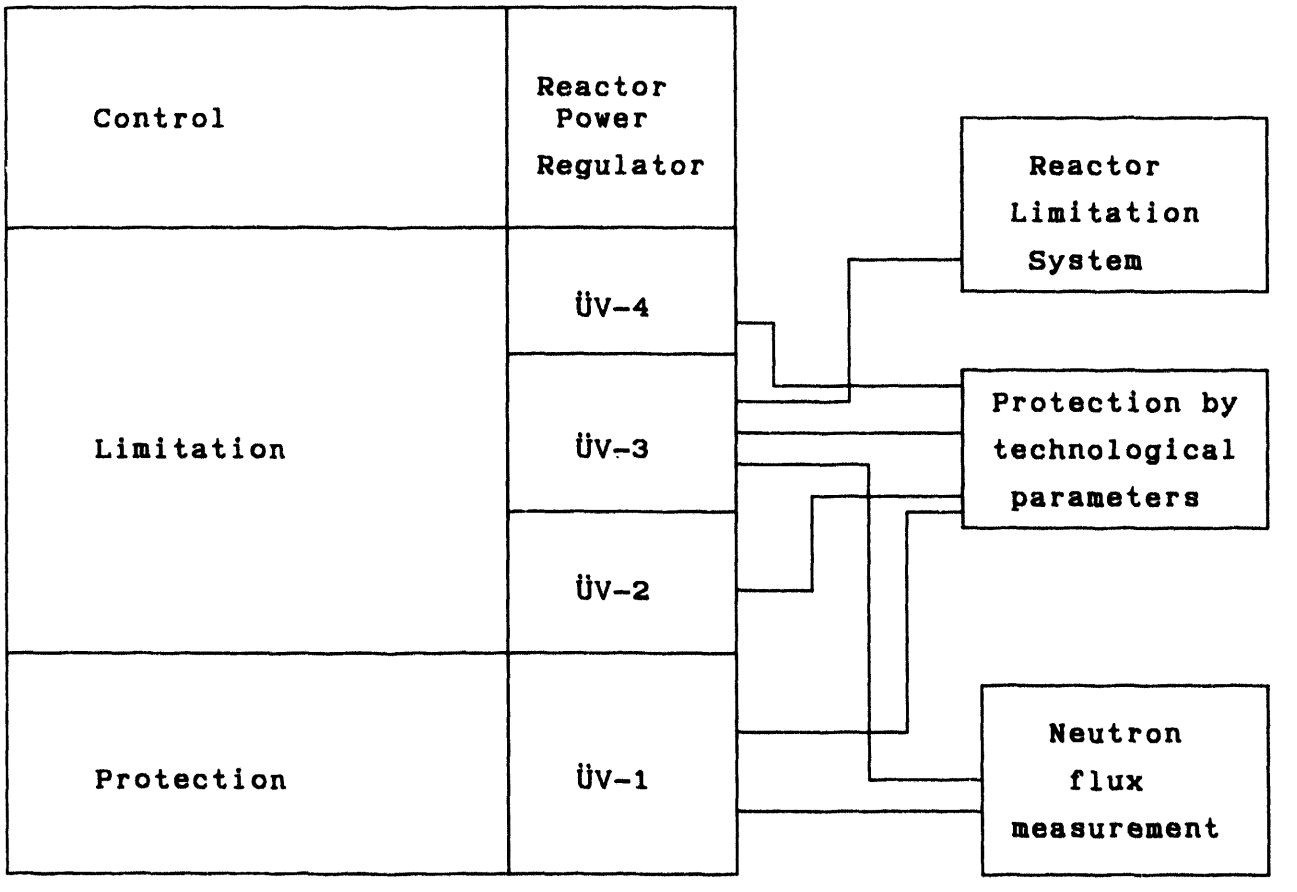
Even with the best efforts in developing realiabale and long life I&C systems for nuclear power plants it is expected that these systems for most plants will require replacements during the life of the plants. The instrumentation and control system of the nuclar power plants designed during the 7o-s and constructed in the 80-s went out-of-date since the nuclear safety is not a static concept and the digital computer technology had undergone rapid improvements during the 7o-s and 8o-s. Simultaneously the operation and the maintenance of the I&C system of those plants described above becomes more and more difficult and expensive. In this context the pure quality of the former Soviet designed process instrumentation system increases the needs of upgrading this system.
In our presentation first I would like to review the main design characteristics of the reactor safety instrumentation of the Paks NPP. Further on I will try to convey to you our view on upgrading the reactor safety instrumentation as seen by the HAEC and its Nuclear Safety Inspectorate.

1. Design and Structure of the Reactor Safety Instrumentation and Control

The I&C systems of the VVER 440/V213 design have been mentioned several times to be one of the weakest points of design. One of the main arguments supporting this opinion is that neither fulfilment of the single failure criterion nor redundancy and diversity of systems have been analyzed formerly in a fully consistent manner. Another one is the deficiencies in manufacturing and in quality assurance.

In the following the basic design concept for the systems, structures and components of the Reactor Safety Instrumentation of Paks NPP will be described. **One of the main feature of Reactor Safety Instrumentation** as it will be shown , that **the different functions of the system (Control - Limitation - Protection) are not separated entirely.**

D e f e n s e in d e p t h



Reactor safety instrumentation

Reactor protectection including:
- Protection by technological parameters (RTV)
- Neutron flux measurement system (NER)
- Central protection panels (PAZ)

Rod movement control system (SZBVR)

Reactor limitation system (RTK)

Reactor power regulation (BTSZ)

Emergency core cooling system (ZÜHR) including:
- high pressure injection system
- low pressure injection system
- box spray-in system
- hydroaccumulators (passive)

Actions of the reactor protection systems

Action are divided into 4 classes:
(ÜV: abbrevation for Emergency Protection)

ÜV-4: Inhibit for withdrawal of the rods. (interruptable)

ÜV-3: Insertion of the rods with normal speed and in normal sequence. (interruptable)

ÜV-2: Insertion of the rods with high speed and in normal sequence. Startup of the boron injection pumps. (interruptable)

ÜV-1: Insertion all of the rods together with high speed (releaseing all drives). Startup of the boron injection pumps. Turbine trip. (uninteruptable)

Analog input signals for the reactor protection

ÜV-1

- Pressure at the core outlet — Pcore out
- Pressurizer level — Lpress
- Overpressure in the box — Pbox
- Pressure step on the core — dPcore
- Pressure decreasing rate in the steam collector — dPsteam/dt
- Stem generator levels — Lsg
- Neutron flux — Nflux
- Period of the neutron flux — Tflux

ÜV-2

- Pressure at the core outlet — Pcore out

ÜV- 3

- Pressure at the core outlet — Pcore out
- Temperature in the hot legs — Tleg
- Stem generator levels — Lsg
- Temperature step on the core (through the Limitation System) — dTcore
- Neutron flux — Nflux
- Period of the neutron flux — Tflux

ÜV- 4

- Pressure at the core outlet — Pcore out
- Temperature in the hot legs — Tleg

Reactor Power Limitation System (RTK)

Function: To limit the reactor thermal power according to the number of MCPs in operation

MCPs in operation	Maximum allowed power
6	103 %
5	86 %
4	69 %
3	50 %
2 or less	0 % (ŰV- 1)

Controlled parameter: Temperature difference between the cold and hot legs dT

Auxiliary supporting parameter: neutron flux

Action: ŰV-3 Redundant construction: 2x3 channel

Majority logic: 2 x 2 out of 3

Reactor Power Regulator (BTSZ)

Functions:

Neutron flux regulation: (basic mode)

- Keeping the flux by control rods within the deadband (+1 % of the setpoint)
- Keeping the main steam pressure by turbine valves within the deadband (44 +0.5 bar)

Main steam pressure regulation (in case of sufficient power variation)

- Keeping the main steam pressure by control rods within the deadband (44 +0.5 bar)

Events and actions of the emergency core cooling system

Small leak

-Opening of the valves of the high and low pressure injection systems

-Switch off the grid circuit breakers

Large leak

-Opening of the valves of the high and low pressure injection systems

-Closing of the box isolation valves

-Switch off the grid circuit breakers, iniciation of the Diesels start up program

High box internal pressure

-Opening of the valves of the low pressure injection and the box spray-in systems

-Closing of the box isolation valves

-Switch off the grid circuit breakers, iniciation of the Diesels' startup program, startup all of the emergency core cooling pumps

Main steamline rupture

-Startup of the emergency feed water pumps

-Opening of the valves of the emergency feed water pumps

-Switch off the grid circuit breakers, iniciation of the Diesels' startup program, startup all of the emergency core cooling pumps

Input signals for the emergency core cooling system

- Overpressure in the box — P_{box}
- Pressure at the core outlet — $P_{core\ out}$
- Pressurizer level — L_{press}
- Pressure decreasing rate in the steam collector — dP_{steam}/dt
- Temperature in the hot legs — T_{leg}
- Stem generator levels — L_{sg}

Control rod banks

37 control rods divided into 6 banks

For shutdown: 5 banks, 6 rods in each. These rods are fully withdrawn from the core during normal operation

For fast power regulation: 1 bank, including 7 rods. These rods are particullary inserted into the core during normal operation

Rods belonging to the same bank are moving together during normal operation

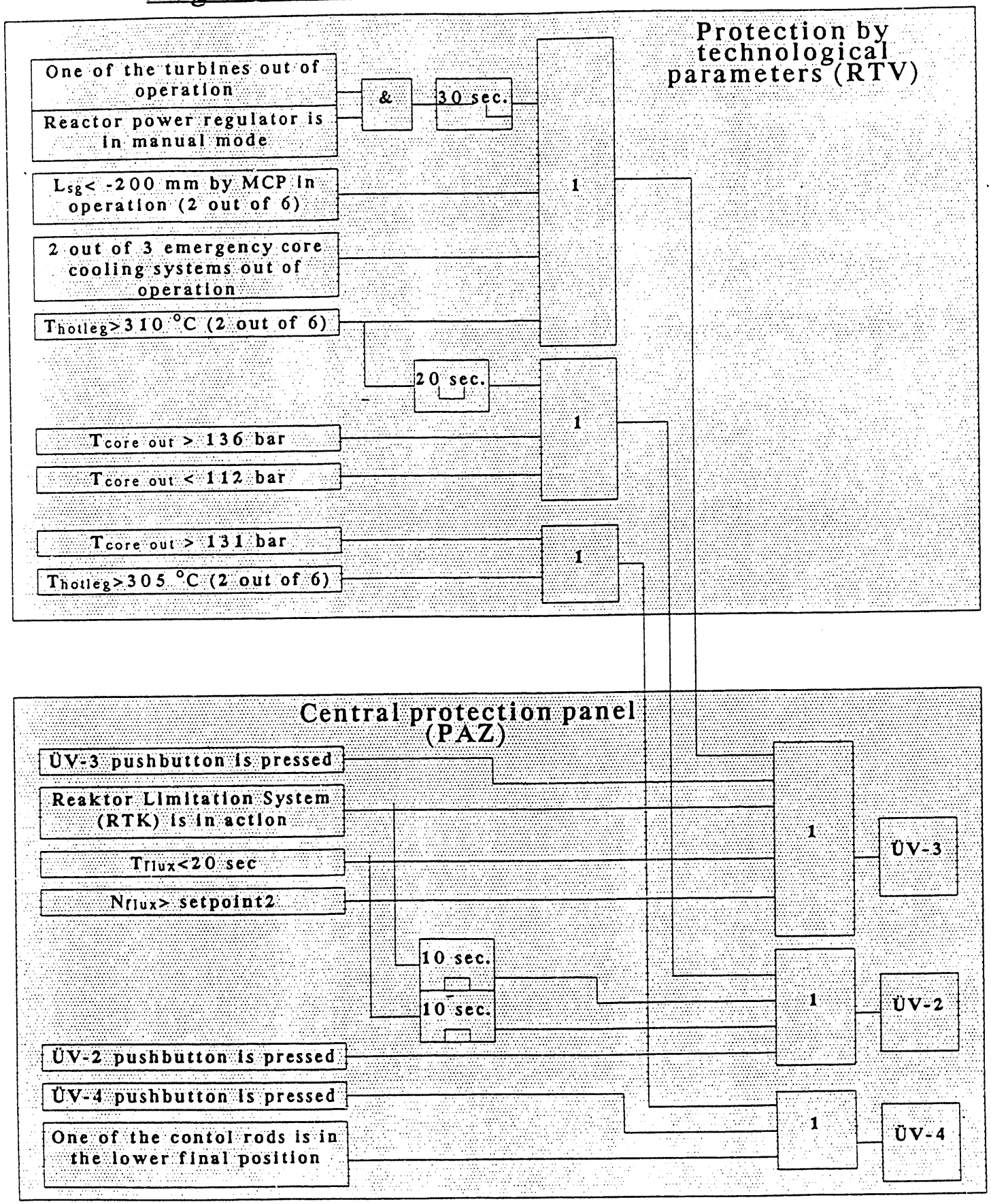
Two kind of movement for each rod:

- Normal speed: 25 mm/s (up and down, active movement by the rod drive)
- High speed: 250-300 mm/s (the drive is switched off, the falling rod is braked by a hydraulic brake)

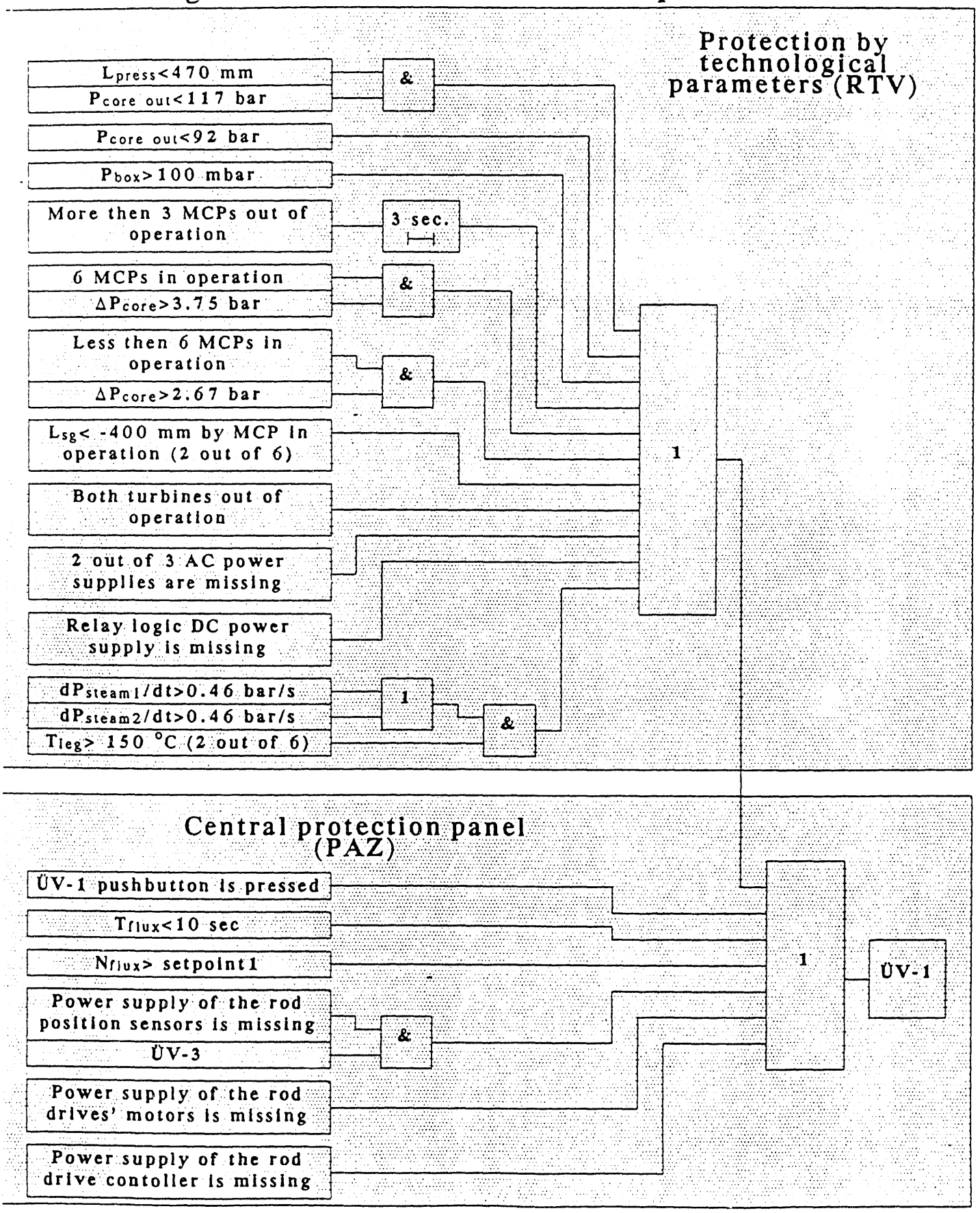
Rod movement sequence:

- Up: banks No. 1,2,3,4,5,6
- Down: banks No. 6,5,4,3,2,1

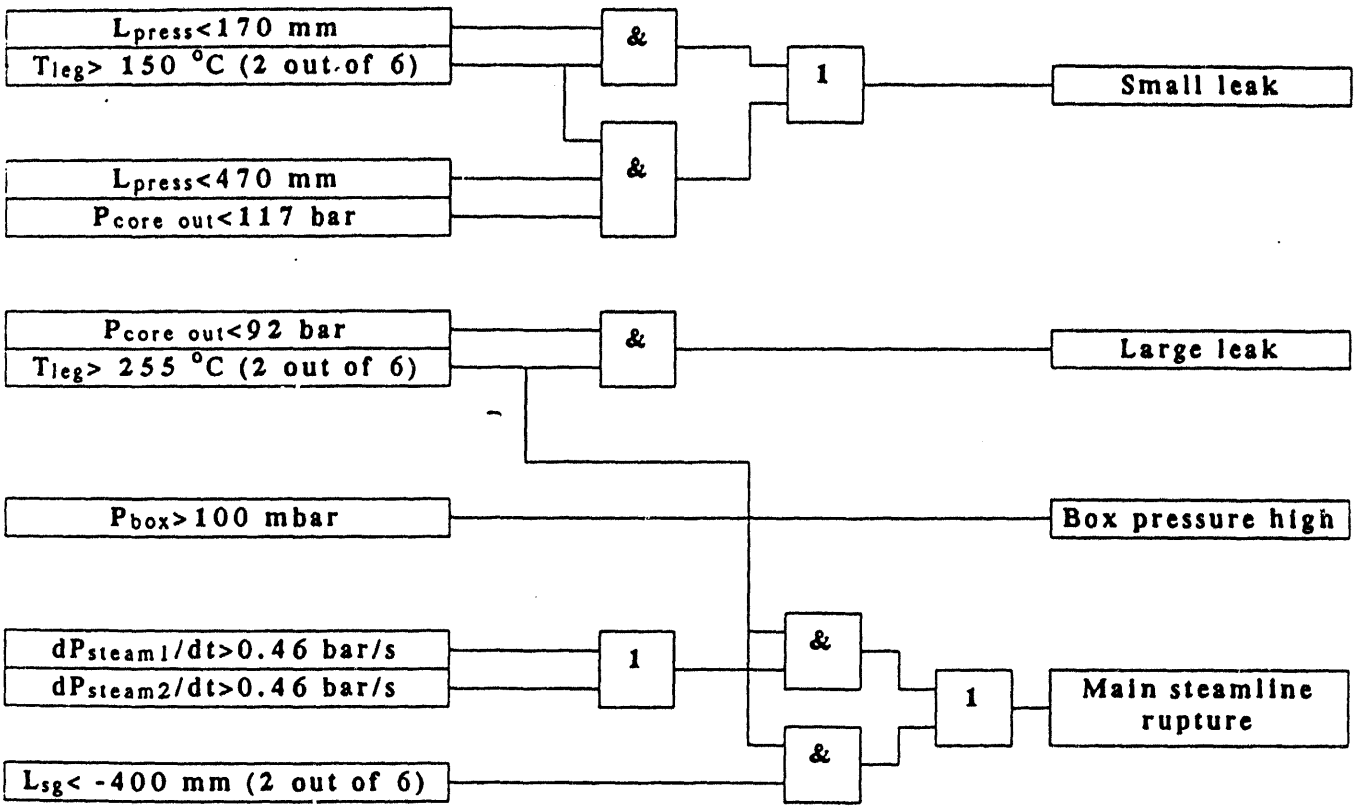
Logic structure of the reactor protection



Logic structure of the reactor protection



Emergency core cooling system—logic structure



2. Reasons for Upgrading the Reactor Safety Protection System

As it has already been mentioned, the most part of the I&C equipments have Soviet origin. The measuring instruments, the relay logic structure of the reactor protection system were designed in the late seventies, so their design concepts are nearly 20 years old.According to this fact, the replacement and modernization are continous tasks of both the nuclear operators and the regulatory organisation. The operators have already got more than 300 permissions to replace I&C equipment.
One of the motivations for modernizing is the lack of spare parts. On the other hand the incorrect behavior of measuring, comparing or switching elements urges the replacement. Up to now there is no change in the structure of I&C systems, only some design insufficiencies were corrected.

The 30 reactor-year experience accumulated at Paks NPP up to now shows that the operation of units is safe. The avarage availability factor for the plant for the last three years is over 86%,(concider refueling outage) the number of reactor scrams is around 1.5/year/unit.
In this 30 reactor-year period the Reactor Protection was actuated 54 times, and 15 of these 54 were human failure or due to hardware deficiencies . No such an event occured, when the system failed to operate in case of real demand for its actuation.

In consequence of slow decreasing of the reliability of relay logics which have been operating for ten years in the first unit, a new concept seems to win introducing programable logical controlers in reactor shut down and emergency cooling systems.

3. Brief Review of Current Plans in Upgrading the I&C

The management of the Paks NPP recognized the necessity and importance of upgrading the I&C system of the NPP and therefore an I&C team was established to work out the principles of this updating including all the aspects of design, installation and finances.

Taking into account the operational experiences, the I&C team focused its attention on upgrading the safety instrumentation and protection system of the plant parallel with the elaboration of the principles of this process.

The upgrading of I&C system of the plant on the one hand has to entirely meet the internationally accepted safety requirements and to increase the efficiency of the production on the other.

Since the safety protection system of the Paks NPP does not match entirely the internationally accepted criteria, i.e. according to an investigation which was presented in Bratislava in December 1990. The reliability of the new upgraded system shall be in full compliance with the internationally accepted value.

The main topics to be considered

- conception af a new emergency control room
- control of the station at plant level
- increasing the functionality of the process control systems
- entire separation of the different functions (operation,limitation, protection) of the present protection system
- fulfilment of the single failure criterion
- energy supply of the safety related I&C systems
- investigation of the seismic resistance of the I&C and its cabling

- replacement or retaining of the present cabling system
- degree of the preservation of the traditianal analog instrumentation
- investigation of the safety panel and its development
- post accident monitoring

4. The Transition from Analog to Digital Technology

In our view, there are many good reasons for not proceeding too rapidly towards digital technology in Hungary.

There is a general trend all over the world in the nuclear industry to harness the μP revolution for the benefit of nuclear power plant design, operation including improving the overall safety and availability of the plant. The existing nucleaar power plants are gradually replacing the obsolete analog systems with modern digital devices.

The transition towards digital equipment has been progressing on both a piecemeal basis and complete replacement of the analog equipment. For a number of reason in Hungary piecemeal changes have been made when problems with analog components have occurred to improve components reliability or simply because of lack of spare parts.

In accordance with the numerous safety concerns described in the relevant literature the following safety concerns have been set forth taking into account both the technical and regulatory aspects of the use of digital technology in safety related systems.

1. The increased information density in a single device greatly increases the consequences of a failure
2. More sever equipment environmental requirements
3. Difficulty of mixing equipment from different vendors
4. Potential for failure propagation
5. Lack of operational experience in a large digital system

Many of the unresolved problems we face are unfortunately associated with software reliability, as yet, software reliability cannot be accurately measured or predicted, so a qualitative and tailored form of engineering judgement is necessary.

In this regard we have the following important issues to cope with:

1. Safety classification of the I&C systems of the Hungarian NPP in acordance with the IAEA 50-SG D3, D8 guides

2. Lack of national standard for software engineering

3. There are too many standards relating to software reliability developed by different international organizations

4. None of the existing standards provide complete guidance as to how to handle digital I&C systems from the licensing point of view.

Process Computing

Replacing computer by computer: the early third generation technology computerized data aquisition systems will be upgraded and replaced by late third generation technology.
The early third generation data aquisition computers could privide simple presentation and display of technological parameters.
The early solutions provided alphanumeric displays and limited capability of archived data. Modernizing is going on continously, nowadays coloured shemes of technology with correct data presentation are available in the controll rooms. The reactor core is represented with a three dimensional temperature and neutron flux modell demonstrating the load of every fuel element and the axial power distribution. This system will be upgraded second time next two years.

General problems

A very important task in handling digital systems is the qualification of firms which prepare themselves for designing, for manufacturing and software developing. The qualifying procedure must be carried on the representatives of the home industry.
There are special conditions in the home economy. Big hungarian firms including the electric and electronical industry, now are not able to ensure the quality is desired nowadays in NPP.
On the other hand, engineers, experts and well qualified co-workers established new firms are ready to win tenders with low prices in the NPP.
One can see, they have no manufacturing background, no capital, and no goodwill. The nuclear regulator has the task to carry on the qualifying procedure.

SIEMENS

STRATEGY TO SAFETY GRADE SYSTEMS REPLACEMENTS

Paper presented at: IAEA/NRC/EPRI SPECIALISTS MEETING
Washington DC

May 5 - 7th 1993

Authors: Dr. Michael Stimler
Kevin E. Sullivan
Irfan Trebincevic

contact addresses:

Kevin E. Sullivan
IrfanTrebincevic
Siemens Power Corporation
P. O. Box 180
Bradenton, Florida 34206
USA
Tel: (813) 723 4053
Fax: 813-723-4210

Contents

1. Introduction

2. Siemens I & C Strategy
2.1 I & C trend in Nuclear Power Plants
2.2 Defense in depth concept.

3. Siemens Digital I & C
3.1 Policy for New Digital I & C Systems
3.2 Categories of I & C Tasks in a Nuclear Power Plant
3.3 Structure of an integrated digital I & C System

4. Safety I & C
4.1 Design Requirements
4.2 Strategy to Safety Grade System Replacement. Case History: Upgrade of Muenleberg (Switzerland) NPP Reactor Protection & Containment Isolation Systems
5. Operational I & C
5.1 System Concept
5.2 Design and Engineering
5.3 Functional and physical decentralization
5.4 Application of operational I & C in Staudinger 5

6. Qualification

7. Control Room Ergonomics

8. Summary

List of figures

1. Introduction

The introduction of digital instrumentation and control systems in nuclear power plants is characterized by the need to satisfy the requirements of safety, reliability and man-machine ergonomics. Today digital I & C systems meet these requirements and the trend in Europe (See Fig. 1) is towards full digital based nuclear power plant control systems.

This paper describes Siemens (KWU) experience in nuclear power plants and development in trends within Europe. Topics which are the subject of major concern to NPP operators addressed in this paper are:

Human Performance Factors - Man- Machine Interface

Operating Philosophy

Safety, Availability and Reliability

Other aspects addressed are: Siemens "defense in depth" concept, description of Siemens digital I & C systems, safety requirements and systems, I & C qualification, control room ergonomics, information systems and retrofitting experience.

2.1 I & C Trend in Nuclear Power Plants

In the past Siemens has employed hardwired control systems together with conventional control room design providing a hardwired parallel interface to the process (see figures 5 and 6). In addition computer based information systems have been used to provide additional data via visual display units (CRT's). Use of digital control systems in the field of e.g. operational reactor control has been implemented. To date most retrofits have been hardwired systems.

One main advantage of the hardwired solutions is the very high availability of these I & C systems, i.e. a very small contribution of the
I & C systems to the average unavailability of SIEMENS-KWU's nuclear power plants as shown in figure 7.

Today and for all future nuclear power plants digital control systems together with the use of display based control rooms will be implemented. Future upgrades will be with digital based systems.

2.2 Defense in Depth Concept

All sections of safety I & C are designed along an advanced philosophy of "Defense in depth". This means that all disturbances and faults are fought by suitable countermeasures. The safety I & C reacts in time and with the optimal intensity on any deviations from the normal condition. In most cases the system is successful in returning the plant into normal operation without disconnecting the plant.

Thanks to the smooth transients resulting from this approach severe stressing of the mechanical components is avoided. This philosophy is one of the reasons that KWU NPPs have a very low reactor trip frequency.

Within this philosophy prevention of faults is given higher priority then removal of faults.

The figure No. 13 explains the concept of "Defense in depth". During normal operation the variables vary within the range controlled by operational I & C. One recognize

- the setpoint and
- the deadband.

Within the deadband there is no intervention of I & C. If variables exceed the deadband they are returned towards normal values by means of operational I & C. If these should not be successful and major transients or disturbances occur in the plant, the core protection systems will take action with increasing intensity. One will recognize these intensities as indicated by the lines at various levels.

The core protection systems return the transients into the normal range without requiring a trip. Temporary load reductions may be necessary however. After the plant has returned to normal operation, full load operation might be feasible again.

If a transient cannot be stopped by the core protection systems, a fault condition might develop to an accident. Continued excursion would bring the plant into dangerous conditions. The reactor trip system will then trip the plant. Subsequently the reactor trip system will return all variables into a safe range.

3. Siemens Digital I & C in Nuclear Power Plants

3.1 Policy for New Digital I & C Systems

For digital system applications, continuous enhancement of safety, availability and cost-effectiveness is likewise the primary goal. Development of new I & C systems must also allow for the continuous process of improvement to advanced light-water reactors.

Fundamental goals are as follows:

- o safety standard must be maintained or improved even further

- o simplification of plant operation
  - by increased automation
  - by improved information systems as decision-making aids
    . in upset operation
    . for early detection of incipient damage

- o incorporation of further safety margins into the mechanical and I & C systems

- o maximum possible use of standard I & C products to achieve
  - high reliability by the use of proven hardware and the associated in-depth standard training package for the maintenance personnel

- high cost-effectiveness

o derivation of consistent verifiable engineering documents
  - by the use of computer-aided planning and design tools

o improved plant maintenance to minimize radiation exposure to personnel and to minimize the personnel requirement during outages
  - by plant components which allow automatic testing
  - by use of computer aided tools

Some constraints related to the properties of digital devices must be observed:

o increased information density within single devices and thereby greater consequences on device failure

o serial processing of programs with an impact on reaction time

o communication via local area networks

o modified environmental requirements

o large-scale data storage and data consistency throughout

o storage of a large amount of data which needs to be updated on device restart.

3.2 Categories of I & C Tasks in a Nuclear Power Plant

To give a harmonious and integrated overall concept for the digital I & C, the tasks of the I & C are subdivided into various categories in line with the importance to safety and operation of the nuclear power plant.

Category S1: I & C tasks that automatically initiate countermeasures in response to accidents where these countermeasures are required in the short-term to prevent inadmissible activity release to the environment, particularly by preventing core damage.
Main requirement: toleration of common-mode failures by diverse, prompt accident identification plus fulfillment of the single failure criterion.

Category S2: I & C tasks that automatically initiate countermeasures in response to accidents where failures of these tasks can only result in

inadmissible activity release or inadmissible core damage in the long term, but where these countermeasures are nonetheless initiated in the short term to minimize activity release to the environment.
Main requirement: toleration of common-mode failures by implementation of manual actions diverse to actions initiated by the automatic systems plus fulfillment of the single failure criterion.

Category S3: I & C tasks for manual or automatic process control for preventive and long-term assurance of safety functions and to assure functional capability of the safety systems.
Main requirements: fulfillment of single failure criterion.

Category B1: I & C tasks required for control of safety variables, for monitoring, testing, on-line diagnosis and for accident review and documentation, as well as other I & C functions with high reliability requirements.

Category B2: I & C functions for process control in normal operation.

Besides the main requirements each category is allocated specific design criteria. The appropriate qualification effort demanded for licensing is graded in line with the importance to safety in accordance with national and international rules and standards (e.g. KTA 3501, IEC 880, IEC 964, IEC 987).

3.3 Structure of an integrated, digital I & C System

The I & C in nuclear power plants is subdivided on the basis of the dedicated technical requirements into two main categories, the safety I & C and the operational I & C (s. Fig. 14).

The **safety I & C** serves primarily to protect personnel and environment against radiation exposure. The systems concerned essentially perform no actions under normal conditions but are required to operate on demand. The safety I & C essentially consist of the safety automation systems for reactor trip, engineered safety features, core protection and radiation monitoring as well as the control room back up and the process interface.

The **operational I & C** comprises all equipment required for process control during normal operation and anticipated operational occurrences:

- the control room with the process control systems and the control room backup
- the process information system
- the non-safety automation systems

. the plant bus system.

Safety I & C and operational I & C systems are of redundant configuration and have dedicated process interfaces. Mechanical equipment with both safety and operational functions are actuated by both types of I & C. Appropriate priority logic ensures that protective actions with extremely high reliability take priority over operational actions.

Signal exchange between safety and operational I & C is performed via a two-channel redundant plant bus system. The safety I & C has multi-channel fiber optic bus systems for signal exchange between the four redundant systems as well as to the processing interface and to the plant bus. Due to the conflicting requirements that it shall not be possible to disable the safety system manually but at the same time still be possible to implement severe accident management procedures, provisions will be made in future plants for severe accident management procedures from a central point, but with the actions possible limited to an absolute minimum.

To allow safe shutdown of the plant in the event of inaccessibility of the control room, a reduced size screen-based control console along with a safety information and control panel are fitted at the remote shutdown station.

4. Safety I & C

4.1 Design Requirements

The Reactor Protection System covers the Reactor Trip System as well as the Engineered Safety Features Actuation System:

The most important of these requirements can be summed up as follows:

i) at least two mutually independent criteria (diversity) shall be used to initiate a safety action; if this is technically impossible, at least different types of sensor equipment must be used for signal acquisition.

ii) the scope of automatic actions taken by the reactor protection system shall be such that no manual intervention is required within the first 30 minutes after the onset of an incident.

iii) the mutually redundant safety I & C subsystems of the reactor protection system shall be physically separated.

iv) it shall be possible to keep an incident under control even if two of the following three situations plus their respective consequential failures occur simultaneously:

(1) common-cause failure,
(2) random failure,
(3) testing/repair/maintenance.

Simultaneous occurrence of a common-cause failure with a random failure need not be postulated to occur within the first 100 hours of repairs.

v) the reactor protection system shall not govern the unavailability of the safety action.

vi) the reactor protection system shall be designed to be largely self-monitoring.

vii) safety actions shall take priority over normal operation control actions.

These requirements form the basis for certain fundamental approaches to the implementation of a German computer-based reactor protection system.

4.2 Strategy to Safety Grade System Replacement. Case History: Upgrade to Muenleberg (Switzerland) NPP Reactor Protecstion & Containment Isolation Systems.

Due to repeated equipment failures and ever increasing difficulties to obtain the necessary spare parts, the Reactor Protection System (RPS) was slated by the customer to either be replaced or be upgraded. Because of considerable risks and prolonged outage time, total replacemnt was rejected. Even the upgrade was considered as a formidable task to be realized within the scheduled outage time. European NPP's generally have short scheduled refueling outages of 30 to maximum 40 days which was the case with Muenleberg NPP in Switzerland. Therefore, a precise upgrade strategy had to be developed.

The customer stipulated that the existing protection system design concept and level of redundancy be retained. The improvements should be achieved by providing the state-of-the-art I&C concepts regarding improved withstand capabilities to earth quakes, lightning and internal system faults. The goal was to achieve longer intervals between inspections by use of the latest qualified and type tested I&C equipment which had to include active failure mode capabilities and processing of analog variables. Above all RPS monitoring/supervision/inspection needed to be improved.

To achieve all this, a "Feasibility" of project study has to be conducted to produce an accurate prediction of the entire project duration, costs, manufacture, factory tests and factory pre-starting including installation, commissioning and start-up, and finally the acceptance by the customer.

The obvious strategy Siemens has taken to accomplish the objection of the projects can be depicted from the time scheulde illustrated in Fig. #21.

Fig. 19 and 20 depict some of the improvements resulted from the project upgrades. The original relay based, fault prone RPS cabinets were grouped together in one location. A new row of I&C cabinets for RPS "C" & "D" groups have been installed in another location separated by a wall from the original RPS. Since the entire system was pre-tested/pre-startedup in the factory before shipment, the plug in cables used during pre-startup have been laid down in the existing cable trays. New RPS groups "C" & "D" have been erected during the "partial installation" time shown in Fig. 21 during which time the original RPS was still fully functioning. Later, during the final 40 days scheduled outage, new RPS groups "A" & "B" cabinets have been installed in its place.

The project was accomplished on time proving that our strategy was correct and should be considered for future jobs as well.

5. Operational I & C

5.1 System Concept

The overall structure of the operational I & C can be represented by a pyramid, this consisting of 5 superimposed layers. Each layer constitutes a hierarchical level which is to a large extent independent of the other layers. Autonomous communication modules are used to interconnect the separate levels. In the event of a fault at a high level, functioning of the lower levels is to a large extent unaffected. Autonomous communication interfaces also serve to reduce the expense associated with technical innovation within a single level, as each level can essentially be withdrawn as a whole and replaced by a new one (modular upgrading).

The five levels of the system are as follows:

- Process control level
- Communication level
- Group control level
- Coupling control level
- Individual control level

Mimic diagram displays serve for sequential operator control and observation on plasma displays driven by high-performance operation processors (type BP). Manual commands are input with the aid of a touch frame which uses infrared light to detect finger movements on the display, which the operation processor converts into commands to the group control level.
Operator actions are carried out in two stages:

- o selection of an item of equipment such as a valve by touching the appropriate symbol on the flow diagram on the display,

- o operation of the item by touching the soft key on the display simultaneously with giving a release command (two-hand operation).

5.2 Design and Engineering

Cost-effective and high-quality processing of large-scale I & C projects is only possible with uniform use of computer-aided design and engineering tools (CAD, CAE). These must include all design phases, from planning to commissioning. High-performance CAE tools are used for software development for the new digital I & C system. On the one hand, these are workstations on which function diagrams are generated graphically and translated automatically into machine code. On the other hand, high-performance programming devices using the language STEP 5 and incorporating a comprehensive library of standard function blocks considerably lessen the programming effort. The workstations and programming devices provide automated retrospective documentation of the programs input into the automation system.

Programs can be loaded either centrally via the plant LAN or decentrally via a programmer or by plugging EPROM modules into the group and coupling control level devices.

5.3 Functional and physical decentralization

The functionally decentralized structure is obtained by assigning the individual programmable controllers and the associated coupling processors to the functional groups and complexes in the process. As a consequence, largely autonomous islands of automation are established per programmable controller communicating with each other by means of the redundant plant LAN. This structure is further decentralized by assigning coupling processor systems to specific sub functions of a functional group. Hence the coupling processor systems are the smallest sub pyramids forming the islands of automation which in turn form the overall pyramid.

Process and group control level equipment is installed in a central electrical and I & C building. The coupling and individual control levels are installed in the central electrical and I & C building and also in all other process buildings. For this purpose, local, controlled-environment electrical and I & C centers (I & C compartments) are provided. Auxiliary and supporting systems in further buildings are connected to the central plant LAN using single-channel LANs and non-interactive repeaters.

Implementation of a physically decentralized concept does not always meet the full acceptance of the operations personnel because, due to the long distances, maintenance and service operations can involve more effort than in completely centralized concepts, but gives the benefit of reduced cabling costs using serial links for data transmission.

5.4 Application of operational I & C in Staudinger 5

The described operational I & C system was implemented in the 500 MW fossil fired power plant Staudinger unit 5. Based on the high degree of automation in this plant with more than 1200 remote controlled actuators, 260 open loop controls and 180 closed loop controls, a "Cockpit Control Room" concept was implemented which means that the plant is operated by one operator with the use of screen based control room equipment only (i.e. sometimes called "Joystick" control philosophy).

To fulfill this concept an advanced philosophy to structure power generating processes by the employment of "functional chains" was developed. This philosophy can be applied to NPPs as well and allows a more clear and transparent automation structure than before.

The implementation of the operational I & C system in Staudinger plant is part of Siemens qualification program for the application of this I & C system in nuclear power plants.

The first connection to the grid was in June 1992 and the hand over to the customer is scheduled for end of 1992.

6. Qualification

In the Federal Republic of Germany, qualification of modern I & C systems for use in nuclear plants is performed to the "safety standards" of the Nuclear Technology Commission (KTA). The specified procedures comprise either type

tests or the documentation of operating experience. For type testing an independent expert checks the qualification documentation provided by the manufacturer and checks proper performance of practical tests. The results of the tests are documented in a test certificate. A large number of the proven test procedures used to date (such as failure effect analyses) are not applicable for digital I & C systems. For this reason, an appropriate qualification concept was developed for BELT-D in conjunction with the independent expert (TÜV-Bayern) commissioned by the licensing authorities.

The basis for this is a new concept for subdividing the functions of the I&C into various categories in line with their significance for the safety and operation of a nuclear power plant as shown in chap. 3.2. The qualification strategy was specified on the basis of these categories for the functions of BELT-D:

- o qualification of hardware by type testing consistent with Nuclear Safety Standard KTA 3503,

- o qualification of software in parallel with development proper on the basis of a "procedure model".

The procedure model required step by step progress in development with the definition of process phases with milestones and reviews for release of the next phase. Major phases are:

- o definition of product specifications for hardware and software preparation of product requirement specifications for hardware and software
- o hardware development (prototype)
- o software development (basic design and implementation)
- o preparation of test specifications
- o component tests
- o system test

Before the start of development the manufacturer prepares work instructions and quality assurance procedures which give detailed and binding descriptions of all process steps of the procedure model and of the associated procedures.

The procedure model is based on the results of detailed review of the milestones by review teams comprising representatives of both the independent expert and the manufacturer. The task of this team is critical analysis of all the product and product requirement specifications against the conceptual formulation and the product implementation envisaged. The team also checks for completeness, correctness and consistency here. The independent expert additionally checks the documents for compliance with applicable rules,

regulations and standards (for example KTA, IEC, IEEE, IAEA, s. fig . 15) and with the quality assurance procedures.

As a rule, it takes several review meetings for each development step and for each product and product requirement specification until the product concerned is accepted by the review team after a step-by-step
interactive optimization process.

After this, approval for the next phase is given. Development and implementation documentation generated in the course of software development are likewise reviewed using review methods optimized for the scope of documentation and amount of details involved.

After successful performance of all the above tasks, the independent expert then draws up an appropriate test/examination certificate which documents qualification of the system tested for use in nuclear plants in line with the categories mentioned earlier and confirms that the system meets the applicable rules, regulations and standards (s. Fig. 23).

7. Control Room Ergonomics

In accordance with German standards for the safety design on NPP's, human factors play a more important role within the list of safety provision and requirements than for example redundancy or diversity. Mainly due to the TMI event, the control room design for NPP's which were in operation as well as those under construction were reviewed in detail and careful consideration of human factors was taken into account.

For the design of the Convoi NPPs a detailed specification for the layout, labeling, location of control and informative elements and mimics was developed in conjunction with German research institutes and KWU design departments. One of the many control room design principles was the universal application of homogenous hardware. Based on numerous case studies performed in a full scale control room mock up the suitability of the control room concept was proven to the licensing authorities.

An additional important feature affecting the control room ergonomics was the inclusion into the control room design of a screen based information level driven by the process information system PRISCA as already mentioned. For this information system detailed technical/scientific research was carried out into the subject of graphic displays which has resulted in basic principles now adopted as standards in Europe. For example this study covered such aspects as color,

structure and arrangements of graphic display elements, use of icons, abbreviations and dynamic data displays.

In connection with the development of the cockpit control room for the PP Staudinger 5 similar investigations to those in the Convoi plants were performed for a fully screen based one man control room. By using 22 pre-defined operating cases (normal and disturbed) the design was verified and validated. After some design changes together with the development of additional software for information evaluation and information compression, in order to reduce the mental burden for the operator, it was proven (to the customer) that the design meets and compliments the operators requirements.

These above mentioned investigations, which will be continuously monitored and verified during normal plant operation, forms a reliable basis for the design of a screen based control room for KWU-NPPs. The basic design principles are based on the process management concept and the distribution of tasks between man and control system. KWU 's philosophy concerning this is described in figure 5.

The licensing procedures are described according to the German Standard KTA 3904 and in the IEC 964. The ongoing qualification work by KWU includes the development of all required specification and QS documents together with each step taken and its associated evaluation and confirmation using a plant simulator which is already in operation.

We are therefore confident that with this approach we will meet the requirements of German NPP operators for a screen based control room in time.

8. Summary

KWU has built a large number of NPP's as turnkey projects. Due to this, KWU has the complete know-how for the design and application of I & C in NPP's including special areas like human factors, qualification procedures and reliability calculations.

Based on Siemens experience with hard-wired I & C systems for nuclear power plants and the demonstrated high availability of these systems Siemens develops digital I & C systems following the trend to use digital systems for both, operational and safety applications. The main advantages of the digital systems are found in the higher degree of automation together with more sophisticated control strategies and in the improved MMI features. The installation of digital I & C systems in nuclear power plants is not only planned for new plants but already practiced for retrofits and replacements.

SIEMENS

In the past :

- o Use of hardwired control systems
- o Use of hardwired control room equipment for operation (control tiles) and monitoring (indicators)
- o Use of digital information systems with visual display units
- o Use of digital control systems for special tasks only (e.g. operational reactor control)
- o Retrofits mostly with hardwired systems

Basis : highly reliable, qualified I & C systems

Today and in future:

- o Use of digital control systems
- o Use of display based control rooms
- o Modernization mostly with digital systems

Basis : fault tolerant structures to meet the reliability requirements and qualification of software

Copyright (C) Siemens AG 1990 All Rights Reserved. Confidential

I&C - Trend in Nuclear Power Plants

Fig 1

SIEMENS

Important design criteria of safety systems I&C :

2 - failure criterion	⟶	degree of redundancy / diversity
30 minutes rule	⟶	automatic countermeasures of safety I&C
defence-in-depth concept	⟶	staggered countermeasures of limitations

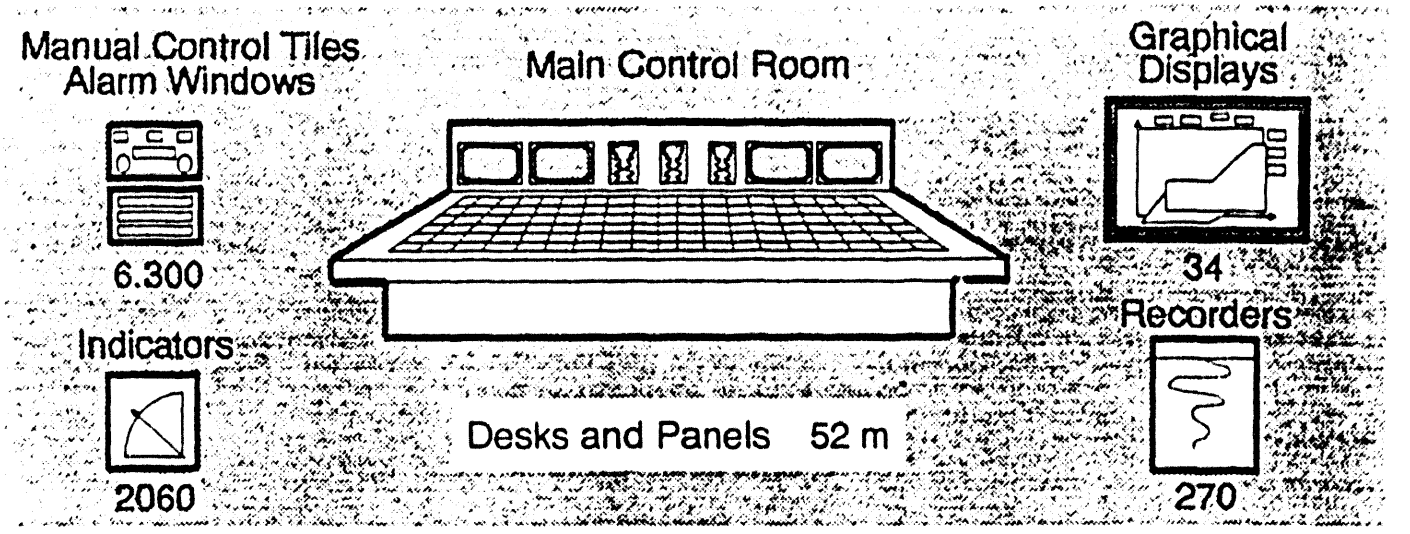
Important develpoment tasks of digital safety I&C :

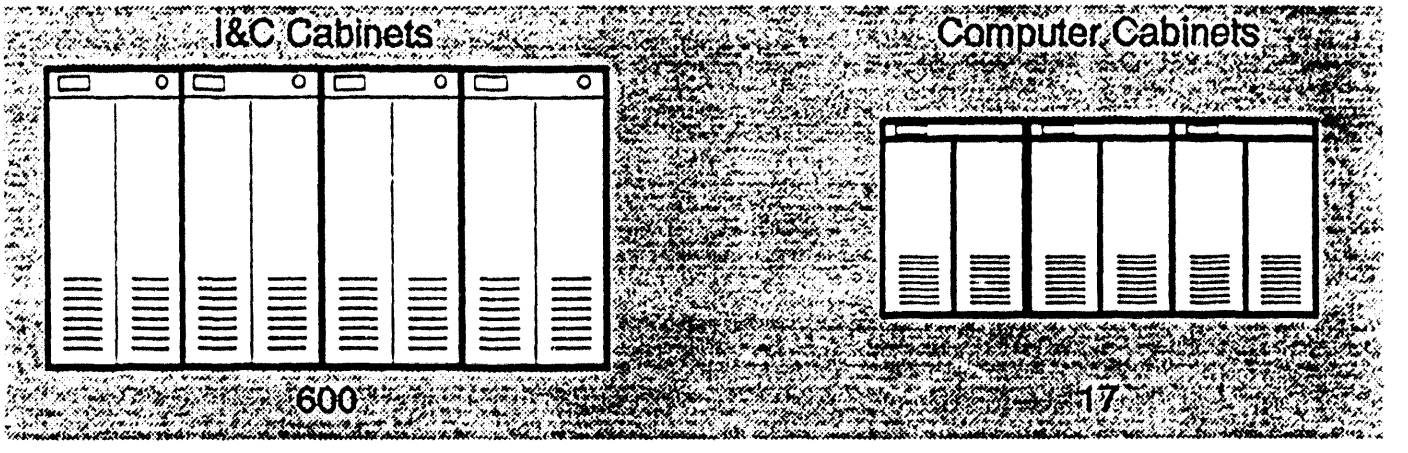
Qualification of hardware	⟶	off-the-shelf hardware
Qualification of software	⟶	off-the-shelf operating systems and communication services
Generation of high-quality I&C application software	⟶	formalized specification and automatic code generation

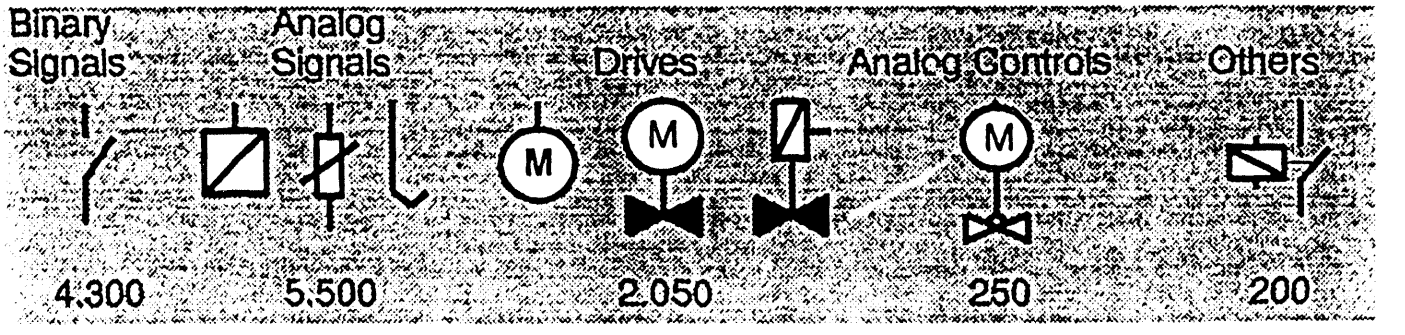
Copyright (C) Siemens AG 1990 All Rights Reserved. Confidential
PCD-2/KWU L 212/Sauer-2/ENGLFOLI/02.12.91/Sr

Basic design principles of digital safety I&C

Fig



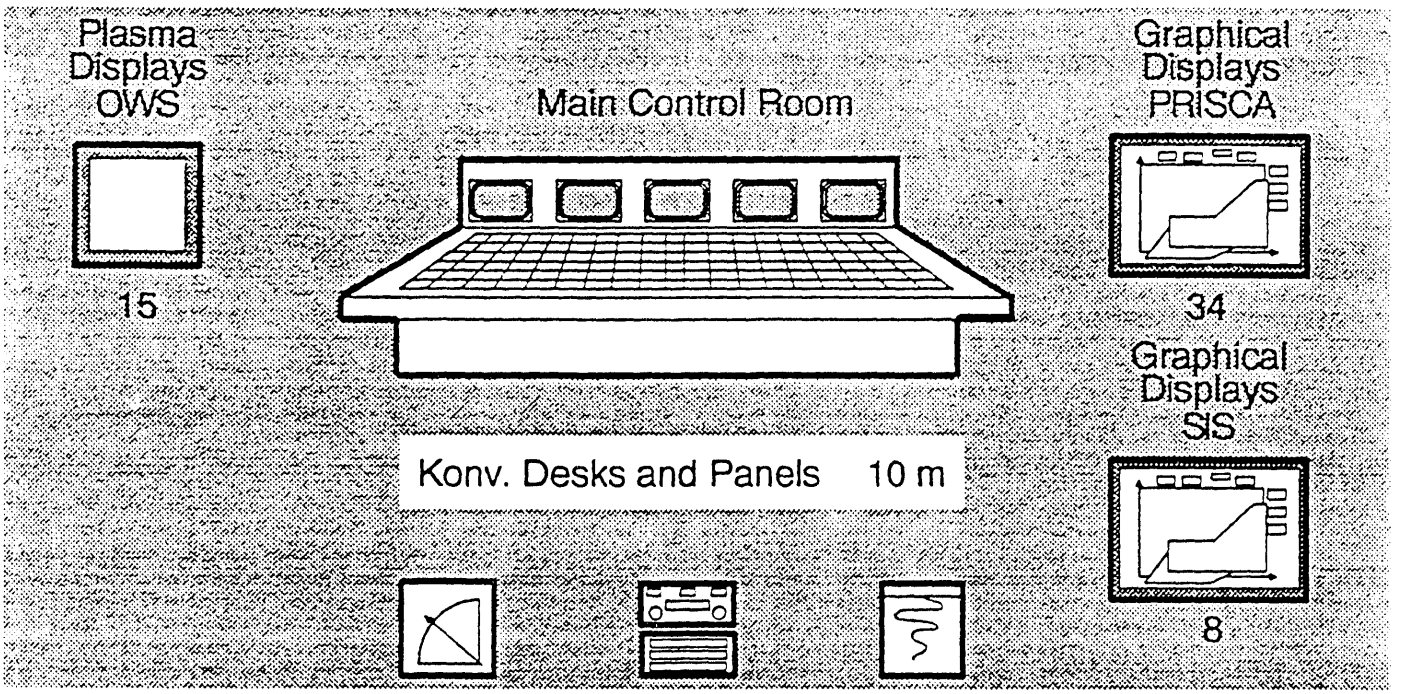


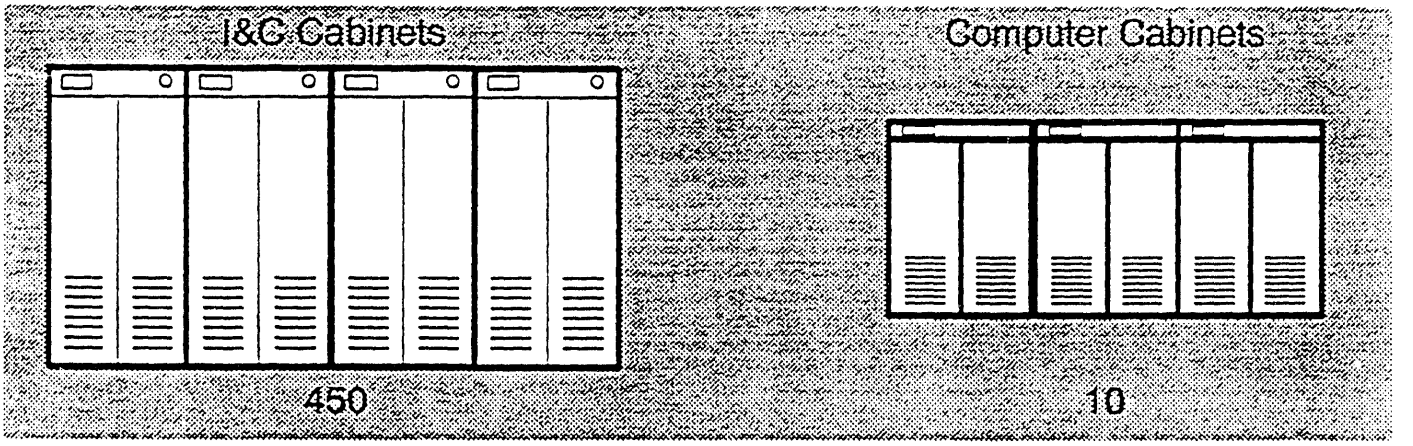


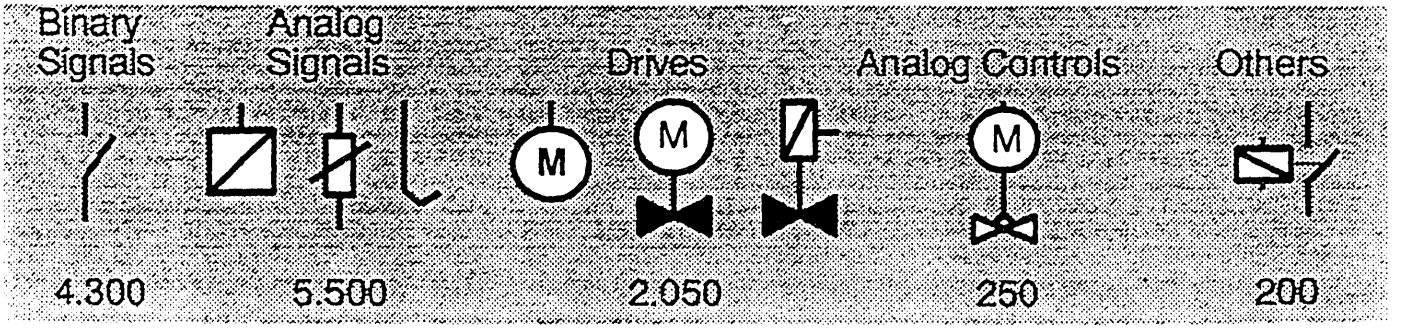
LOCHNER/LT_MENGE/KONVOI/L212/09.07.91/Lo

I&C-Figures in a Convoi 1300 MW PWR NPP with hardwired I&C-Systems

Fig 3





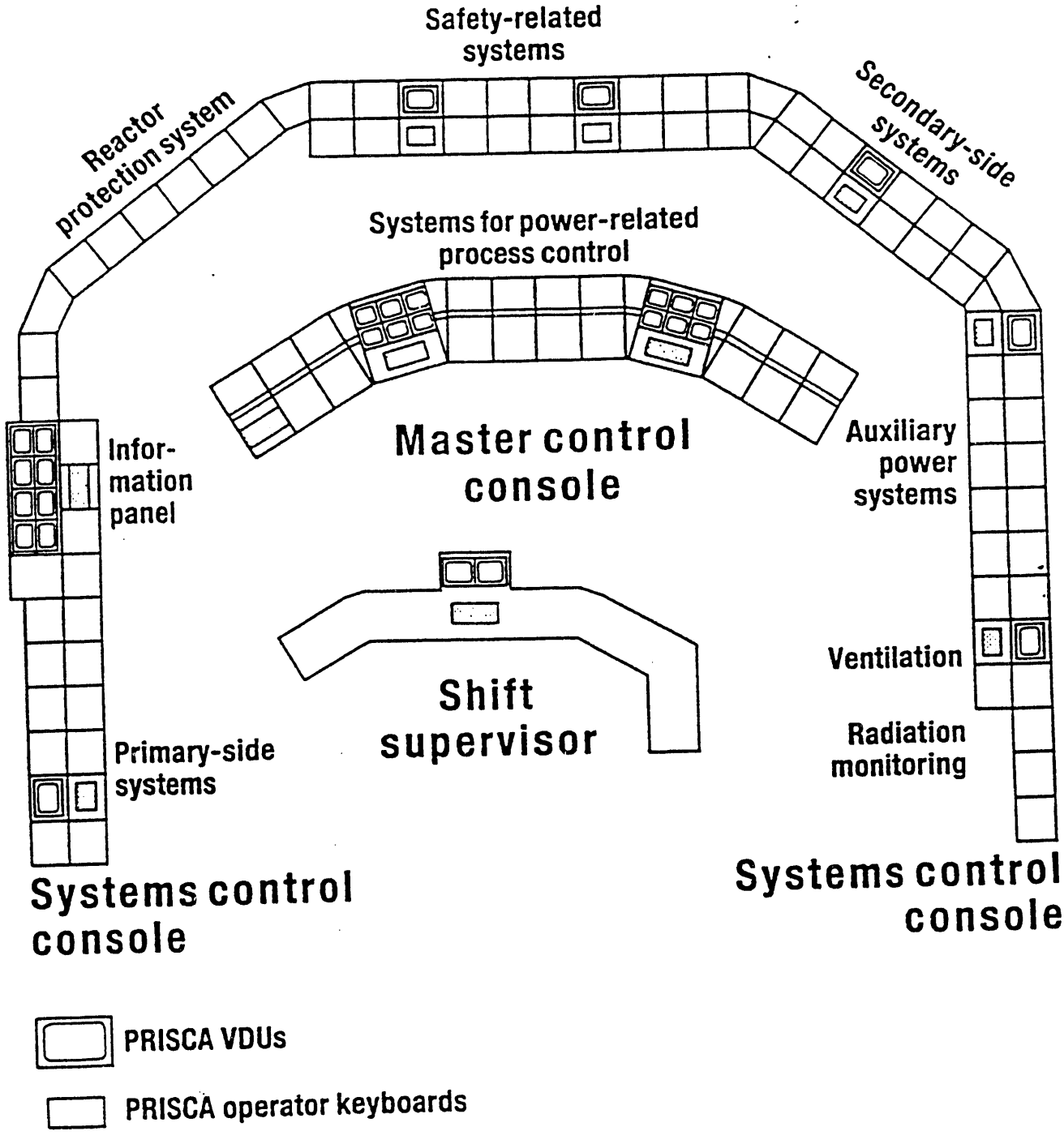


LOCHNER/LT_MENGE/KONVOI/L212/09.07.91/Lo

I&C-Figures in a Convoi 1300 MW PWR NPP

Fig

SIEMENS

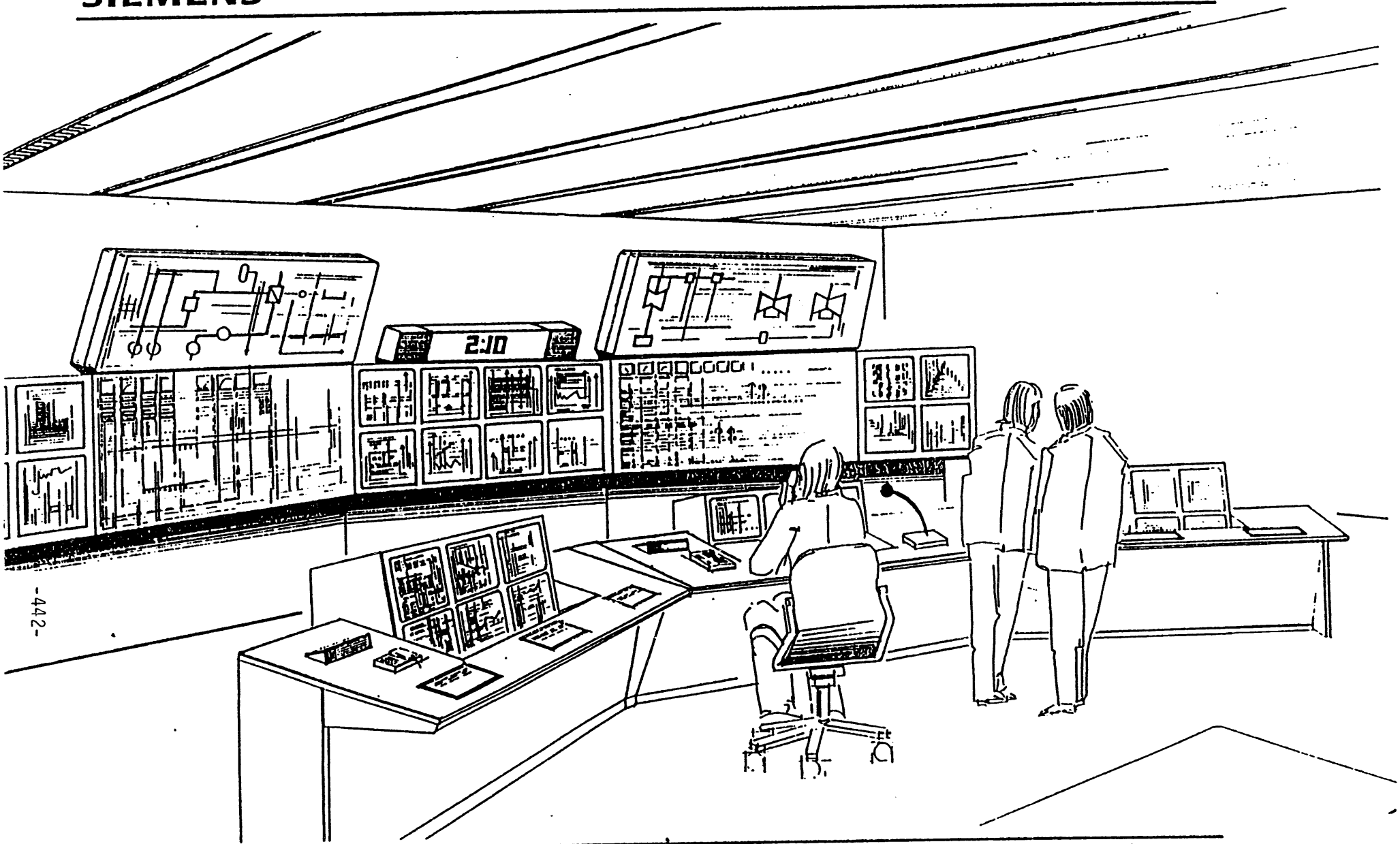


Control Room of the Konvoi-Plants

UB KWU
UB 333
E88 008 e

Fig 5

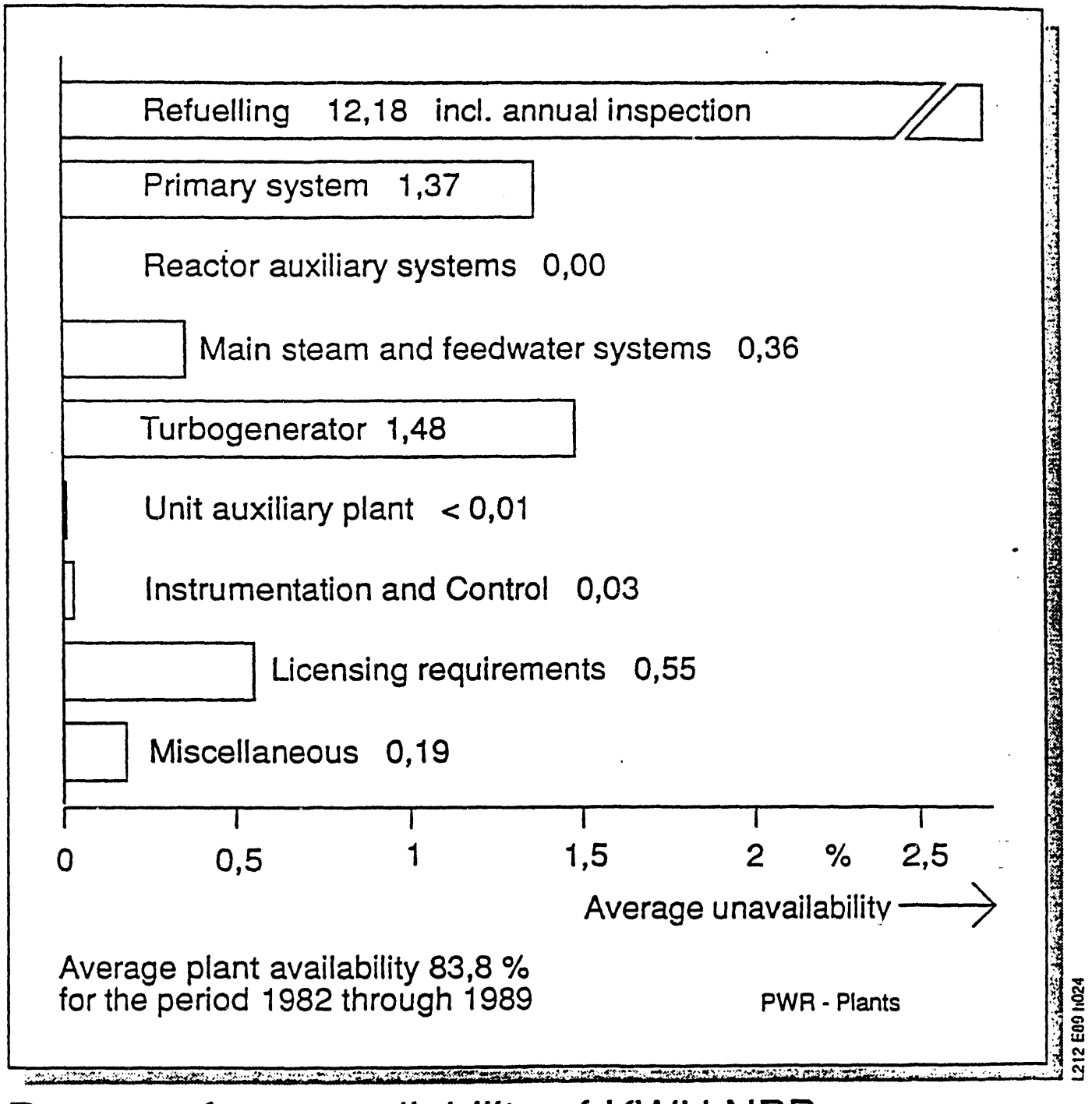
SIEMENS



Draft of a Display Control Room for NPP's

KWU L2-12 90 11o-mo

SIEMENS



Reasons for unavailability of KWU NPP s

Fig 7

- Generate high-quality I&C application software

- Master the common-mode failure particularly for system software

  e.g. off-the-shelf operating systems, communication services

- Qualify off-the-shelf hardware

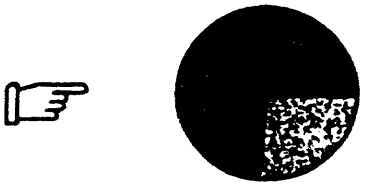
Important Tasks of the Development

KWU
E451
11.09.91

Fig. 8

Error distribution for extended conventional programmed systems

Source : TUV Norddeutschland



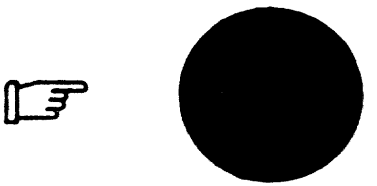
coding 27%

Achievable error density **2. 10^{-3} errors/statement**

Source : Electrical and control aspects of the sizewell B PWR, Int. Conf. Sept. 15, 92

By use of partially formalized coding methods error density can be limited to **3. 10^{-5} errors/statement**

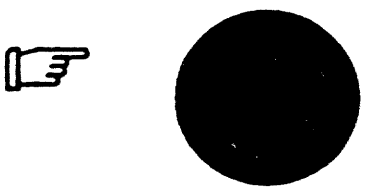
Source : Electrical and control aspects of the sizewell B PWR, Int. Conf. Sept. 15, 92



coding 0.5%

By use of rigorous formalized coding methods error density can be limited to **< 1. 10^{-6} errors/statement**

Source : SILT development

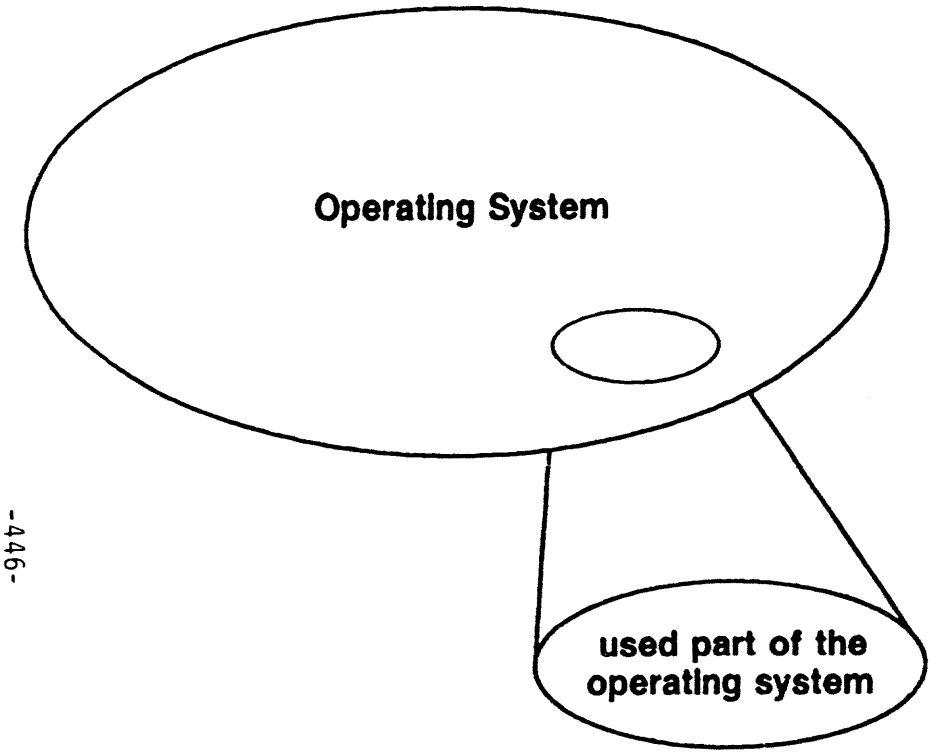


coding 0.0099%

EQUIPMENT DIVERSITY IS NOT ADEQUATE TO COPE WITH SOFTWARE ERRORS.

CODING ERRORS CAN BE NEGLECTED BY USE OF FORMAL METHODS.

Evaluation of software errors



only a small part of the operating system is used

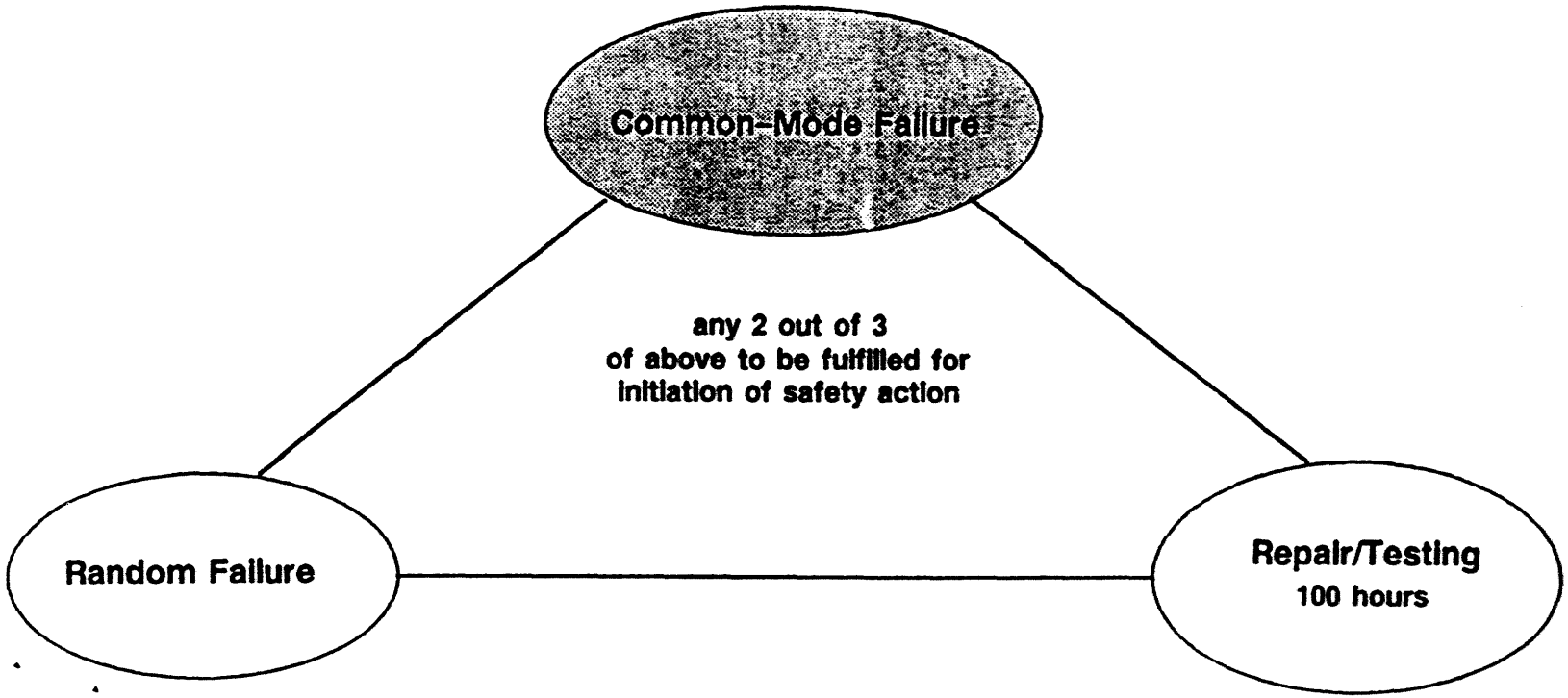
Methods to realize a system behaviour which is independent of the plant conditions

- all tasks are running cyclically
- all messages are transmitted cyclically
- all system services are used cyclically
- no interrupt handling

Methods to avoid common-mode failures

- loosely coupled redundant nodes
- different cycle time in redundant nodes
- different combinations of tasks in redundant nodes
- different data combinations in redundant nodes

Design Criteria for Software in Safety I&C



Failure Combination

Fig 11

SIEMENS

Data acquisition and preprocessing

Accident identification

Subsystem control

Majority voting and priority control

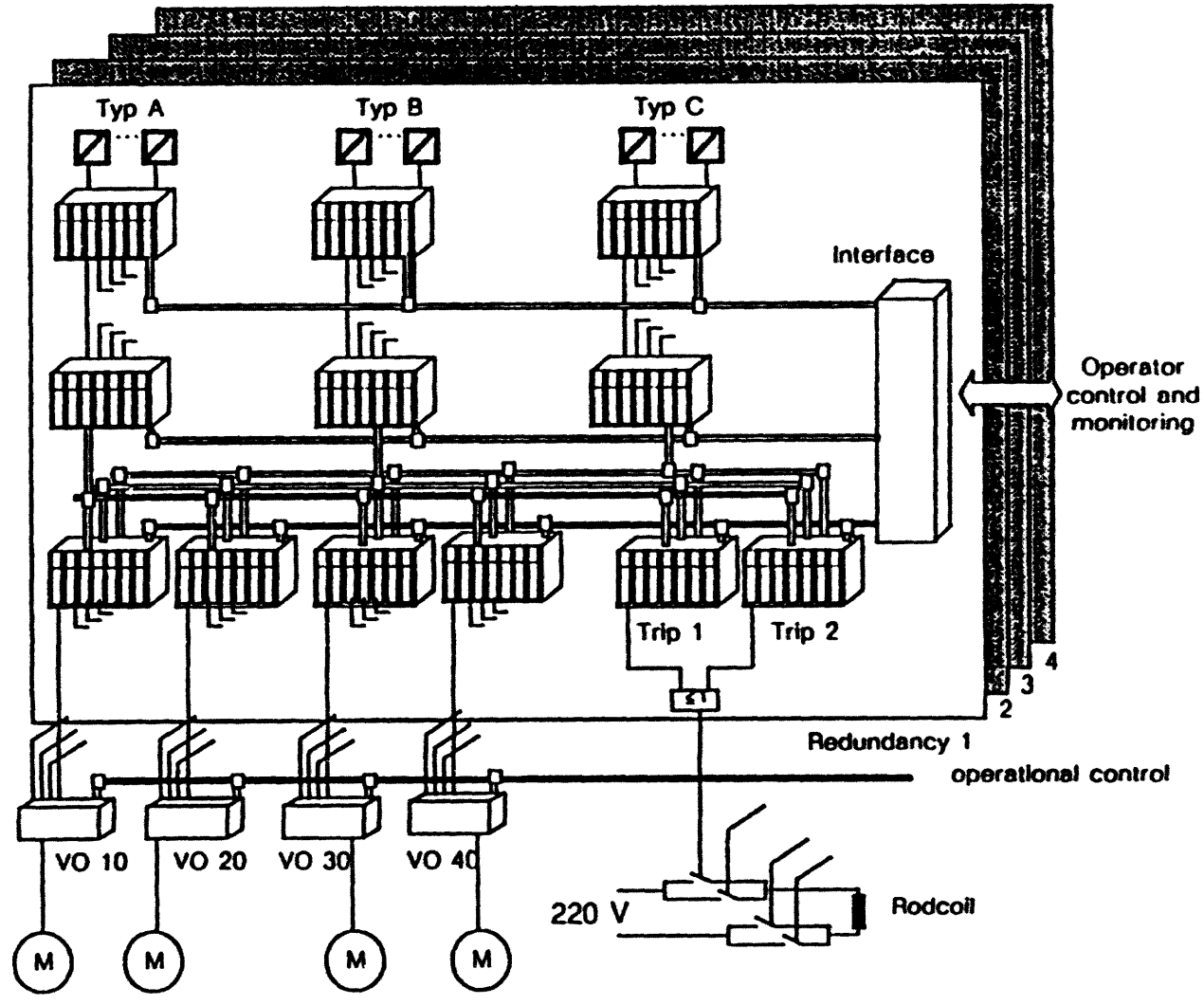


Fig 1

Structure of Safety I&C

KWU E451
9.7.91

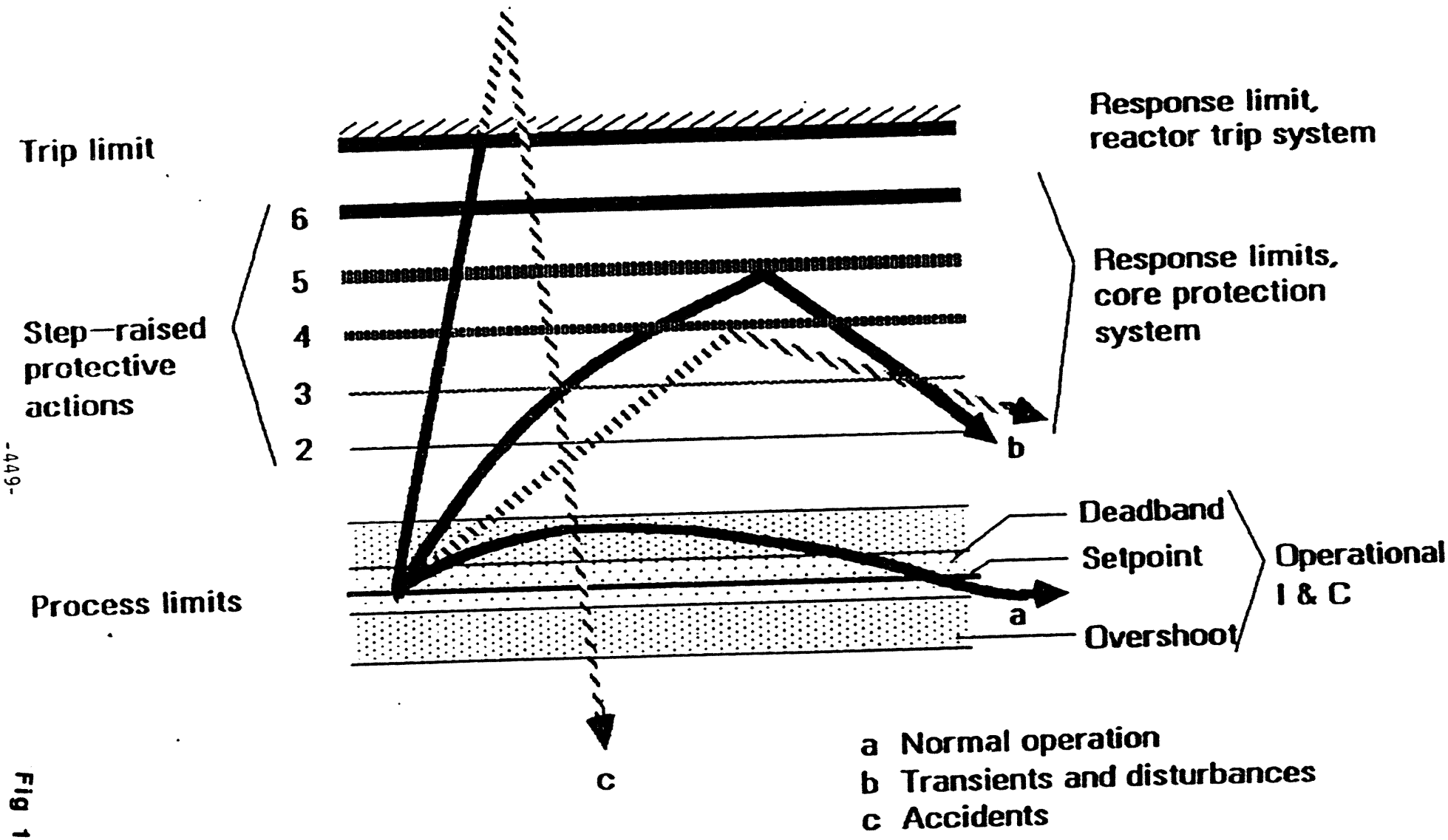
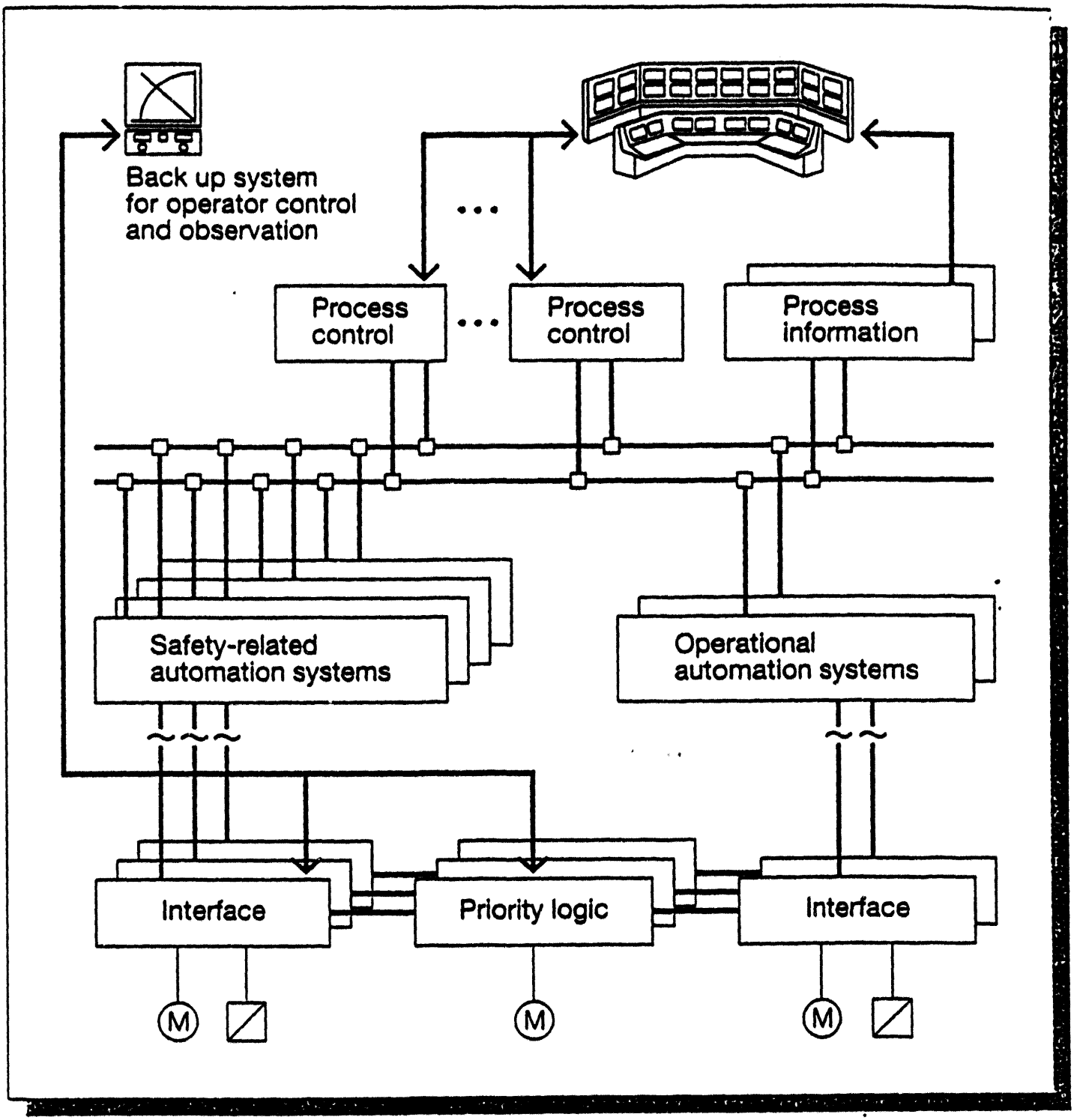


Fig 13

Copyright (C) Siemens AG 1991 All Rights Reserved Confidential

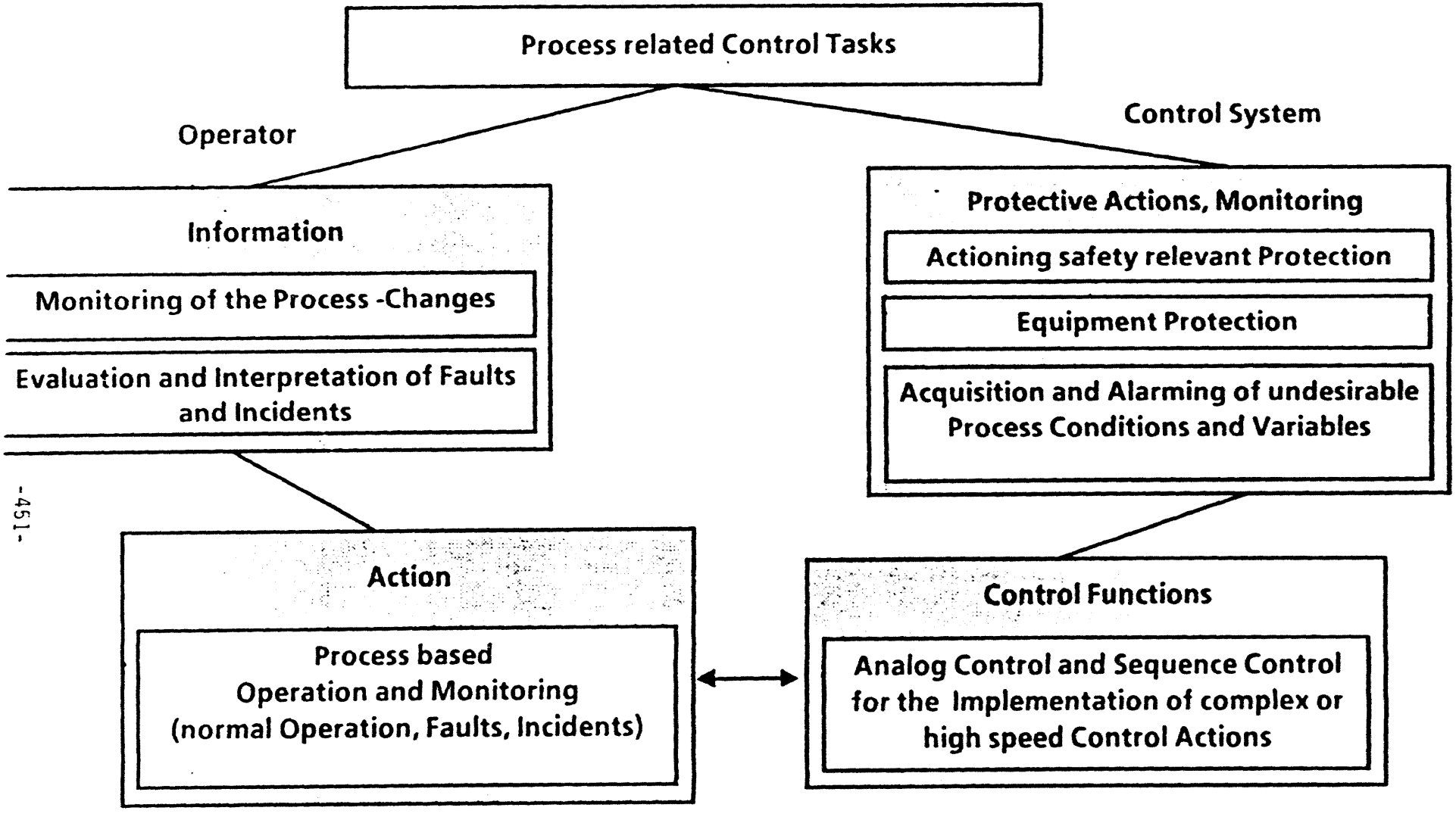
efence in depth concept of I & C

SIEMENS



Overall structure of I&C system in a nuclear power plant

Fig 1

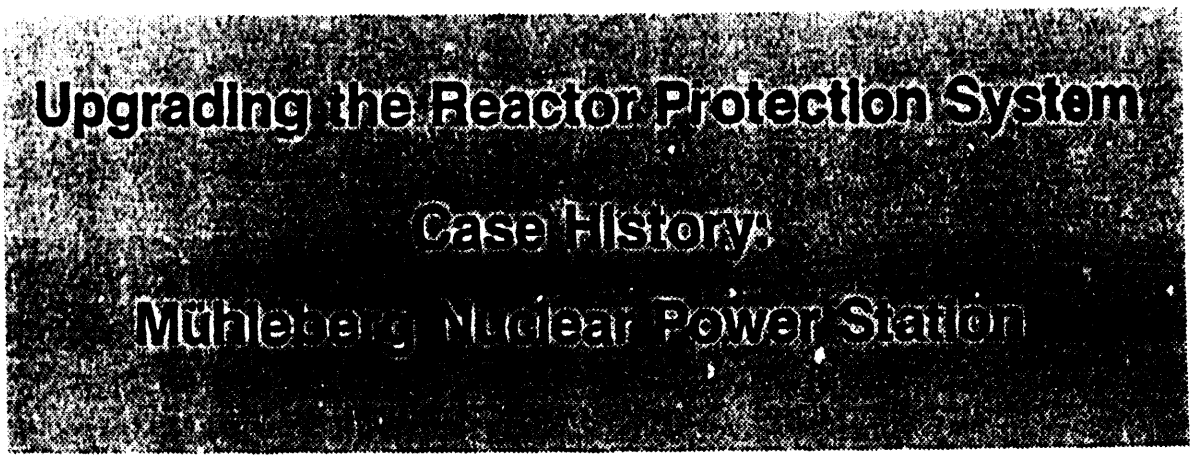


PWR-Process Management Concept
Task Split for Process related Control

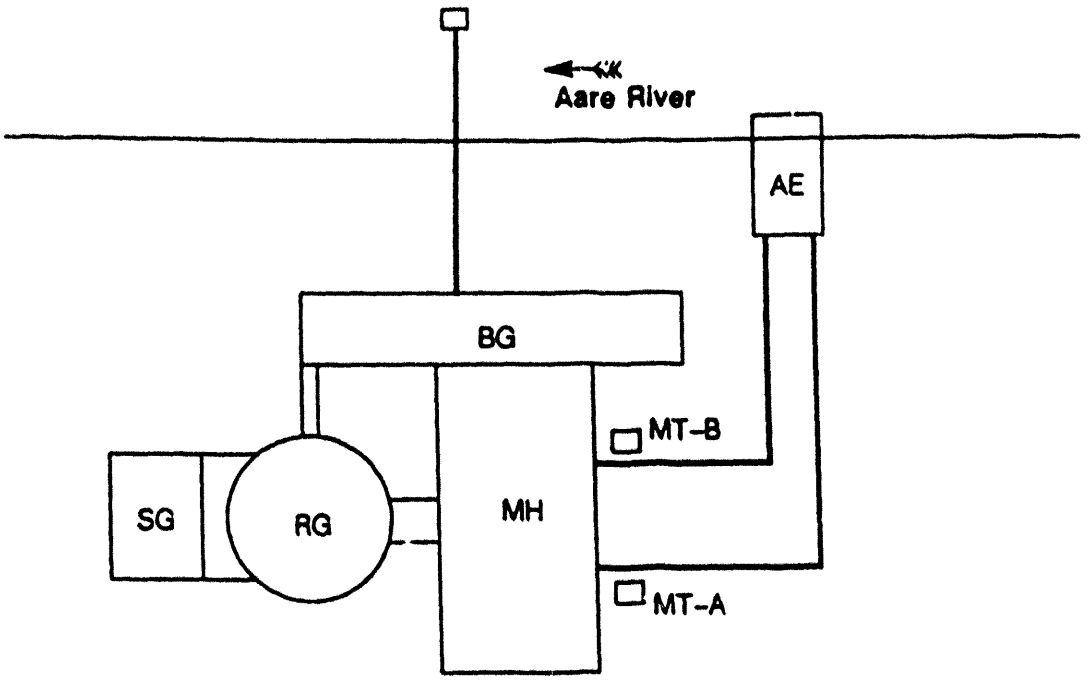
Fig 15

KWU L2/Ho-mai
10.07.1992

Copyright (C) Siemens AG 1992 All Rights Reserved Confidential


Upgrading the Reactor Protection System
Case History:
Mühleberg Nuclear Power Station

Plant Data



AE: Pump house
BG: Control building
MH: Turbine building
MT: Main transformer
RG: Reactor building
SG: Emergency standby building (SUSAN)

Operator:	**Bernische Kraftwerke AG**
Reactor type:	**BWR**
Output (electrical)	**2 x 160 MWe** (2 Turbine generators)
Operating since:	**1972** (Availability factor >80 %)
Suppliers:	**General Electric** (GE,USA) **Brown Boveri Co** (BBC, Switzerland)

Project Identification

Upgraded System

Reactor protection system for initiation of protective actions
"scram" and
"containment isolation" .

Reason for Upgrade

Increasing number of equipment failures and difficulty in procuring spare parts for existing reactor protection system based on binary sensing in relay circuitry.

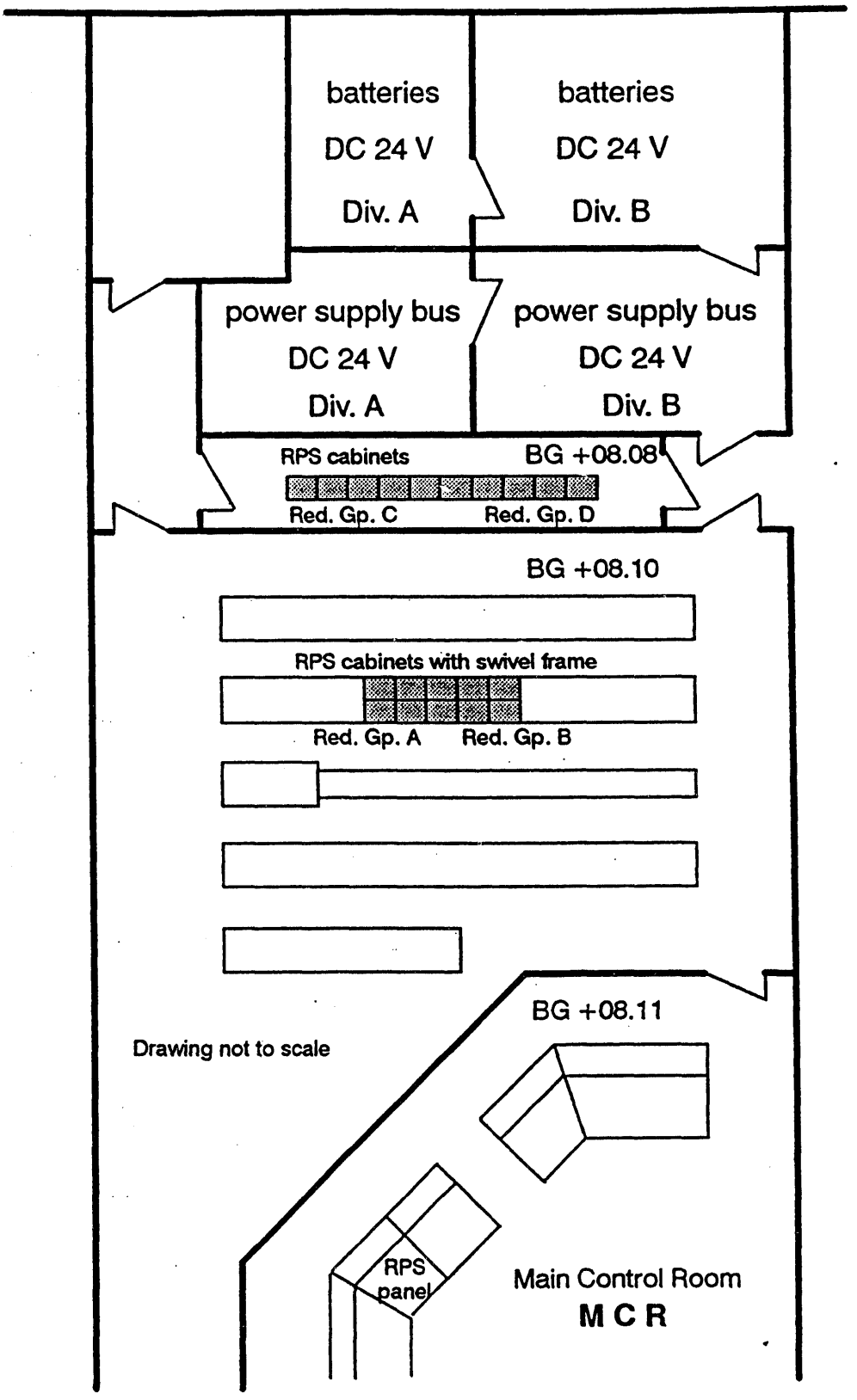
Requirements Stipulated by Plants Operator for New I & C System

No license for a new plant concept, thus requiring retention of the following:

- Existing system design concept
- Existing redundancy structure.

Design to state-of-the-art technology, as follows:

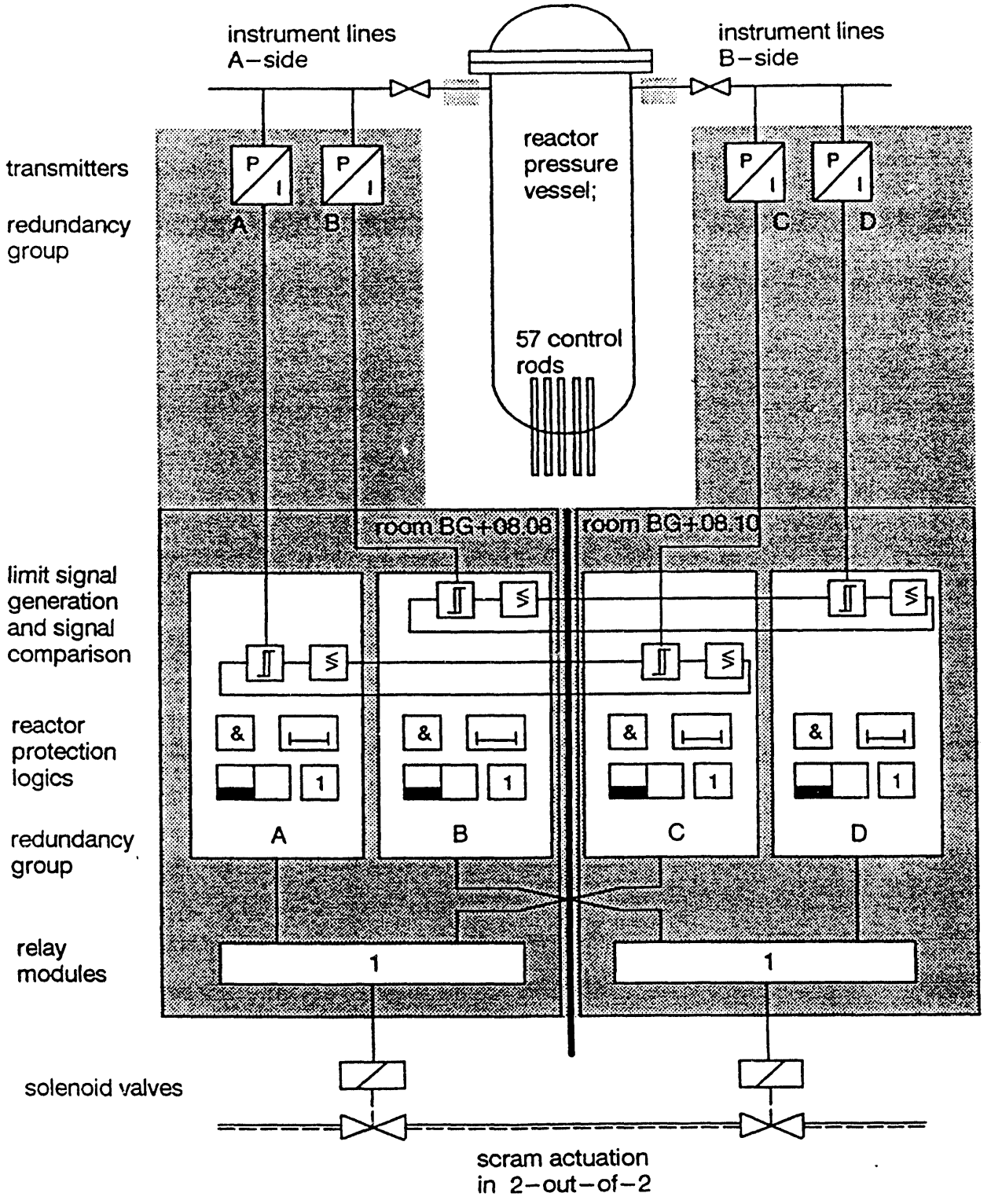
- Designed to withstand earthquakes, lightning, fire and internal accidents
- Use of qualified equipment (type tested)
- Processing of analog process variables
- Equipment systems with "active failure mode" capabilities
- Improved inspection capability and ease of monitoring
- Longer intervals between inspections



Arrangement of RPS Cabinets

Fig 19

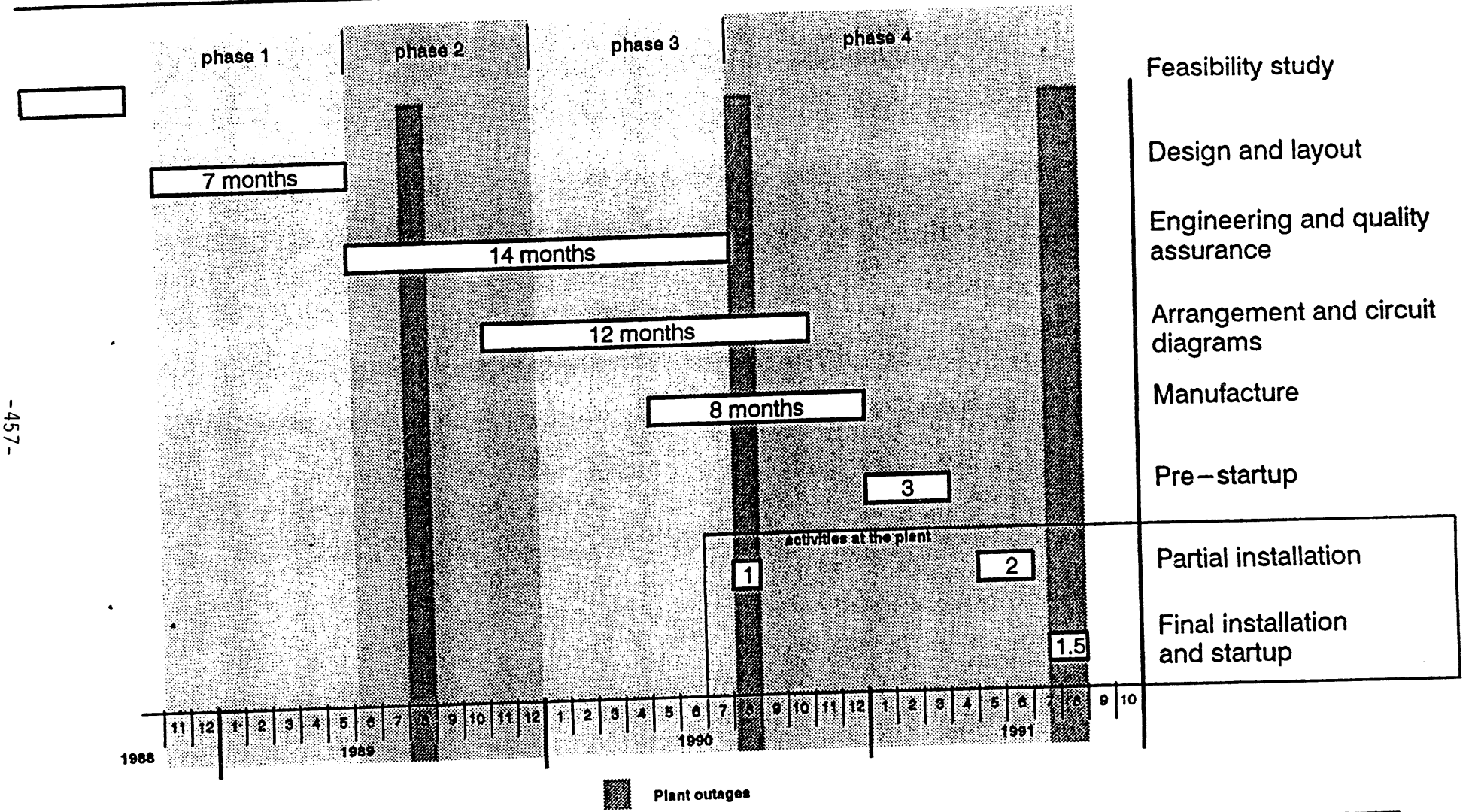
Siemens



Redundancy Structure of Reactor Protection System

Fig 2

Siemens



Time Schedule

Fig 21

Feasibility study for complex backfitting projects with information about

- I & C concepts
- defintion of equipment systems
- proposed technical solutions
- configuration of interfaces
- inspection concepts
- boundary conditions of the plant
- total technical effort and expenditure
- time framework and measures to reduce the period required for integration in the plant

Main advantages

- establishing an I & C concept which is agreed between the operator and manufacturer
- foundation for preparing a concrete offer with a clearly defined scope of supply and services

Regulations for hardware components of the system for Operational I&C

IEEE 279 (1971)
Criteria for Protection Systems for Nuclear Power Generating Stations

IEEE 323 (1983)
Standard for Qualifying Class 1E Equipment for
Nuclear Power Generating Stations

IEEE 344 (1987)
Recommended Practice for Seismic Qualifications of Class 1E Equipment
for Nuclear Power Generating Stations

KTA 1401
Allgemeine Forderungen an die Qualitätssicherung
(Engl. von KTA–GS,9/88)

KTA 3501
Reaktorschutzsystem und Überwachungseinrichtungen des
Sicherheitssystems (Engl. von GRS–1987)

KTA 3502
Störfallinstrumentierung

KTA 3503
Typprüfung von elektrischen Baugruppen des Reaktorschutzsystems
(alter Stand Engl. von GRS)

Parts of IEC 987 (1989)
Programmed Digital Computers important to Safety for
Nuclear Power Stations

Regulations for software components of the system for Operational I&C

IEC 880 (1986)
Software for Computers in the Safety Systems of Nuclear Power Stations

ISO 9000–3 (1992)
Qualitätsmanagement und Qualitätssicherungsnormen;
Teil 3 : Leitfaden für die Anwendung von ISO 9001 auf die Entwicklung,
Lieferung und Wartung von Software

Parts of:

ANS–10.4.–1987

IEEE 828 (1983)
Standard for Software Configuration Management Plans

IEEE 829 (1983)
Standard for Software Test Documentation

IEEE 1008 (1987)
Standard for Software Unit Testing

IEEE 1012 (1986)
Standard for Software Verification and Validation Plans

Copyright © SIEMENS AG 1993 All Rights Reserved

SESSION 7

MODERNIZATION

Instrumentation and Control System Upgrade Plan for Operating PWR Plants in Japan

Modernization of the Borssele NPP Reactor Protection System

The Role of International Standards in the Design of Modern I&C Systems for Nuclear Power Plants

IAEA Specialists Meeting

on

Experience in Aging,Maintenance

and Modernization of Instrumentation

and Control Systems for Improving

Nuclear Power Plant Availability

Rockvill,Maryland,USA

5-7 May,1993

Instrumentation and control system upgrade plan for operating PWR plants in Japan

Hirofumi Ishii

Mitsubishi Atomic Power Industries, Inc.

2-4-1 Shibakouen, Minato-ku, Tokyo 105 JAPAN

ABSTRACT

Digital technology has been applied to all non-safety grade instrumentation and control (I&C) systems in the latest Japanese PWR plants, and has achieved more reliable and operable systems, easier maintenance and cable reductions. In the next stage APWR plants, the digital technology will be also applied to all the I&C systems including safety grade systems.

Parallel to the above efforts, many backfitting programs in which the digital technology is applied to operating plants are under way to improve reliability and operability. The backfitting programs for operating plants are proceeded in the following two phases, synthesizing various utility's needs to improve plant availability and operability, improvement of digital technology, and complexity of the practicable replacement procedures.

- Phase 1 ; Partial application of digital technology
  The digital technology is partially applied based on the following methods:
  (a) replace several analog circuit cards with one board digital controller
  (b) add digital control systems to analog control systems as backup controls
  (c) apply digital control systems to auxiliary control systems
  All above methods have been already applied to several operating plants and planned to be applied to many other plants. The following items are examples applied to the operating plants:
  - Improved main feedwater control system
    - automatic correct input selection from redundant input signals
    - automatic digital backup control systems for analog control systems
    - automatic transfer of redundant pneumatic subsystems
  - Advanced feedwater bypass control system
    - continuously changes control constants following plant operating power
  - Radio-active Waste Processing System

- Phase 2 ; Complete application of digital technology
  The digital technology is completely applied based on the following methods;
  (d) replace analog non-safety grade I&C systems with digital systems
  (e) replace all analog I&C systems including safety grade with digital systems
  Above method (d) and (e) are not yet applied to operating plants, but a basic design stage of the method (d) for several operating plants has been finished and a feasibility study of method (e) has been just started. In the design stage and the study, effective procedures and technique of replacement and schedule of development and application will be discussed, considering the digital I&C system of APWR and digital technology of other industries.

This paper presents examples of the partial application of digital technology to operating plants, and the contents of basic design for the complete application of digital technology.

1. INTRODUCTION

In Japanese operating PWR plants except the latest plants, the instrumentation and control (I&C) system consists of conventional analog computing modules and electro-magnetic relays, etc. Analog computing modules are periodically replaced with new modules to prevent them from aging degradation. Particularly, old box type analog computing modules which were applied to the first generation plants have been almost all replaced with card type analog computing modules because it is very difficult to keep spare parts.

Operating experiences at these plants are satisfactory. However, their design practices are now ten to twenty years old, and it is difficult to satisfy various utility's upgrading needs.

- improve plant availability and reliability
- improve plant control capability
- improve maintainability

Also, it will become difficult to keep spare parts of card type analog modules same as old box type modules in the future. Furthermore, digital I&C systems are widely used and are the main trend in most industries. In order to fulfill these requirements, a completely digitized I&C system is adopted to non-safety grade I&C system in the latest PWR plants.

According to these trend, many backfitting programs for applying the digital technology to the operating plants are proceeded in the following two phases:

- Phase 1 ; Partial application of digital technology
- Phase 2 ; Complete application of digital technology

Transition from analog technology to digital technology is shown conceptually in Appendix A.

2. PARTIAL APPLICATION OF DIGITAL TECHNOLOGY (PHASE 1)

Considering complexity of a complete application, digital technology has been partially applied to operating plants in the first step. Typical methods of the partial application are as follows:

(a) replace several analog circuit cards with one board digital controller
(b) remain existing analog control systems and add digital control systems as backup control systems
(c) apply digital control systems to auxiliary control systems

In order to improve the operability and reliability of operating plants, the above methods have been already applied to several operating plants and planned to be applied to other operating plants. Appendix B shows partial applications of digital technology planned and those applied to operating plants. Examples applied to operating plants are as follows:

(1) From the viewpoint of operability:

One board digital controller is selected to improve control capability with a smaller number of additional equipment. This digital controller is designed to install easily in the analog control rack, i.e. composed in the same size card as the analog card, can use same power supply for the analog cards, etc. This digital controller can be partially applied to specific functions which are desired to improve control capability. Figure 1 shows the architecture of advanced feedwater bypass control system which is a example of application. This control system has improved the control capability to continuously change its control constants according to plant operating power.

The feature of one board digital controller is as follows:

- One board type ; including single CPU, memory, and process I/O
- Size ; same as analog card
- Software ; single task, no interaption, constant time interval
- Self-diagnosis ; watch dog, memory cneck, range over, etc.
- Process I/O ; maximum 8 A/Is, 4 A/Os, 8 D/Is, 8 D/Os
- Sampling time ; minimum 100 msec.
- Interface level ; 0～10 VDC
- Maintenance ; connect lap top maintenance tool

(2) From the viewpoint of reliability:

A digital control system is additionally applied to an analog control system as a backup control system and a diagnostic system. The target of the backup control system is selected based on operational experiences and a reliability analysis. A rack mounted type architecture is selected to the digital control system which performs backup and diagnostic functions. This digital control system consists of card frames and support equipment, and these equipment are mounted in a rack independent of the analog control system. A simple software architecture (such as, single task, constant time interval, minimum functions, no interaption, etc.) is developed and applied to easily verification. Typical application examples of the digital control system are as follows:

① Process sensor level

A digital diagnostic system is applied to automatically select a correct input signal from redundant process sensors.

② Control system level

A digital control system is applied as backup controls which automatically overrides control functions at the failure of main analog control system.

③ Actuator level

A digital diagnostic system is applied to automatically select a correct subsystem from redundant pneumatic subsystems of one control valve.

The digital control system has been applied to the improved main feedwater control system. Figure 2 shows the conceptual block diagram of the main and backup control systems of improved main feedwater control system.

3. COMPLETE APPLICATION OF DIGITAL TECHNOLOGY (PHASE 2)

Digital technology is completely applied based on the following methods:
(a) replace non-safety grade I&C systems with digital systems
(b) replace all safety and non-safety grade I&C systems with digital systems
Above methods are not yet applied to operating plants, but basic design stage of (a) has been finished and feasibility study of (b) has just been started.

The contents of basic design (i.e. method (a)) are shown below:
- Investigation
- Basic design for application of digital control system
- Practical replacement procedures

3.1 Investigation

On-site investigation of the following items is intensively made in order not to cause critical problems:
- Rack arrangement
- Interface between digital control systems and other systems
- Dismantlement and installation of racks
- Cable routing
- Electric power capacity

3.2 Basic design for application of digital control system

3.2.1 Digital control system architecture

(1) Design Principles

Considering features of digital technology, the digital control system applied to the I&C system of operating plants has been studied based on the following design principles:

- Plant safety

  Any plant transient condition caused by a single random failure in this system should not exceed design base transients.
- Plant availability

  To improve the plant availability in the order of one, a MTBF (Mean Time Between Failure) target is chosen to be longer than 100 years.
- Plant control capability

  The system should be able to obtain higher control capability than the analog control system, and meet the needs of plant automation.
- Maintainability

  A system MTTR (Mean Time To Repair) target is chosen to be less than 30 minutes. This target assumes that the maintenance personnel stands by with tools and spare parts. Furthermore, a software maintenance tool that the I&C maintenance personnel can easily use should be available.

• System flexibility
The system should provide appropriate margin for the increase of plant equipment and functional modifications in the future.

(2) Conceptual design
The following shows the conceptual design of the Reactor Control System, which is a typical example of defining system architecture based on the design principles:

(a) Plant safety
One microprocessor processes as many I&C channels as possible from the economical standpoint. Therefore, in case of failure, all channels in the system loose their functions and a multiple transient may be caused. The distributed system architecture has been adopted in order to prevent multiple transients (which exceed the design base transient), according to the conception of group-distribution shown in Figure 3. Furthermore, the distributed system architecture should be considered and required as not to relocate channels in racks as possible.

(b) Plant availability
Each control subsystem should have a redundant architecture in order to prevent plant trip or transient caused by a failure of the digital control system. A duplex redundant system architecture with automatic switching by self-diagnostic functions has been selected.

(c) Plant control capability
• Sampling time of digital control system
As a result of simulation test for main control systems, a sampling time of less than one second was enough to apply the digital control system to the reactor control system of the PWR. Taking account of this result and a selected hardware processing capability, the sampling time was finally decided to 0.3 seconds for the reactor control system.
• Improvement of control functions and plant automation
It is easier to add many functional improvements and new automatic control functions by digital control system. The following functional improvement items were planned to be applied to operating plants:
- Improvement of individual control functions (10 items are planned) such as, Main Feedwater Control, Letdown Line Pressure Control, Main Steam Dump Control, Pressurizer Pressure Control, etc.
- Automation of local controls
- Automatic control system for plant heat up and cool down
- Automatic daily load follow operation

(d) Maintainability
In order to accomplish the design target (MTTR is less than 30 min.), the following should be considered:

• Immediate identification of a failed portion

In case that a failure occurs in a system, the failed portion should be identified by means of online self-diagnostic functions and alarm information should be transmitted to the main control room in order to request maintenance personnel to repair the system. In the main control room, alarm information should be classified into some groups according to operator's reactions. In the instrumentation rack room, maintenance personnel needs more detailed alarm information, which should be broken down into a each module level. These detail information are displayed on a plasma display on each rack and LEDs in each module.

• Easier maintenance

The failed system is repaired easily by replacing a failed card or a component by a spare card or a component under online condition. To repair the duplex portion of the system, the failed subsystem is overridden by backup control system while the total system can keep its automatic control function. To repair the single portion of the system, related control function must be manually operated.

Furthermore, a software maintenance tool is available. It provides a powerful graphical interface, and shows the application software in graphic block diagram form. Therefore, maintenance personnel, who are not a computer expert, can easily maintain the system.

(e) System flexibility

Replacement of main control boards, plant computers and relay racks, and functional modifications have been adopted or planned for operating plants. Therefore, the system should provide appropriate hardware and software margin and flexibility. Design target is that a mounting rate of card is less than 80% and a CPU load factor is less than 80%.

3.2.2 Hardware architecture

A duplex system is adopted as a basic architecture of the digital control system for the complete application phase. The conceptual architecture of the duplex digital control system is shown in Figure 4.

Figure 4 shows one set of digital control subsystem. The digital control system is composed of the distributed digital control subsystems. In case of the reactor control system of operating plants, the digital control system is distributed into 5 to 8 subsystems. (5 is for the two loop plant and 8 is for the four loop plant.)

(1) Rack and card arrangement

Considering the results of the investigation Section 3.1 and the basic design for application of digital control system Section 3.2, arrangement of racks and cards has been studied based on the following practices:

(a) The number of new racks should not exceed the number of conventional analog control racks.
(b) Main control functions should be arranged based on the optimal group distribution such as shown in Figure 3.
(c) In order to use existing cables efficiently, the other controls should not be relocated from the arrangement of the analog control system.
(d) In case that some controls are moved to other racks by practice (b), wiring terminals should be provided in existing rack for cable routing. Their existing cables are connected with their wiring terminals and new cables are installed from existing rack to other rack.
(e) The system should provide appropriate margin for the future increase in plant equipment.
(f) The size of racks for the digital control systems should be the same as that of existing racks for analog control systems.

(2) Periodic system test

Periodic system tests of the digital control system in plant shutdown schedule are much simpler than that of the analog control system, as the integrity of digital system is continuously checked by self-diagnostic functions during its operation. The following are minimum testing items of periodic system test for the digital control system:

- maintenance of electric power
- checking of automatic transfer function in the duplex system and signal selective function
- checking and calibration of the portion of analog input/output

3.2.3 Reliability of digital control system

It should be confirmed by means of FTA that the reliability (plant trip probability) of digital control system is improved compared with that of analog control system. In case of a typical two-loop plant, the plant trip probability is improved about 1/8.

3.3 Practical replacement procedures

The practical replacement of digital control system is planned based on plant shutdown schedule, considering the following procedures:

- Experiences acquired in the latest plants which adopt digital system.
- Transmitters and I/P converters should be replaced with 4～20mA types and also on-site practical investigation should be finished before the replacement of digital control system.
- Functions, which have to control and monitor plant during plant shutdown, should be installed on temporary racks.
- Existing cables are sufficiently taken care and used again.

4. CONCLUSION

Applications of digital technology to operating PWR plants have been started now and expanding from partial to the entire I&C systems.

In partial applications of digital technology, for example, a digital backup control system applied to the improved main feedwater control system was first implemented in 1991, and it is being backfitted and planned to many operating plants. Further, the one board digital controller which has been applied to the advanced feedwater bypass control system and other partial control systems will be implemented in 1994.

The complete application of digital technology will be implemented in the near future. In case of the replacement of analog non-safety grade I&C system with digital system, basic design stage has been already finished. Futhermore, the study of application of total digital I&C systems including safety grade systems to operating plants has just been started. (This system was originally developed for APWR plant.)

5. REFERENCES

i) TAGUCHI,S., et al., " Improvement on Reliability of Control System in PWR plant, " IAEA Specialist's Meeting, Apr. 1984.

ii) UTSUMI,M., NAKAO,T., " Backfitting of The Improved Feedwater Control System in Japanese PWR Plant, " IAEA Specialist's Meeting, Nov. 1987.

iii) TAKASHIMA,M., et al., " Microprocessor-based Reactor Protection System for PWR Plants in Japan, " IAEA Specialist's Meeting, May. 1988.

iv) NAGAI,T., et al., "Application of Integrated Digital I&C System in Japanese PWR Plants", OECD/NEA-IAEA International Symposium on Nuclear Power Plant Instrumentation and Control, May. 1992.

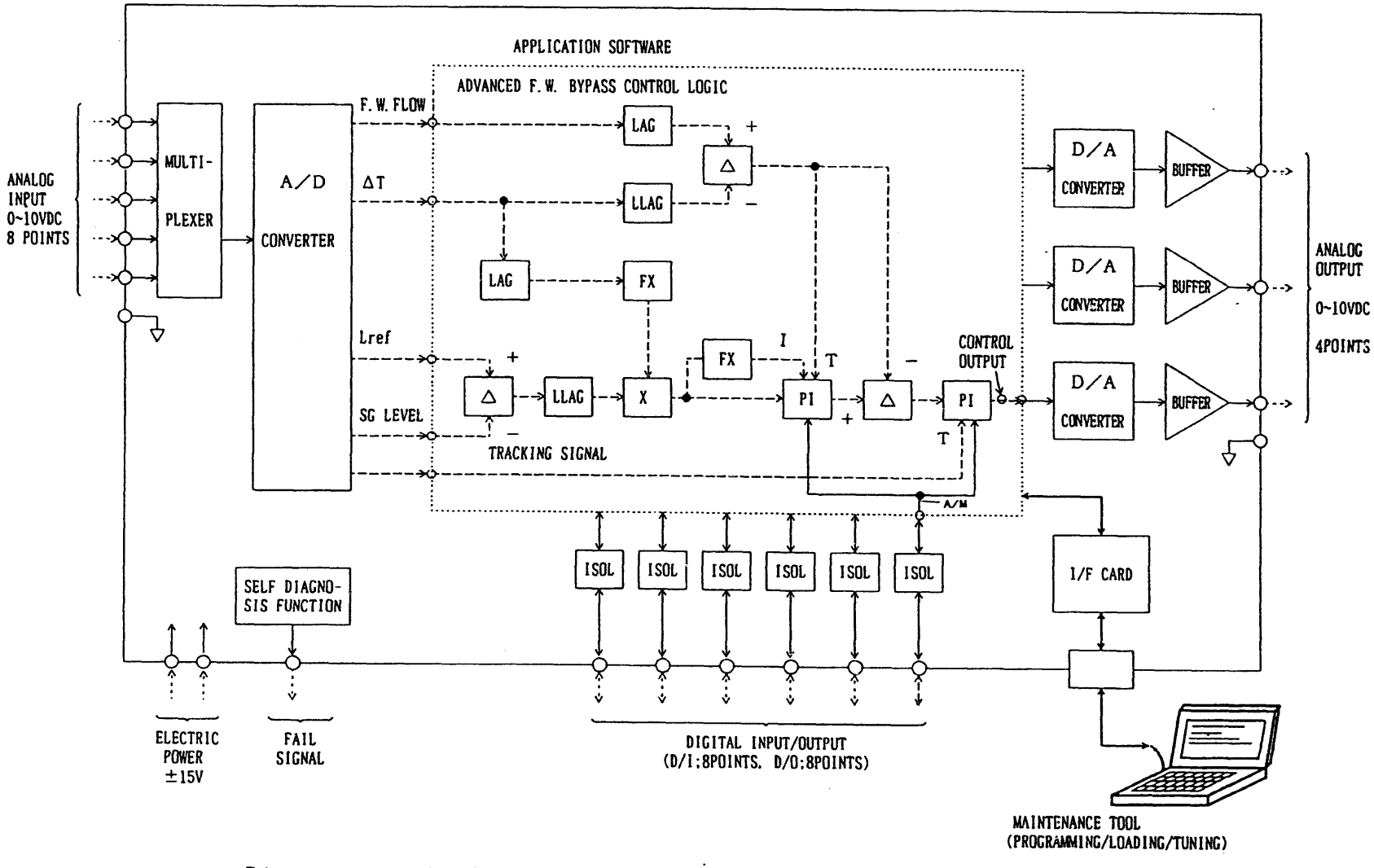


Figure 1 : Architecture of One Board Digital Controller

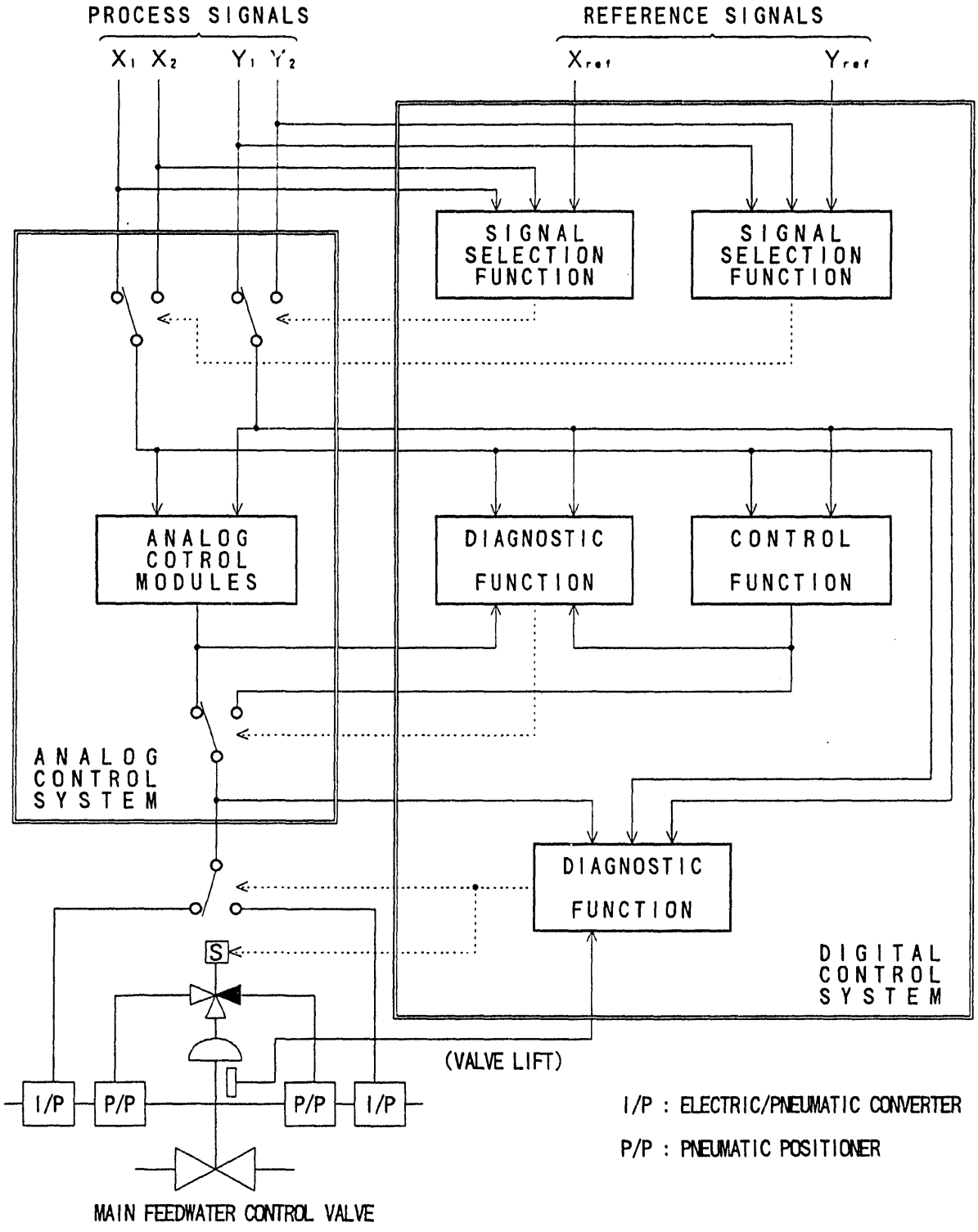
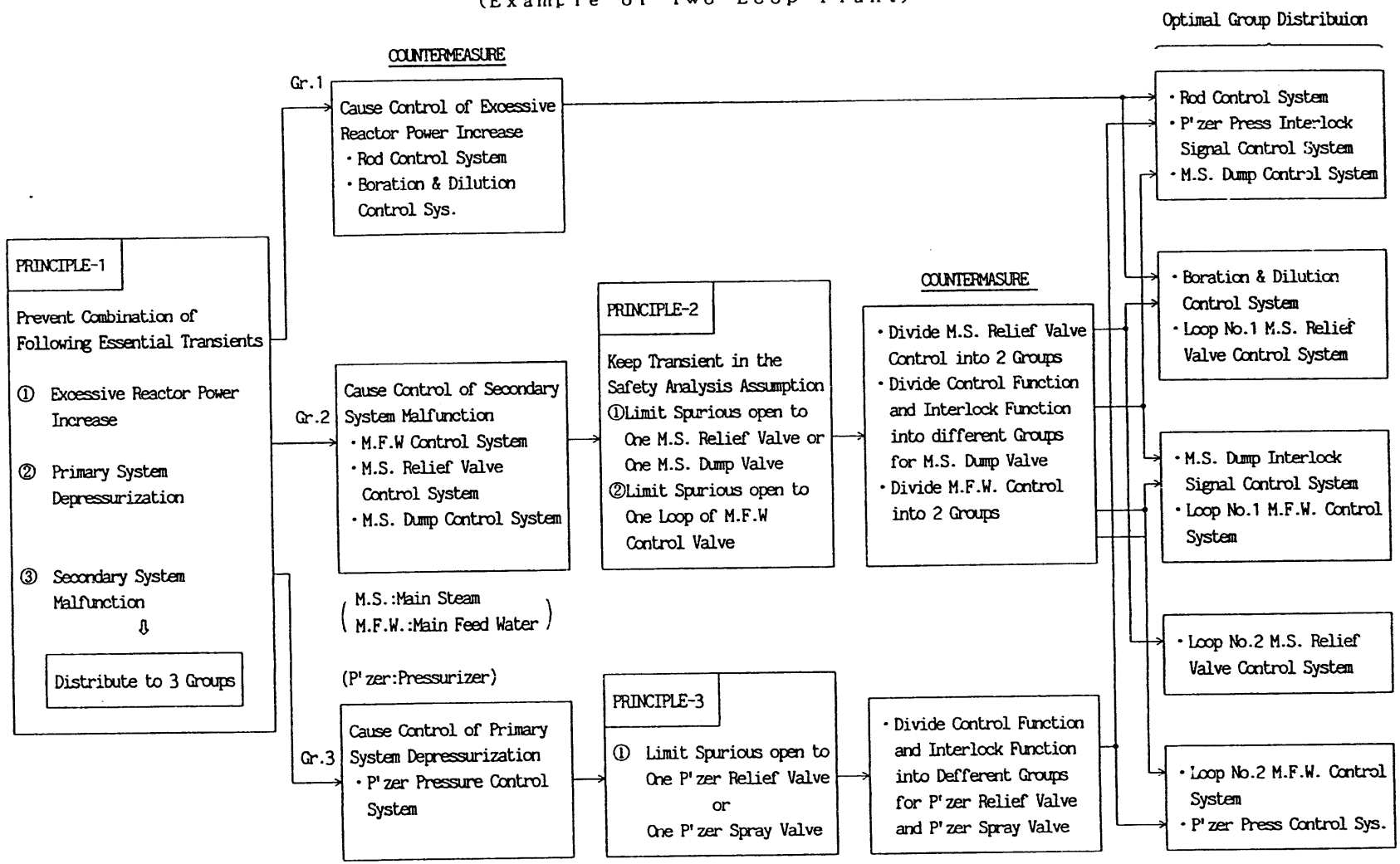


Figure 2 : Improved Feedwater Control System Architecture

Figure 3 : Conception of Group Distribution
(Example of Two Loop Plant)



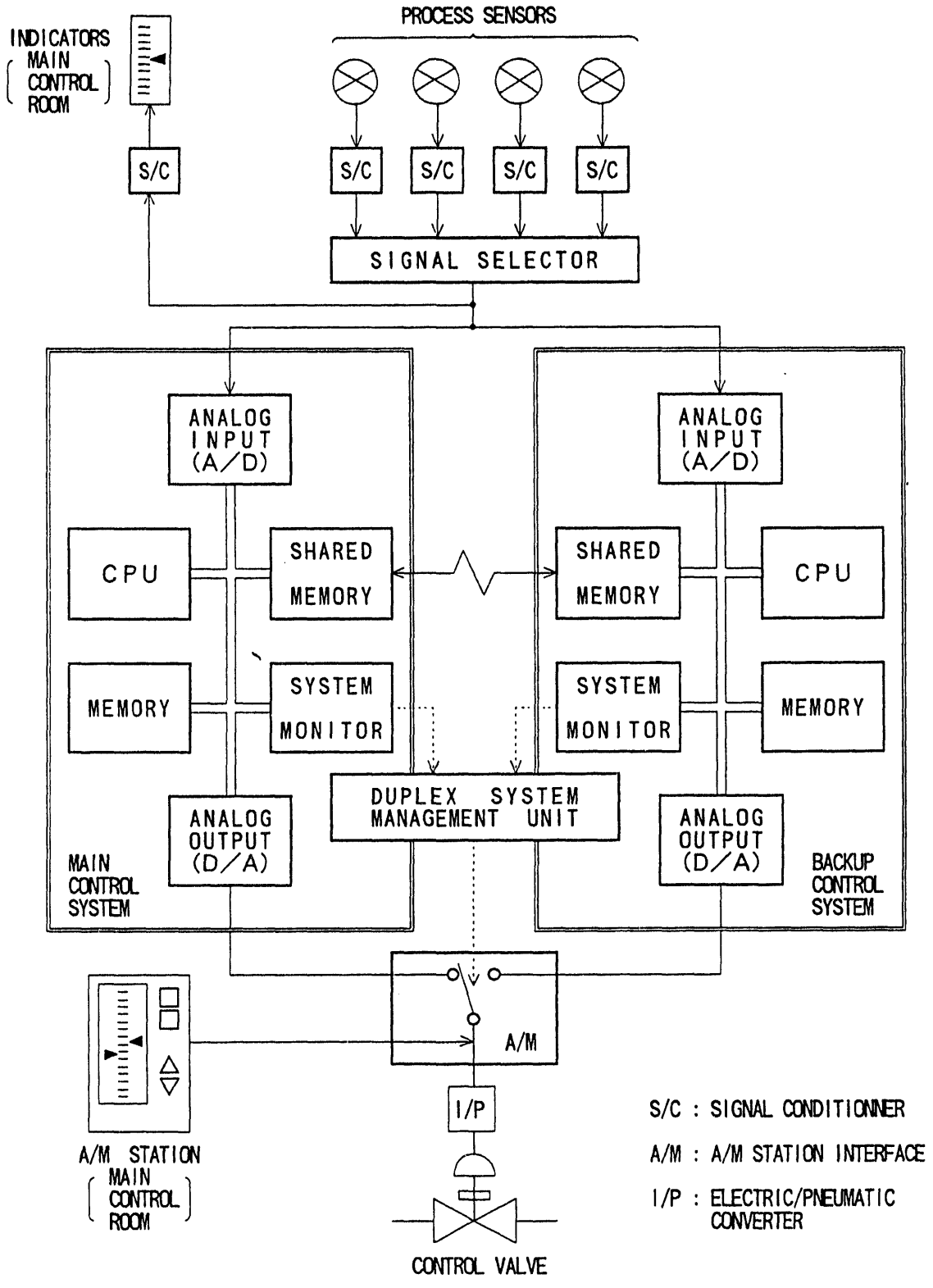
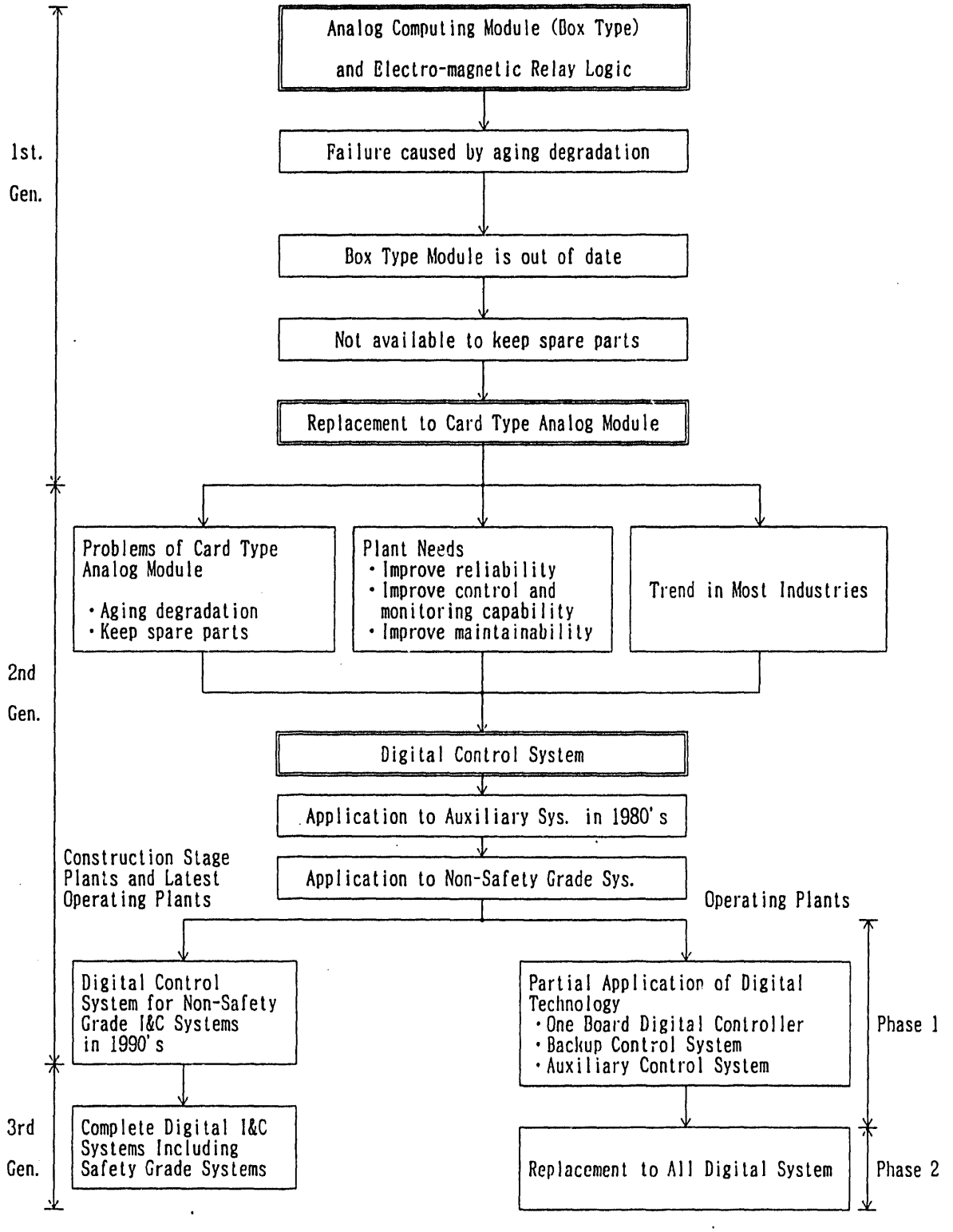


Figure 4 : Digital Control System Architecture

Appendix A :
Transtition of Digital Technology for I&C System



Appendix B : Pratial Application of Digital Technology

● : installed in some plants
○ : planned to apply
△ : proposed only

One Board Digital Controller , (Application — (a)*)	Backup Control System (Application — (b)*)	Auxiliary Control System (Application — (c)*)
○ Advanced F.W. Bypass Cont. Sys. ○ Advanced Main F.W. Cont. Sys. ○ Reactor Make-up Water Flow Cont. Sys. ○ Reactor Vessel Level Indication Sys. △ Letdown Line Press. Cont. Sys. △ Letdown H.X. Outlet Letdown Line Temp. Cont. Sys. △ RCP Seal Injection Flow Cont. Sys. △ M.S. Dump Cont. Sys. △ P'zr. Press. Cont. Sys. △ Automatic Transfer Logic Between F.W. Bypass Cont. Valve and Main F.W. Cont. Valve.	● Improved Main F.W. Cont. Sys. – automatic correct input selection from redundant input signals – backup control system at the failure of main control system – automatic correct subsystem selection from redundant pneumatic subsystems of a valve – automatic transfer logic between F.W. Bypass Cont. Valve and Main F.W. Cont. Valve	● Boric Acid Evaporator ● Waste Disposal Evaporator ○ Spent Resin Disposal Sys.

* Application – (a) : replace several analog circuit cards with one board digital controller
– (b) : add digital control systems as backup control systems
– (c) : apply digital control systems to auxiliary control systems

Ministry of Social Affairs and Employment
Directoraat-Generaal van de Arbeid
Kernfysische Dienst
(Nuclear Safety Department in the Netherlands)

Lecture for the IAEA-IWG-NPPCI
Specialist Meeting 5-7 May, 1993

Modernisation of the Borssele NPP Reactor Protection System

Introduction

Since a few years the obligation to evaluate the safety level periodically against the state of the art is established in the licences of nuclear power installations in The Netherlands. This was leading to backfitting programmes for both nuclear power plants in this country. These programmes are in an engineering phase these days.
One of the plants to be backfitted is the Borssele NPP. This is a 450 MWe PWR, in operation since 1973. Design and construction is from Siemens/KWU. Its concept is from an earlier date than for instance the KWU-Konvoi design and thus shows more ramification and less separation in process, electrical and instrumental redundancies than more recent plant types.
To combat dependencies in failure modes an additional bunkerized civil structure, Building 33, had been already erected in 1985. This building meets redefined requirements for flood, gas cloud explosion and external fire. It provides space for the functionally and physically separated redundancies of emergency suppletion systems for the primary as well as the secondary loop. Independency has been acquired by its own power supply. These systems provide a certain back up for the primary volume control, the core injection system and the auxiliary feed water supply in case of an external event.
The present backfitting programme is also utilizing the design considerations of these Bld.33 systems.

Plant backfitting programme

The plant backfitting programme is based on a re-assessment of the existing safety systems and a probabilistic safety analysis. An extension of the list of design based accidents has been incorporated. Deviating from the original design base, external accidents like earth quake and airplane crash are now being considered.
Important backfitting items are :

- increasing the number of emergency cooling water (VF) pumps from three to four,
- increasing the number of nuclear intermediate cooling (TF) pumps from three to four,
- addition of a spare well cooling system (VE) to have a back up if the emergency river water intake (VF) might be blocked,
- upgrading of the steam blow-off systems (RA),
- renewal of main steam lines in the containment,

- increasing secondary spare suppletion capacity (RS),
- renewal of the primary relief valves (PORV's),
- replacement of emergency dieselgenerators, increasing capacity with approx. 75 %

Within the scope of the backfitting project also a lot of upgrading will be executed on the electrical and I&C systems. Examples are :

- replacement of the process presentation computer system,
- new control panels in the control room,
- a spare control room in a bunkerized building.

Shortcomings existing reactor protection system

In view of this plantwide backfitting programme the existing RPS exhibits the following shortcomings.

- the location of cabinets in Building 05 provides insufficient protection against the newly defined external events (ref. fig.1.),
- incomplete physical separation of electrical redundancies,
- too less space for extension of cabinets inside the existing room,
- only partly self-testing,
- the number of operational bypasses can hardly be diminished,
- economical obsolescence.

Removal to the protected area

The backfitting programme comprises an evaluation of the RPS-process logics as well as the location of the cabinets.
With respect to the accident resistance the backfitting programme divides the plant systems and components in EVI- and EVA/EVI-resistant.
The expression EVI (Einwirkungen von innen) reflects accidents and disturbances with an internal origin, for instance LOCA. EVA/EVI (Einwirkungen von aussen und von innen) comprises also the external events fire, explosion, aircraft crash, flood and earth quake.
As EVA/EVI-resistant civil structures are specified the containment (Bld.01), the secondary containment (Bld.02), the emergency suppletion building (Bld.33) and a planned extension of the latter (Bld.35). EVA/EVI-resistant systems are the passive part of the primary circuit and its safety relevant active components, a part of the secondary systems and some safety systems, e.g. aforementioned emergency suppletion systems.
The EVA/EVI-resistant envelope is reflected by fig.1.
That specific part of the SCRAM-action which reacts fail-safe on any loss of power remains in its non-EVA/EVI-resistant room, but will be renewed on a components or parts level. The major part of the reactor protection system will be completely new erected within the EVA/EVI-resistant civil structure.

Architecture

The RPS is based on hardwired logic. The system architecture, which is basically shown in fig.2 remains unchanged.
Most safety systems have been arranged in a 1:2 redundant configuration, which is a part of the original plant design concept.

Both process redundancies hereby shown are activated by a 2:3 voting logic. Three analogue trains, containing sensing, transmitting and arithmetic, provide the input to binary trains being composed of limit value monitors, comparison elements and said voting logic.
In the analogue trains the mA-signals are transduced to a VDC level. The signals are elaborated by a Siemens Teleperm C8000R system. Said binary trains are provided by a Siemens EDM dynamic magnetic core system. The connection between this dynamic pulse logic and the motor control centres c.q. component actuating devices is mainly provided by Siemens Iskamatic B logic boards. The dynamic pulse outputs are transduced by special actuation formation modules (RAG Abschlussglieder).
Fig.2 also shows the physical separation of redundancies and levels in signal elaboration inside the EVA/EVI-resistant structure.

An exception is formed by the SCRAM-division of the reactor protection system. This is consisting out of two parts:
- a part activated by essentially the N-flux signals,
- a part activated by other process conditions.

The N-flux part remains located in the vicinity of the control room in the non-EVA-resistant Building 05. This is allowed because of its failure safe features due to loss of power.
Its architecture is presented in fig.3.
Analogue elaboration of signals is executed in the cabinets AT 1 u/t 4 (Siemens Teleperm B'). The binary outputs from the limit monitors are presented to three logic trains, each with 2:3 voting logic. Each train provides a triggering signal to two relay 6-contacts systems. Such a relay 6-contacts system also shows a 2:3 voting configuration. Deactivation of one relay 6-contacts system is already sufficient to generate a reactor trip.
The cabling between this part of the RPS and the control rods is running in two concrete tunnels.

That part of the SCRAM action which is activated by other conditions than the N-flux, will be established in the EVA-resistant area (bld.33 and 35). Two blocks of three signals each, coming from corresponding 2:3 voting systems in EDM logic, are tieing into the aforementioned relay 6-contacts systems. Reference is given to fig.3 and 4.

Priority control

Safety relevant components in the plant (pumps, valves, etc.) may be activated from the following levels.
- the reactor protection system,
- the control room, including its manual and automatic control facilities,
- a smaller spare control room in the new EVA-resistant building 35, which might be used in case of un-inhabitability of the main control room after an external event.

Mutually conflicting commands are excluded by priority control modules (Siemens Iskamatic B type AV 31) which provide the final commands to the plant components. These modules assure under all circumstances the highest priority to signals from the RPS.
The AV 31 module provides several opportunities for a hierarchical structure. Configurations applicable to NPP Borssele are presented in the preliminary Options A up to E, shown in respectively fig. 5 up to 9.

Some of these options show connections with the following central operator key commands.

- manual RPS-command YZ 01 (BUMS Prüfung), to be operated from the main control room to allow component testing from the main control room (Options B and E), simultaneously blocking the manual operation of some of these components from the spare control room (Option E),
- manual RPS-command YZ 02 (BUMS), to be operated from the spare control room to block the actuation of specific components from the main control room (Option C and D), simultaneously allowing the manual operation of some of these components from the spare control room. (Option C).

The Options A and B are referring to EVI-resistant plant components, the Options C, D and E are applying to EVA/EVI-resistant components.

Physical separation and isolation

The reactor protection system layout is based on the German rule KTA 3501, which prescribes availability of the system during defined combinations of failures. One of these is the common cause failure together with a random failure.
As a common cause failure may be presumed the internal area event, leading to unavailability of all electric components in the applicable room. The configuration shown by fig.2 applies to this requirement.

KTA 3501 par.4.7 requires separation of the RPS from other systems. This leads to the definition of "fire" rooms wherein decoupling modules are to be located. A fire room provides a barrier to prevent any higher voltage from outside entering a room with electronic RPS cabinets. (for instant 220 VAC from the main control room)
Examples are given in fig. 5 u/t 9.
Galvanic separation is established by isolation devices from the Siemens Iskamatic B series.

Interfaces

Since 1988 a process presentation system is in operation which presents operational and safety relevant process information to the control room. During the last years the system has been expanded a.o. with connections to staff departments.
The equipment will be replaced because the extension required by the backfitting programme is not possible within the existing computer system.
The backfitting programme requires also a new control room panel layout.
The renewal of the panels will be based on modern ergonomic principles.

Testing, maintenance and qualification

In the existing system the 2:3 voting elements are part of the static logic behind the RAG actuation formation modules (ref. fig.2). As contrasted with the dynamic logic this part of the existing RPS is not self-testing. In 1987 a special system (YT) has been developed to test RPS channels during operation of the plant.

The new configuration makes this test system superfluous because the dynamic logic will include said voting systems. The other new systems like Iskamatic provide improved diagnostic and failure warning features.

The applied I&C systems are qualified according KTA-rules.
In the N-flux part of the SCRAM action the older Siemens DM and Simatic P will be maintained after a thorough revision on parts level.
Suitable parts from the dismantled RPS will be revised and kept in stock on the plant. Appointments with the supplier have been made to maintain services and deliveries.

Conclusion

The backfitting programme removes the aforementioned shortcomings in the reactor protection system. Improved and more recent I&C systems from the same manufacturer will be applied. The programming will remain hard wired.
A hierarchical architecture is designed by using priority voting modules.
The original location of the RPS in the civil structure of the plant does not provide the opportunity to meet to-day's requirements for separation of redundancies. The latter will be acquired by locating the new system in protected buildings forming a part of the external events resistant envelope.
This approach also provides the opportunity to a systematic implementation of the new I&C and a relatively short outage time for making connections to the plant.
The conceptual design of the reactor protection system has been accepted by the Netherlands nuclear regulatory body.

The Hague, 29 April, 1993
Y.van der Plas

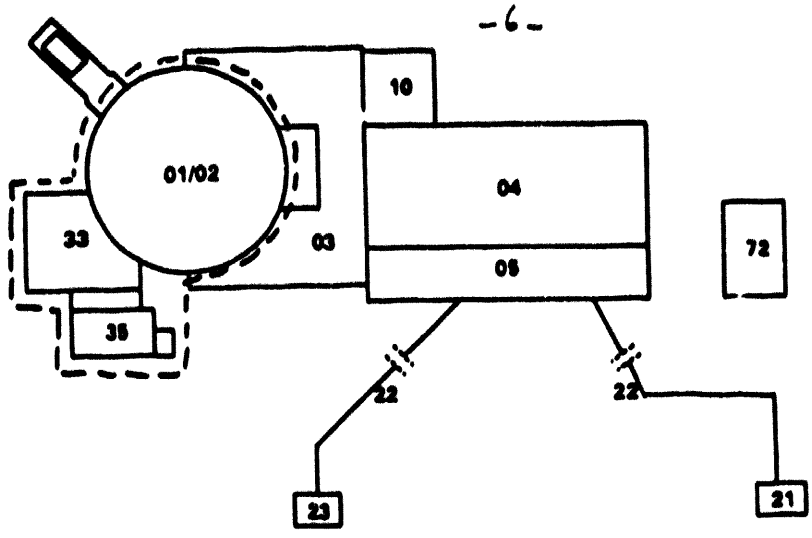


Fig.1. Plant lay-out
with EA/EVI-envelope (– – – –)

Building 01 : containment
02 : reactor building ring room
03 : additional reactor building
04 : turbine building
05 : electrical rooms and control room
33 : emergency suppletion systems building
35 : spare control room

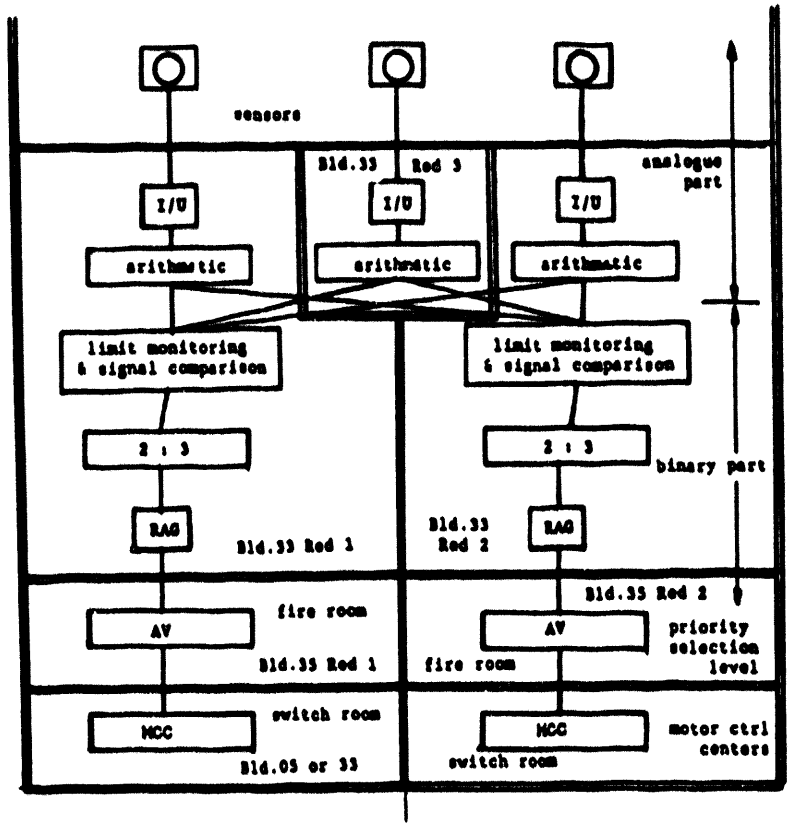
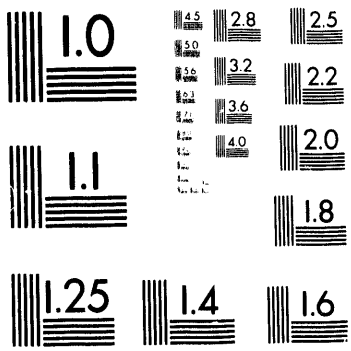


Fig.2. System architecture (general lay-out)


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6

6 of 6

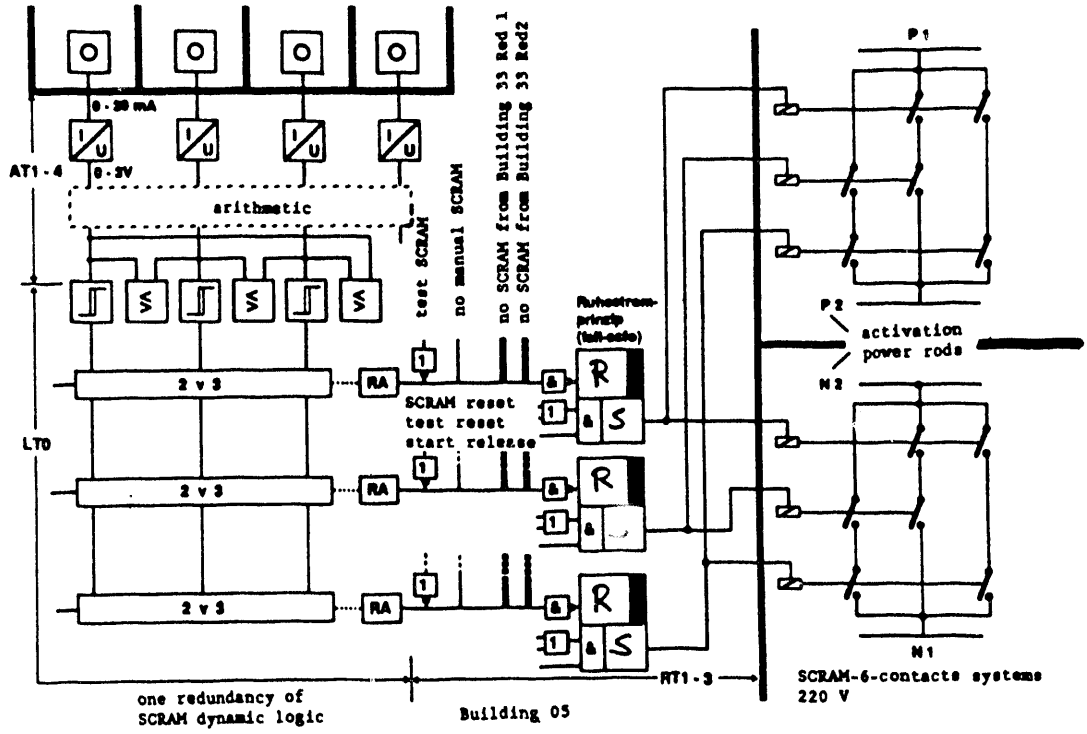


Fig.3. SCRAM-action, initiated by N-flux

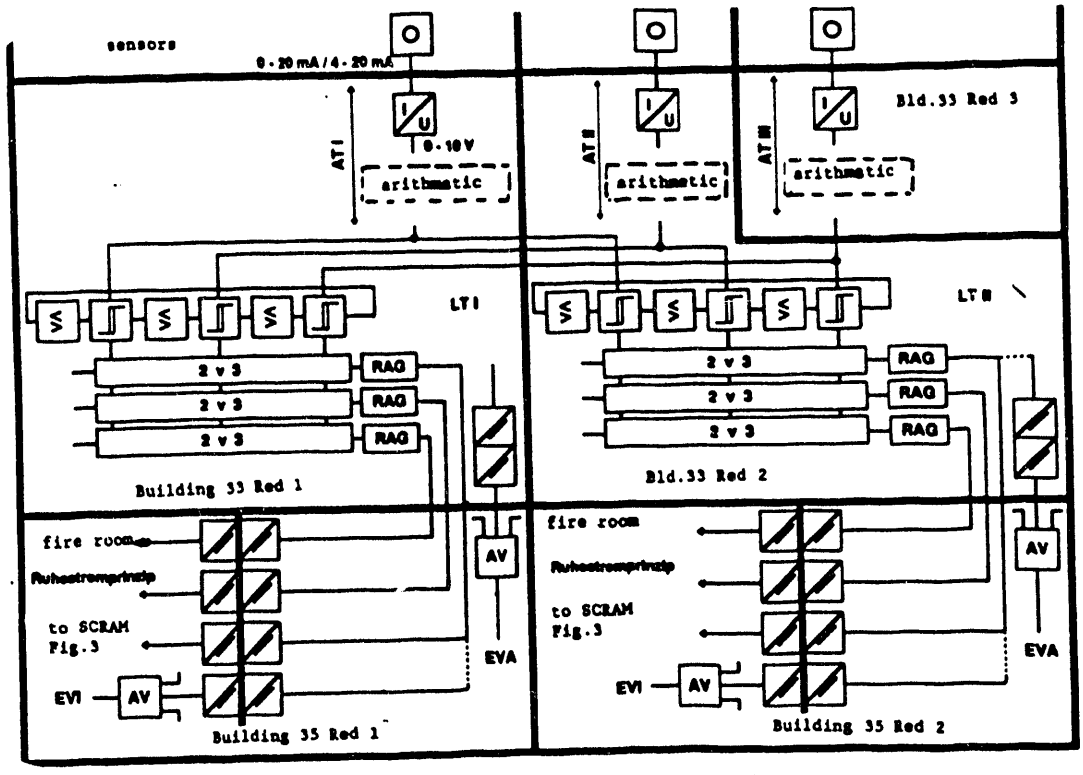


Fig.4. SCRAM-action (RESA), initiated by primary and secundary loop conditions (pressures, levels, temperatures, DNB)

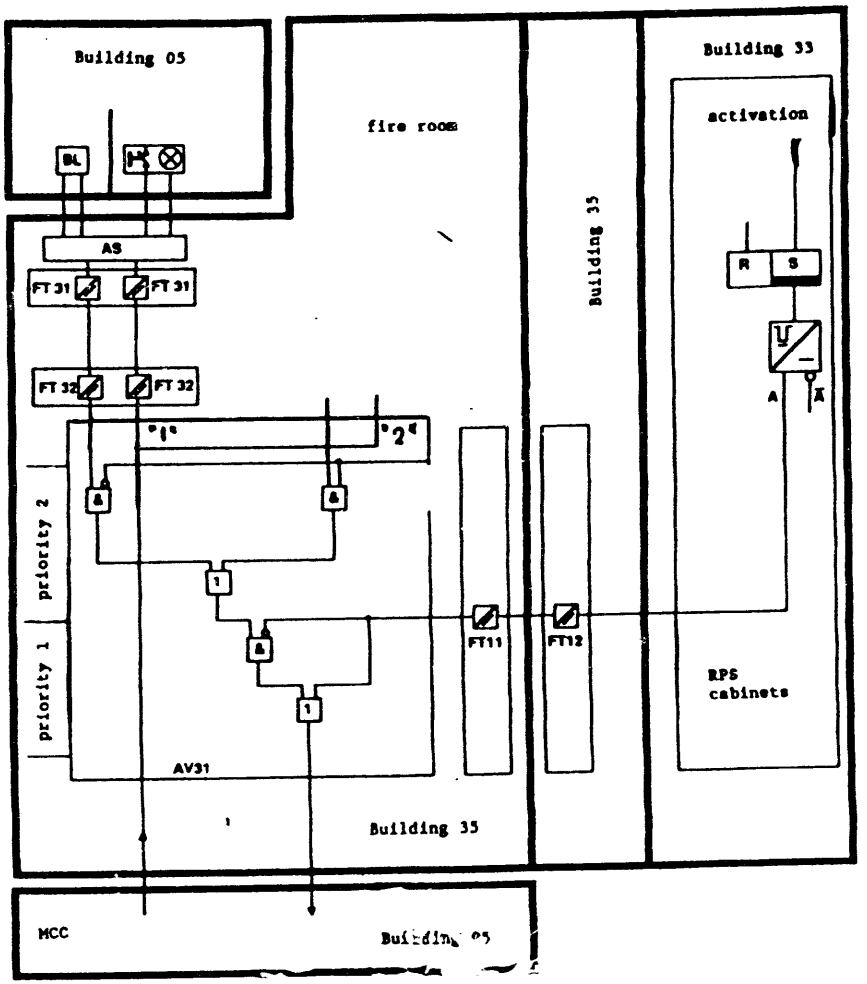


Fig.5. Option A, priority selection for EVI components without any manual command YZ 01 and 02.

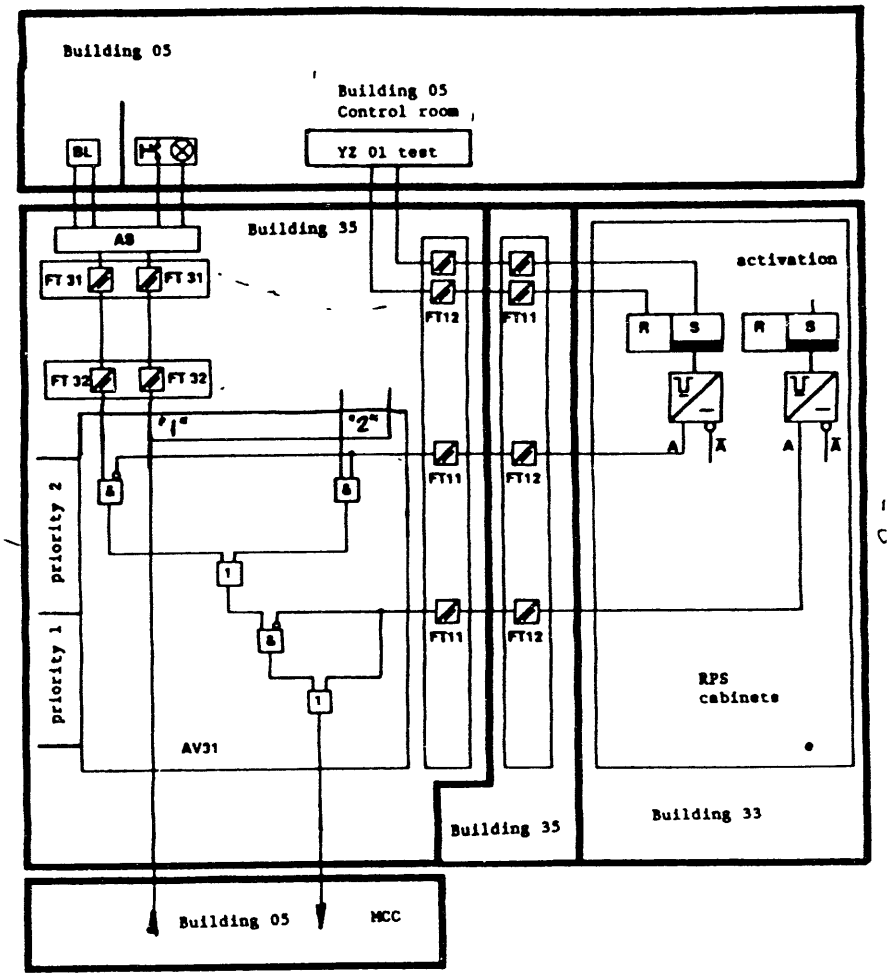


Fig.6. Option B, priority selection for normally not manually operated EVI components with manual command YZ 01 for testing the component from main control room.

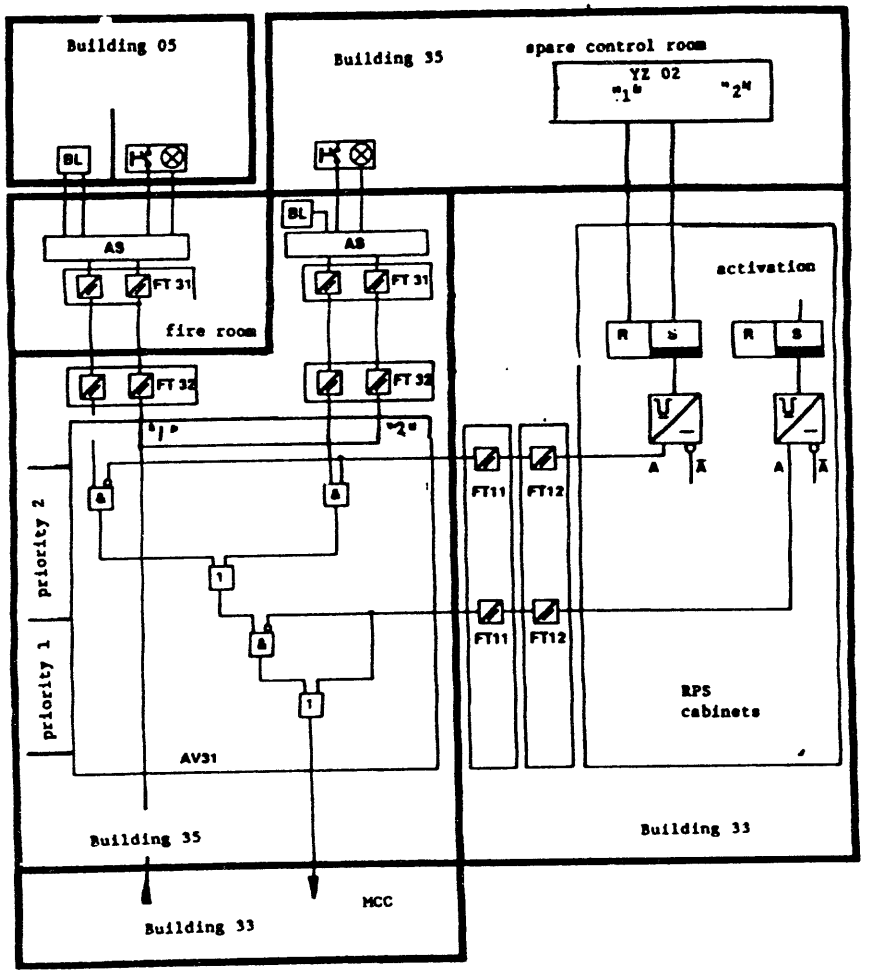


Fig.7. Option C, priority selection for EVA/EVI components with manual command YZ 02 for switching the operation from main control room to spare control room.

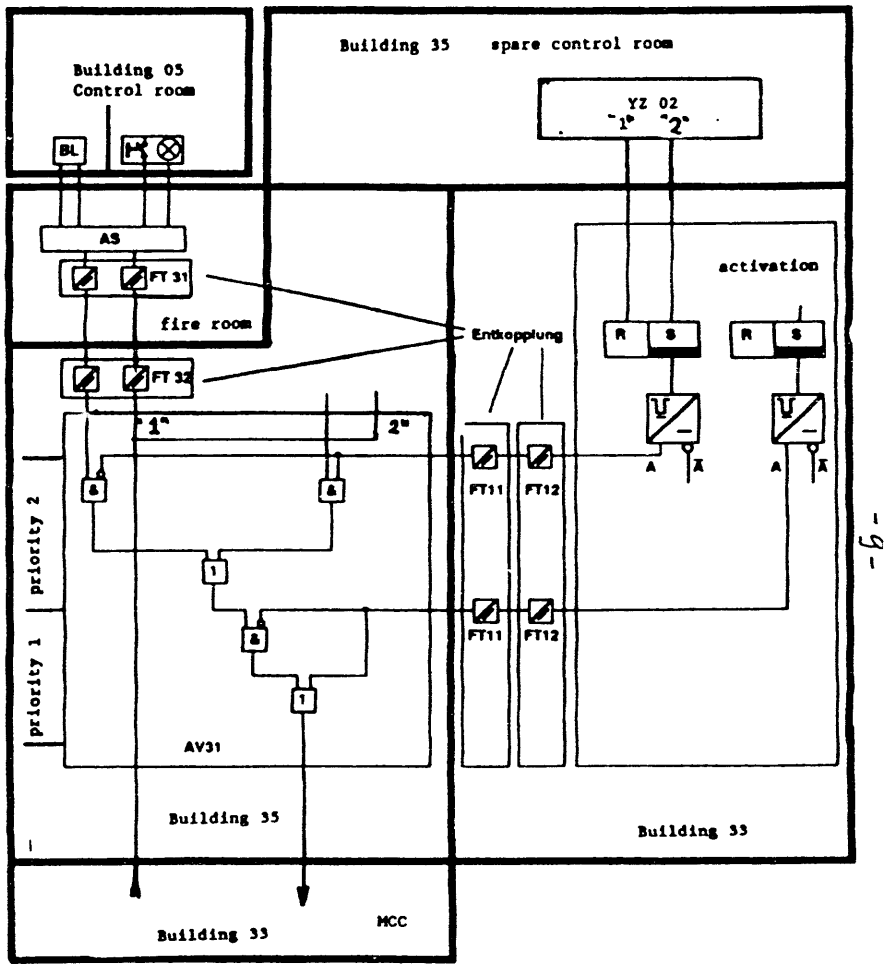


Fig.8. Option D, priority selection for EVA/EVI components with manual command YZ 02 for blocking the operation from main control room.

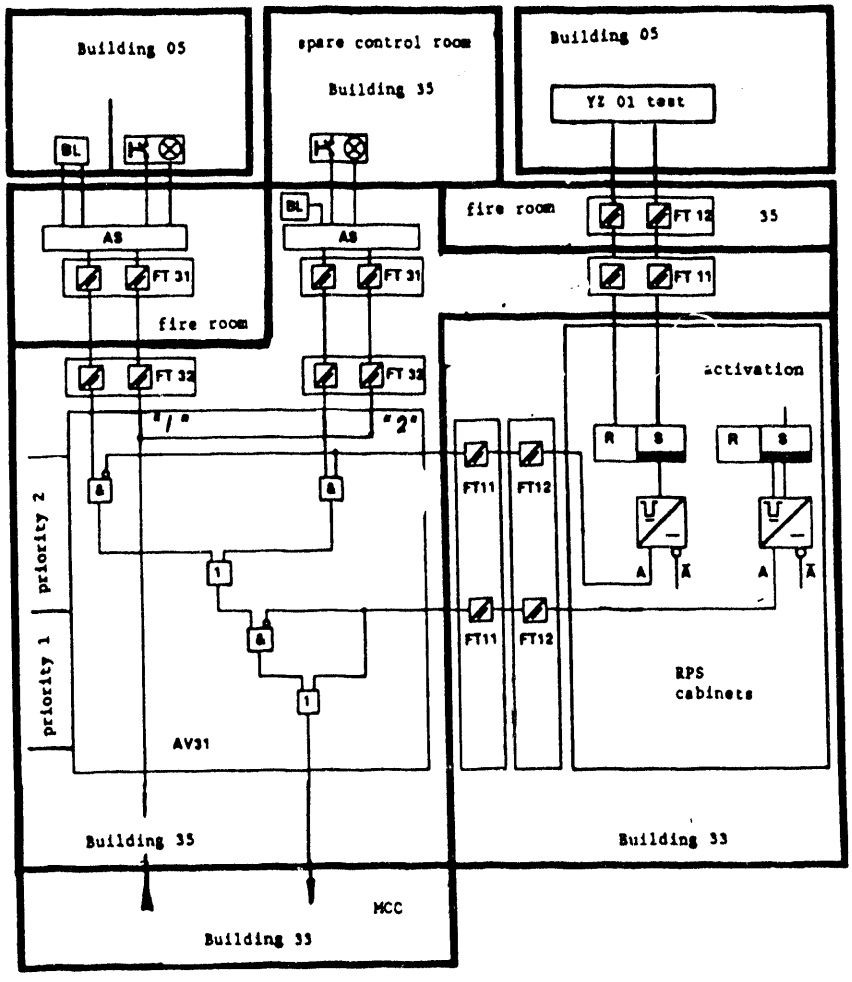


Fig.9. Option E, priority selection to test from main control room those EVA components which are normally operable from spare control room.

BL	I&C normal operation
AS	command module
AV 31	priority selection module
FT	decoupling

THE ROLE OF INTERNATIONAL STANDARDS IN THE DESIGN OF MODERN I&C SYSTEMS FOR NUCLEAR POWER PLANTS

BY
JOHN M. GALLAGHER
CHAIRMAN, IEC SC 45A [1]

[1] MR. GALLAGHER IS NOW EMPLOYED BY THE U.S. NUCLEAR REGULATORY COMMISSION IN THE INSTRUMENTATION AND CONTROL BRANCH OF THE OFFICE OF NUCLEAR REACTOR REGULATIONS. THE MATERIAL IN THIS PAPER IS A FACTUAL PRESENTATION OF ACTIVITIES RELATED TO MATTERS THAT INVOLVE THE IEC AND DOES NOT REPRESENT ANY SPECIAL ENDORSEMENT BY THE NUCLEAR REGULATORY COMMISSION.

HISTORY OF IEC AND ISO

IEC

NEED FOR AN INTERNATIONAL ORGANIZATION TO DEVELOP STANDARDIZED FEATURES OF ELECTRICAL EQUIPMENT TO PROMOTE INTERNATIONAL TRADE AND COMMERCE WAS PROPOSED AT THE ST LOUIS EXPOSITION IN 1904.

THE INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC) WAS ESTABLISHED AND STARTED OPERATION IN 1906 WITH LORD KELVIN AS THE FIRST PRESIDENT.

THE TECHNICAL COMMITTEE FOR NUCLEAR INSTRUMENTATION, TC 45, WAS CREATED IN 1958.

TWO SUBCOMMITTEES WERE CREATED AT THE FIRST TC 45 MEETING IN 1960.

- SC 45A: REACTOR INSTRUMENTATION
- SC 45B: RADIATION PROTECTION INSTRUMENTATION,

FIRST SET OF IEC SC 45A STANDARDS WERE ISSUED BETWEEN 1966 AND 1977 AND DEALT WITH;

- GENERAL PRINCIPLES OF NUCLEAR POWER REACTOR INSTRUMENTATION EQUIPMENT AND SYSTEMS

AND

- COVERED BOTH DESIGN REQUIREMENTS AND GENERAL SAFETY PRINCIPLES FOR THE INSTRUMENTATION SYSTEMS.

ISO

THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) WAS FOUNDED IN 1946 BY 25 NATIONAL STANDARDS ASSOCIATIONS.

THIS WORLDWIDE SPECIALIZED ORGANIZATION FOR STANDARDIZATION IS THE LARGEST OF THE MANY VOLUNTARY GROUPS FOR INDUSTRIAL AND TECHNICAL COOPERATION.

ISO BRINGS TOGETHER THE INTEREST OF BOTH PRODUCERS AND USERS AND ITS WORK COVERS ALMOST EVERY AREA OF TECHNOLOGY.

- MAJOR EXCEPTION IS THE ELECTROTECHNICAL AREA, WHICH IS THE RESPONSIBILITY OF THE IEC.

THE ISO/IEC AGREEMENT OF 1976 FORMED A SYSTEM OF INTERNATIONAL STANDARDIZATION. AFTER SEVERAL YEARS OF EFFORT ISO/IEC DIRECTIVES ARE NOW IN PLACE COVERING;

- PART 1: PROCEDURES FOR THE TECHNICAL WORK
- PART 2: METHODOLOGY FOR THE DEVELOPMENT OF INTERNATIONAL STANDARDS
- PART 3: DRAFTING AND PRESENTATION OF INTERNATIONAL STANDARDS

AN ISO/IEC JOINT TECHNICAL PROGRAMMING COMMITTEE WAS ESTABLISHED FOR THE PURPOSE OF AVOIDING OR ELIMINATING OVERLAP IN THE TECHNICAL WORK OF ISO AND IEC. CLOSE LIAISON BETWEEN IEC TC 45 AND ISO TC 85, NUCLEAR ENERGY, IS MAINTAINED TO AVOID OVERLAP IN THE AREAS OF RADIOACTIVITY MEASUREMENTS AND RADIATION PROTECTION.

COOPERATION BETWEEN IAEA AND IEC

In 1976 the International Atomic Energy Agency Board of Governors approved the publication of IAEA Safety Standards and IAEA Safety Guides.

- The Safety Standards comprise the Agency's basic safety standards, specialized regulations and codes of practice and are mandatory for the Agency's own operations and the Agency-assisted operations.

- The Safety Guides supplement the Safety Standards and recommend procedures that might be followed in implementing them.

Review of the early IAEA drafts of safety guides for design showed significant duplication in the work of the IAEA and IEC SC45A, especially in the area of I&C systems in protection, control and monitoring functions for Nuclear Power Plants (NPP's).

An agreement between the IAEA and the IEC on a cooperative arrangement to minimize this duplication was reached in 1981. This agreement states:

- the IAEA is responsible for the development of safety principles for instrumentation, control and electrical systems in NPP's

- the IEC is responsible for the design requirements that realize these safety principles.

- the IAEA is invited to participate in IEC TC 45 and SC45A meetings

- the IEC is invited to participate in the development of relevant IAEA Safety Guides.

RESULT OF THIS AGREEMENT WAS THE IEC DECIDED NOT TO REAFFIRM THE EARLIER SET OF IEC 231 STANDARDS THAT DEALT WITH PRINCIPLES OF I&C SYSTEMS BUT INSTEAD TO DEVELOP STANDARDS BASED ON PRINCIPLES GIVEN IN SAFETY DESIGN GUIDES, ESPECIALLY:

- 50-SG-D3, 1980, PROTECTION SYSTEM AND RELATED FEATURES IN NPP'S
- 50-SG-D7, 1982, EMERGENCY POWER SYSTEMS AT NPP'S
- 50-SG-D8, 1984, SAFETY-RELATED INSTRUMENTATION AND CONTROL SYSTEMS FOR NPP'S.

THIS DECISION FORMED A MAJOR THRUST FOR THE DEVELOPMENT OF IEC SC 45A STANDARDS FOR MODERN I&C SYSTEMS AS WILL BE SEEN BELOW.

IEC SC 45A PUBLICATIONS RELEVANT TO MODERN I&C TECHNOLOGIES

o APPLICATION OF DIGITAL COMPUTER SYSTEMS

THE FIRST IEC PUBLICATION DEALING WITH THE APPLICATION OF DIGITAL COMPUTERS TO NPP'S WAS IEC 643-1979, GUIDE TO THE APPLICATION OF DIGITAL COMPUTERS TO NUCLEAR REACTOR INSTRUMENTATION AND CONTROL.

THIS WAS IN THE FORM OF A GUIDE RATHER THAN A STANDARD BECAUSE OF THE OPINION OF SEVERAL NATIONAL COMMITTEES THAT THE TECHNOLOGY WAS TOO NEW TO BE A SUBJECT FOR STANDARDIZATION.

THE FIRST DRAFT, WRITTEN BY UK AND GERMAN EXPERTS, WAS SUBMITTED IN 1972 AND WAS PRIMARILY BASED ON THE EXPERIENCE IN THE UK WHERE THE SOPHISTICATION OF PLANT PROCESS COMPUTERS IN NPP'S HAD ADVANCED TO THE INCLUSION OF OPERATOR AIDS SUCH AS:

- ALARM ANALYSIS FUNCTIONS
- SPECIAL CALCULATIONS FOR MONITORING SELECTED PHYSICAL PROCESS BEHAVIORS.

WHILE THE MAJORITY OF THE COUNTRIES THAT WERE ACTIVE IN THE DEVELOPMENT OF NUCLEAR POWER WERE APPLYING DIGITAL COMPUTERS TO MONITORING, AND IN SOME LIMITED CASES CONTROL TASKS,

- ALMOST ALL OF THE APPLICATIONS WERE OUTSIDE THE PURVIEW OF REGULATORY AUTHORITIES
- A STANDARD ON THE SUBJECT WAS VIEWED AS AN IMPEDIMENT TO CREATIVE APPLICATIONS, SINCE DEVIATIONS FROM THE STANDARD MIGHT BECOME A SOURCE OF CONTENTION.

THE ATTITUDE AMONGST NATIONAL COMMITTEES FOR THE NEED FOR A STANDARD FOR THE APPLICATION OF DIGITAL COMPUTERS CHANGED IN THE MID TO LATE 70'S, ESPECIALLY IN THE U.S. AND FRANCE, WHEN DESIGNS USING DIGITAL COMPUTERS IN THE SAFETY SYSTEM WERE PROPOSED.

THE U.S. INCREASED THE ACTIVITY IN LATE 70'S TO DEVELOP A STANDARD BY FORMING A JOINT IEEE/ANS WORKING GROUP, WHICH PRODUCED ANSI/IEEE-ANS-7-4.3.2-1982, STANDARD CRITERIA FOR DIGITAL COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER GENERATING STATIONS.

THE DECISION WAS MADE TO LIMIT THE CONTENT OF THIS STANDARD TO GENERAL TOP LEVEL REQUIREMENTS FOR:

- THE COMPUTER SYSTEM
- SOFTWARE DEVELOPMENT
- VERIFICATION AND VALIDATION.

THE INITIAL IEC DRAFT STANDARD, PREPARED BY A GROUP OF U.S. EXPERTS IN THE LATE 70'S, EXPANDED THE PROPOSED CONTENT BEYOND THE U.S. STANDARD TO INCLUDE MORE DETAILED REQUIREMENTS, AS REQUESTED BY THE EUROPEAN MEMBERS OF THE IEC, ESPECIALLY FRANCE, GERMANY AND ITALY.

EARLY IN THE DEVELOPMENT OF THIS STANDARD MEMBERS OF A SPECIAL EUROPEAN STUDY GROUP FOR SAFE SOFTWARE, TC-7, REQUESTED AND WERE PERMITTED ACTIVE PARTICIPATION IN IEC SC45A/WGA3. THEY HAD DEVELOPED DETAILED RECOMMENDATIONS FOR:

- DESIGN AND CODING OF SAFETY RELATED SOFTWARE
- LANGUAGE, ITS TRANSLATOR, LINKAGE EDITOR, ETC.
- SOFTWARE TESTING

SOME OF THESE DETAILED REQUIREMENTS WERE INCORPORATED INTO THE BODY OF THE DOCUMENT HOWEVER THE MAJORITY WERE PLACED IN APPENDICES.

THIS STANDARD WAS FINALLY PUBLISHED IN 1986 AS IEC 880, SOFTWARE FOR COMPUTERS IN THE SAFETY SYSTEM OF NPP'S

THE STANDARD HAS BEEN USED AS A PRINCIPAL REQUIREMENTS DOCUMENT FOR NUCLEAR POWER PLANT PROJECTS IN THE UK, FRANCE AND ITALY (THE PUN PROJECT, WHICH WAS TERMINATED).

WHILE IEC 880 MADE REFERENCE TO IAEA 50-SG-D3 IT WAS RECOGNIZED THAT A COMPANION DOCUMENT WITH REQUIREMENTS FOR THE HARDWARE FOR COMPUTER SYSTEMS IMPORTANT TO SAFETY WAS NEEDED AND WORK ON THIS SUBJECT WAS INITIATED DURING THE FINAL PHASE OF APPROVAL FOR IEC 880.

THE SCOPE FOR THE COMPUTER SYSTEM WAS EXPANDED TO INCLUDE BOTH THE SAFETY SYSTEM, AS DEFINED BY IAEA 50-SG-D3, AND SAFETY RELATED SYSTEMS AS DEFINED BY IAEA 50-SG-D8.

THE DOCUMENT ALSO INCLUDES REQUIREMENTS FOR OFF-THE-SHELF AVAILABLE EQUIPMENT, E.G. HARDWARE WITH BUILT-IN SOFTWARE, THAT PROVIDES AN ALTERNATIVE TO IEC-880.

THE STANDARD WAS PUBLISHED IN 1989 AS IEC 987, PROGRAMMED DIGITAL COMPUTERS IMPORTANT TO SAFETY FOR NPP'S.

SUPPLEMENT TO IEC 880; THIS IS THE FIRST OF AT LEAST TWO SUPPLEMENTS PLANNED FOR IEC 880 FOR THE PURPOSE OF INCORPORATING REQUIREMENTS FOR DESIGN MATTERS THAT HAVE DEVELOPED SIGNIFICANTLY IN BOTH IMPORTANCE AND MATURITY OVER THE PAST SEVERAL YEARS. THIS FIRST SUPPLEMENT ADDRESSES;

- DIVERSITY AGAINST COMMON MODE FAILURES
- FORMAL SPECIFICATIONS AND DESIGN METHODS
- AUTOMATIC TOOLS
- USE OF PRE-EXISTING SOFTWARE

IN ADDITION THE SCOPE OF THIS SUPPLEMENT WILL INCLUDE SAFETY RELATED SYSTEMS, BASED ON IEC 1226, AS WELL AS SAFETY SYSTEMS.

THERE ARE ALSO TWO ADDITIONAL STANDARDS UNDER DEVELOPMENT THAT ARE PRIMARILY RELATED TO THE APPLICATION OF DIGITAL COMPUTER BASED SYSTEMS:

- FUNCTIONAL REQUIREMENTS FOR MULTIPLEXING SYSTEMS IN NPP'S
- METHODS AND CRITERIA FOR ELECTROMAGNETIC INTERFERENCE IN NPP'S

o CLASSIFICATION AND GRADED REQUIREMENTS FOR I&C SYSTEMS IMPORTANT TO SAFETY

THE MOST RECENT COMPLETED IEC STANDARD IN THIS GENERAL AREA OF I&C SYSTEMS IMPORTANT TO SAFETY IS IEC 1226, THE CLASSIFICATION OF INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY FOR NPP'S. THIS STANDARD WILL BE PUBLISHED IN 1993. THE STANDARD DEALS WITH THE DIFFICULT AND OFTEN CONTROVERSIAL SUBJECT OF CLASSIFICATION AND GRADED REQUIREMENTS FOR I&C FUNCTIONS, SYSTEMS AND EQUIPMENT (FSE) BASED ON THEIR IMPORTANCE TO SAFETY.

THE SAFETY PRINCIPLES FOR THE STANDARD WERE TAKEN FROM IAEA 50-SG-D8 WHERE THREE CATEGORIES OF IMPORTANCE TO SAFETY ARE DEFINED, IN ADDITION TO A CATEGORY THAT HAS NO DEFINED SAFETY ROLE.

THE STANDARD ESTABLISHES A METHOD OF CLASSIFICATION OF THE INFORMATION AND CONTROL FUNCTIONS FOR NPP'S AND THE INSTRUMENTATION AND CONTROL SYSTEMS AND EQUIPMENT THAT PROVIDE THOSE FUNCTIONS.

THE CATEGORIZATION METHOD IS BASED ON QUALITATIVE CRITERIA AND DOES NOT REQUIRE RISK ASSESSMENT RESULTS. THE RESULTING CLASSIFICATION THEN DETERMINES RELEVANT DESIGN CRITERIA. THE DESIGN CRITERIA ARE MEASURES OF QUALITY BY WHICH THE ADEQUACY OF EACH FSE IN RELATION TO ITS IMPORTANCE TO PLANT SAFETY IS ENSURED, NAMELY:

- FUNCTIONALITY
- RELIABILITY
- PERFORMANCE
- ENVIRONMENTAL DURABILITY
- QUALITY ASSURANCE (QA).

o DESIGN OF THE MAIN CONTROL ROOM

AN AREA NOT USUALLY ASSOCIATED WITH I&C SYSTEMS, BUT OF EQUAL IMPORTANCE FOR THE SAFE OPERATION OF NPP'S IS THE MAIN CONTROL ROOM.

IEC SC 45A UNDERTOOK THE DEVELOPMENT OF A STANDARD FOR THE DESIGN OF CONTROL ROOMS OF NPP'S IN 1982. BACKGROUND MATERIAL FOR THIS WORK INCLUDED VARIOUS IEEE NPEC SC-7 COMPLETED AND DRAFT DOCUMENTS AND NUREG-0700.

IN ADDITION FRANCE, THE UK, GERMANY AND JAPAN, WHO PROVIDED THE SECRETARY FOR THIS COMPLEX ACTIVITY, SUPPLIED A SIGNIFICANT AMOUNT OF MATERIAL FOR THE DEVELOPMENT OF THE STANDARD.

THE STANDARD IEC 964, DESIGN FOR CONTROL ROOMS OF NPP'S WAS PUBLISHED IN 1989. THE APPLICATION OF THIS STANDARD WAS PRIMARILY FOR NEW CONTROL ROOM DESIGNS.

THIS STANDARD ESTABLISHES REQUIREMENTS FOR THE:

- MAN/MACHINE INTERFACE IN THE MAIN CONTROL ROOMS OF NPP'S
- SELECTION OF FUNCTIONS
- DESIGN CONSIDERATIONS AND ORGANIZATION OF THE MAN/MACHINE INTERFACE
- PROCEDURES TO VERIFY AND VALIDATE THE FUNCTIONAL DESIGN.

THE REQUIREMENTS REFLECT THE APPLICATION OF HUMAN ENGINEERING PRINCIPLES AS THEY APPLY TO THE MAN/MACHINE INTERFACE DURING NORMAL AND ABNORMAL PLANT CONDITIONS.

AN EXTENSIVE APPENDIX IS PROVIDED TO EXPLAIN THE CONCEPTS USED IN THE STANDARD INCLUDING THE BASES FOR THE FUNCTIONAL DESIGN OF THE CONTROL ROOM AND FOR THE DEVELOPMENT OF THE FUNCTIONAL DESIGN SPECIFICATIONS.

A NEW IEC STANDARD, OPERATOR CONTROLS IN NPP'S, HAS RECEIVED FINAL APPROVAL AND WILL BE PUBLISHED IN 1993. THIS STANDARD EXPANDED ON GUIDANCE GIVEN IN THE APPENDIX OF IEC 964 AND PROVIDES REQUIREMENTS FOR THE DESIGN OF CONTROL STATIONS IN THE MAIN CONTROL ROOM APPLICABLE TO BOTH NEW DESIGNS AND RETROFITS TO EXISTING CONTROL ROOMS.

OTHER CONTROL ROOM STANDARDS THAT ARE UNDER DEVELOPMENT INCLUDE:

- VDU APPLICATIONS TO MAIN CONTROL ROOMS IN NPP'S; THIS STANDARD IS SIMILAR TO THE OPERATORS CONTROL STANDARD IN THAT IT EXPANDS ON GUIDANCE GIVEN IN THE APPENDIX OF IEC 964 AND PROVIDES REQUIREMENTS FOR THE DESIGN OF VDU DISPLAYS IN THE CONTROL ROOM AND IS APPLICABLE TO BOTH NEW DESIGNS AND RETROFITS.

- VERIFICATION AND VALIDATION OF CONTROL ROOM DESIGN OF NPP'S; THIS STANDARD ALSO EXPANDS ON GUIDANCE GIVEN IN THE APPENDIX OF IEC 964, USING EXPERIENCE RECENTLY GAINED IN SEVERAL COUNTRIES, TO PROVIDE REQUIREMENTS FOR THE VERIFICATION AND VALIDATION OF BOTH NEW CONTROL ROOM DESIGNS AND MODIFICATIONS TO EXISTING DESIGNS.

o ADVANCED MEASUREMENT AND MONITORING SYSTEMS

In addition to the general standards that deal with modern digital computer based I&C systems, standards for special modern instrumentation and control systems have also been published or are under development. Published standards include:

- IEC 911 (1987), Measurements for monitoring adequate core cooling within the core of pressurized light water reactors
- IEC 960 (1988), Functional design criteria for a safety parameter display system for NPP's
- IEC 988 (1990), Acoustic monitoring systems for loose parts detection - Characteristics, design criteria and operational procedures.

Standards under various stages of development include:

- Measurements for monitoring adequate cooling within the core of boiling light water reactors. The scope of this proposed standard is similar to IEC 911.
- Monitoring of internal structures in pressurized water reactors
- Monitoring of power oscillations in boiling water reactors
- Nuclear instrumentation and electrical systems for the safe operation of RMBK type reactors. This is a joint project with the IAEA and the Commission of European Communities.

SUMMARY

IN ADDITION TO THE ABOVE IEC SC 45A HAS DEVELOPED MANY STANDARDS FOR RADIATION MONITORING SYSTEMS FOR NPP'S COVERING THE RANGE OF NORMAL OPERATION AND BOTH ACCIDENT AND POST-ACCIDENT CONDITIONS.

THE MAIN COMMITTEE, TC 45, HAS BEEN A LEADER IN THE DEVELOPMENT OF STANDARDS FOR SPECIAL MEASUREMENT SYSTEMS USING GENERALIZED MODULAR AND DISTRIBUTED I&C SYSTEM TECHNOLOGY SUCH AS THE CAMAC AND FASTBUS SERIES OF STANDARDS.

THE INTERNATIONAL ELECTROTECHNICAL COMMISSION IS DEVELOPING A MASTERPLAN; THE IEC STRATEGY FOR THE FUTURE. THE INTRODUCTORY STATEMENT TO THIS PLAN PROVIDES A GOOD CLOSING STATEMENT FOR THIS PAPER.

"THE IEC IS THE ORGANIZATION RESPONSIBLE FOR DEVELOPING INTERNATIONAL ELECTROTECHNICAL STANDARDS BY THE VOLUNTARY CONSENSUS PROCESS.

IT HAS A CURRENT CATALOGUE OF MORE THAN 100,000 PAGES OF STANDARDS - IN THE COMPLETE DOMAIN OF ELECTRICAL, ELECTRONIC, COMMUNICATION AND RELATED TECHNOLOGIES - WHICH IS INCREASING AND UP-DATING AT A RATE OF 15,000 PAGES PER ANNUM.

MORE THAT 10,000 EXPERTS AROUND THE WORLD ARE ENGAGED IN THIS PROCESS.

INTERNATIONAL TRADE IN MANUFACTURED GOODS, OF WHICH THE ELECTROTECHNICAL PRODUCTS ARE APPROACHING 50%, DEPEND SIGNIFICANTLY ON THE IEC OUTPUT."

SESSION 8

MODERNIZATION ISSUES

Software Maintenance and Re-Validation for Nuclear Power Plants

Reliability Analysis of Microprocessor-based Control and Protection Systems in Nuclear Power Plants

Recent Activities within Nuclear Electric Related to the Qualification of Digital Systems and the Extension of Maintenance Intervals

Qualification Issues Associated with the Use of Advanced Instrumentation and Control Systems Hardware in Nuclear Power Plants

SOFTWARE MAINTENANCE AND RE-VALIDATION FOR NUCLEAR POWER PLANTS

MR R G PHOENIX

ROLLS-ROYCE AND ASSOCIATES LIMITED

PO Box 31
Derby
DE24 8BJ
England

ABSTRACT

When designing a new I&C system, software can be developed using modern software engineering methods. However, existing systems cannot, by definition, have been developed using such techniques. Thus consideration should be given to methods for maintaining ageing software. Requirements for software changes can arise from several sources. Several problems can be encountered when becoming involved in maintaining ageing software. Solutions to these problems come from the employment of modern software engineering techniques, including complete emulation of the original hardware, reverse/re-engineering and redesign. The choice of which technique(s) to use can depend on cost and whether it is possible to demonstrate the required integrity. Furthermore, the extent of modification, the likelihood of further changes and further maintenance problems can all have a bearing.

1. INTRODUCTION

Rolls-Royce and Associates (RRA) has over 30 years experience in the design, supply and in-service support of nuclear steam raising plants. This responsibility extends to the development and procurement of all aspects of the reactor plant and utilises a broad base of skills from project management through to quality assurance, safety and reliability.

When designing a new I&C system, software can be developed using modern software engineering methods. However, existing systems cannot, by definition, have been developed using such techniques. Thus consideration should be given to methods for maintaining ageing software. This paper will discuss the methods which can be applied in the maintenance of software for I&C systems on nuclear power plants.

Requirements for software changes can arise from several sources, including:

- Obsolete underlying hardware
- Fitting to a new plant
- Addition of extra I&C systems
- Correcting/modifying requirements or design to enhance performance or safety.

Note that the software itself does not degrade.

Several problems can be encountered when becoming involved in maintaining ageing software :

- Written in low level or "obsolete" languages.
- Poor documentation.
- Modern design methods not employed in the first place.
- Shortage of memory/CPU power means software is probably written for efficiency in very specific circumstances. This can be cryptic, unmaintainable and very difficult to modify.
- Original V&V may be unrepeatable, poor and undocumented.
- Software (including documentation) degraded by multiple changes.
- Modifications must be justified to current standards.
- Not possible to quantify the reliability of the modified systems by arguing from reliability of the existing system.

Solutions to these problems come from the employment of modern software engineering techniques, including :

- Complete emulation of the original hardware.
- Reverse/re-engineering.
- Redesign.

The choice of which technique(s) to use can depend on cost and whether it is possible to demonstrate the required integrity. Furthermore, the extent of modification, the likelihood of further changes and further maintenance problems can all have a bearing. Each of these solutions are discussed in detail below.

2. EMULATION

Modern computer hardware and software have brought about considerable speed and capacity improvements. This has allowed the achievement of original performance, despite emulation. Hence emulation can now be considered as a realistic possibility for addressing some of the above problems.

Emulation software must itself be validated, and this is very challenging [1]. Very slight performance changes owing to the emulation software may affect the timing responses of a program. This can lead to unexpected or intermittent problems, which can be infuriatingly difficult to pinpoint. This problem is exacerbated by the fact that most systems which require platform emulation tend to be those which are most susceptible to timing problems.

Any new hardware for a system must be maintained and may become obsolete. Emulation software may be affected by the hardware maintenance activities, since pin compatible replacements will not be perfect functional and performance equivalents. Thus the emulation software itself needs to be maintained. This requires a detailed understanding of both the system and emulation platforms, which is not easy to retain in the long-term [2]. Validation of the system on the new emulation platform is difficult. (The systems which need emulation are often the most difficult to validate anyway). It is doubly difficult to make functional changes to the application software, because it is limited by its original platform. Hence the Application software developers must retain knowledge of the original platform.

The decision to use emulation as a solution to the problems of maintaining ageing software is normally made on the basis of existing software maintainability. If the software is already considered unmaintainable, emulation is chosen. Of course this implies that the software is no longer properly understood, and has implications on any attempt to validate it.

3. REVERSE ENGINEERING

Reverse engineering is the process of recovering design information from the existing software, and converting this into a modern methodology format. This process can be laborious without automated tools [3], and it is debatable whether the resulting software can be validated to modern standards (since it is based on ageing software). Other tasks to be performed in the reverse-engineering process include re-documentation, code-conversion and testing.

3.1 Re-documentation

This is the process of recovering design information from existing source code. Once this is done, documentation of the design can be provided. There are four areas of software design which can be documented : structure charts, or high-level design; code comments; mini-specifications; requirements documents. Good documentation is key to the future maintenance of programs.

Structure charts give a high level overview of a program. They essentially show the calling hierarchy of modules within a program, a kind of high-level map of the program. The ability to include structure charts as part of existing computer aided software engineering (CASE) tools is required. In other words, structure charts must be produced within any existing CASE tool, to facilitate future maintenance.

Code comments improve the understanding of modules within a program for future maintenance personnel. Mini-specifications, or M-Specs, are the low-level design of a particular module. They are language independent. They can be written in numerous forms, the most common being to use structured English.

Requirements documents usually exist for most systems; however, they may be outdated compared with the actual implementation. Although requirements documents should not describe actual implementation details, it may be that requirements included as implementation have not been documented. Thus there may be situations where reverse engineering must go right back to requirements, and update them. Requirements documentation needs information over and above the source code, namely the original requirements and any amendments to them (which can be derived from the code).

Many of the above processes can be automated. For example, software tools are available which can automatically generate structure charts from a piece of source code. They effectively "parse" the program and produce the structure chart accordingly. Clearly, such tools offer enormous advantages over manual performance of the task, since they can produce a chart in minutes rather than hours.

3.2 Re-Engineering

This is the process of making changes to programs where instances of undesirable programming have been identified, or in order to improve the understanding of a program. It can also improve the efficiency of a program.

Identifying areas to change is undertaken by static analysis of the program. This should highlight such things as redundant code, over-complex code and unreachable code. Once this process has been completed, the appropriate changes to the program can be implemented. These changes could include module restructuring, program restructuring (to take advantage of code redundancy) and elimination of undesirable code features. This will require re-documentation, as well as code changes, since M-Specs will certainly have changed, and the overall structure of the program may also have changed.

A consideration for this process is the possibility of improving the existing user interface to the program. The advent of Window environments allows for user-friendly interfaces (Graphical User Interfaces - GUIs) to be provided for programs. If the existing arrangements for providing program input and receiving program results are complicated, this option may need to be considered.

As with re-documentation, re-engineering can be automated. Tools are available which can unscramble code (and make it readable), calculate quality metrics, and determine non-standard features of a programming language used in a particular program. In fact, there are tools which cover virtually the entire static analysis process.

3.3 Code Conversion

This is the process of converting existing programs to be able to execute in a new environment, without changing the functionality of the program. This can mean a change of operating system, a change of language, or both.

A change of operating system usually occurs when existing programs are transferred from old computers to new. For example, from a mainframe to workstations. It is likely that the implementation of a programming language on the old system will be incompatible with that of the new. An example would be that accessing files may be different. Hence some conversion work is required.

A change of language normally involves an upgrade in the language. For example, from Fortran 4 to Fortran 77. In such situations, the appropriate standards bodies try to ensure that programs written in the old version will be compatible with the new. The fact that a new, and presumably better, version exists however, should be considered. Programs could be converted so as to make use of some of the new language features. Also, it is possible that the standards bodies have not considered all language aspects, thus causing difficulties with the later language.

Another possible situation is that of converting programs written in one language to another, entirely different language. For example, an Algol program to a Fortran program. This may be desirable because functionality used in the older language may be incompatible with new quality assurance standards (e.g. GOTO statements). Furthermore, programming languages can become obsolete, like anything else. Remaining with an obsolete language means that obsolete skills have to be maintained, and advantage cannot be taken of new tools and techniques.

Although code conversion should not change the functionality of a program, there are situations where this cannot be avoided. For instance, word lengths in one implementation of a language may be different from another. This may create a need to change existing source code, to ensure that the program still performs its original task. RRA have experience of difficulties with word lengths, where an existing program was written with a language that utilised 36-bit length words. On conversion, the target language utilised word lengths of 32 bits. This led to instabilities in numerical methods that the source code utilised. This in turn led to a significant escalation in the costs of converting the code, which was unpredictable at the outset. Of course, it can now be identified as a risk.

Code conversion is a task which would benefit from automation. However, few tools are available which can perform code conversion. This is not surprising, since there are a very large number of combinations of languages which could be converted from and to. Hence the importance of language standards, and the use in software development of those standards, is paramount.

3.4 Testing

If any of the processes described above have led to changes in the source code, then the process of testing the program must be carried out. This is equivalent to the forward engineering test process, except that only changed modules need be unit tested. Thus the process consists of reviewing those modules which have changed, unit testing the same modules, integration and system testing, and finally user acceptance testing.

A point to note is the problem of what to test against [4]. In forward engineering, modules are tested against their relevant specifications. In reverse engineering, re-engineered modules must be tested against the original code. There will be some situations where this is not worthwhile, such as the case when modules have had functional changes incorporated. In these cases, it will be necessary to re-document the functionality of the old code, combined with the new changes, and test as in the forward engineering process.

There may be situations where a program is well-structured, well written and well documented, in accordance with quality standards of today. However, if there is no adequate record of testing performed on the code, it will never be of an acceptable level of quality. Testing is an essential means of demonstrating that software is high quality. Thus this process may have to be utilised in situations where little has changed in the code, simply to satisfy the relevant quality standards.

4 REDESIGN

There may conceivably be situations where it is impractical or impossible to attempt to reverse engineer a program. This may be caused by a number of things, such as monolithic code which cannot be unscrambled or total dependency on the particular language implementation. It may even be that some features available in the source language are not available in the target language (e.g. virtual allocation of memory, recursion).

If such a situation arises, an alternative solution will have to be justified, according to the individual case. Consideration will need to be given to factors such as whether it is really still required and how much it would cost to redevelop it.

Clearly, redevelopment is an expensive option. Its choice will depend on the maintainability of the existing system. If changes are required which cannot be implemented owing to the nature of the existing software, then redesign will have to be considered. It does have the benefit of ensuring that the software is written to modern standards, and should therefore be maintainable in the future. Furthermore, it should ensure that the software can be validated. It should be stressed that the redesigned program will be more efficient than a re-engineered or emulated one. Extra functionality can be added and the program can be made to handle greater capacity. The program will hence be more maintainable and validatable.

5 DISCUSSION

There are several aspects of software maintenance which are pertinent to discuss in the context of this paper, other than maintenance problems and solutions. . These are highlighted below.

Software should be considered as a business asset. Computer hardware finds its way onto company balance sheets, but software rarely does. This requires a culture change in the way that we actually view software. Clearly this would present some accounting problems. Its depreciation pattern is difficult to predict since it doesn't deteriorate on its own. It degrades if changes are made to it, or the platform becomes obsolete or if the system around it changes.

An ongoing plan is required to ensure that skills and tools are available to maintain a software system. There is also a need to plan what to do when retaining the relevant skills and tools is no longer cost effective.

The two points above are related : Continuous strategic planning for software maintenance (adaptation and redesigns) means that your software can always remain a worthwhile asset ie the cost of recycling useful information from it will not exceed its value. Furthermore, software resides on magnetic media and is amenable to automated processing. Planning for automated processing of software (ie standardising wherever possible) helps to keep maintenance costs low.

6 CONCLUSIONS

There are clearly many inherent problems involved with the maintenance of ageing software. This paper has addressed some of the problems pertinent to those programs involved with nuclear installations. Several solutions to the problems were discussed, including emulation, reverse engineering and redesign. Each of these has its merits, and the choice for their use should be made on an individual program-by-program basis.

REFERENCES

[1] MITCHELL, Managing Complexity in Software Engineering.

[2] JACKSON, System Development.

[3] SPURR, LAYZELL, CASE Current Practice Future Prospects.

[4] MYERS, The Art of Software Testing.

RELIABILITY ANALYSIS OF MICROPROCESSOR-BASED CONTROL AND PROTECTION SYSTEMS IN NUCLEAR POWER PLANTS

John S. Wiesemann, Functional Design and Reliability Technologies
Westinghouse Electric Corporation, USA

Glenn E. Lang, Nuclear Safety
Westinghouse Electric Corporation, USA

Gilbert W. Remley, Design Engineering
Westinghouse Electric Corporation, USA

ABSTRACT

This paper will present an overview of the objectives, methods, and limitations associated with the reliability assessment of microprocessor based control and protection systems being put into use today. The paper will be structured in a top down format presenting a general method which may be applied when assessing these types of systems. Specific discussion will be presented regarding current issues in the area of safety and licensing. Generic and unique methods which have been developed to assess these systems in a practical and efficient manner will be discussed, including discussion of the "Functional Block Analysis" method which may be used to predict the effectiveness of on-line checks and diagnostics. The incorporation of this data, both qualitatively and quantitatively, into system level models and results will be discussed. As a final note, general observations and findings regarding the typical performance of these systems, as demonstrated by the methods discussed, will be presented.

PAPER

1. INTRODUCTION

As control and protection systems become increasingly implemented on microprocessor-based systems in nuclear power plants, the demand for standard and proven methods of assessing and demonstrating the reliability required to support the licensing of these systems has received increased emphasis. This is compounded by a number of issues which typically accompany the introduction of this type of system, including complexity, dependence on microprocessors, software reliability, detectability

of failures, and practicality of analysis. The intent of this paper is to present some key aspects and techniques which have been applied in conjunction with general reliability analysis methods to effectively demonstrate the system reliability while addressing the issues listed above. Rather than discussing the detailed implementations of the reliability tools which may be applied, emphasis is put on the reasons and objectives for applying each of the methods. Further, this paper discusses aspects of the reliability techniques as applied to microprocessor-based systems, rather than statistical reliability assessments based on actual operating experience.

2. APPROACH

In general, one of the purposes of performing a reliability assessment is to provide a technically correct modeling and estimation of a systems' expected performance. However, this objective alone may not be sufficient to constitute the overall approach which is necessary in obtaining licensing approval from the responsible regulatory authority to implement a particular microprocessor-based system design. The reliability assessment must be developed to demonstrate that the microprocessor-based system enables the plant to meet the overall plant safety goal. Further, the overall results of the reliability assessment may be required to be presented to enable review by licensing authorities who do not have a detailed knowledge of the technologies utilized. Finally, many licensing processes are based on adherence to standardized methods and previously applied techniques which set precedence for the industry. These aspects must be considered when selecting the techniques to be used in the reliability assessment.

3. METHODOLOGY

3.1 Random Failures

The following sections present methods which may be applied to the qualitative and quantitative determination of the impacts of random failures of the microprocessor-based systems under assessment.

3.1.1 Fault Tree Analysis

The Fault Tree Analysis (FTA) is a standard method for reliability analysis, in which failures that can lead to an undesired event, such as "System Failure", are grouped together logically to form a model which uses the individual component failure contributions, and the information obtained from supporting Failure Modes and Effects Analyses and Functional Block Analyses, discussed below, to obtain results pertaining to the given undesired event. While FTA performed for analog systems typically represent the hardware layout and logic of the system, the FTA implementation for microprocessor-based systems may require an alternate approach. This is because analog systems typically have a one-to-one correspondence between the individual hardware parts and the individual functions performed, whereas with microprocessor-based systems, one hardware part may perform many functions, and may therefore require multiple FTAs arranged functionally to cover each application.

To be able to demonstrate a sufficient level of system reliability with the FTA model, one may also be required to take credit for the on-line diagnostic features and self checking which are performed by microprocessor-based systems. Further, the default states of the system which result upon detection of faults must be determined and considered. These states may be detectable, undetectable, safe, unsafe, or a

combination thereof. Each of these factors must be considered when generating the FTAs and may be supported by the methods discussed below.

3.1.2 Failure Modes and Effects Analysis

The Failure Modes and Effects Analysis (FMEA) is a method where the system is systematically assessed for all postulated single failure modes of the individual components, to determine the effects on the sub-system and system level operation of the design. This method is a well established and accepted method for supporting both the qualitative effects and quantitative impacts of system faults, and is presented in detail in various sources such as IEC-812 and MIL-1629. While the FMEA approach is entirely applicable to analog systems, as the number of functions performed by individual components within the typical microprocessor-based system makes the method less practical to apply.

In order to perform a classical FMEA on a digital system, one would be required to proceed pin-by-pin for each chip within the system for any given state or line of code the system may be executing, and assess the effects of the potential failure modes. While this may be possible, it represents an extensive effort for which a more practical approach is desirable and available. This is the Functional Block Analysis approach presented below.

3.1.3 Functional Block Analysis

The Functional Block Analysis (FBA) method is similar to that of the traditional FMEA method, but is organized by functions of the system being assessed, rather than by components. IEC-812, Section 2.2.4 states that there exist drawbacks and limitations to applying traditional FMEA to complex systems with multiple functions. This is

because of the quantity of detailed system information which must be considered, and is further compounded by the number of possible operating modes which are achievable. The FBA method specifically addresses these limitations and drawbacks of the FMEA approach by functionally organizing the analysis, thus enabling the assessment of microprocessor-based functions in an efficient and practical manner, versus the traditional piece-by-piece FMEA approach. It is important to note that in application, the FBA method covers the same hardware that is covered by the FMEA method. The difference is that groups of hardware may be addressed as functional units within the FBA and specific failure analysis is started at the equivalent functional level. The following paragraphs describe the major elements in performing the FBA.

3.1.3.1 Step 1.

The first step in performing the FBA is to establish the Functional Blocks to be assessed. To do this, the fundamental required functions of the system are listed. From this list, the applicable sections of hardware which perform these functions are identified. Note that these blocks of hardware typically overlap, as single hardware elements may perform multiple functions. In some cases, for example input/output devices, may be implemented with a majority of analog hardware. In these cases, the standard FMEA approach may be applied. For each of the remaining Functional Blocks, an assessment is performed. This is typically done using a table format similar to that of the FMEA.

Each FBA assesses the performance of the system in relation to a main functional objective. For this main function, a list of the possible sub-function failures which could in turn defeat the main function are generated. These sub-function failures are then further disaggregated, going to the component level, if necessary. In general, failure modes of functions that have no encompassing

detection method, or only partial coverage, are further assessed for lower level functional and component failures, to identify their appropriate coverage and/or level of impact. Failure modes of higher level functions which can adequately be addressed by one or more methods of detection, are not broken down any further. This methodology focuses the detailed analysis effort on the areas which require it, enabling efficient and practical execution of the analysis.

As an example, consider a hypothetical amplifier circuit which is comprised of a number of components. Rather than assessing each individual component, the circuit is viewed as a functional block with one main function, for example; "Provide a Specified Gain". Possible functional failure modes might include; "Increase in Gain", "Decrease in Gain", "Inverted Gain", and "Non-Linear Gain". Suppose that due to checking performed by a downstream circuit, all failure modes except "Decrease in Gain", are detectable and safe. The detection method provided by the downstream circuit would be listed as covering the other functional failure modes and no further analyses for those cases would be required. For the case of the undetectable "Decrease in Gain" failure mode, further analysis of the amplifier circuit may now be performed to determine which, if any, of the individual parts could cause this particular event. By focusing the effort, to specific groups of hardware for specific functional modes, the practicality and efficiency of the analysis process may be greatly increased.

3.1.3.2 Step 2.

The various diagnostics, and operational features which are applicable to the associated functional failure modes are listed. Note that not all of the methods listed as Detection Methods are directly used to detect the failure. In some cases, there is an indirect application of the method which detects the failure,

due to side effects of the failure. In other cases, the method tends to inhibit or prevent occurrence of the failure, or in other words, detect the failed mechanisms which could cause the failure. Also, it is not required that all of the available diagnostics are listed. The more applicable cases are listed to the point where sufficient coverage is demonstrated. The detection methods list those diagnostics which are typically applied on-line as part of the cyclic operation of the system.

3.1.3.3 Step 3.

Once the individual failure modes and applicable detection methods are identified, the analysis is performed to determine the resultant effect of the postulated failure accounting for the application of the associated detection methods. The general default states for the system are listed for the failures which are detected and/or have no effect. Failures which are not detected list the possible faulted conditions that could occur.

The relative contribution in terms of failure rate, for those failure modes or component failures which are not detectable or fail-safe are then determined. The contributions for the detected and fail-safe failure modes are not required. The contributions are generally presented in units of "failures per million hours" which is the standard unit for typical electronic component failure rates. A conservative "percentage" contribution may be given for components which are potentially undetectable but demonstrate an extremely low probability of occurrence as compared to the overall board failure rates.

By summing the contributions of the potentially undetectable and unsafe failures, an overall contribution of unsafe failures for the Functional Block may

be obtained. This in turn, may be used to support the quantitative data input to the FTA analyses.

3.2 Design Deficiencies

The following sections present methods which may be applied to the qualitative and quantitative determination of the impacts of design deficiencies which may be inherent in a particular system.

3.2.1 Common Mode Failure

Typically, a Common Mode Failure (CMF) model is included in the assessment of microprocessor-based systems to account for the possibility of events or failure causes which can lead to the failure of all paths in a redundant configuration. While the contribution due to simultaneous multiple random hardware failures across redundant trains may be relatively low, the CMF contributions often completely dominate the final results. Therefore a specific effort must be applied to ensuring that applicable CMF models are used and that the associated parameters are appropriate. Two CMF modeling techniques are frequently applied. These are the Beta-Factor method, and the Multiple Greek Letter (MGL) method. It should be noted at this point that the Beta-Factor method is many times applied to handle many levels of redundancy as a standard method. This can produce conservative results, as it is simply the first term of the MGL method, which is a more comprehensive CMF model. The MGL CMF failure contributions are quantitatively modeled using the MGL method, by summing the individual hardware random failure contributions times their calculated

CMF as a function of Beta-, Gamma-, and Delta-Factors for each group of similar or redundant components identified in the system for a given function and operating mode. That is;

$$CMF(\text{System Function}) = \Sigma_i^N CMF_{\text{Individual}}(\tilde{A}_i, \beta_i, \gamma_i, \delta_i)$$

The application of the MGL method to similar or redundant groups of hardware in the CMF assessment addresses the potential for failures which could defeat the intended redundancy or independence of systems sharing identical components or components with similar designs. The following factors are used in the MGL method.

- β Conditional probability that the common cause of a component failure will be shared by one or more additional components (Beta)

- γ Conditional probability that the common cause of a component failure that is shared by one or more additional components will be shared by two or more components additional to the first (Gamma)

- δ Conditional probability that the common cause of a component failure that is shared by two or more additional components will be shared by three or more components in addition to the first (Delta)

When modeling the CMF contribution of a two-way redundant system, the Beta-Factor method is appropriate, as it is effectively the application of the terms of the MGL which apply. When modeling a three or four-way redundant system however, additional terms of the MGL are applied which in effect give credit for the additional lines of redundancy. For example, Beta would be applied to handle the first and second redundant groups of the system, while Gamma and Delta would account for the

addition of the third and fourth sets of redundant equipment respectively. Credit can be taken for a two, three, four or more channel redundancy through application of the MGL method.

One of the major concerns regarding the development of the MGL CMF model is centered about the assignment of the individual MGL factors. Although some benefit is derived from the application of the Gamma and Delta factors of the MGL method, the Beta factor typically provides the dominant portion of the CMF contributions and therefore draws the majority of the attention. One suitable source for the derivation of Beta-Factors for microprocessor-based control and protection systems is the Rolls Royce & Associates method, "RAA/7692: Numerical Values for Beta Factor Common Cause Failure Evaluation - STF, Rolls-Royce and Associates Limited Technical Memorandum, February, 1986". In this method a systematic approach is presented in which various design attributes are categorized according to their impact on the potential for common mode failure inherent in the design. By choosing the characteristics that most aptly describe the system under assessment, a number a factors are obtained, and when combined, form the resultant Beta-Factor which is desired. The resultant Beta-Factors which can be obtained range from 0.03 to 0.3 for non-diverse systems, and 0.01 to 0.1 for diverse systems. The attributes include the following: Design Categories such as Separation, Similarity, Complexity, and Analysis; Operation Categories such as Procedures and Training; and Environment Categories such as Control and Tests. In addition to being a supportable method for derivation of Beta-Factors which apply to microprocessor-based systems, the technique is presented in a clear and general form which may be used to develop the attributes and factors required for the support of the additional CMF factors for microprocessor-based systems and other technologies.

3.2.2 Hardware versus Software Failures

There are many perceived differences between hardware and software failures, each of which stem from the differences between the understanding of analog and digital systems. Two of those differences are discussed here. The first difference is in regard to complexity and the second involves the incorporation of software with the digital system.

3.2.2.1 Complexity

The issue of complexity regarding digital systems should not be based on the extent of integration of multiple functions which were previously performed by separate dedicated analog modules (or on the perception that the small size of digital components in relation to the number of analog components that are duplicated, makes the digital component complex and impossible to assess). It has been demonstrated that many microprocessor chip architectures implementing hundreds of thousands of transistor equivalents have demonstrated superior failure rates as compared to a that of a typical single power transistor used in common analog circuits. With regard to the consolidation of multiple functions within fewer hardware components, this cannot be fairly assessed without crediting the benefit of the on-line diagnostic functions and features which are available in digital systems. Application of the FBA method has proven effective in demonstrating qualitatively and quantitatively the performance of digital systems incorporating these factors.

3.2.2.2 Incorporation of Software

It is assumed for this discussion that a comprehensive Verification and Validation (V&V) effort is performed as part of the design process for the digital system software.

Two key industry and regulatory documents are available that provide guidelines for performing a V&V program. These are ANS/IEEE-7-4.3.2-1982 "Application Criteria for Programmable Digital Computer Systems in Safety Systems on Nuclear Power Generating Stations" and IEC 880, "Software for Computers in the Safety Systems of Nuclear Power Systems". In order to be able to account for software failure in a reliability assessment, two key assumptions are made. These are:

1. No Random Software Failures

Software does not wear out, age, or degrade in extreme environments, as a resistor, or processor chip does. There are no failure mechanisms for software, and therefore does not fail as a function of time. Although the hardware on which the software resides (e.g., memory chips) and the hardware which executes the software (e.g., processor chips) can fail causing the software to be altered, such that a system failure occurs, these examples are all random hardware faults that can be assessed using the methods presented above.

2. Any potential for Software Failures is due to Design Deficiency or Common Mode Failure.

As there are no Random Software Failures, the remaining potential for Software Failures exists only in the domain of Design Deficiency and Common Mode Failure. Many models which assess the reliability of software support this position. At the core of these models are typical input variables such as Number of lines of code and Language used. All of these aspects are in regard to the design phase of the software. This is the point at which errors, or the potential for failures, is introduced into the software. Unlike MIL-217E which predicts the expected failure rate for electronic components by applying a

number of environmental and hardware configuration factors, the software models are centered about the design attributes.

Hardware and Software CMF events are introduced in the design phase for the same reasons. As an example, a design which is incapable of recognizing an input signal of a particular level, can be realized by an oversight in the design of the software limits which accept that signal, or equivalently by an oversight in the design of the power ratings which accommodate the same signal. In either case, the factors which allow for the propensity of hardware or software design deficiencies can be minimized as part of a formalized design process. The reliability assessment can use this information to form the basis for a Qualitative Filter Model, presented below.

3.2.3 Qualitative Filter Model

One method which may be applied to qualitatively address the issue of Software as well as Hardware Design Deficiencies is by application of a Qualitative Filter Model. In this model, the defenses inherent in the design process and planned operation of a system are grouped and discussed to qualitatively demonstrate that the potential for software errors will be below an acceptable level. This model can be thought of as a series of software error filters with each successive filter reducing the number of potential software errors. This model is complementary to the MGL CMF method in that it is not a function of the random hardware failure contributions of the system. The effectiveness of the filtering is based on the effectiveness of each design stage and the independence of each stage. Example stages or filters include; Structured Design Processes, Design Reviews, Standardized Design Implementation, Design Testing, Safe Failure Modes, Functional Diversity, Verification and Validation, Feedback of Experience, Quality Operator Interfaces, Periodic Proof Testing,

Defensive Measures Analysis, and Design Approach Philosophy. Note that these aspects are equally applicable to the hardware design process. By listing the attributes of the software design process with regard to aspects such as those listed above, one can present an effective qualitative model which not only gives support to the software issue directly, but also places the software design issue in proper perspective with regard to the established hardware design issues and methods.

4.0 SUMMARY

The reliability of microprocessor-based systems can be effectively demonstrated using a number of techniques, some of which have been presented in this paper. Organization by function rather than by component, offers a large advantage when considering the performance of microprocessor-based systems. Additionally, proper consideration and assessment of the software failure contribution as a function of the design phase rather than that of a random failure type can help address this issue in the correct perspective. By keeping these factors in mind, a solid comprehensive approach may be developed which uses general reliability methods, enhanced by specific techniques, to qualitatively and quantitatively demonstrate microprocessor-based system reliability.

Recent Activities within Nuclear Electric Related to the Qualification of Digital Systems and the Extension of Maintenance Intervals.

G.P. Holt

Safety Instrumentation and Software Group
Technology Division
Nuclear Electric plc
Barnwood, Gloucester, UK.

ABSTRACT.

Nuclear Electric is pursuing a programme of modernisation and enhancement of existing control and safety C&I systems to improve power plant availability and increase power output. This paper describes recent experience in qualifying digital systems for safety applications. Also described is the work currently in hand to reduce the frequency of maintenance periods for safety C&I equipment.

The qualification of digital systems is shown to be a more rigorous and much more extensive (and thus costly) exercise than the qualification of conventional equipment. This is illustrated by brief references to two software-based safety systems, the Single Channel Trip System at the Dungeness "B" AGR and the Primary Protection System for the new PWR at Sizewell "B".

The emphasis of the paper is on the use of Application Specific Integrated Circuits (ASICs) in safety systems, to reduce, or eliminate dependence on software for the fulfilment of requirements which need implementations that are complex or of a high functional density. Recent experience in the development of a prototype safety system based on ASICs, The Gaseous Activity Monitor and Trip Equipment (GAM), is used to illustrate their possible benefits and potential problems.

When using complex integrated circuits like microprocessors or ASICs in digital systems a difficulty arises in analysing the failure modes of the system. Efforts to overcome this difficulty led to the development of a method for performing failure analyses based on functional blocks. The techniques and benefits of such an approach are outlined.

Finally, efforts to reduce maintenance costs, yet at the same time enhance safety, are leading towards an extension of maintenance intervals, for some safety equipment, from 3 months to 4 months and also towards lengthening the period between AGR outages from 2 years to 3 years.

1. INTRODUCTION.

Nuclear Electric is currently modernising and enhancing the existing control and safety C&I systems at its nuclear power stations, to improve power plant availability and increase power output. Digital electronics is playing an ever increasing role in such systems.

Modern digital equipment can offer the user several attractive benefits. It can provide a wide variety of available functions within a small physical space, enabling the automation of processes or the provision of safety which may not be possible with other equipment and may also offer relatively easy re-configuration of its functions and application. In addition its use can result in less manual calibration and maintenance and cabling requirements can be reduced through the use of multiplexing and data link techniques. However such benefits are gained at a cost. That cost is the amount of work required to demonstrate that the system is acceptable, not only before initial use but also after any changes are made during its operational life.

This paper emphasises the possible benefits from the use of Application Specific Integrated Circuits (ASICs) in digital safety systems. To enable a comparison to be made with the effort required to qualify software-based systems and the associated problems, brief reference is made to experience of qualifying two software-based safety systems. In such systems it is accepted that at present there is no widely accepted method of quantifying the effect on system reliability of errors in the software. In the UK, the licensing authority (NII) have adopted a special procedure[1] upon which to base a safety justification. The problems and workload associated with making a safety justification for software based systems, have led Nuclear Electric to explore the use of ASICs to provide a safety system with the functionality of a software based system but without the software. This experience is described in detail.

The use of Very Large Scale Integrated Circuits (VLSI) like microprocessors and ASICs, requires an approach to analysing failure modes other than that of a traditional FMEA. A method of analysing failures based on functionality is described.

A topic of equal interest is the need for less frequent maintenance of equipment, not just for reduced operating costs but for increased safety. The approach taken by Nuclear Electric to achieve longer maintenance intervals at its AGR power stations is described.

2. QUALIFICATION OF DIGITAL SYSTEMS.

For digital systems employed in a safety role, 'qualification' embraces all of the work which is necessary in order to provide a safety justification. The design, the methods used in the implementation of the design and the final product, must be shown to be capable of performing its safety function with the necessary reliability in its operating environment. For conventional analogue equipment, correct behaviour can be verified by performing tests on a limited number of sample points within the equipment's required functional envelope. Interpolation and extrapolation of the results of such tests is an accepted way of demonstrating complete conformance with

the requirements, based on the assumption that analogue equipment follows some form of continuous characteristic. The characteristic of digital equipment is not continuous. Digital systems contain very many discrete states, correct operation in one of these states does not necessarily infer correct operation in any other state. Much greater effort is required to qualify digital systems, using a variety of methods, than is the case with analogue equipment. Ideally, for complete confidence in the design, every single state should be tested. In reality the number is limited by what is practicable. Because of this shortfall in test coverage, greater emphasis is placed on analysing and assessing the design. A further problem arises when advantage is taken of the ability to re-configure digital systems. Any changes that are made might appear to be simple and of low implementation cost but the result could be a need for partial or total re-qualification. These concerns are relevant whether or not a digital system depends on software for its functionality.

2.1 Digital Systems With Software.

The problems that exist in attempting to adequately qualify software based systems have yet to be resolved. Software failures are systematic, they are due to errors in the design and implementation of the software. There is no accepted method of determining software reliability. Nuclear Electric are actively involved in the development of software based systems[2] and in establishing means by which they may be qualified[3][4].

The first digital protection equipment with embedded software to be installed and licensed at Nuclear Electric's power stations, is the Single Channel Trip System (SCTS) at the Dungeness "B" AGR. Dungeness B was commissioned in 1982 and had been operating for 10 years with its operating temperature limited to 580°C, well below the design target of 675°C. The protection provided by the SCTS system, against operating the reactor with spurious restrictions in gas flow, caused by gag-related failures, has enabled the channel gas outlet temperature to be raised to 650°C. It is intended, shortly, to achieve the design target of 675°C.

The SCTS (fig 1) is a 4 way redundant system which processes just one parameter, channel gas outlet temperature, with a 2oo4 voted output connected into the reactor guardlines. Its functionality is determined by embedded software, written in Intel Assembler language and resident in two processing units, a Trip Algorithm Computer and a Vote Algorithm Computer. Test signals are interleaved with thermocouple inputs and processed to produce a dynamic output pattern that is checked by hardwired pattern recognition logic. The software has been qualified using the static analysis tool MALPAS which checks all paths through the software; by comparison between the object code and the assembler source by means of a disassembler, thus verifying the integrity of the tools used to generate the object code; by demonstrating that procedures for high quality design have been used throughout. System and hardware design aspects have been subjected to independant assessment by hand. Final equipment qualification has been demonstrated by module & subsystem tests, integration tests and function-proving tests carried out during commissioning.

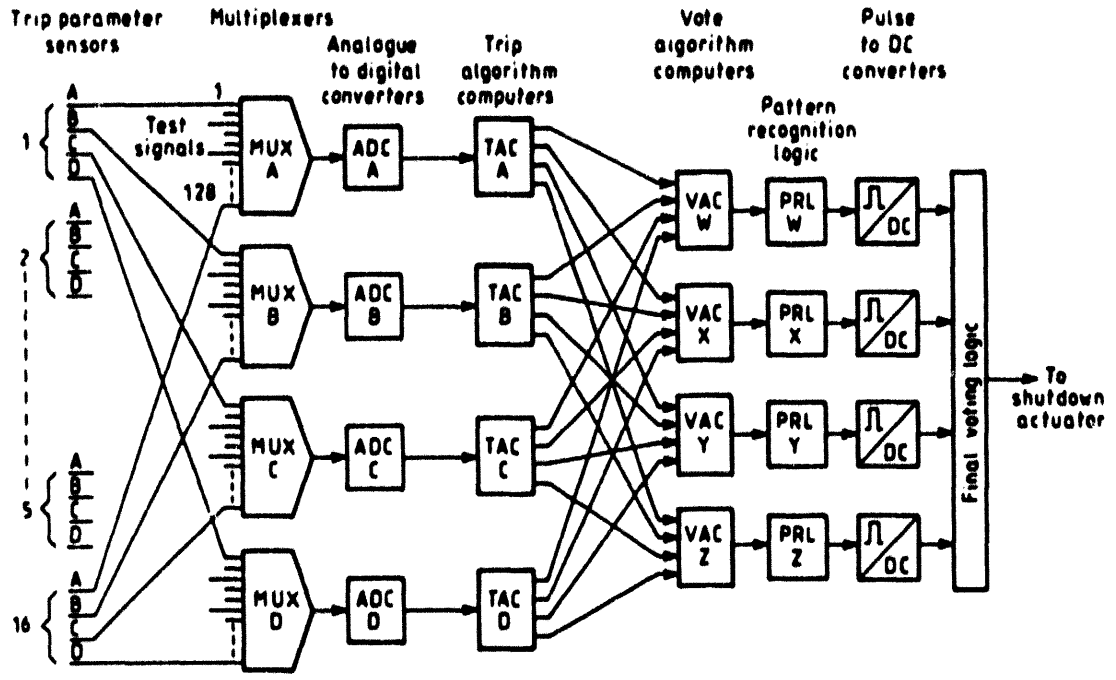


Figure 1. Dungeness "B" Single Channel Trip System.

The Primary Protection System (PPS) (fig 2) for the Sizewell B PWR is a digital system which provides reactor protection based on the processing of many parameters. It is therefore much larger and more complex than the SCTS and consequently requires a great deal more effort to qualify it. Its functionality is determined by embedded software, written in PLM with some Intel assembler and resident in distributed processing modules. The PPS has been described in detail elsewhere[5] but a brief overview of the main tasks in its design qualification is illustrative of the amount of effort required to qualify a large, digital protection system. To qualify the software the MALPAS static analysis tool is being used together with a source-to-object code comparator tool that has been developed by Nuclear Electric[6]. The path from specification to embedded code is thereby qualified. Extensive dynamic testing[7] of a production standard prototype using a functional model of the PPS as a benchmark, provides further demonstration of the software design integrity. These activities are in addition to the verification performed by the suppliers, Westinghouse. All aspects of the PPS design have been assessed in detail. All of this work has been performed by teams which are independent of the design team. The design team have to demonstrate adherence to strict procedures for high integrity design and conformance with standards. A production-standard prototype of the deliverable equipment has been subjected to a series of type tests and validation tests, both at a modular level and as an integrated unit. All deliverable equipment has been

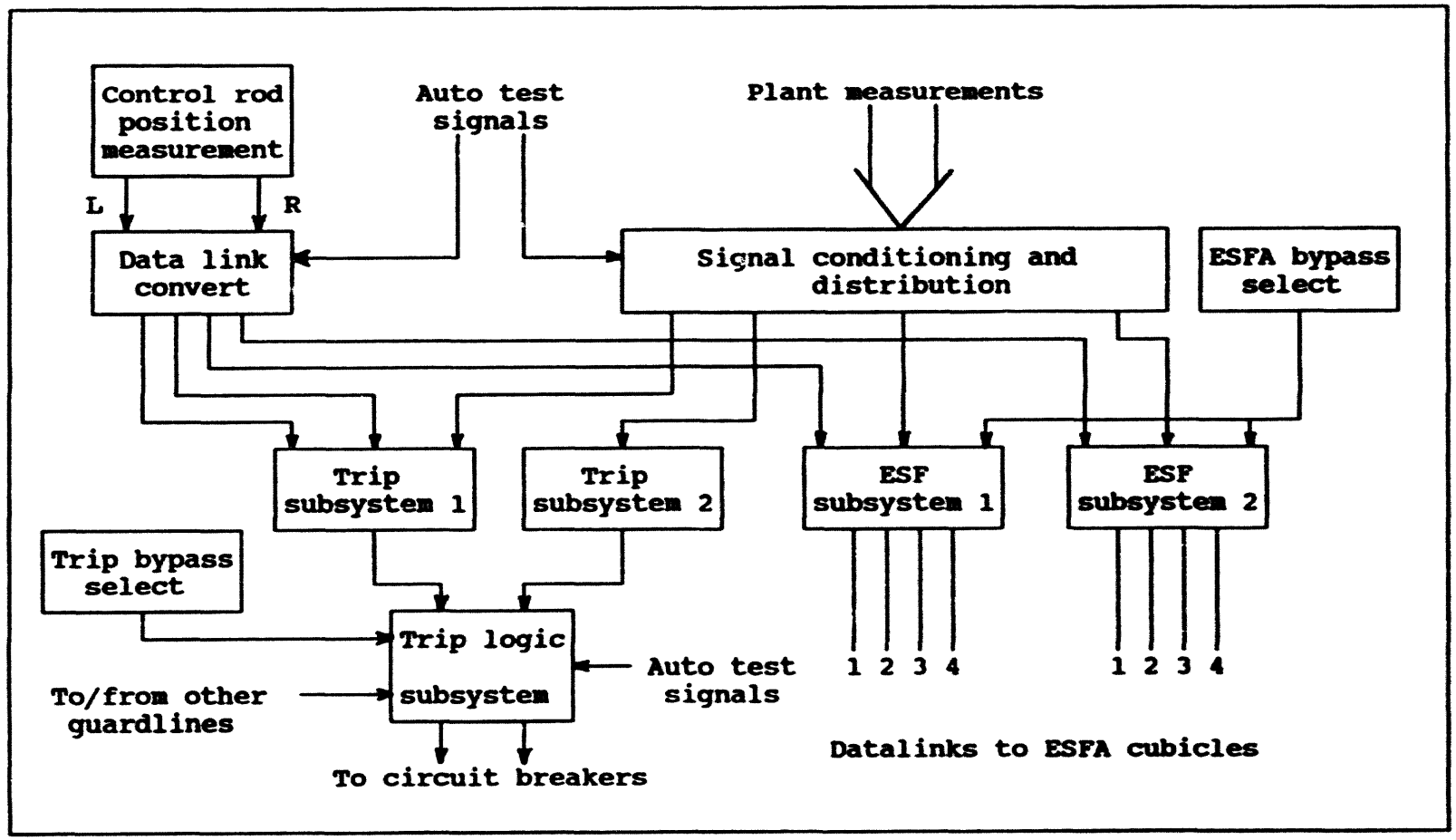


Fig 2. PPS Block Diagram, one Guardline.

subjected to comprehensive factory acceptance tests which encompass system functional tests as well as equipment post-manufacturing tests. Once the complete PPS has been installed at Sizewell, it will be subjected to a one year 'burn-in' period, prior to reactor operation. The total effort expended on the design and qualification of the PPS is in excess of 500 man years[5], more than half of which has been expended on qualification.

2.2 Digital Systems Without Software.

The words "digital system" are often taken as being synonymous with, or as a subset of, "software-based system". However, digital systems need not contain software, not even if a high functional density is required. An example of such a system is the Gaseous Activity Monitor and Trip equipment (GAM), which has been installed on a trial basis at the Hinkley Point "B" AGR. GAM, see figure 3, which was designed and developed by Siemens Plessey Controls Ltd under contract to Nuclear Electric, is a prototype protection system based on Application Specific Integrated Circuits (ASICs); no software other than an off-line interface controller is contained within the equipment. GAM is a redundant, 4 channel system, which monitors the level of Kr88 present in the CO_2 coolant of an AGR, generating a reactor trip on a 2oo4 vote if the level rises above a trip threshold. The goal is to trip the reactor within 30 seconds of the failure of a few fuel pins and yet have a spurious trip rate of no more than 1 in 100 years.

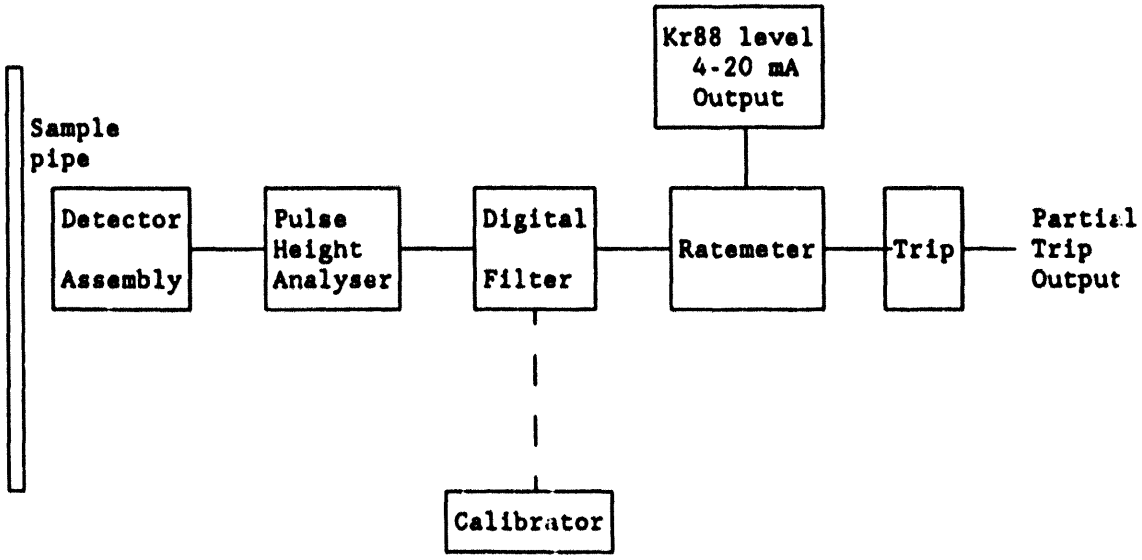


Figure 3. Gaseous Activity Monitor & Trip Equipment, one channel.

The design principle is based on matrix convolution/deconvolution to identify a single isotope from the gamma spectrum. The energy distribution of the line spectra associated with each gamma emitting isotope in the coolant, is broadened by the losses associated with the collimator, scintillator and photomultiplier components in the equipment front end. The resolution of the ^{88}Kr lines from the other major gamma emitters, including ^{16}N and ^{41}Ar, is consequently reduced, as illustrated in Fig. 4.

The process of broadening can be seen as the convolution of the line spectrum Phi, of an emitter with the detector energy efficiency matrix, E, producing an observed spectral energy distribution, C. The GAM equipment deconvolutes the observed spectra to derive Phi using the equation: Phi = I times C, where I = E -1 is the inverse of the efficiency matrix, as detailed in Fig 5.

The GAM equipment consists of 4 redundant channels. Each channel uses a collimated detector assembly containing a sodium iodide scintillator and photomultiplier tube, which feeds a pulse amplifier in order to generate a pulse stream related to those gamma emitting isotopes present in the coolant gas. A pulse height analyser and digital filter set up to discriminate a single isotope, in this case 88 Kr, feed an up/down ratemeter & counter to give the level of 88Kr released from the fuel. The digital filter uses coefficients of the matrix I, which are derived by an off line computer and stored in EEPROM.

The pulse height analyser, digital filter, EEPROM, ratemeter & counter are all implemented in a single ASIC. The ASIC approach was taken because it was decided to avoid the problem of having to qualify software, a problem which accompanies any design based on microprocessors. A design based on logic ICs was ruled out because of the number of devices required and the consequent bulk and low reliability. When we accepted, in 1991, the proposed use of ASICs in the GAM equipment we were aware that a large scale custom IC had not been used before in a reactor protection system. In judging the use of an ASIC to be acceptable, the following facts were considered:

i) ASIC technology is now mature.
ii) There is adequate history of their use.
iii) Libraries of verified and well-used cells are now available.
iv) Design tools offer a repetitive and closely controlled development process.
v) Simulators enable design verification.
vi) Fault detection circuits can be designed-in.
vii) Fault simulation techniques are automated and offer high percentage coverage (up to 99%) of "stuck-at" type faults for post-production testing of individual devices.
viii) Standard cell and compiled array ASIC architectures need not contain unused circuits and functions.

Optimised Array architecture is used for the ASIC in the GAM equipment. The ASIC manufacturer, ES2, maintains a library of ASIC circuit elements comprising pre-compiled arrays. These elements have been evaluated and characterised as part of the qualification process leading to Mil Std 883C approval. They are used in all ES2 ASIC designs. Assurance is thus provided

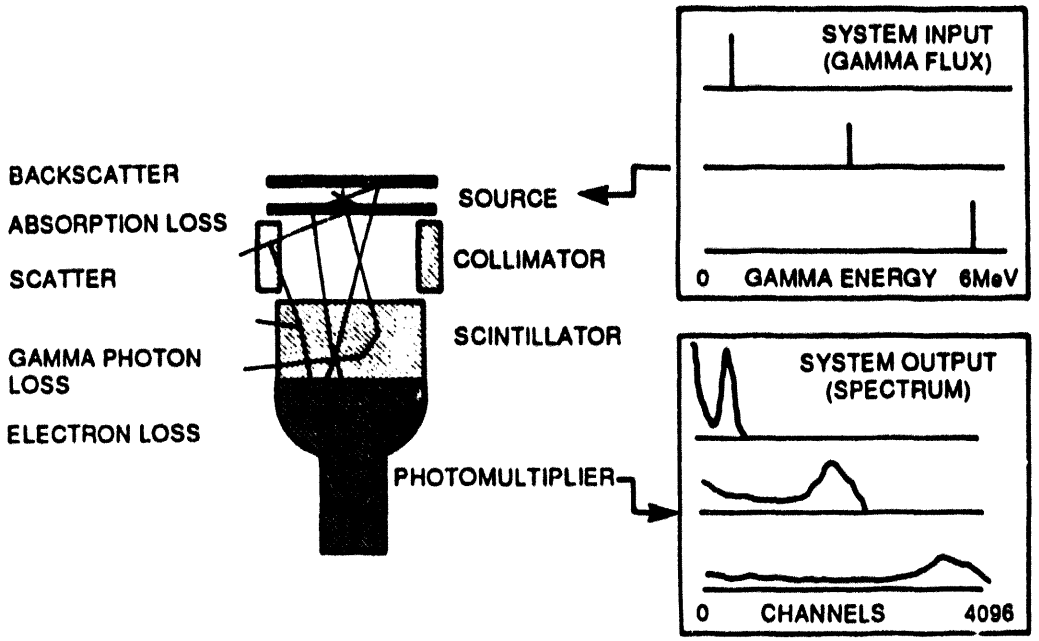


Figure 4. Gam Front-end Losses.

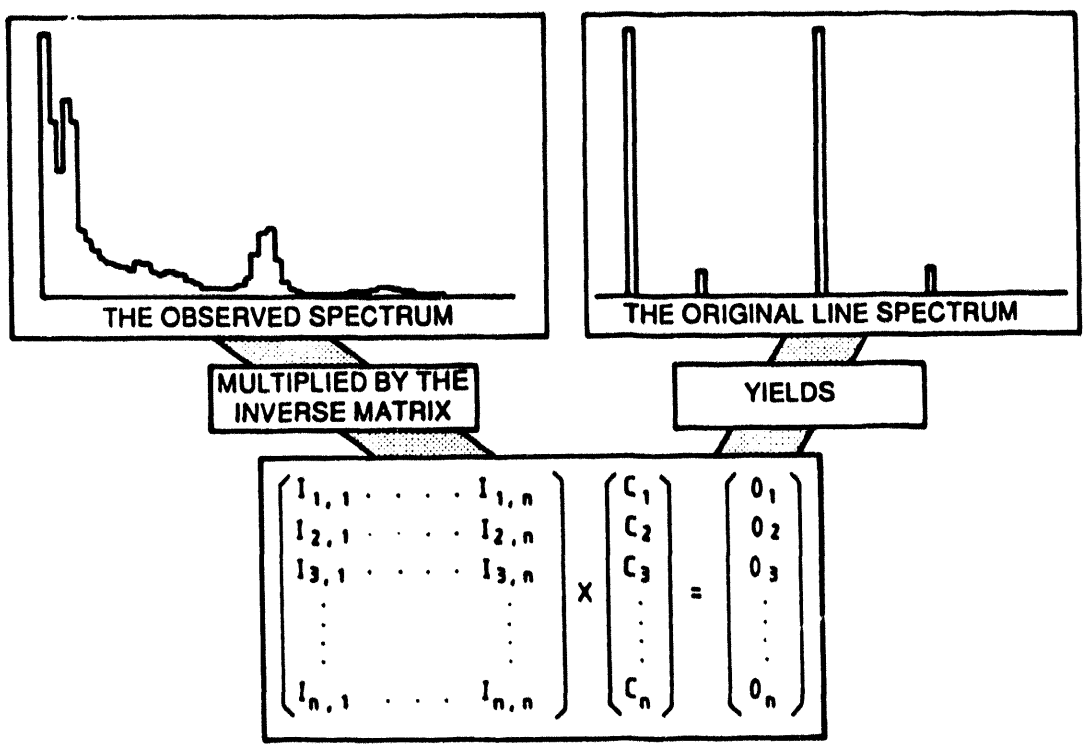


Figure 5. GAM Matrix Deconvolution.

that the circuit elements have been verified and that they have been subjected to previous use (ES2 have fabricated over 700 ASIC designs) including medical and military high reliability applications. Furthermore, only those elements selected by the designer appear in silicon. If changes to the design are required once the device has been fabricated, only those modules affected are changed in the composite 'mask' prior to re-fabrication, thus the chances of introducing errors to those areas that are not part of the changes, are reduced.

The GAM ASIC design requirements were captured on a modular basis, using the SOLO 1400 Hardware Design Language (HDL). As part of the design iteration, error detection circuits were included following the results of failure analyses performed during the design process. Design modules were verified manually against the HDL requirements. Part of this process included generating functional test patterns with which to test the design functionality using a simulator. Ultimately these patterns are combined with additional patterns, which may be automatically generated, to test for the presence of defects in the silicon at the end of the production line. They are checked for the proportion of faults they cover by applying them to a computer model of the desired circuit in which "stuck-at" faults can be simulated. By this method it is possible to test a very high percentage (approaching 100%) of circuit nodes. The actual percentage of nodes that can be tested depends upon the controllability and the observability of the design. These are measures of the ease with which internal circuit nodes can be set to logic 0 and to logic 1 and the ease with which internal nodes can be seen to be at logic 0 or 1, given the limitation of performing these actions via the device i/o pins. Test coverage of 100% means full controllability and observability of all internal nodes, it does not mean exhaustive testing of all circuit input and output state combinations. With the GAM ASIC, 98% coverage was achieved.

The main concern with the use of ASICs (though the concern is not confined to ASICs) is proving the correlation between actual device functionality and the required functionality. As with any other product, hardware or software, the difficulty of demonstrating functional correctness grows with complexity. For mass produced devices this concern can generally be allayed by a history of widespread use. However those ASICs based on libraries of cells or pre-compiled arrays also benefit from the widespread use of those cells in other ASICs, whereas mass produced devices do not necessarily benefit from all of the design-time features listed above.

When compared to the software design cycle, the ASIC design process can be seen to be at an advantage because the designer is provided with a limited number of verified cells, which can be interconnected in a limited number of ways and the effects of that interconnection can be checked automatically during design time. The software designer has access to an almost infinite combination of sequences of instructions and data. Unlike the cell-based ASIC design, the majority of software designs will not be built with modules taken from a library which covers all of the required functions. With software there is therefore greater scope for design errors and a consequent need for greater effort to show that no errors exist.

Although ASICs have been available for ten years, serious consideration of their use in equipment for nuclear power stations, particularly safety systems, is something of a novelty. Nuclear Electric are not alone in investigating their usefulness. Proposals for their use in nuclear safety systems have recently been made by the Centre For Atomic Research in India[8] and by Ontario Hydro in Canada[9].

Though we have only just begun long term trials with the prototype GAM equipment, our experiences with ASICs have so far been positive. Certainly we believe that they have the potential for a future in control & safety systems for nuclear plant, though in order to make an acceptable safety case it is possible that architectures may need to be restricted to those offering characterised modules or cells. Because the GAM equipment is still at the prototype stage it has not been necessary to license the design, therefore the attitude of the licensors remains unknown. However it is not believed to represent an insurmountable problem given the case for the use of ASICs as outlined above, indeed making the case may get a little easier in the near future. The recognised limitation of the ASIC fault simulators in only simulating "stuck-at" faults is now being addressed, with the appearance of simulators[10] giving additional coverage of bridging and "stuck-on" faults as a minimum and of a new method to detect such faults where the quiescent current, I_{ddq}, is measured. With such tools, the claims for test coverage will be more meaningful and provide greater confidence in device integrity, though this is at present disputed by those who claim that better test coverage does not necessarily mean reduced field failure rates[10].

ASICs are particularly attractive for an application that needs a digital solution but where the significant overhead of software qualification can be avoided, or is not justifiable, the GAM system is an example but there are other ways in which they might be used. For example, they could be used to enhance the reliability of software-based systems by employing them to provide error detecting and sanity checking. In software-based systems it is common practice to use the processor to perform error detection and sanity checks upon its own operation. Using an ASIC to perform such functions would not only introduce diversity into the error detection function but would also reduce the total amount of software in the system.

2.3. Failure Analysis of Digital Hardware.

The hardware in the digital systems described above is designed around either, microprocessors and their derivatives, together with their families of support devices, or ASICs. When it comes to determining reliability and the nature of failures of these devices, their functional density and flexibility create problems for the designers and assessors of systems that incorporate them.

The reliability of any system, particularly a safety system, is of prime importance. Numerically it is calculated from component failure rates, taking into account redundancy, the effects of common mode failures and the proportion of failures that are safe. This latter aspect is very important and needs to be supported by a detailed failure analysis.

A conventional approach to failure analysis follows an FMEA process of postulating the failure of components in each of a small number of modes, to determine the effects of each failure mode on the operation of the circuit and susbsequently the system.

Microprocessors and other complex devices, like ASICs, are not amenable to such an approach because of the unknown effects of failures. The simple expedient often adopted for less complex integrated circuits of considering only short circuit and open circuit failures of package pins, is only partially effective for devices with failure modes that cannot be modelled wholly by "stuck-at" faults. (It is estimated[11] that 30% of faults in CMOS VLSI are not represented by the stuck-at model). An additional problem associated with failure analyses of microprocessor based systems is that the system functionality is ultimately determined by the software. Any failure analysis must therefore encompass the effect of hardware failures on the execution of the software.

Faced with overcoming these problems in recent assessments of the Sizewell B microprocessor based system and the GAM equipment described above, it was decided that a failure analysis based on partitioning the system into functional blocks and defining functional failure modes was the only practical approach; a so-called Functional Block Analysis (FBA). Starting with a comprehensive knowledge of the system, functional blocks are delineated from subsystem level, down to a block representation of the microprocessor or ASIC if necessary. Failure modes of functional blocks are then postulated, correlated with embedded methods of fault detection and related to component failure rates, to arrive at dangerous failure rates for the functional blocks.

To illustrate the FBA process, take as an example the typical processor-based, real time control system shown in figure 6.

This is then split into functional blocks, as shown in Figure 7.

Functional failure modes are then tabulated for each block together with the coverage provided by failure detection mechanisms. Where coverage for any functional block is inadequate, then that functional block is itself split into functional blocks. If necessary, this process can continue until the lowest level is reached where individual complex ICs are treated as comprising functional blocks.

A failure rate for a functional failure mode is derived from the failure rates of the components whose failures produce the functional failure mode under consideration. To reduce pessimisms in dangerous failure rates, if component failure rates can be apportioned to failure modes this is done, otherwise the whole failure rate is used. Apportionment need only be done for failures that are shown by analysis to be unrevealed and therefore dangerous. Summation of the dangerous failure rates then leads to a functional block dangerous failure rate which can be expressed as a percentage of the total failure rate for that functional block. A rate for dangerous failures of the whole system/subsystem can thus be achieved. It is generally considered that the dangerous failure rate and the number of dangerous failure modes must be less than 10% of their respective totals for the equipment to be acceptable and judged to be of equivalence to fail-safe.

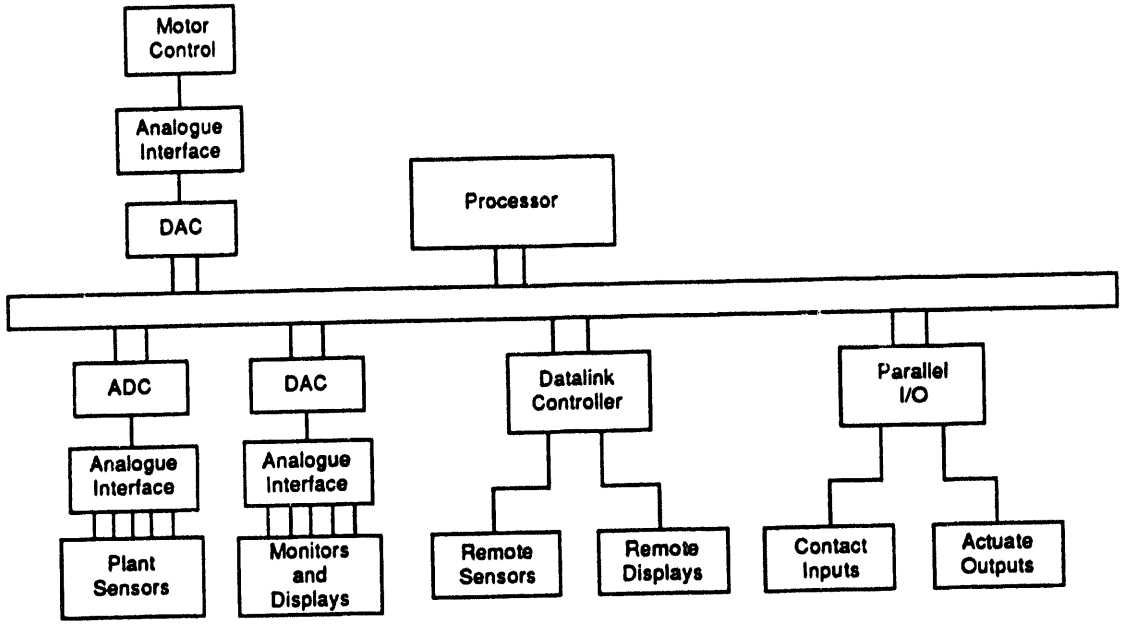


Figure 6. Schematic for typical distributed architecture system.

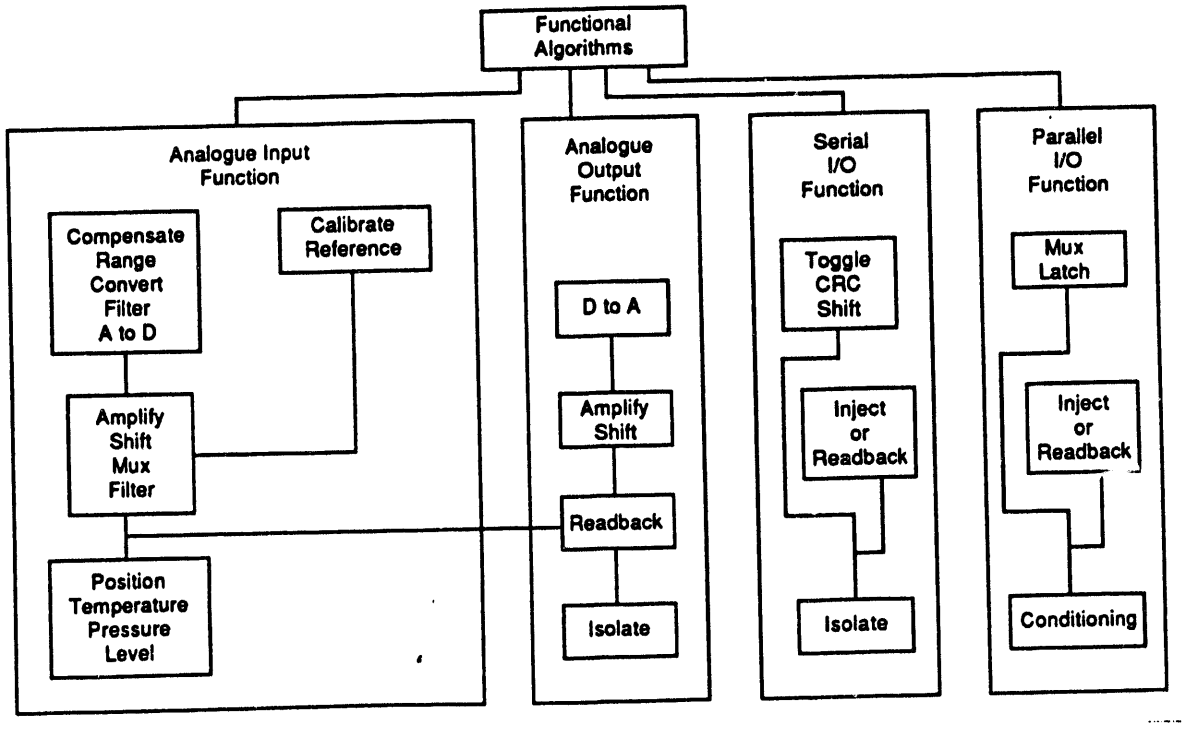


Figure 7. Functional block representation of figure 6.

3. MAINTENANCE INTERVALS.

Increasing the length of time between planned occurrences of maintenance and calibration, leads to reduced operating costs and can provide increased safety by reducing the probability of equipment being set-up incorrectly due to human error.

Reducing the maintenance of safety equipment is a sensitive subject, the justification for so doing needs to be clear. The maintenance interval is an important factor in calculating the overall reliability or availabilty of equipment. In a redundant protection system, staggered maintenance of redundant channels, with the same maintenance interval for each channel, is used to achieve a better overall reliability figure without having to increase the reliability of the individual channels. At existing power stations the protection systems were designed many years ago and their reliability figures were calculated using predicted failure rates. Over those years of operation, real failure rate data has been collected which shows the predicted failure rates to have been pessimistic. By re-visiting the overall reliability calculations but using observed failure rates rather than predicted failure rates it is possible to justify increasing the maintenance interval. At Heysham 2 AGR the present maintenance interval for the main guardline is 3 months, calculations using observed failure rates show that a case for testing at a 6 monthly interval could be justified. It is however, likely that an interval of 4 months would be used, initially, to ensure that no deterioration in failure rates occurred due to less frequent maintenance. The existence of a secondary guardline which provides diverse protection for frequent reactor faults, gives support to the case.

In addition to increasing maintenance intervals for specific protection equipment, a decrease in the statutory outage frequency is being sought for the AGRs, from once every 2 years to once every 3 years. In terms of the effect on reactor protection systems, such a change is not as drastic as it may at first appear. Protection systems are always of a redundant design using majority voting an a 2oo3 or 2oo4 basis. They are designed to be tested and maintained with the reactor at power. Not a great deal of their maintenance and testing activities rely on the reactor being shutdown. Sensors, manual trip buttons and the control rod release mechanism are the significant items normally dependant on a reactor outage for testing. The arguments for testing these items on a 3 yearly basis rather than biennually are straightforward and have been constructed for Heysham 2, Heysham 1 and Hartlepool AGRs but have yet to be approved by The Regulator. Essentially such items would require a common mode failure of low probability in order to cause a protection system failure. Changing the test period by such a margin does not significantly affect the probabilities involved.

With new equipment, the aim must be to reduce the involvement of humans in the maintenance and calibration processes. With digital equipment automatic self calibration and fault detection can be continuously performed as background tasks to the prime functions. Automatic testers can be used to reliably and repetitively check equipment when off line. The provision of such facilities should enable less frequent maintenance intervals and more reliable operation.

4. CONCLUSIONS.

Digital systems can provide real benefits and for some functions are a necessity. However, the burden of qualifying their design is significant, extremely significant if software is involved. ASIC devices can offer an alternative method of achieving high functional density without recourse to software. Nuclear Electric has experience of qualifying digital systems for use in reactor protection roles, both with and without software.

Digital equipment, particularly where complex components like ASICs or microprocessors are involved, require failure analyses that go beyond traditional FMEA techniques. Analyses using functional representations and failure modes have been used to show "equivalence to fail-safe" for digital equipment.

Increasing the length of maintenance intervals for existing equipment can be justified by re-visiting the reliability calculations, if the observed failure rates show that the predicted failure rates were sufficiently pessimistic. Advantage should be taken of new digital systems, to minimise the need for human involvement in routine maintenance and calibration. Maintenance and testing of reactor protection systems does not prejudice the acceptability of increasing the period of time between reactor outages.

7. REFERENCES.

[1] HUNNS D.M., WAINWRIGHT N., Software-based protection for Sizewell B: the regulator's perspective, Nuclear Engineering International, September 1991.

[2] HUGHES G., HALL R.S., Recent Developments in Protection and Safety Related Systems for Nuclear Electric's Power Plant, IAEA Symposium on Nuclear Power Plant Instrumentation and Control, Tokyo, May 1992.

[3] HALL R.S., HUGHES G., Implementation of Safety Related Computer Systems, Associated Research and the Development of Standards, CANDU Owners Group Computer Conference, Markham, Ontario, 11-13 November 1990.

[4] HUGHES G., HOLT G., WINSBORROW L.A., Recent Activities on PES Assessment and Development in Nuclear Electric, SRD Annual Technical Symposium on the Reliability of Programmable Electronic Systems, Risley 18 March 1992.

[5] Forum on Safety Related Systems in Nuclear Applications, Royal Academy of Engineering, London, 28th October 1992.

[6] PAVEY D.J., WINSBORROW L.A., Demonstrating Equivalence of Source Code and PROM Contents, 4th European Workshop on Dependable Computing (EWDC-4), Prague, April 1992.

[7] TOOLEY P.A., STOKES P.,Dynamic Testing of the Primary Protection System, International Conference on Electrical and Control Aspects of the Sizewell "B" PWR, Cambridge, UK 14-16 September 1992.

[8] MURALIDHARAN R., SESHADRI V.R., KUMARAVADIVELU C., Safety Logic For Fast Breeder Reactor, IAEA Symposium on Nuclear Power Plant Instrumentation and Control, Tokyo, 18th - 22nd May 1992.

[9] KOZAK J., CHOU Q.B., ACHTMAN A., A Non-Computerised Design Option for Safety Systems of Nuclear Power Plants, IAEA Symposium on Nuclear Power Plant Instrumentation and Control, Tokyo, 18th - 22nd May 1992.

[10] "Technology report", Electronic World News, 20th January 1992.

[11] LALA P.K., Fault Tolerant and Fault Testable Hardware Design, Prentice Hall.

Instrumentation and Controls Division

QUALIFICATION ISSUES ASSOCIATED WITH THE USE OF ADVANCED INSTRUMENTATION AND CONTROL SYSTEMS HARDWARE IN NUCLEAR POWER PLANTS*

Kofi Korsah
Oak Ridge National Laboratory
Oak Ridge, TN 37831-6010

Christina Antonescu
NRC Office of Nuclear Regulatory Research
Rockville, MD 20852

IAEA Specialists Meeting on
Experience in Ageing, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability

Rockville, Maryland
5-7 May, 1993

"The submitted manuscript has been authored by a contractor of the U.S. Government under contract No. DE-AC05-84OR21400. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes."

*Research sponsored by the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, under Interagency Agreement 1886-8179-8L and performed at Oak Ridge National Laboratory, managed by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under contract DE-AC05-84OR21400.

The submitted manuscript has been authored by a contractor of the U S Government under contract No DE AC05-84OR21400 Accordingly the U S Government retains a nonexclusive royalty-free license to publish or reproduce the published form of this contribution or allow others to do so for U S Government purposes

ABSTRACT

The instrumentation and control (I&C) systems in advanced reactors will make extensive use of digital controls, microprocessors, multiplexing, and fiber-optic transmission. Elements of these advances in I&C have been implemented on some current operating plants. However, the widespread use of the above technologies, as well as the use of artificial intelligence with minimum reliance on human operator control of reactors, highlights the need to develop standards for qualifying I&C used in the next generation of nuclear power plants. As a first step in this direction, the protection system I&C for present-day plants was compared to that proposed for advanced light water reactors (ALWRs). An evaluation template was developed by assembling a configuration of a safety channel instrument string for a generic ALWR, then comparing the impact of environmental stressors on that string to their effect on an equivalent instrument string from an existing light water reactor. The template was then used to address reliability issues for microprocessor-based protection systems. Standards (or lack thereof) for the qualification of microprocessor-based safety I&C systems were also identified. This approach addresses in part issues raised in Nuclear Regulatory Commission policy document SECY-91-292, which recognizes that advanced I&C systems for the nuclear industry are "being developed without consensus standards, as the technology available for design is ahead of the technology that is well understood through experience and supported by application standards."

1. INTRODUCTION

In 1991, the Nuclear Regulatory Commission (NRC) initiated the Qualification of Advanced Instrumentation and Control Systems Program at Oak Ridge National Laboratory to develop an understanding of the technical issues involved in evaluating long-term properties and performance of "advanced" digital instrumentation and control (I&C) systems proposed for use in advanced light water reactors (ALWRs). The objective is to support the development of standards that will help ensure the operability and qualification of such I&C systems in a nuclear power plant environment.

Initial studies under this program have focused on protection systems and the I&C portions of engineered safety feature (ESF) actuation systems. Some of the hardware issues identified for the proposed systems that were studied are reported in this paper, and others can be found in references 1 and 2.

The forthcoming change from completely analog systems to fully digital-computer-based I&C systems can lead to significant benefits. These benefits include reduced stress on I&C components from frequent maintenance and testing cycles due to the self-testing/diagnostic capabilities of microprocessor-based systems and the potential reduction in system costs and cabling due to sharing of data transmission lines via multiplexing equipment. However, the introduction of digital technology in safety-related systems of nuclear power plants also 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? To what extent can existing qualification standards and acceptance criteria be extended to protection system I&C proposed for ALWRs?

To answer these questions, an evaluation template was developed by assembling a configuration of a protection system for a generic ALWR, then comparing the impact of environmental stressors on system components to their effect on an equivalent channel from an existing light water reactor. Hardware issues considered in the template include typical I&C components and materials and methods of protection against the environment. Functional issues considered include independence, communication methods, and capability for test and calibration. The template is then used to address qualification issues for microprocessor-based protection systems.

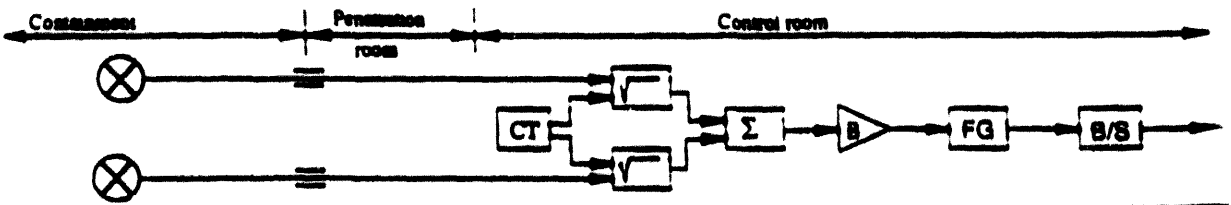
2. ENVIRONMENTAL, FUNCTIONAL, AND AGING DATA TEMPLATES FOR PROTECTION SYSTEMS

We addressed functional and environmental qualification issues for ALWR protection system I&C by developing an environmental, functional, and aging data template for the protection channel of each current ALWR design. Using information provided by manufacturers, we identified environmental conditions and stressors to which I&C equipment in reactor protection channels may be subjected. The resulting data were then compared to a similar template for an instrument string typically found in an analog protection channel of a present-day nuclear power plant.

A typical instrument string (e.g., reactor coolant flow) is shown in Fig. 1. The figure, adapted with modification from reference 3, shows environmental conditions typically found at the location of major components in the string, materials in the system components that contribute to system aging, and the stressors that contribute to component degradation. Note that Fig. 1 refers to identifiable analog components in the "path" of a (flow) process variable monitored for a protection system function. In a microprocessor-based protection system, however, this identification of individual components through trip bistable circuitry is not meaningful following the multiplexer(s), because a single microprocessor may perform multiple functions under software control. Thus, Fig. 2 shows an environmental, functional, and aging data template for a protection channel of a generic ALWR. Because of space considerations, only an abridged version is presented in this paper. The following discussion refers to Figs. 1 and 2.

2.1 Transmitters and Cables

Although several similarities exist in the approach taken by ALWR manufacturers in the implementation of protection system I&C, some differences also exist. For example, in some cases, the transmitters performing protection system functions will be hardwired to the protection cabinets, whereas in others, the signal from containment will be processed by multiplexing equipment strategically located throughout the plant outside containment. In all cases studied, indications are that conventional analog transmitters will be used 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 electromagnetic interference/radio-frequency interference (EMI/RFI) sources to which instrumentation within containment will be subjected. Under normal plant operating conditions, transmitters are subjected to aging stressors from temperature, moisture, radiation, and vibration, with elevated temperature being the dominant stressor in most cases.[3,4] However, transmitters may also be subjected to aging stressors from testing and maintenance practices, the monitored

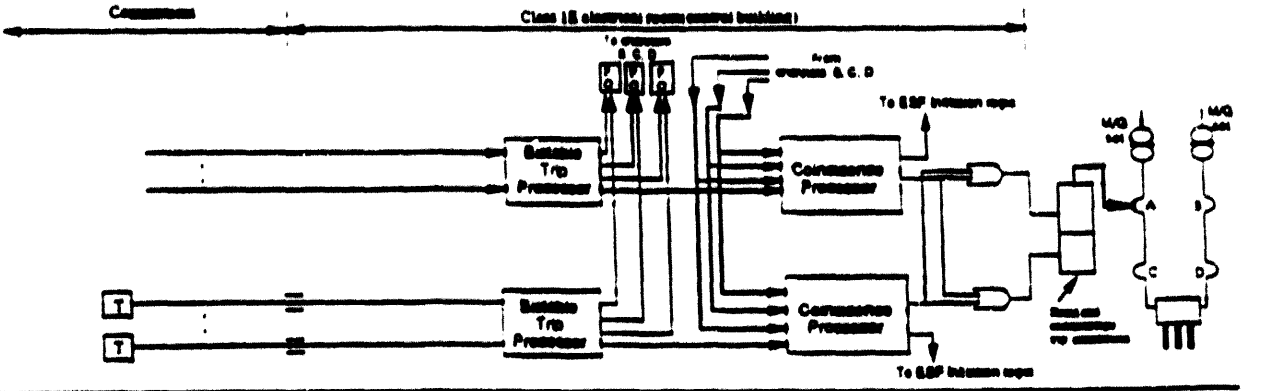


	Flow transmitter	Reactor building cable	Reactor building penetration	Penetration room cable	Calibration/ test module	Square root extractor	Summing circuit	Buffer amplifier	Function generator	Power/low comparator bistable
Functions performed in software	None									
Radiation	~ 4×10^4 rad over 20 years			<4×10^2 rad over 40 year plant life						
Ambient temperature	Average temperature in containment: ~120 deg.F. Average containment 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 supplies, inverters, interlocks, and bypass modules.									
Signal type	Pressure to current transducers (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[a] Sheath: Neoprene[a] Outer jacket: Galvanized steel			Several types of transducers 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: Silicone oil. Isolation diaphragm: 316 stainless steel. Housing seals: Ethylene propylene.[a] Electronic components: Seals and insulating materials used on electronic components.[a] Circuit boards: Epoxy glass laminate.[a]					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.

[b] Materials subject to aging degradation.

Fig. 1. Environmental and aging data template for coolant flow string in an analog protection channel (adapted from ref. 3).



	Transmitters	Processors (main and subsystem). (Transmitters are considered to make processing system cabinets.)	Bistable trip processors evaluate trips based on the digitized sensor values exceeding a specified setpoint	Processors evaluate the local coincidence logic based on the state of the four bistable trip signals and provide bypasses.	Switchgear
Functions performed in location	None		Multiplexer scanning, sensor-out-of-limit detection, digital data acquisition. Channel trip communication. Provides sensor data to the STP through communication (datalink) digital communication equipment.		None
Radiation	$< 3 \times 10^6$ rads gamma (60 yr total dose).		Total integrated dose over 60 yr: $<= 10^7$ rads gamma.		
Ambient temperature	60° - 110° F. Average transmitter operating room: -40° to 240° F	-77° F ambient in battery room. Design basis for instrumentation (not available)			
EMI/RFI	Operate accurately 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. Parameter tests used are CS01, CS02, CS06, RS03, and RS04.			
Insulators	Reactor coolant piping, pressure vessel, conts. 110 VAC and 120 VDC power supplies, inverters, monitors, and bypass modules.				
Seismic	Temperature, radiation, chemical, vibration, maintenance and maintenance handling, environmental system		Maintenance/testing system, operator compensates inside cabinet, electromagnetic interference. Seals can adversely affect electronic components far removed from the source of the smoke or fire.		
Channel independence	Where sensor and processor systems have redundant sensor input requirements, redundant Class 1E sensors that are used independently by each channel of the protection system may, in some cases, also be used by the control system. In such cases fiber optic (or environmental electrical isolation devices) are used to ensure electrical independence. Separate processors are used for calculating trip functions and communication functions.				Switchgear systems are located in the electrical equipment rooms which are geographically separate from each other.
Materials	Transmitters will be identical to those found in present-day power plants. MATERIALS IN CAPACITANCE TYPE PRESSURE TRANSDUCERS[a]: Housings: Aluminum with epoxy polyester paint or 316 stainless steel. Fill fluids: Silicon oil. Isolation diaphragms: 316 stainless steel. Housing seals: Elastomer proprietary.[a] Elastomer components: Seals and retaining materials used on electronic components.[a] Circuit boards: Epoxy glass laminate.[a]		Optical fibers will be used for interchannel communications. The following specifications are typical of type(s) to be used: FIBER MATERIAL: Silicon dioxide (pure and doped). SECONDARY BUFFER: polyimide or epoxy. STRENGTH MEMBER: Aramid yarn or epoxy. OUTER JACKET: Flame retardant elastomeric polyethylene. FLAMMABILITY: Tested to IEEE Std 383-1974 OPERATING LIMITS: -20° C to 80° C (operating) 0 to 100% (relative humidity).		
	MATERIALS SUBJECT TO AGING DEGRADATION IN CABLES: Insulation (cross linked polyethylene). Sheath (Neoprene). Outer jacket (Galvanized steel).		Seals and retaining 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. [b] Materials subject to aging degradation.		ESF: Engineered safety features. BTP: Bistable trip processor. F.O.: Isolation via optical fiber. RPS: Reactor protection system.		

Fig. 2. An abridged environmental and aging data template for the protection channel of a generic advanced light water reactor.

process, and power supply variations. Humidity levels under normal plant conditions should not pose a problem for nuclear-qualified transmitters, because such transmitters are sealed for design-basis accidents such as main steam line breaks.

Currently, most transmitters for use within containment have a qualified life of 10 to 40 y, depending on type, materials of construction, and other factors. For example, a strain-gauge transmitter typically has a qualified life of 40 y, but a differential capacitance transmitter may be qualified for only 10 y. Seals and gaskets for transmitters may have a much shorter qualified life (e.g., 4 y).[3] It is reasonable to assume that the performance and lifetime of transmitters will be the same for ALWRs as for conventional reactors.

Although conventional analog transmitters are most likely to be used, I&C systems for the next generation of nuclear power plants are still evolving, and it is possible that some form of "smart" transmitter technology could be used in future plants. Work is progressing on the development of several technologies with low power capabilities (e.g., complementary metal-oxide semiconductor silicon-on-insulator) that can withstand a total radiation dose of several tens of megarads.[5] This development 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 resulting in reduced personnel exposure, (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.[6] Existing 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 oil-filled transmitters.[7] This type of failure significantly increases the transmitter's response time and may also limit its dynamic range. These effects, however, are not observable during steady-state operation. Technologies that are currently being investigated for the development of improved pressure-sensor performance include fiber-optic and mechanical tuning-fork resonance frequency.[6]

As with transmitters, cable types and connections within ALWR containments are not likely to be different from those used in present-day reactors. Stressors that are known to enhance cable degradation include temperature, radiation, and moisture. Cable materials experience ambient temperature and radiation for long periods of time. Under accident conditions, however, cables 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 y, and their performance and lifetime will be substantially the same for ALWRs as for conventional reactors.

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 the ESF systems. Several environmental stressors or their synergistic effects can result in aging and increased failure rates for certain fiber-optic cables. These stressors include high humidity and high temperature,[8] inadequate cable designs, and improper choice of fiber coatings.[9] However, protection system cabinets are typically located in an area having a lower radiation level than exists in containment. Temperature and humidity

levels are also less harsh. Typically, the set of protection system cabinets for *each* protection channel of an ALWR will be placed in individual Class 1E rooms geographically separated from each other. Ambient temperatures at such locations have been estimated to be between 65 and 75°F, and humidity levels are likely to be similar to present-day control-room environments. Aging tests have shown that, with suitable coatings, present-day fibers can withstand at least a 20-y exposure to an extreme outside plant climate.[10] This longevity suggests that the proposed application of optical fibers in the control systems and in the interface between the protection system and the ESFs in nuclear power plants should be encouraged. (The environment of such cabinets and systems is generally less harsh than in containment.) This conclusion appears to be supported by a study of the performance of fiber-optic cables from several vendors.[11] The study, which was conducted to determine the radiation sensitivity of commercially available radiation-hardened fiber-optic cables, concluded that fiber-optic cables are currently available that perform reliably in nuclear reactor environments. Although some fibers fluoresce enough under radiation to obscure low-strength (nanowatt) signals, others (such as pure-silica-core fibers) exhibit no significant performance change with doses as high as 3800 Gy. In fact, any conventional transmitter will couple about 10^6 times as much light into fibers as flourescence does.

2.2 Stressors

The same stressors that contribute to I&C system age degradation in present-day reactors will also affect ALWRs. Examples are elevated temperature, smoke, chemical spray, vibration, radiation, moisture, environmental cycling, and EMI/RFI.

EMI/RFI is an important stressor because of increased use of microprocessor-based technology in ALWR safety-critical I&C systems. A study of the *licensee event report* database over a 10-y period (1982–91) shows that the fraction of EMI/RFI-related protection system events is significant compared to traditionally recognized environmental stressors such as elevated temperature.[1] Although digital systems typically have higher noise margins than those of analog systems, their failure modes are often quite different and much less predictable. Also, trends toward the use of higher clock frequencies, lower logic voltage levels, and ever-denser packages lead to increasing probability of upsets. The increasing levels of integration tend to decrease the noise immunity of the digital devices. Although on-chip protection methods help somewhat to protect the devices against interference-induced damage, the record shows that they have not eliminated upset problems. Studies show that even fault-tolerant systems generally do not achieve reliable system performance in some high-EMI environments.[12] Ongoing research under the I&C qualification program is geared toward improving our understanding of microprocessor behavior in EMI/RFI fields.

Smoke is another important stressor because it may cause electronic systems relatively far removed from a fire to degrade and malfunction over time. Fire-produced particulates that settle on electronic boards and other equipment contain chlorides and sulfides. In the presence of moisture and air (oxygen), the particulates form electrolytes that can erode the metal interconnections on electronic boards or other metal contact surfaces, thereby causing degradation and system faults long after the occurrence of a fire.

We investigated the precautions taken by ALWR manufacturers to protect safety systems against smoke. In general, smoke/particulates are not monitored inside the protection system cabinets. Rather, the entire plant protection system will be designed and qualified for the worst-

case operating conditions that can be expected during plant life, and each of the Class 1E equipment rooms will have smoke and temperature sensing as part of the fire protection system.

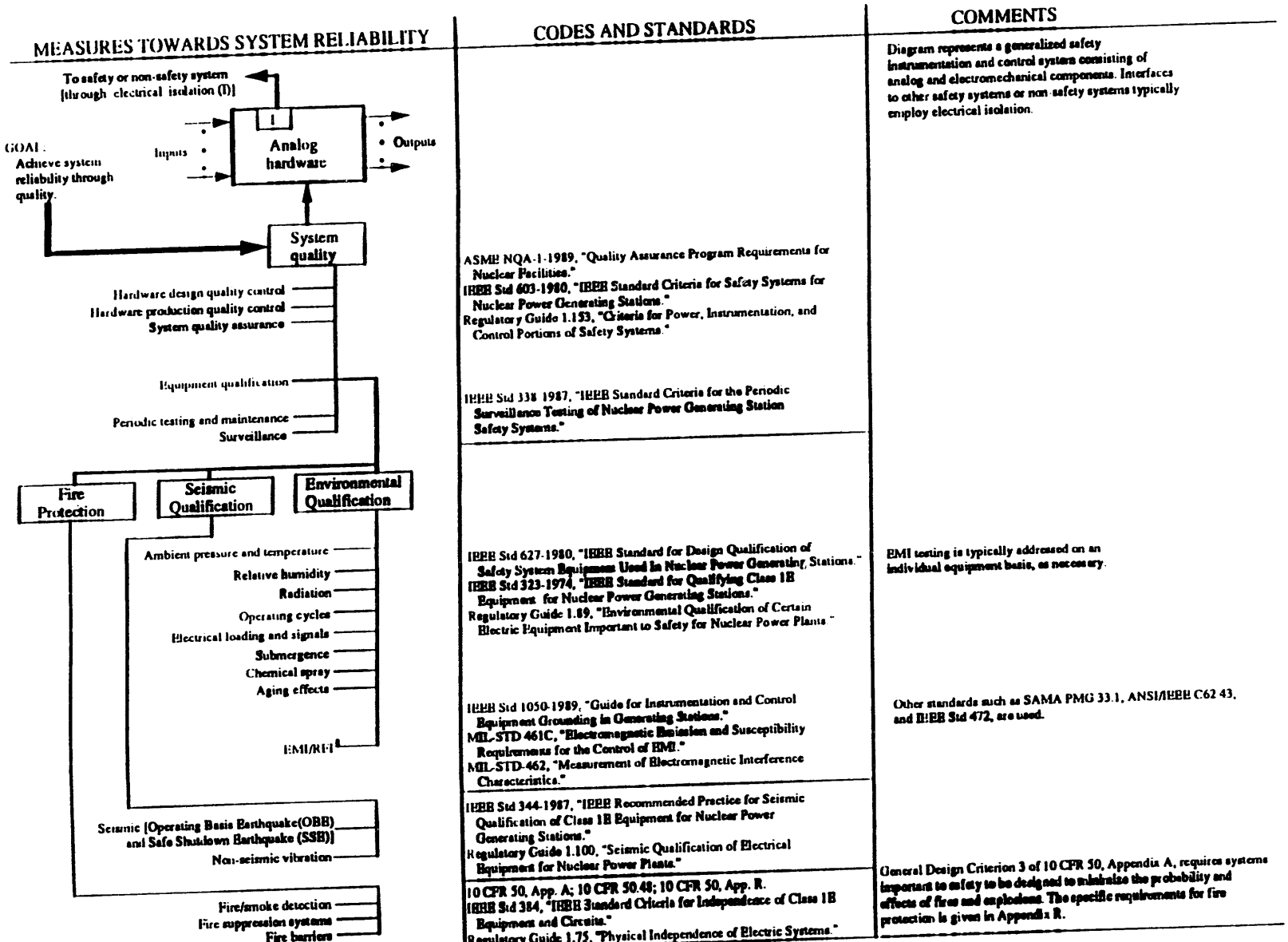
3. QUALIFICATION OF MICROPROCESSOR-BASED SAFETY SYSTEMS

In this section, we summarize our study by addressing reliability issues for microprocessor-based safety systems from a *systems* (integrated hardware/software) approach and identifying standards (or lack thereof) for such systems. Where standards are available, areas that may need modification in view of the introduction of advanced I&C in the safety systems of nuclear power plants are discussed. This approach addresses, in part, issues raised in NRC document SECY-91-292, which recognizes that advanced I&C for the nuclear industry "is being developed without consensus standards, as the technology available for design is ahead of the technology that is well understood through experience and supported by application standards."

Figure 3 depicts the qualification process for a generalized (analog) safety system in a present-day nuclear power plant. It also identifies the most significant standards related to the particular qualification activity. Figure 4 identifies some areas in the qualification process that could be (or are being) strengthened for application to microprocessor-based safety systems. As illustrated in the figures, the goal of qualification is to achieve a high degree of *reliability* through the maintenance of quality at various levels of design, implementation, and operation of the safety system.

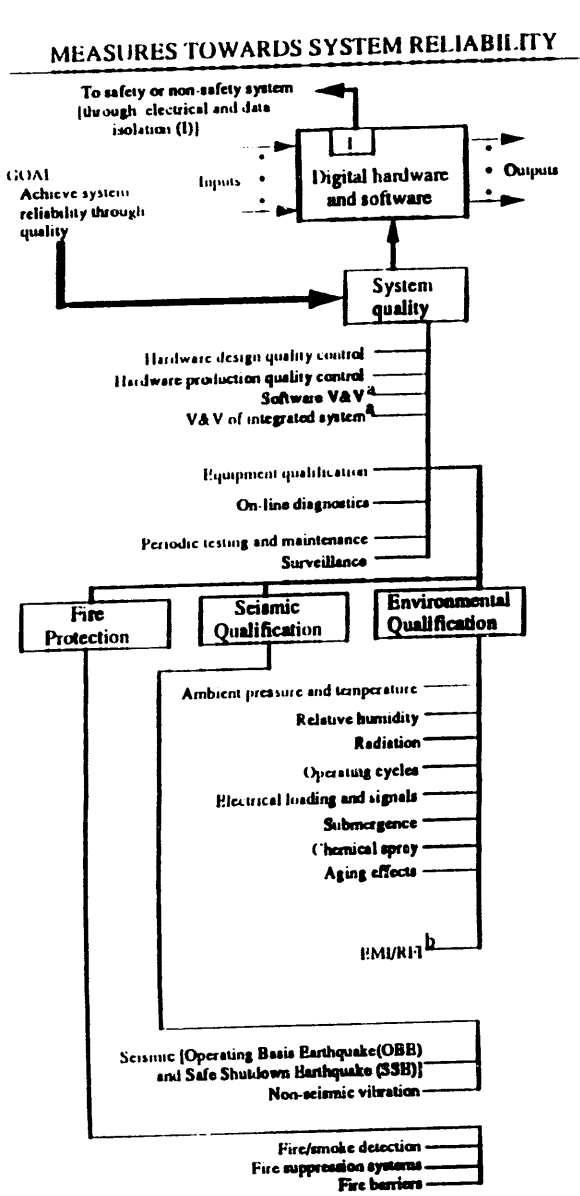
Requirements for functional reliability of safety systems is embodied in IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," and IEEE Std 603-1980, "Criteria for Safety Systems for Nuclear Power Generating Stations." IEEE Std 279-1971 is endorsed by Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." The requirements in IEEE Std 603 are independent of the specific equipment used and thus apply to both analog and microprocessor-based safety systems. In fact, Regulatory Guide 1.153 encourages the application of advanced technology such as programmable digital computers in the operation of nuclear power plants if such technology serves to improve safety. However, the nature of computers/microprocessors poses new challenges to both the functional and environmental requirements (e.g., independence, separation, diversity, common mode failure, EMI/RFI effects) for safety system I&C. These issues have been discussed elsewhere[2] and reflect the minimum set of issues that need to be considered to maintain the reliability of microprocessor-based protection systems at the levels achievable with current analog systems. (It is reasonable to compare reliability measures, acceptance criteria, and standards with those used for analog systems because considerable experience with the latter has been accumulated over the years.) Reliability involves maintaining a high level of confidence in the *design* of the system hardware and software. System verification and validation (V&V) methods are currently the best means of achieving this. It is recognized that ANSI/IEEE 7-4.3.2-1982 is inadequate in addressing acceptance criteria for microprocessor-based safety I&C, and these issues are being addressed in the next revision of this standard.[13]

As depicted in Figs. 3 and 4, reliability of safety system I&C also includes ensuring a high level of confidence that the system will perform adequately in its *environment* under normal, design-basis, and postdesign-basis event conditions. Qualification ensures that Class 1E equipment can perform its safety function(s) with no failure mechanism that could lead to



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

Fig. 3. Measures taken to achieve system reliability in present-day nuclear power plants.



CODES AND STANDARDS	COMMENTS
	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.
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."	ANS/IEEE 7-4.3.2 - 1982 is inadequate in addressing issues relating to microprocessor-based I&C. These issues are being addressed in the next revision of IEEE 7-4.3.2.
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 Power Generating Stations." Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear 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 PMG 33.1, ANSI/IEEE C62.43, and IEEE Std 472, are used.[b] However, specific criteria for EMI/RFI qualification for the nuclear power industry is lacking.
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.

Fig. 4. Methodology for building reliability into microprocessor-based safety systems.

common-cause failures under postulated accident conditions. As illustrated in Figs. 3 and 4, equipment qualification is generally handled under environmental, seismic, and fire protection criteria and standards.

Environmental qualification methods are embodied in IEEE Std 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 Std 323-1983 provides further clarification of these environmental qualification procedures. Although NRC has not specifically endorsed the 1983 version, it has commented that IEEE Std 323-1983 neither alters the industry guidance provided nor does it alter 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 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 Std 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. 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 is stipulated in General Design Criterion 3 of Appendix A of 10 CFR Pt. 50 and IEEE Std 384, "Independence of Class 1E Equipment and Circuits." General Design Criterion 3 requires that structures, systems, and components important to safety be located to minimize the probability and effects of fires and explosions. IEEE Std 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 Pt. 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 must be capable of detecting, containing, and suppressing a fire. In addition, the system must 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.

4. CONCLUSIONS

This paper has addressed qualification issues for safety system I&C for the next generation of nuclear power plants. From comparison of present-day analog protection systems with their ALWR counterparts as well as standards used for their qualification, it appears that a combination of good engineering design, excellent V&V and qualification procedures, and diversity can result in reliable microprocessor-based safety I&C systems. To achieve this goal, however, adequate standards need to be established. Currently, the standard that establishes criteria for the use of computers in safety systems is ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems of Nuclear Power Generating Stations." This standard is endorsed by Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants." However, ANSI/IEEE-ANS-7-4.3.2-1982 does not adequately reflect the rapid developments in computer technology. A rewrite of the standard is therefore needed and is currently in progress[13] and is likely to include an expanded software section and an amplification of the IEEE Std 603 requirements to reflect advances in computer technology.

With the increased application of microprocessor technology to reactor safety systems, EMI/RFI emission and susceptibility criteria need to be established for the nuclear power plant environment.

In existing plants, physical separation and fire protection requirements, rather than environmental qualification of the Class 1E equipment, are generally relied upon to mitigate the consequences of a fire. This approach seems to be also reasonable for the next generation of nuclear power plants.

5. REFERENCES

1. KORSAH K., et al., "Environmental Qualification and Functional Issues for Microprocessor-Based Reactor Protection Systems," 20th Water Reactor Safety Information Meeting, Bethesda, MD, Oct. 21-22, 1992.

2. KORSAH K., ANTONESCU C., "A survey of issues associated with microprocessor-based reactor protection systems," ICONE-2 (Proc. 2d Int. Conf. Nucl. Eng., San Francisco, March 1993).

3. MEYER, L., Nuclear Plant Aging Research on Reactor Protection Systems, NUREG/CR-4740, Idaho Natl. Eng. Lab. (1988).

4. GEHL, A. C., HAGEN, E. W., Aging Assessment of Reactor Instrumentation and Protection System Components, NUREG/CR-5700, Oak Ridge Natl. Lab., TN (1992).

5. LERAY, J. L., et al., CMOS/SOI hardening at 100 mrad(SiO_2), IEEE Trans. Nucl. Sci., NS-37 6 (1990) 2013.

6. WEISS, J. M., SHEPARD, R. L. , "Evaluation of advanced pressure sensor technology," (Proc. 8th Power Plant Dyn., Control Test. Symp., May 27-29, 1992) 1 (1992) 2.01-2.09.

7. "Oil Loss Syndrome in Rosemount Pressure Transmitters," Analysis and Measurements Corp., comp., Knoxville, TN (1991).

8. MATTHEWSON, M. J., KURKJIAN, C. R., Environmental effects on the static fatigue of silica optical fiber, J. Am. Ceram. Soc. 71 3 (1988) 177-83.

9. DOTY, K. M., LONG, K. J., "Prediction of shipboard fiber optic cable service life," (Proc. Int. Soc. Opt. Eng., SPIE) 1174 (1989) 205-18.

10. AT&T network systems, Lightguide Digest 1 (1992).

11. Optical fibers in radiation environments, EPRI, Pub. TR-100367 (1992).

12. HANSON, R. J., Interference effects on microprocessor and subsystem performance, Eval. Eng. (May) 155.

13. MATRAS, J. R. Technical note: rewriting the standard on the functional requirements for computers used in safety systems of nuclear power plants, Nucl. Saf. 32 3 (1991) 375-79.

PARTICIPANTS

INTERNATIONAL ATOMIC ENERGY AGENCY

Specialists Meeting
On
Experience in Ageing, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability

May 5-7, 1993 USA

LIST OF PARTICIPANTS

CANADA

Mr. W. J. Beattie
Atomic Energy of Canada
Chalk River Laboratories, Station 90
Chalk River, Ontario, Canada K0J 1J0
Tel. 613-584-3311 ext. 4771
FAX 613-584-1261 or 4024

Mr. L. A. Gonzalez
Ontario Hydro, Research Division
800 Kipling Avenue, KR308
Toronto, Ontario, Canada M8Z 5S4
Tel. 416-207-5876
FAX 416-207-5555

FINLAND

Mr. Samuel Koivula
Finnish Centre for Radiation
and Nuclear Safety
P.O. Box 268
SF-00101 Helsinki, Finland
Tel. 3580-7082-356
Fax 3580-7082-392

Ms. Kaisa Simola
Technical Research Centre of Finland
P.O. Box 34
sf-02151 Espoo, Finland
Tel. 358-0-456-6774
Fax. 358-0-456-6475

GERMANY

Mr. Arndt Lindner
Institut for Scherheitstechnologie
Forschungsgelande
D-8046 Garching, Germany
Tel. 089-32004 208

GERMANY (Continued)

Dr. Werner Hofmann, Hofmann Consultants
Parkalle 14
Stadland 1 -, Rodenkirchen,
D-W-2883, Germany
Tel. 49-4732-1418
Fax 49-4732-8345

HUNGARY

Mr. Sandor Elo
Hungarian Atomic Energy Commission
P.O. Box 565
Budapest, H-1374, Hungary
Tel. 361-1327-390
Fax 361-1427-598

Mr. Karoly Hamar
Hungarian Atomic Energy Commission
Pf. 676
Budapest 114, H01539, Hungary
Tel. 361-155-04-93
Fax 361-155-76-93

INDIA

Mr. S.P. Chaganty
Bhabha Atomic Research Centre
Electronic Division
Trombay, Bombay - 400 085, India
Tel. 556-30-60 ext. 2855
Fax 91-22-5560750

JAPAN

Mr. Hirofumi Ishii
Mitsubishi Atomic Power Industries, Inc.
4-1 Shibakoen 2-Chome, Minato-Ku
Tokyo 105, Japan
Tel. 03-3433-8251
Fax 03-3433-8208

THE NETHERLANDS

Mr. J. W. de Vries
Manager, E, I&C EPZ
Project Backfitting (NPP Borssele)
P.O. Box 711
5600 AS Eindhoven, Netherlands
Tel. 31-1100-21000
FAX 31-1105-2320

Mr. IJ Van der Plas
Ministry of Social Affairs
and Employment, Nuclear Safety Dep
P.O. Box 90801
Den Haag, NL-2509 LV, Netherlands
Tel. 31-70-3335540
Fax 31-70-3334018

SPAIN

Mr. J. Alonso
TECNATOM S.A.
KM. 19 Ctra. No. 1 Madrid-Ira
San Sebastian de Los Reyes
Madrid 28709 Spain

SWEDEN

Mr. Jan Bendiksen
Vattenfall AB, Ringhals
S-43022 Vaeroebacka, Sweden
Tel.46-340-679-07
Fax 46-340-679-56

SWITZERLAND

Mr. Winfried P. Kunz
Goesgen Nuclear Power Plant Switzerland
Kernkraftwerk Goesgen-Daneiken AG
Postfach 64
Ch-4658 Daeniken, Switzerland
Tel. (01141)-62-65 16 65
Fax (01141)-62-65 22 01

UNITED KINGDOM

Dr. Suzanna G. Burnay
AEA Technology
Harwell Laboratory, B 528.10
Didcot, Oxfordshire, OX11 ORA, UK
Tel. 0235-434908
Fax 0235-434136

Mr. John Leslie Fowles
Nuclear Electric Plc
Berkely Technology Centre
Berkeley, Gloucestershire
GL13 9PB, UK
Tel. 0453-812384
Fax 0453-812157

UNITED KINGDOM (continued)

Mr. Graham P. Holt
Nuclear Electric
Location 18 Ext, Barnwood
Gloucester, GL4 7RS, UK
Tel. 0452-653755
Fax 0452-653506

Mr. Christopher D. Jones
Nuclear Electric plc
Dungeness "B" Power Station
Romney Marsh
Kent, TN29 9PX, UK
Tel. 44(0)679-20551
Fax 44(0)679-21331

Mr. Russell G. Phoenix
Rolls Royce and Associates
P.O. Box 31
Derby, DE24 8BJ, UK
Tel. 332-661461 ext. 4926
Fax 0332-661630

Mr. Ian C. Smith
AEA Technology
Winfrith
Dorchester, Dorset,DT2 8DH, UK
Tel. 44(0)305-203482
Fax 44(0)305-2035-40

IAEA

Mr. Andrei N. Kossilov
Division of Nuclear Power
Wagramerstrasse 5, P.O. Box 100
Vienna, A-1400, Austria
Tel. (43)-1-2360-2796
Fax (43)-1-234564

USA

Mr. David C. Bardo, ECAD Div.
CM Technologies Corporation
1026 Fourth Avenue
Coraopolis, PA 15108
Tel. (412)262-0734
Fax. (412)262-2250

Dr. Peter J. Esseff
Educational Systems for the Future
c/o Dr. George C. Rudy
Halliburton NUS
910 Clopper Road
Gaithersburg, MD 20878

USA (Continued)

Mr. Paul D. Ewing
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, TN 37831-6318
Tel. 615-576-5019
Fax 615-574-4058

Mr. Dwayne N. Fry
Oak Ridge National Laboratory
3500, MS6009, P.O. Box 2008
Oak Ridge, TN 37831-6009
Tel. 615-574-5565
Fax 615-574-4058

Mr. Pranab K. Guha
Department of Energy
Office of Nuclear Safety
Mail Stop GTN/D432
Washington, DC 20585
Tel. 301-903-7089

Mr. H. M. Hashemian
Analysis and Measurement
Services Corporation
9111 Cross Park Drive
Knoxville, TN 37923-4599
Tel. 615-691-1756
Fax 615-691-9344

Mr. Kofi Korsah
Oak Ridge National Laboratory
P. O. Box 2008
Oak Ridge, TN 37831-6010
Tel. 615-576-6064
Fax 615-574-4058

Mr. Glenn Lang
Westinghouse Electric Corporation
Pittsburgh, PA

Mr. Robert Lofaro
Brookhaven National Laboratory
Upton, New York

Ms. Jane Sandstrom
Rosemount Inc
12001 Technology Drive
Elen Prairie, MN 55344
Tel. 612-828-3286
Fax 612-828-3261

USA (Continued)

Dr. George C. Rudy
Halliburton NUS
910 Clopper Road
Gaithersburg, MD 20878

Mr. Kevin Sullivan
Siemens Power Corporation
P.O. Box 180
Bradenton, FL 34206

Mr. Greg Suski
Lawrence Livermore Laboratory
Tel. 510-423-8070
FAX 510-423-0186

Mr. Yoji Takayama
Mitsubishi Heavy Industries, Ltd.
Room 340, SMC-5747, Assumption Hall,
1345 Vickroy St.
Pittsburgh, PA 15282
Tel. 412-434-7736

Mr. Irfan Trebincevic
Siemens Power Corporation
P.O. Box 180
Bradenton,FL 34206

Mr. Robert E. Uhrig
University of Tennessee
306 Pasqua Engr Bldg.
Knoxville, TN 37996-2300
Tel. 615-974-3110
Fax 615-974-0668

Mr. J. Wiesemann
Westinghouse Electric Corporation
Pittsburgh, PA

Dr. Dan Wilkinson
EPRI
Nuclear Power Division
3412 Hillview Ave
P. O. Box 10412
Palo Alto, CA 94303
Tel. 415-855-2426
Fax 415-855-1026

Mr. See-Meng Wong
Brookhaven National Laboratory
Upton, New York

USNRC

Mr. Satish K. Aggarwal
US NRC
Washington DC, 20555
Tel. 301-492-3829
Fax 301-492-3696

Ms. Christina Antonescu
U.S. NRC
5650 Nicholson Lane, MS NLS-217B
Rockville, MD 20852
Tel. 301-492-3824
Fax 301-492-3696

Mr. S. V. Athavale
U. S. NRC
Washington, DC 20555
Tel. 301-504-2974
Fax 301- 504-2250

Ms. Ellen Brouns
U. S. NRC
Washington, DC 20555
Tel. 301-504-2344
FAX 301-504-3707

Mr. John Calvert
U. S. NRC
Region I
King of Prussia, PA
Tel. 215-337-5144

Mr. Matt Chiramal
U. S. NRC
Washington, DC 20555
Tel. 301-504-2845
Fax 301- 504-2250

Mr. Cliff Doutt
U. S. NRC
Washington, DC 20555
Tel. 301-504-2847
Fax 301- 504-2250

Ms. Ann Dummer
U.S. NRC
Washington, DC 20555
Tel. 301-504-2831

USNRC (Continued)

Mr. John Gallagher
U. S. NRC
Washington, DC 20555
Tel. 301-504-3217

Mr. Hukam C. Garg
U. S. NRC
Washington, DC 20555
Tel. 301-504-2929

Ms. Anna May Haycraft
U. S. NRC
Washington, DC 20555
Tel. 301-504-3075
FAX 301-504-3707

Mr. George Hubbard
U. S. NRC
Washington, DC 20555
Tel: 301-504-2870

Mr. Joe Joyce
U. S. NRC
Washington, DC 20555
Tel. 301-504-2842
Fax 301- 504-2250

Mr. Paul Loeser
U. S. NRC
Washington, DC 20555
Tel. 301-504-2825
Fax 301- 504-2250

Mr. Jerry L. Mauck
U. S. NRC
Washington, DC 20555
Tel. 301-504-3248
Fax 301- 504-2250

Mr. Evangelo C. Marinos
U. S. NRC
Washington, DC 20555
Tel. 301-504-2911

Mr. R. Kamalakar Naidu
U.S. NRC
MS 9D4 Washington, DC 20555
Tel. 301-504-2980
Fax 301-504-2260

Mr. Scott Newberry
U. S. NRC
Washington, DC 20555
Tel. 301-504-1183
Fax 301- 504-2250

NRC (Continued)

Mr. Steve Reynolds
U. S. NRC
Washington, DC 20555
Tel. 301-504-3245

Mr. William H. Ruland
U. S. NRC
Region I
King of Prussia, PA.
Tel. 215-337-5227

Ms. Deirdre Spaulding
U. S. NRC
Washington, DC 20555
Tel. 301-504-2821
Fax 301- 504-2250

Mr. Carlton Stoiber
Director, Office of International Programs
U. S. NRC
Washington, DC 20555

Mr. Jit Vora
U. S. NRC
Washington, DC 20555
Tel. 301-492-3845
Fax 301- 504-2250

Dr. Jared Wermiel
U. S. NRC
Washington, DC 20555
Tel. 301-504-2821
Fax 301-504-2260

DATE
FILMED
1/6/94
END