

OAK RIDGE NATIONAL LABORATORY LIBRARIES



3 4456 0604238 7



OAK RIDGE NATIONAL LABORATORY

operated by

UNION CARBIDE CORPORATION

for the

U.S. ATOMIC ENERGY COMMISSION

CENTRAL RESEARCH LIBRARY
DOCUMENT COLLECTION

OAK RIDGE NATIONAL LABORATORY
CENTRAL RESEARCH LIBRARY
DOCUMENT COLLECTION

LIBRARY LOAN COPY

DO NOT TRANSFER TO ANOTHER PERSON

If you wish someone else to see this
document, send in name with document
and the library will arrange a loan.

UCN-7969
13, 3-671

ORNL-NSIC-29
UC-80 — Reactor Technology

2

PROTECTION INSTRUMENTATION SYSTEMS IN LIGHT-WATER-COOLED POWER REACTOR PLANTS

H. G. O'Brien

C. S. Walker

NUCLEAR SAFETY INFORMATION CENTER

NSIC

NUCLEAR SAFETY

A BIMONTHLY REVIEW JOURNAL PREPARED BY NSIC

Nuclear Safety covers significant developments in the field of nuclear safety.

The scope is limited to topics relevant to the analysis and control of hazards associated with nuclear reactors, operations involving fissionable materials, and the products of nuclear fission.

Primary emphasis is on safety in reactor design, construction, and operation; however, safety considerations in reactor fuel fabrication, spent-fuel processing, nuclear waste disposal, handling of radioisotopes, and related operations are also treated.

Qualified authors are invited to submit interpretive articles, which will be reviewed for technical accuracy and pertinency. Authors will be advised as soon as possible of acceptance or suggested changes. Send inquiries or 3 copies of manuscripts (with the draftsman's original line drawings plus 2 copies, and with continuous-tone glossy prints of photographs plus 2 copies) to J. P. Blakely, Oak Ridge National Laboratory, P. O. Box Y, Oak Ridge, Tennessee 37830.

Nuclear Safety is prepared by the Nuclear Safety Information Center at Oak Ridge National Laboratory for the U.S. Atomic Energy Commission, Division of Technical Information. For subscriptions, address Superintendent of Documents, U.S. Government Printing Office, Washington, D. C. 20402. The subscription rate is \$3.50 per year. Below is an order blank for your convenience.

U.S. GOVERNMENT PRINTING OFFICE
DIVISION OF PUBLIC DOCUMENTS
WASHINGTON, D.C. 20402

OFFICIAL BUSINESS
RETURN AFTER 5 DAYS

POSTAGE AND FEES PAID
U.S. GOVERNMENT PRINTING OFFICE

Name _____
Address _____
City _____ State _____ Zip _____

TO INSURE PROMPT, ACCURATE SHIPMENT, PLEASE PRINT OR TYPE CORRECT ADDRESS ON MAILING LABEL ABOVE

MAIL ORDER FORM T-1

Superintendent of Documents, Government Printing Office, Washington, D.C. 20402

FOR USE OF SUPT. DOCS.

Enclosed find \$ _____ (check, money order, or Supt. of Documents coupons). Please enter my subscription to NUCLEAR SAFETY for one , two , or three years, at \$3.50 a year; \$1.00 additional for foreign mailing.

Please charge this order
to my Deposit Account
No.

Name _____
Address _____
City and State _____

ZIP Code _____

Contract No. W-7405-eng-26

Nuclear Safety Information Center

PROTECTION INSTRUMENTATION SYSTEMS IN LIGHT-WATER-COOLED
POWER REACTOR PLANTS

H. G. O'Brien C. S. Walker

OCTOBER 1969

OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee
operated by
UNION CARBIDE CORPORATION
for the
U.S. ATOMIC ENERGY COMMISSION

Printed in the United States of America. Available from Clearinghouse for Federal
Scientific and Technical Information, National Bureau of Standards,
U.S. Department of Commerce, Springfield, Virginia 22151
Price: Printed Copy \$3.00; Microfiche \$0.65

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:

- A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or
 - B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.
- As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor, to the extent that such employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

FOREWORD

The recent surge in the building of large nuclear power plants, particularly with the projected desirability of using urban sites for such installations, has focused attention on many aspects of the AEC's responsibilities for licensing reactors and insuring the public safety. Since the industry is "young," meaningful, long-term operating experience is sparse and the definition of the possible accident spectrum, as well as a set of firm design requirements, is subject to a largely analytical approach that necessarily involves conservative judgments. As plant designs become standardized and operating experience on the newer large reactors is gained, the inevitable process of refinement and of acquiring confidence in the operation of the plants will occur. This relatively slow evolutionary approach to acquiring firm design standards and criteria is not felt to be conducive to achieving the great national benefits of atomic energy within a reasonable time, in terms of the conservation of resources, combating air pollution, and the multitude of gains resulting from low-cost electricity.

As part of the effort to improve on this approach, the Regulatory Review (Mitchell) Panel recommended the formation by the AEC of a Steering Committee on Reactor Safety Research to coordinate the needs of the Regulatory Program with the direction of the safety research and development programs. This committee, in turn, recommended that several studies be undertaken to provide guidance for the research and development projects, and this was, in turn, implemented by the AEC Division of Reactor Development and Technology into the series of discussion reports herein described. It was intended that these reports provide a comprehensive assessment of the present status of specific aspects of nuclear safety and, by identifying accepted technology and the technology needing further experimental verification, that they enhance the understanding and confidence in this new industry.

Accordingly a number of the safety aspects of large light-water power reactors were selected by the AEC* as subjects for detailed study to

*Letter from Milton Shaw (Director, AEC Division of Reactor Development and Technology) to ORNL, March 28, 1966.

ascertain whether gaps in knowledge exist and where a research and development program could be of benefit. The subjects selected cover many of the areas for which inadequate factual bases exist and in which research that duplicates expected conditions is very difficult to perform. In general the subjects are in areas considered critical in the safety analysis of power reactor installations. Eight subjects were identified and a state-of-technology type of discussion report was prepared on each. The reports, which are directed primarily toward a technical-management audience, generally compare existing or planned plant applications with what is capable of being done at this time. Such comparisons have helped to identify inadequacies in assumptions, available data, or general basic knowledge so that, together with the opinions of experts in a particular field, areas of meaningful research and development have been identified.

This report is one of the series of eight companion reports listed below:

<u>Title</u>	<u>Author</u>	<u>ORNL-NSIC No.</u>
Missile Generation and Protection in Light-Water-Cooled Power Reactor Plants	R. C. Gwaltney	22
Potential Metal-Water Reactions in Light-Water-Cooled Power Reactors	H. A. McLain	23
Emergency Core-Cooling Systems for Light-Water-Cooled Power Reactors	C. G. Lawson	24
Air Cleaning as an Engineered Safety Feature in Light-Water-Cooled Power Reactors	G. W. Keilholtz, C. E. Guthrie, and G. C. Battle, Jr.	25
Testing of Containment Systems Used with Light-Water-Cooled Power Reactors	F. C. Zapp	26
Review of Methods of Mitigating Spread of Radioactivity from a Failed Con- tainment System	R. C. Robertson	27
Earthquakes and Nuclear Power Plant Design	T. F. Lomenick and C. G. Bell	28
Protection Instrumentation Systems in Light-Water-Cooled Power Reactor Plants	H. G. O'Brien and C. S. Walker	29

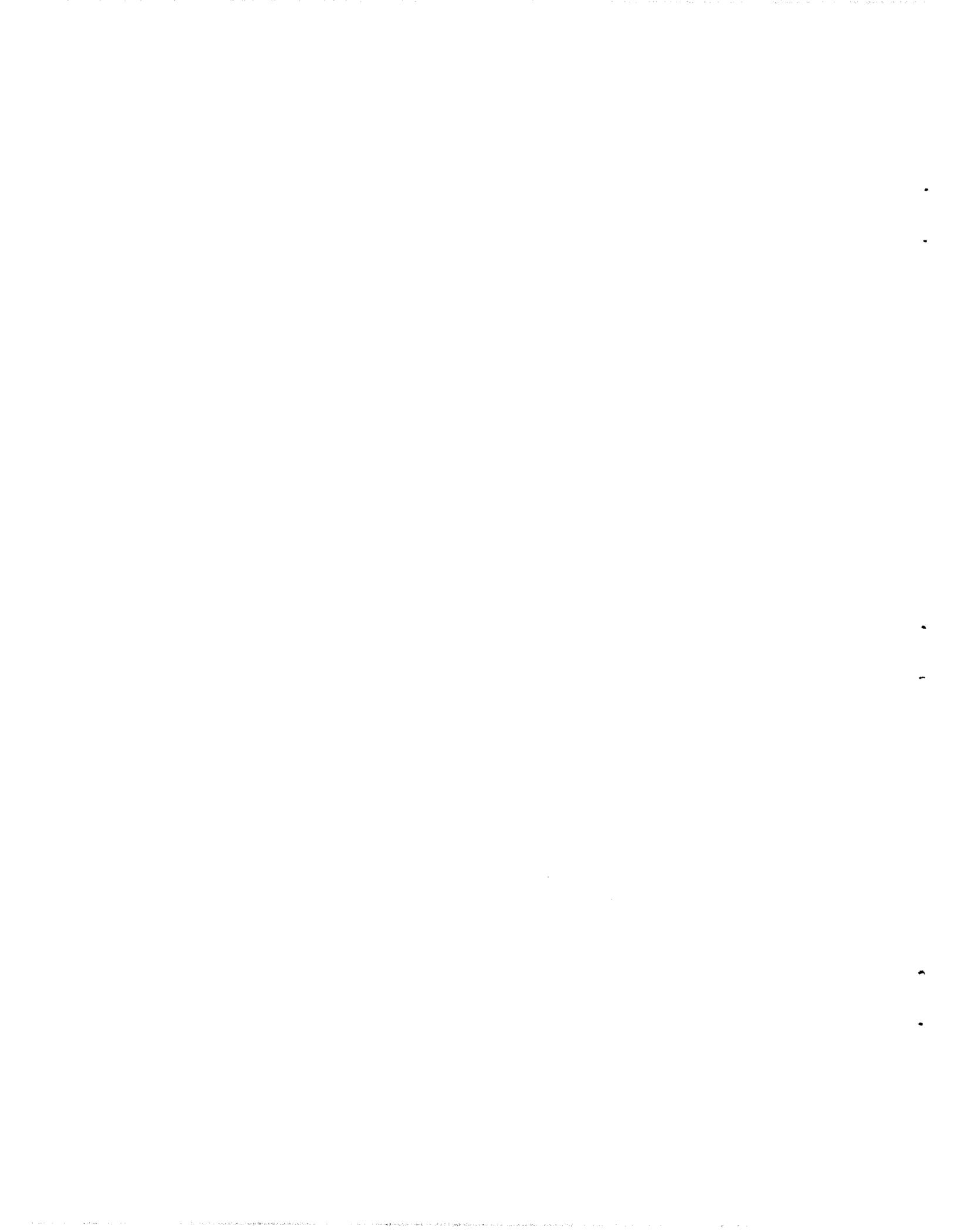
Although not specifically one of this series, a related discussion report on reactor pressure vessels, ORNL-NSIC-21, edited by G. D. Whitman, G. C. Robinson, and A. W. Savolainen, has also been prepared at ORNL.

The general approach in the preparation of these reports was to select a primary author-investigator knowledgeable in the subject area and to establish committees of experts to review the work at several stages during its preparation. Review groups were formed both from within ORNL and outside. The external review committee members were drawn principally from other national laboratories, universities, and private research institutes - in all, 52 individuals participated and are identified in the reports. In some cases, part of the material used was developed and/or written by a subcontractor, who is similarly identified. In all cases, correspondence and/or visits were made to many sources of information, particularly to reactor operators, suppliers, architect-engineers, and public utilities, as well as to the appropriate national laboratories. This wide use of acknowledged experts was made in an attempt to include their opinions and knowledge toward the ultimate goal of achieving, through intensive research and development programs, well-defined design criteria to insure the public health and safety and to maintain a viable nuclear power industry. However, in all instances the authors have expressed conclusions and recommendations that reflect their own judgment and not that of any particular group, such as the AEC, reactor designers, or utilities.

In most subject areas more information was developed than it has been possible to include in the body of the reports prepared in this series. In some instances, such information has been included in the appendices and in other instances this information will be included in more technically oriented reports to be published in the near future. In addition, it is expected that additional discussion reports will be written on some of the many other safety aspects of large water-cooled reactors, as well as other types of reactors as they come into wider usage.

J. W. Michel
Coordinator, Discussion Papers
Oak Ridge National Laboratory

Wm. B. Cottrell
Director, Nuclear Safety Program
Oak Ridge National Laboratory



PREFACE

The Nuclear Safety Information Center was established in March 1963 at the Oak Ridge National Laboratory under the sponsorship of the U.S. Atomic Energy Commission to serve as a focal point for the collection, storage, evaluation, and dissemination of nuclear safety information. A system of keywords is used to index the information cataloged by the Center. The title, author, installation, abstract, and keywords for each document reviewed is recorded on magnetic tape at the central computer facility in Oak Ridge. The references are cataloged according to the following categories:

1. General Safety Criteria
2. Siting of Nuclear Facilities
3. Transportation and Handling of Radioactive Materials
4. Aerospace Safety
5. Accident Analysis
6. Reactor Transients, Kinetics, and Stability
7. Fission Product Release, Transport, and Removal
8. Sources of Energy Release Under Accident Conditions
9. Nuclear Instrumentation, Control, and Safety Systems
10. Electrical Power Systems
11. Containment of Nuclear Facilities
12. Plant Safety Features
13. Radiochemical Plant Safety
14. Radionuclide Release and Movement in the Environment
15. Environmental Surveys, Monitoring and Radiation Exposure of Man
16. Meteorological Considerations
17. Operational Safety and Experience
18. Safety Analysis and Design Reports
19. Bibliographies

Computer programs have been developed that enable NSIC to (1) produce a quarterly indexed bibliography of its accessions (issued with ORNL-NSIC report numbers); (2) operate a routine program of Selective Dissemination of Information (SDI) to individuals according to their particular profile of interest; and (3) make retrospective searches of the references on the tapes.

Other services of the Center include principally (1) preparation of state-of-the-art reports (issued with ORNL-NSIC report numbers); (2) cooperation in the preparation of the bimonthly technical progress review, Nuclear Safety; (3) answering technical inquiries as time is available, and (4) providing counsel and guidance on nuclear safety problems.

Services of the NSIC are available without charge to government agencies, research and educational institutions, and the nuclear industry. Under no circumstances do these services include furnishing copies of any documents (except NSIC reports), although all documents may be examined at the Center by qualified personnel. Inquiries concerning the capabilities and operation of the Center may be addressed to

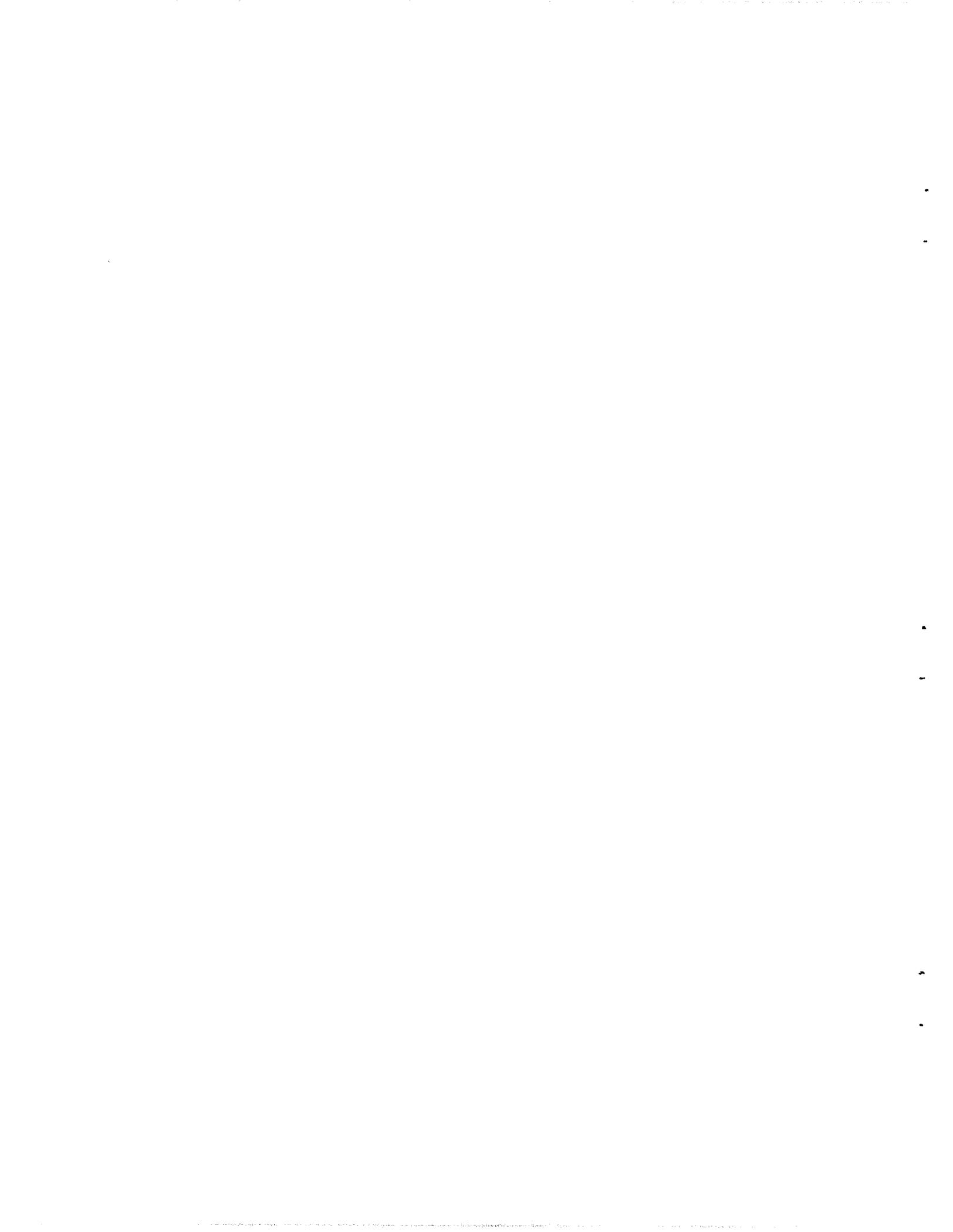
J. R. Buchanan, Assistant Director
Nuclear Safety Information Center
Oak Ridge National Laboratory
Post Office Box Y
Oak Ridge, Tennessee 37830
Phone 615-483-8611, Ext. 3-7253
FTS 615-483-7253

ACKNOWLEDGMENTS

The role and requirements of the instrumentation of reactor protection system have been discussed with many people in the government, industry, and national laboratories, especially at ORNL. Because of these many sources of information, it is impossible to single out and credit any individual for contributions to this report.

All who were contacted gave freely of their time and effort in providing the needed material. Without their interest and help, the preparation of this report would have been impossible.

A list of persons directly associated with the preparation of this report is given in Appendix A.



CONTENTS

	<u>Page</u>
ABSTRACT	xv
1. INTRODUCTION	1
1.1 Role of Protection System	1
1.2 Scope of Review	3
1.3 Terminology	4
1.4 Review of Current Practice	5
2. SUMMARY	7
2.1 Plants Selected	7
2.2 Brief Descriptions of Reactor Shutdown Systems	7
2.2.1 General Features	7
2.2.2 Oconee Nuclear Station	10
2.2.3 Palisades Nuclear Power Station	12
2.2.4 Robert Emmett Ginna Nuclear Power Station	14
2.2.5 Browns Ferry Nuclear Station	14
2.3 Brief Descriptions of Instrumentation Systems for Engineered Safety Features	17
2.3.1 General Features	17
2.3.2 Oconee Nuclear Station	19
2.3.3 Robert Emmett Ginna Nuclear Power Station	19
2.3.4 Palisades Nuclear Power Station	21
2.3.5 Dresden Nuclear Power Plant	23
2.4 General Comments	24
2.5 Summary of Conclusions and Recommendations	25
3. TYPICAL INSTRUMENTATION FOR REACTOR SHUTDOWN SYSTEMS	28
3.1 Oconee Nuclear Station	28
3.1.1 Instrument Channels	28
3.1.2 Logic Arrangement	30
3.1.3 Power Sources	35
3.1.4 Testing Arrangement	36
3.1.5 Isolation of Circuits	37

3.2	Palisades Plant	37
3.2.1	Instrument Channels	37
3.2.2	Logic Arrangement	41
3.2.3	Power Sources	44
3.2.4	Testing Arrangement	45
3.2.5	Isolation of Circuits	46
3.3	Robert Emmett Ginna Nuclear Plant No. 1	47
3.3.1	Instrument Channels	47
3.3.2	Logic Arrangement	49
3.3.3	Power Sources	51
3.3.4	Testing Arrangement	53
3.3.5	Isolation of Circuits	55
3.4	Browns Ferry Nuclear Power Station	56
3.4.1	Instrument Channels	56
3.4.2	Logic Arrangement	57
3.4.3	Control Rod Drive Scram Subsystem	60
3.4.4	Air Supply and Scram Discharge Subsystems	62
3.4.5	Power Sources	64
3.4.6	Testing Arrangement	65
3.4.7	Isolation of Circuits	65
4.	TYPICAL INSTRUMENTATION SYSTEMS FOR ENGINEERED SAFETY FEATURES	67
4.1	Palisades Plant	68
4.1.1	Instrument Channels and Major Functional Requirements	68
4.1.2	Typical Logic Arrangement and Actuation Channel	68
4.1.3	Power Supplies	79
4.1.4	Testing Arrangements	80
4.1.5	Isolation of Circuits	80
4.2	Oconee Nuclear Station, Units 1 and 2	81
4.2.1	Instrument Channels and Major Function Requirements	81
4.2.2	Typical Logic Arrangement and Actuation Channel	83

4.2.3	Power Sources	86
4.2.4	Testing Arrangements	86
4.2.5	Isolation of Circuits	87
4.3	Robert Emmett Ginna Nuclear Plant No. 1	87
4.3.1	Instrumentation Channels and Major Functional Requirements	87
4.3.2	Typical Logic Arrangement and Actuation Channel	89
4.3.3	Power Sources	94
4.3.4	Testing Arrangements	94
4.3.5	Isolation of Circuits	96
4.4	Dresden Nuclear Power Station, Unit 2	96
4.4.1	Instrument Channels and Major Functional Requirements	96
4.4.2	Typical Logic Arrangements	99
4.4.3	Power Sources	109
4.4.4	Testing Arrangements	110
4.4.5	Isolation of Circuits	110
5.	COMPARISON AND DISCUSSION OF INSTRUMENTATION FOR REACTOR PROTECTION SYSTEMS	112
5.1	General Features	112
5.2	Testability of the Instrumentation of the Reactor Shutdown Systems	114
5.3	Effects of Circuit and Component Failures in the Instrumentation of the Reactor Shutdown Systems	117
5.4	Testability of the Instrumentation of the Engineered Safety Features	121
5.5	Effects of Circuit and Component Failures in the Instrumentation of the Engineered Safety Features	122
6.	CONCLUSIONS	128
6.1	Information Availability	128
6.2	System Performance	128
6.3	Design Variances	129
6.3.1	Safety and Serviceability	130
6.3.2	Plant Variables	130
6.4	Optimization of Design Features	131

6.5	Design of Engineered Safety Features	132
6.6	Recent Improvements in Designs	132
6.6.1	Plant Variables Used to Initiate Engineered Safety Feature Action	133
6.6.2	Control Rod Release Circuits	133
6.6.3	Separation of Redundant Actuation Channels	133
7.	RECOMMENDATIONS	134
7.1	Documentation of Designs	134
7.2	Information Needed to Develop Design Bases for Protection Systems	134
7.2.1	Experimental Tests of Accident Consequences	135
7.2.2	Experimental Tests of Spurious Operation of Protection Systems	135
7.2.3	Accident Initiation Rates	135
7.3	Performance Testing Under Accident Conditions	136
7.4	Instrument and Component Tests	136
7.5	Direct Measurement of Safety Variables	137
7.6	Safe Failure Modes	137
7.7	Design of Instrumentation Systems	137
7.7.1	Single Failure	138
7.7.2	Testing Provisions	138
7.7.3	Diversity	139
7.7.4	Interaction Between the Protection and Operation Systems	139
7.7.5	Isolation Between Redundant Channels of the Protection System	140
7.7.6	Energizing to Initiate Protective Action	141
	REFERENCES	143
	APPENDIX A. REVIEWERS, CONSULTANTS, AND INFORMATION SOURCES	147

ABSTRACT

This report describes and comments on the designs of four typical protection instrumentation systems for boiling- and pressurized-water power reactors and states the resulting conclusions and recommendations of the authors. Current practices in protection system designs vary widely, indicating differences in design criteria, as well as the lack of commonly recognized "best ways" in design approaches for carrying out similar functions. Authoritative information on the design bases or assumptions was not available in every case. Design approaches and techniques are in transition. The design of the instrumentation systems for the engineered safety features presents a considerably more complex problem than the design of the reactor shutdown system.

1. INTRODUCTION

The instrumentation systems now being designed for protection of commercial light-water-cooled power reactor plants are described in this report and reviewed from the standpoint of system logic arrangement and features used to achieve a high probability of operating when called upon and at the same time avoiding unnecessary actuation of protective devices.

1.1 Role of Protection System

Instrumentation is used in a nuclear power plant to (1) obtain data on the operation of the plant, (2) provide operational signals for manual or automatic control of the plant, and (3) provide signals that initiate automatic protective actions. This review is concerned only with the instrumentation systems in the third category; that is, those in the protection system.

The purpose of a protection system is to prevent the reactor from reaching unsafe conditions or to mitigate the consequences of such conditions. The consequence of greatest concern is the release of radioactive material (usually fission products) into the primary vessel or secondary containment structure or into the environment outside the plant boundaries in amounts in excess of the limitations imposed by federal regulations.¹ The protection of the public from radiation presents one end of the spectrum of protective requirements. At the other end of the spectrum, the protection system is used to prevent damage to the plant, with accompanying economic loss.

It would not be practical to build a protection system that could cope with every conceivable accident situation, so in practice a set of accidents somewhat more severe than might reasonably be expected to occur is selected as the design basis for the protection system. The design basis includes limits on severity of certain types of environmental conditions, such as earthquakes, fires, and floods, during which protection must be achieved. However, nuclear plant protection systems are not designed to provide assured protection for extremely severe accidents with

magnitudes greater than those selected, on the assumption that the chances of such occurrences are extremely remote.

Typical protection systems include the reactor shutdown system and, where provided, the systems that are necessary for containment, such as emergency core cooling, containment isolation, containment pressure reduction, emergency power sources, and air filtration. The assemblage of equipment required to effect rapid shutdown of a reactor we call the reactor shutdown system, and we take the engineered safety features to include all the other types of protection systems mentioned above.

The reactor operation system consists of the instrumentation, controls, and related devices for routinely starting up, operating, and shutting down the reactor plant. (The term control system is often used to designate the reactor operation system.) The reactor operation system monitors and exercises control with the objective of operating the reactor within its design limits at all times. The operation system may also take minor corrective action to forestall a reactor shutdown. The instrumentation in the operation system includes, in general, all instrumentation in the plant that is not part of the protection system.²

One rather obvious requirement is that the probability of failure of the protection system to carry out a required function when it is needed must be made exceedingly small. A customary manner of meeting this requirement is to provide redundancy of mechanisms and instruments associated with each function. In order to prevent unnecessary interference with plant operation, there is also a strong demand that many of the functions be carried out only when they are needed. Logic arrangements within the instrumentation systems are designed to achieve low probability of failure to function when needed, as well as low probability of spurious action, where detrimental, despite failures of single devices. Such arrangements can require that an action be initiated only when two or more instruments have coincident output signals indicating the need for such action. For example, a two-of-four logic system has input from four instrument channels, and coincidence of trip signals from two of these channels is required to initiate protective action.

1.2 Scope of Review

The design of a protection system involves the major steps of (1) determining the potential (or design-basis) accidents that the protection system must cope with, (2) examining the consequences of these accidents, (3) selecting bounds of permissible or safe reactor behavior, (4) selecting plant variables and sensors that will be used to initiate protective action, (5) determining the type of actions and the performance characteristics the protection systems must have, (6) designing instrumentation, actuators, control rods, valves, emergency cooling pumps, etc., that will provide adequate protection for the reactor and the public for the design-basis accident conditions, and (7) designing system arrangements for the instrumentation and actuators that will initiate protective action with a reliability commensurate with the need. All these steps must be included in the systems engineering approach that is the most important ingredient in achieving adequate protection systems.

This review is centered on the last step in the above list. We have examined the system and logic arrangements used in current designs and the potential reliability of the information-handling systems for initiating protective action. The instrumentation includes all the devices (sensors, amplifiers, signal processors, bistable devices, logic matrices, and associated power supplies, for example) used for sensing the process variables and for handling the transmission of information to the actuators. The instruments are considered as complementary to the system or logic arrangement, and the instruments themselves are discussed primarily in relation to the effects of their failures on the operation of the overall protection systems. A similar treatment is given the actuators, and their sources of power, that carry out the actions initiated by the instrumentation.

Some of the points we emphasize in this review are listed briefly below:

1. coincidence, redundancy, and diversity,
2. logic arrangement,
3. effect of loss of power,
4. on-line testing,

5. single or multiple buses for actuators,
6. isolation of operation and protection systems,
7. isolation of redundant protection system channels,
8. effects of single failure,
9. special problems peculiar to each design.

All these items are associated with the reliability of protection instrumentation systems. An examination of the instrumentation alone is not sufficient to determine whether the protection system is adequate for the potential accidents.

A protection system must provide the necessary functional capability to cope with potential accidents, together with high reliability of so doing when required. This in turn requires high reliability in individual pieces of equipment. The assurance of the functional capability involves a careful examination of all potential accidents, providing protection systems that can mitigate the consequences of these accidents, and an effort to eliminate sources of common mode, or systematic, failures in the protection system. We have not undertaken the difficult tasks of evaluating (1) the design basis, (2) the ability of the protection systems to give adequate protection for potential accident situations, and (3) the performance characteristics of the sensors and actuators. The assurance of high reliability of equipment involves providing long-life equipment and the means for its testing and maintenance, in addition to the nine points listed above. The potential accidents that are currently being considered in the design of power reactors and the emergency equipment provided to cope with these accidents are reviewed in companion papers in this series by Lawson,³ Zapp,⁴ and McClain.⁵

1.3 Terminology

There is considerable variation and confusion over the terminology (or jargon) used in current descriptions of protection systems. The terminology includes, for example, protection systems (formerly safety systems), reactor shutdown systems (or scram systems), secondary shutdown systems, engineered safety features (formerly engineered safeguards), emergency core-cooling systems, containment "control system," etc. For

these reasons, the protection system is defined in some detail above. The remaining terms and nomenclature specific to this field are defined in a report by Hanauer and Walker² that is auxiliary to this report. We have also tried to use the designer's terminology wherever it is reasonably compatible with that used by Hanauer and Walker.

1.4 Review of Current Practice

In this review we examined typical designs of protection instrumentation systems of boiling-water and pressurized-water reactors. There are four suppliers of such reactors in the United States, and correspondingly, there are four somewhat different protection system designs. Boiling-water reactors are supplied by the General Electric Company, and pressurized-water reactors are supplied by the Babcock & Wilcox Company, Combustion Engineering, Inc., and the Westinghouse Electric Corporation. Reference to more than one reactor supplied by a particular company was sometimes necessary to fully illustrate a typical design from the best available information. It is probably worth noting that the design of the protection system (which includes all the engineered safety features) includes efforts of the reactor supplier, the operating utility, and the architect-engineer. For some reactors now being designed the reactor supplier is providing the design of the complete protection system, while in at least one instance (Palisades Station), the architect-engineer is designing the engineered safety features.

The information used in this review was obtained from safety analysis reports and from personal communications during recent months with the manufacturers and operating utilities (and in one case the architect-engineer) associated with the plants discussed. It should be noted that the quantity and detail of descriptive information we obtained varied from plant to plant. Since we wished to examine only the latest plants, the descriptions reflect the latest information; however, since all plants are in the design stage, some final design details may vary from those described.

Criteria for the design of instrumentation systems for reactor protection are in a state of evaluation and are controversial in many respects.

This is another way of saying that standard, or commonly used, methods of solving many design problems have not yet evolved. Criteria are in various stages of development through the efforts of organizations such as the U.S. Atomic Energy Commission,⁶ the International Electrotechnical Commission,⁷ and the Institute of Electrical and Electronics Engineers.⁸ The principles we used in this review are those set forth earlier by Hanauer and Walker.²

Historically the reactor shutdown system and the engineered safety features are described and discussed separately in the safety analysis reports, and therefore we discuss them separately in this report. The reactor shutdown system instrumentation is taken up in Chapter 3, and the instrumentation of engineered safety features is discussed in Chapter 4. The system arrangements are summarized in Chapter 2. We compare and comment on the system designs in Chapter 5. Our conclusions and recommendations are given in Chapters 6 and 7, respectively.

2. SUMMARY

Current practice in the design of protection instrumentation systems for commercial light-water-cooled power reactor plants is summarized and reviewed in this report. These systems are examined with respect to the arrangement of components in systems (rather than the details of the components themselves) and the features provided to achieve a high probability of being able to operate when called upon and at the same time avoiding unnecessary actuation of protective devices.

2.1 Plants Selected

We selected several of the newer plants as examples of current practice in the design of protection systems. These plants, along with their AEC docket numbers, operating utilities, and designers of their protection systems are listed in Table 2.1.

2.2 Brief Descriptions of Reactor Shutdown Systems

2.2.1 General Features

Several types of logic arrangements are used in reactor shutdown systems, but the two-of-three and two-of-four logic arrangements are the most common for the instrumentation. Several system arrangements are used to avoid the possibility that a single failure within the protection system will prevent a scram when one is required. These include redundancy in instrument channels and circuit breakers that interrupt power to the control rod drives to initiate a scram and division of the control rods into separate groups. The instruments and relays in the reactor shutdown systems of all the reactors are deenergized and power to the control rod drives is turned off to initiate a scram. Thus, these systems are fail-safe with respect to loss of power supplies for either the instruments, logic channels, or actuators.

Several system arrangements are used to reduce the chances of a spurious scram caused by the loss of a single power supply and other single failures. In general, all the designs employ coincidence of instrument

Table 2.1. Plants Reviewed

Plant	Reactor Type	Operating Utility	Reactor Supplier
Oconee Nuclear Station, Unit 2	Pressurized water	Duke Power Company	Babcock & Wilcox Company
Palisades Nuclear Power Station	Pressurized water	Consumers Power Company of Michigan	Combustion Engineering, Inc., reactor shutdown system; Bechtel Company, engineered safety features
Robert Emmett Ginna Nuclear Power Station, Unit 1	Pressurized water	Rochester Gas and Electric Company	Westinghouse Electric Corporation
Browns Ferry Nuclear Station, Unit 1 (reactor shutdown system)	Boiling water	Tennessee Valley Authority	General Electric Company
Dresden Nuclear Power Plant, Unit 2 (engineered safety features)	Boiling water	Commonwealth Edison Company	General Electric Company

channel trips and have separate power supplies for the individual instrument channels; most designs have separate power supplies for the multiple matrices (or sets of logic matrices), and most have two parallel (and separate) sources of power serving the control rod drives; so the loss of any of these individual power supplies would not produce a spurious scram. These features also permit on-line testing of instrument channels and logic matrices, as well as interruption of power from individual parallel power supply paths for control rod drives.

Two types of arrangements are used for the instrument channel logic that are here called general and local coincidence⁹ and are illustrated in Fig. 2.1. In a general coincidence arrangement, the output signals

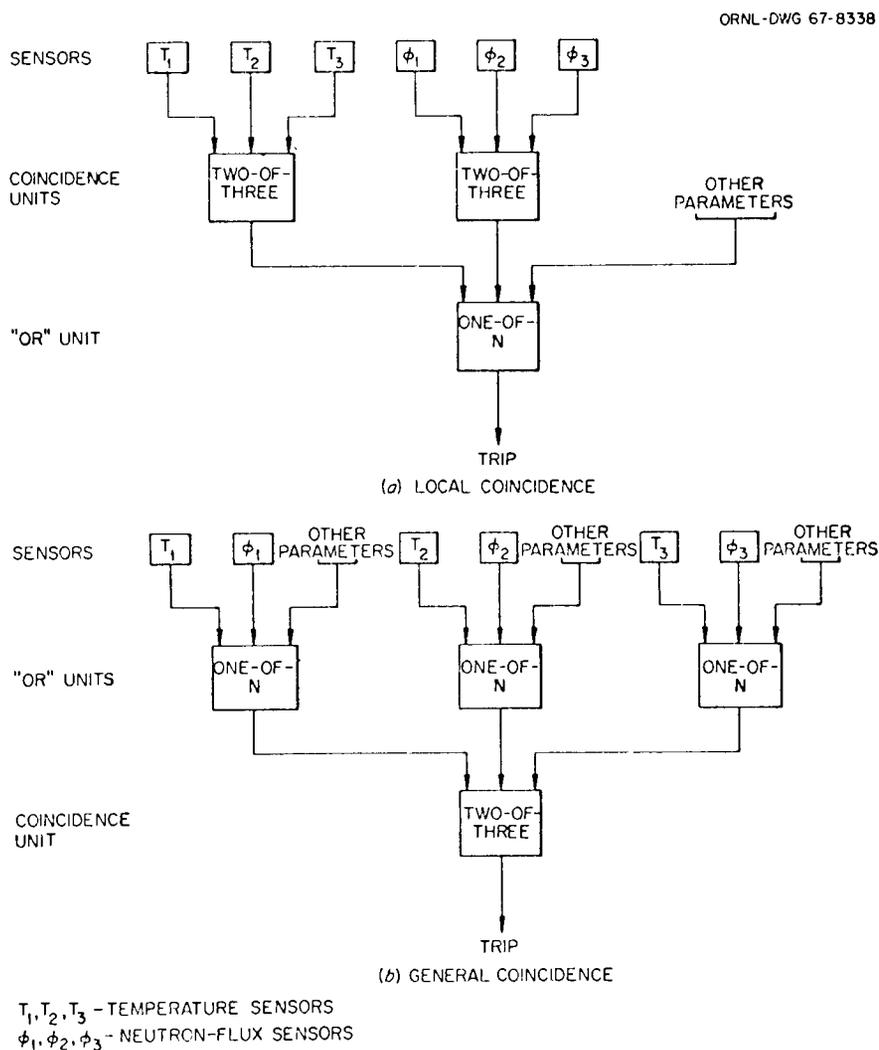


Fig. 2.1. Types of Coincidence Logic.

from one of the redundant channels associated with each plant variable are grouped together to form a one-of-N logic channel. In a system with four instrument channels for each plant variable, there are four one-of-N logic channels (or sets of instrument channels - often designated protection channels). The output signals of the four one-of-N channels feed one or more coincidence logic matrices, and trip signals from two instrument channels (not in the same set or one-of-N logic channel) for either the same or different plant variables initiate system action. In local coincidence, the output signals for the redundant instrument channels for one plant variable feed a coincidence logic matrix. The output signals of the logic matrices for each plant variable are then combined in one or more one-of-N logic matrices, and two instrument channels for the same variable must trip to initiate system operation.

Brief descriptions of the shutdown systems of the following four reactors are given below: Oconee, Palisades, Ginna, and Browns Ferry.

2.2.2 Oconee Nuclear Station

The reactor shutdown system for Oconee is shown in simplified form in Fig. 2.2. In general, four instrument channels for each plant variable feed trip signals (deenergize to trip) to four one-of-N logic channels. These in turn feed four two-of-four logic matrices (deenergize to trip) to form a general coincidence system. Each matrix is arranged to trip one breaker (deenergize to trip). Power from actuator power supply A must flow through two breakers in series to supply the control rod drive buses. These buses are fed in a similar manner from power supply B, and either power supply path is adequate to hold up the control rods. Thus a scram requires trip signals from two instrument channels for the same or different plant variables, trip signals from two one-of-N logic channels, a trip signal from one two-of-four logic matrix in each pair, and the opening of at least one breaker of the pair in each of the parallel power supply paths to obtain a power interruption that initiates a gravity scram. The control rods and release mechanisms are divided into the equivalent of five groups of rod release circuits (or buses) below the first breaker in each power supply path. In "logic language," to obtain a scram the Oconee reactor shutdown system employs the following: a two-

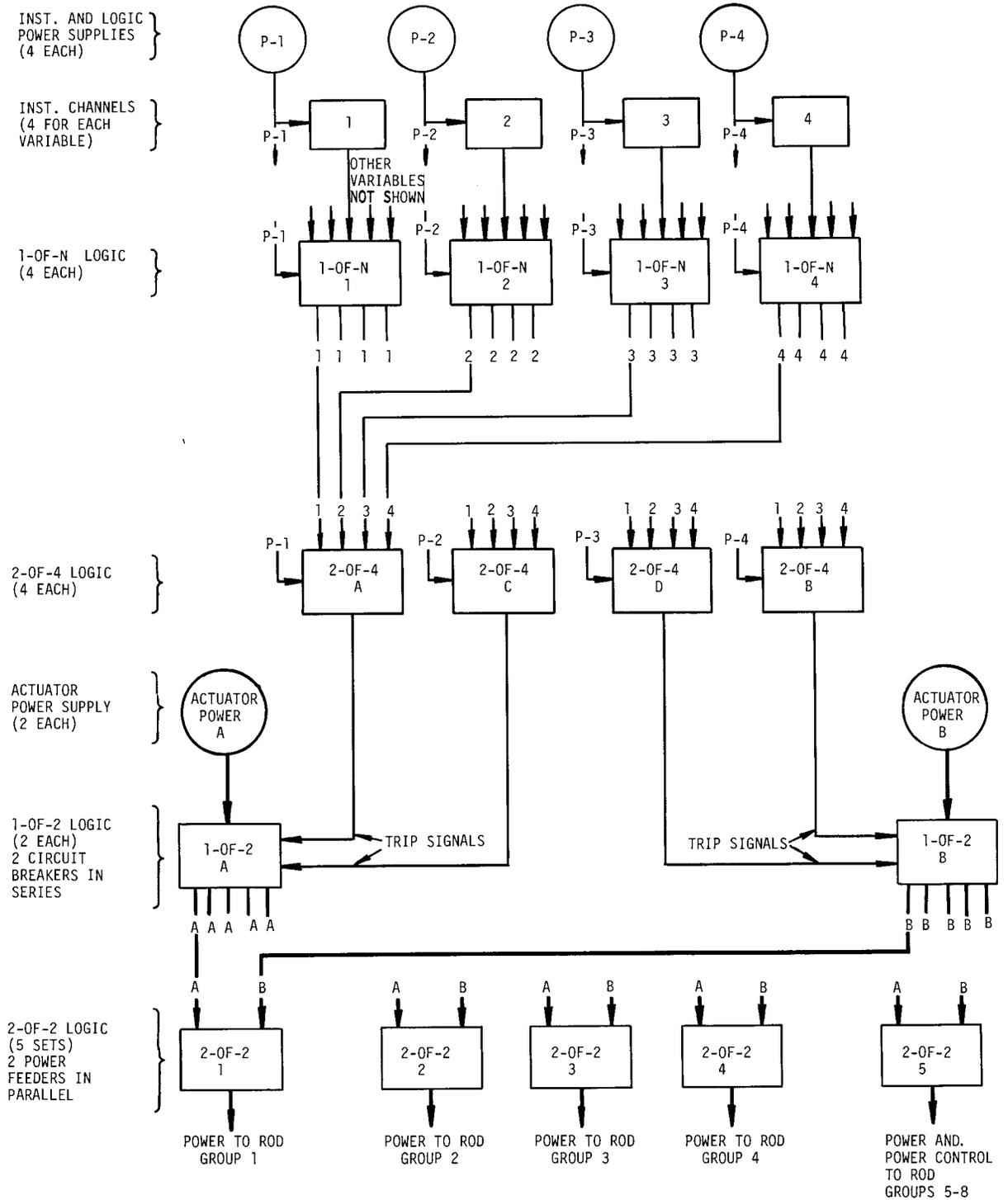


Fig. 2.2. Simplified Logic Diagram for Reactor Shutdown System in Oconee Station.

of-four logic arrangement of the instrument trip signals, a one-of-two logic arrangement of the two logic matrices and breakers that are set to interrupt one actuator power supply path, and a two-of-two logic arrangement for the two feeder systems that supply power to the control rod drives.

2.2.3 Palisades Nuclear Power Station

The Palisades system employs somewhat complex logic arrangements and on-line testing provisions. The system shown in simplified form in Fig. 2.3 actually provides local coincidence in a two-of-four logic arrangement. In most cases four instrument channels monitor each plant variable and feed trip signals (deenergize to trip) to six logic (ladder) matrices. These ladder matrices produce two-of-two logic trip signals (deenergize to trip) for all pair combinations of the four instrument channels. A trip signal from one of the ladder matrices produces trip signals in all four one-of-six logic matrices. These in turn trip all four power trip relays, or contactors (deenergize to trip). Power (120-v ac) from actuator power supply A must flow through the contacts of two power trip relays arranged in series to supply the dc buses for the clutches in the control rod drives. These buses are fed in a similar manner from power supply B, and either of the parallel power supplies is capable of holding up all control rods as a group. Thus a scram requires trip signals from two instrument channels for the same plant variable, a trip signal from one logic ladder matrix, a trip signal from one one-of-six logic matrix in each pair, and the opening of at least one power trip relay in the pair in each of the parallel feeders to interrupt power to clutch buses and initiate a gravity scram. The control rods and release mechanisms are divided into two groups of control rod release circuits (or buses). In "logic language," to obtain a scram the Palisades reactor shutdown system employs the following: a two-of-four logic arrangement of the instrument trip signals, a one-of-two logic arrangement of the two power trip relays that are set to interrupt the actuator power from one feeder line, and a two-of-two logic arrangement of the two feeder lines that supply power to the control rod clutches.

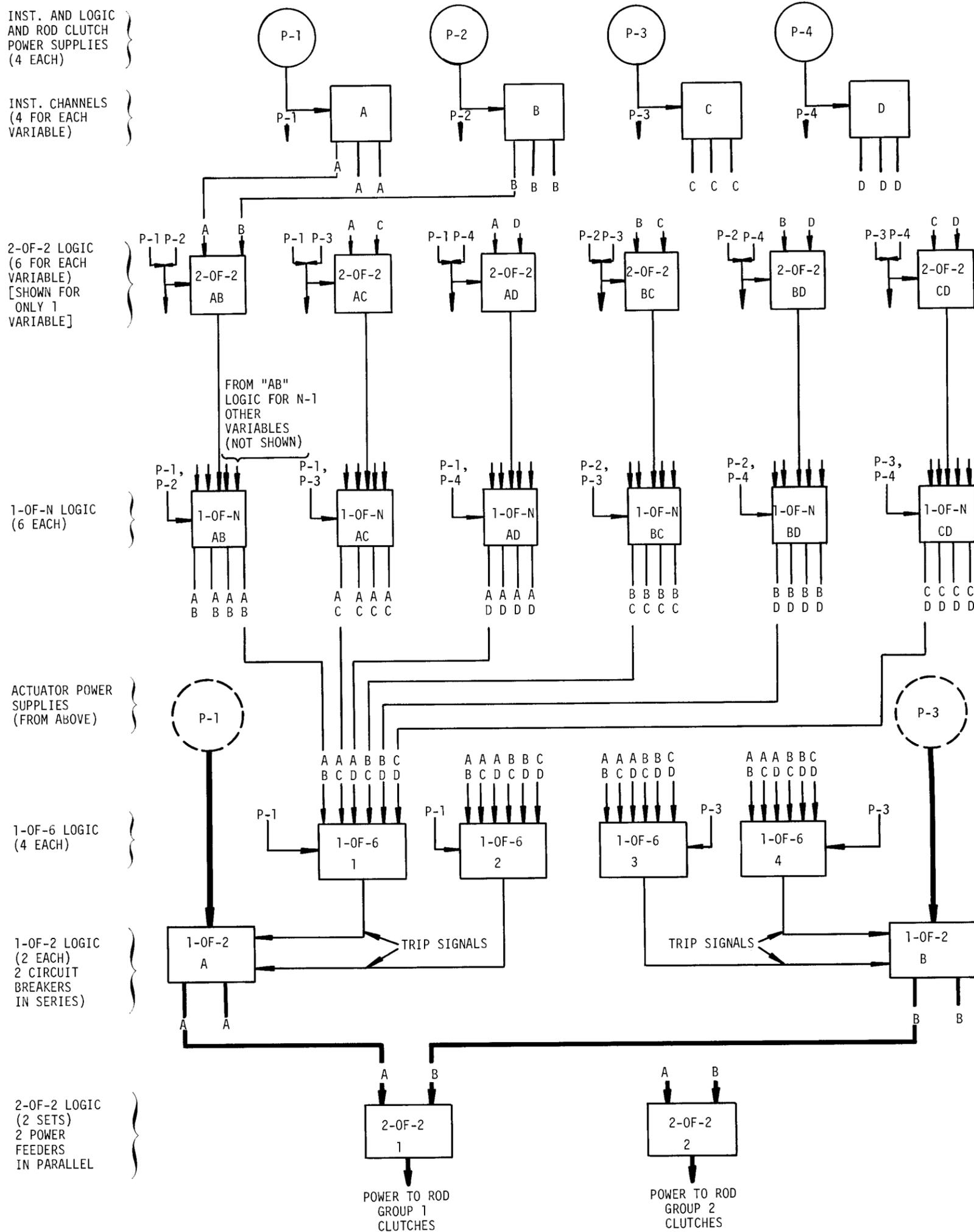


Fig. 2.3. Simplified Logic Diagram for Reactor Shutdown System in Palisades Plant.

2.2.4 Robert Emmett Ginna Nuclear Power Station

The reactor shutdown system for Ginna is shown in simplified form in Fig. 2.4. Different numbers of instrument channels are used for different plant variables. These feed trip signals (deenergize to trip) to two duplicate sets of logic matrices that use local coincidence for each plant variable. The most common arrangement is two-of-four logic. The duplicate logic matrices are connected in series in two separate circuits, or one-of-N logic channels (deenergize to trip). Each logic channel is arranged to trip (deenergize to trip) a circuit breaker. The two "trip" circuit breakers are arranged in series to interrupt the single three-phase ac feeder circuit that supplies power to the control rod drives and initiate a gravity scram. Thus a scram requires trip signals from two instrument channels for the same plant variable, a trip signal from one logic channel (or series of matrices), and the opening of at least one circuit breaker to interrupt power to the control rod drives. The three-phase ac power for the control rod drives is supplied by two motor-generator sets connected in parallel ahead of the trip circuit breakers. In "logic language," to obtain a scram the Ginna reactor shutdown system employs the following: a two-of-four logic arrangement of most of the instrument trip signals, and a one-of-two logic arrangement of two logic channels and breakers that interrupt the power supply path to the control rod drives.

2.2.5 Browns Ferry Nuclear Station

The reactor shutdown system for Browns Ferry is shown in simplified form in Fig. 2.5. In general, four instrument channels for each plant variable feed trip signals (deenergize to trip) to four one-of-N logic matrices as part of a general coincidence system. Two of these in turn feed four one-of-two logic matrices (deenergize to trip). This grouping is designated logic channel A in Fig. 2.5. The other two one-of-N logic matrices feed a similar group of four one-of-two logic matrices in the B logic channel. One one-of-two logic matrix in logic channel A is arranged to deenergize the solenoid of one scram pilot valve in the pneumatic portion of each of the rod drives in one of four groups of rods and rod release circuits. The matching one-of-two logic matrix in channel B deenergizes the second solenoid valve in each of the rod drives in that group.

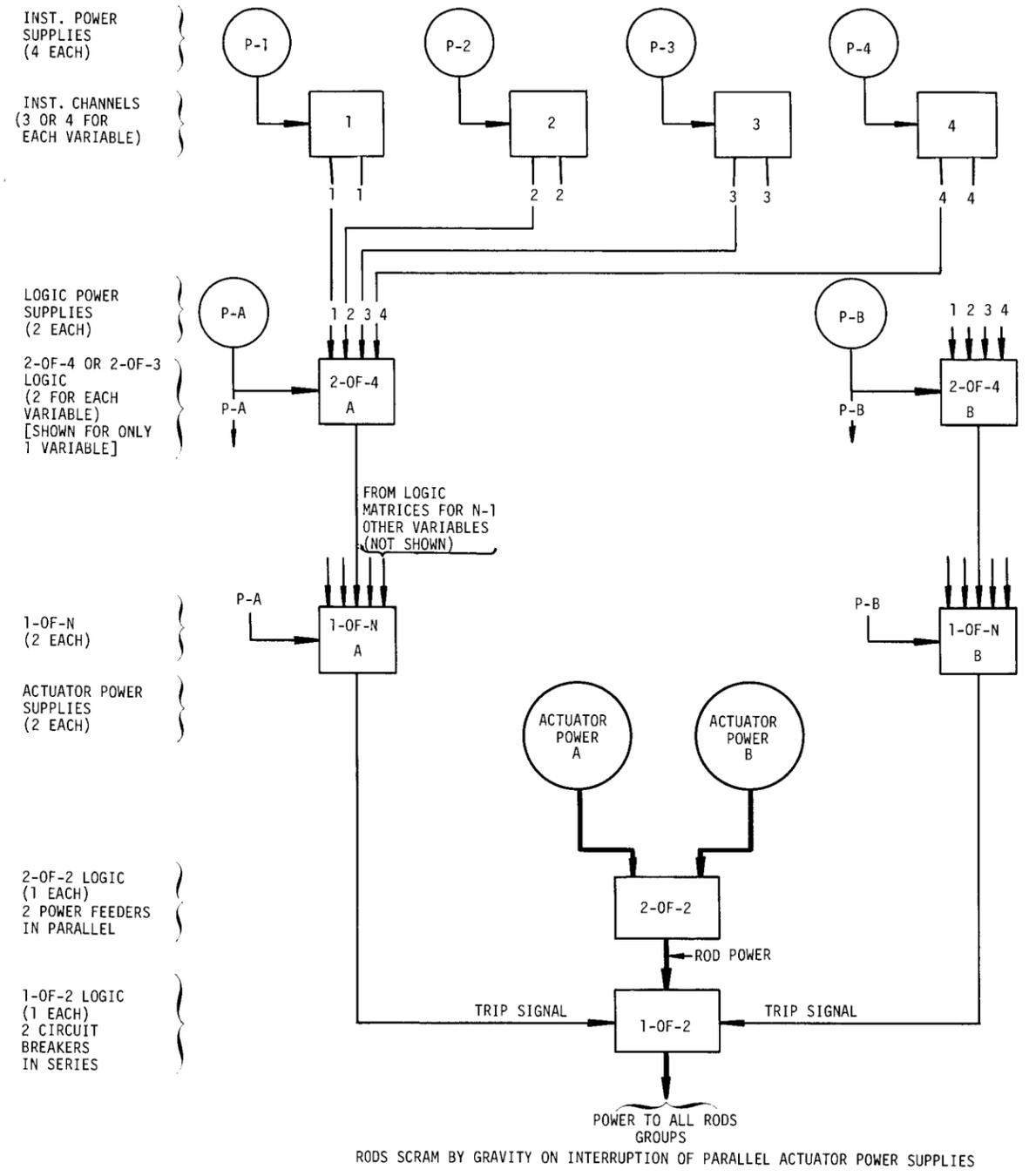


Fig. 2.4. Simplified Logic Diagram for Reactor Shutdown System in Ginna Plant.

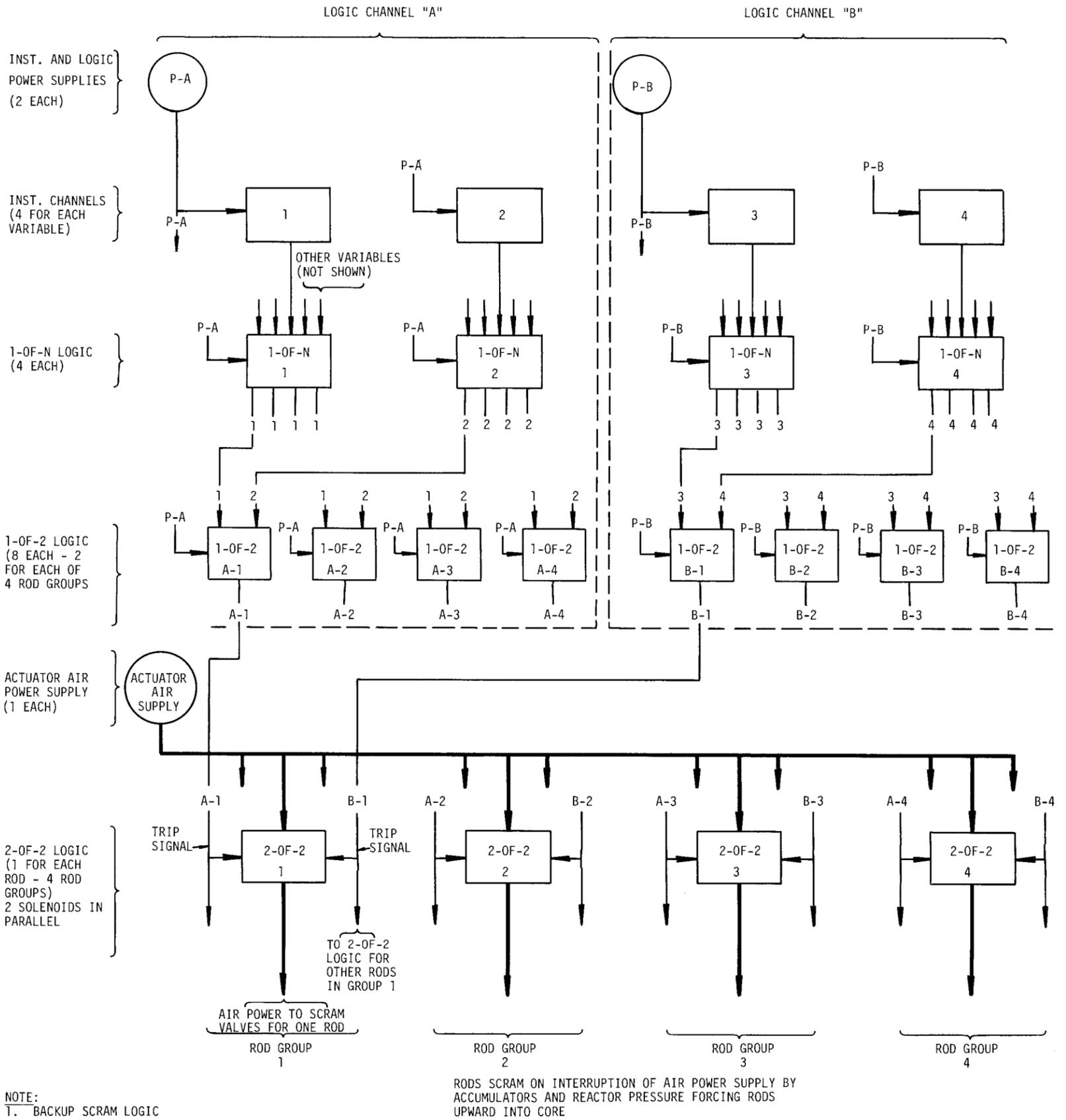


Fig. 2.5. Simplified Logic Diagram for Reactor Shutdown System in Browns Ferry Station.

The two solenoid valves that control each rod drive are arranged so that both must be deenergized to interrupt the air pressure going to the diaphragm operators of the scram valves. This in turn causes water pressure from an accumulator and the reactor vessel to cause the hydraulic drive cylinder to move the control rod upward into the core. Thus a scram requires trip signals from two instrument channels for the same or different variables (with one associated with logic channel A and the other with logic channel B), trip signals from two one-of-N logic matrices (used in different logic channels), trip signals from the one-of-two logic matrices in both logic channels, and the closing of both scram pilot valves to interrupt the air pressure controlling the hydraulic drive cylinder for each rod. A single plant instrument air supply serves all rod drives. A set of backup scram valves, not indicated on the diagram, relieves the air pressure for the entire set of rod drives. In "logic language," to obtain a scram the Browns Ferry reactor shutdown system employs the following: a one-of-two logic arrangement of two sets of two instrument trip signals and a two-of-two logic arrangement of the two logic channels and scram pilot valves that control the hydraulic drive cylinders. This system is often designated as a "one-of-two-taken-twice" arrangement.

2.3 Brief Descriptions of Instrumentation Systems for Engineered Safety Features

2.3.1 General Features

Several system arrangements are used to avoid the possibility that a single failure within the protection system will prevent initiation of engineered safety action. Most engineered safety systems are based on the use of two redundant subsystems, with either subsystem for a particular function being capable of independently carrying out that function. Each subsystem has its own logic system (designated an actuation channel or logic channel), logic power supply, process components (such as pumps), process electric power, etc. The inner containment isolation valves are part of one engineered safety subsystem, and the outer isolation valves in the same pipe line are part of a separate engineered safety subsystem.

A single set of redundant sensors for each plant variable serves duplicate logic matrices in the actuation channels for each of the two subsystems for a given function. Since failure of one subsystem and its associated actuating system and power supply would inhibit the overall engineered safety function, the single-failure criterion is applied on a subsystem basis rather than to the circuits for the individual subsystems. Thus, ordinary relay and motor-control design techniques are used in each of the actuation channels beyond the logic matrix of initiating or inhibiting signals. In general, single relays, contacts, timers, interlocks, etc., are used in the actuation channels, and consequently each of the dual subsystems is subject to single failures that can disable that subsystem.

Several system arrangements are used to reduce the chances of spurious initiation of an engineered safety feature action because of the loss of a single power supply or other single failure. In general, all relays associated with the instrument channels are usually deenergized to initiate engineered safety actions; however, all designs employ coincidence of instrument channel trip signals and have separate power supplies for individual instrument channels, so the loss of an individual supply will not initiate spurious action. The majority of the logic matrices and the logic output, or actuation, relays in the actuation channels must be energized to initiate the engineered safety feature action. The pumps (except those in the high-pressure coolant injection subsystem in Dresden-2) and most of the valves, including those for containment isolation, are motor driven and require electric power to operate. This "trip aspect" for the logic matrices and logic output relays is used to prevent spurious initiation of engineered safety functions on the loss of power supply for the logic matrix in an actuation channel, since spurious operation of some of the engineered safety systems could produce either safety problems or economic penalties. Such a failure of the logic power supply in one actuation channel would prevent one of the engineered safety subsystems from being put into operation (even if actuator power were available); however, this would not prevent the overall engineered safety function from being carried out by the other engineered safety subsystem.

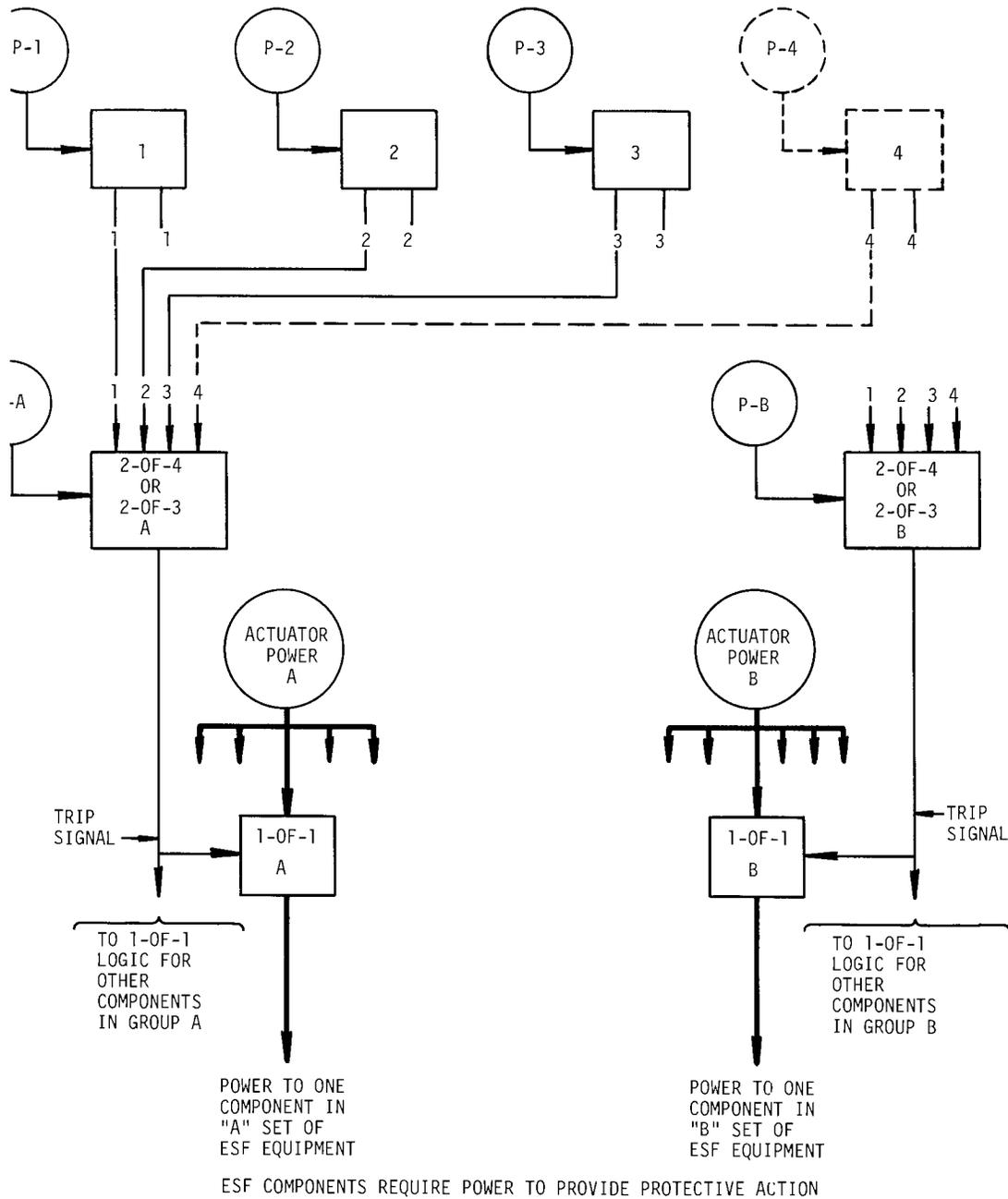
The three pressurized-water plants (Palisades, Oconee, and Ginna) have similar logic arrangements. The simplified logic diagram in Fig. 2.6 illustrates a typical system arrangement. The main differences between the different plants and the various engineered safety systems in one plant are in the logic arrangements of the output signals from the instrument channels in the front portions of the actuation channels. A number of different logic arrangements are used, with two-of-three and two-of-four arrangements being the most common. Figure 2.6 shows only the inputs from one plant variable and thus does not reflect the several different methods used to combine the signals from different plant variables. The initiation of an engineered safety action requires the minimum of trip signals from two instrument channels, a trip signal from a logic matrix, and a trip signal from one actuation channel to start one of the redundant sets of engineered safety equipment for that function.

2.3.2 Oconee Nuclear Station

Three instrument channels for each plant variable are employed in two-of-three logic arrangements with general coincidence of the plant variables in the Oconee system. All engineered safety features have the basic arrangement shown in Fig. 2.6. The instrument channels for initiating reactor building spray are an exception in that six pressure switches are used (three for each matrix in the two actuation channels) rather than the three instrument channels that serve both actuation channels for the other engineered safety functions.

2.3.3 Robert Emmett Ginna Nuclear Power Station

The Ginna engineered safety actuation system also has the basic arrangement shown in Fig. 2.6; however, the initial logic in each actuation channel is somewhat more complicated. For instance, in each actuation channel logic arrangement any one of three pairs of coincident pressurizer low-level and low-pressure signals actuates the emergency core cooling systems. This function can also be initiated by the two-of-three logic matrices for two other variables with local coincidence. Containment spray systems employ coincidence of two sets of two-of-three logic matrices in each of the duplicate actuation channels for that engineered safety



S SINGLE SETS OF MOTORS, VALVES, ETC., TO SERVE EITHER ONE OR SEVERAL ESF FUNCTIONS.
 PMENT PERFORMS THE SAME FUNCTIONS.
 FOR THE INDIVIDUAL MOTORS AND VALVES LATCH-IN OR SEAL-IN ONCE THEY ARE STARTED WITH
 OGIC.
 OF SEVERAL PLANT VARIABLES.

2.6. Simplified (Partial) Logic Diagram for Typical Actuation or Engineered Safety Features at Oconee, Ginna, and Palisades

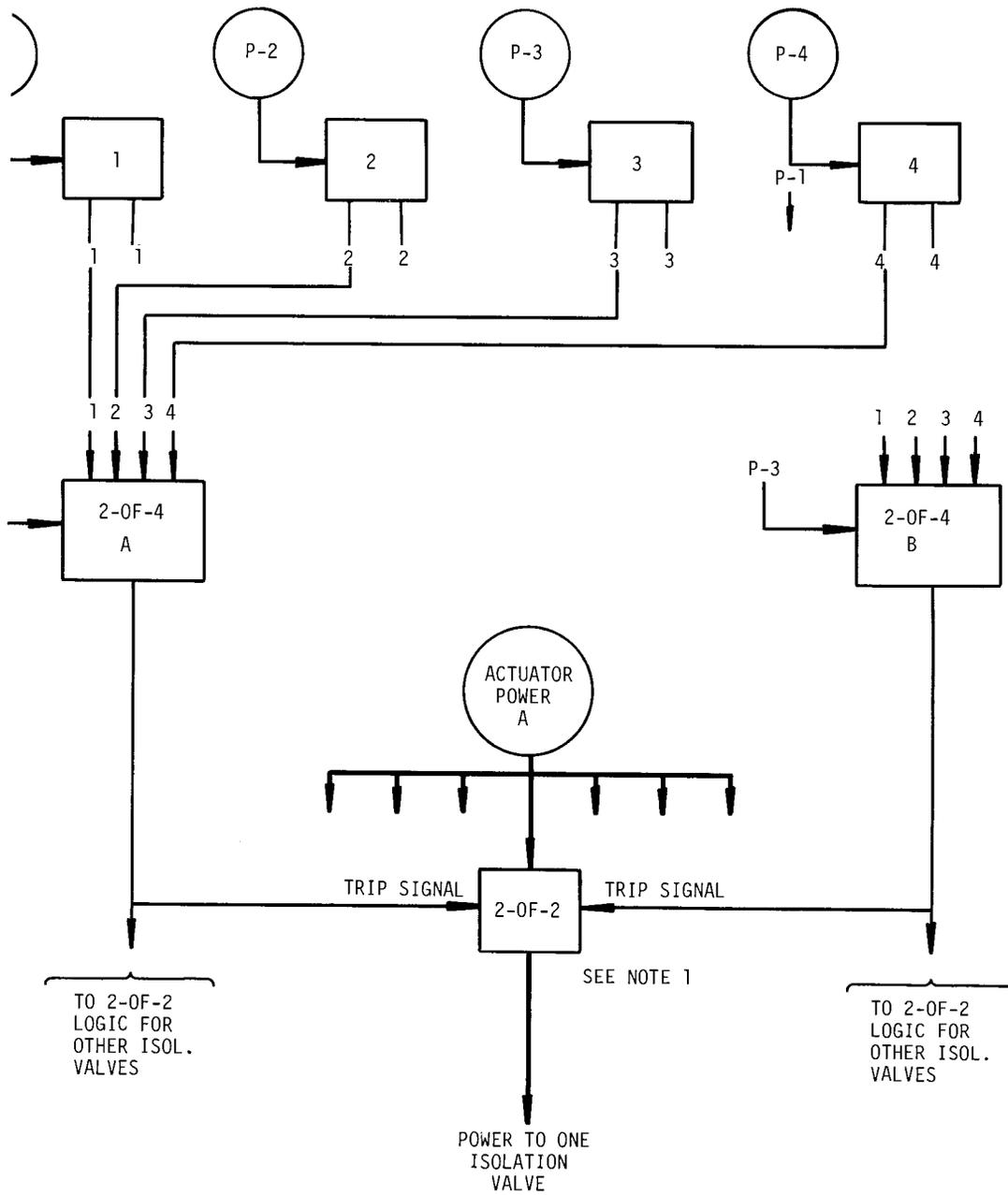
function. Six containment-pressure instrument channels serve these four sets of two-of-three logic. The instrument channels used to initiate the containment spray are exceptions in that they are deenergized to trip, whereas the instrument channels for the other engineered safety functions are energized to trip and initiate action.

2.3.4 Palisades Nuclear Power Station*

Most of the engineered safety actuation systems in Palisades, except the containment isolation system, have the basic arrangement shown in Fig. 2.6. In general, four instrument channels for each plant variable serve duplicate two-of-four logic matrices in each of the two actuation channels. The system uses local coincidence of the plant variables. In one exception to the pattern, the outputs of two two-of-four logic matrices for containment high pressure are combined in a two-of-two logic arrangement in each of the safety injection actuation channels that initiate core and containment cooling, whereas the two two-of-four matrices for the other plant variable that initiates safety injection are used individually in the two safety injection actuation channels.

The containment isolation system in Palisades has a different arrangement, as shown in Fig. 2.7. The two duplicate actuation channels for one plant variable are combined in a final two-of-two logic arrangement in control circuits for the individual isolation valves. The actuation channels for a second plant variable are also combined in a final

*Since the completion of this report in June 1969, G. S. Keeley of Consumer's Power Company has informed us that the designs of the safety injection and containment isolation actuation systems of the Palisades Plant are being revised. The constraints of time did not permit modification of the descriptions; however, in general, both of these actuation systems are being revised to follow the general pattern used in the other two pressurized-water reactors reviewed, which are described briefly in Section 2.3.1 and Fig. 2.6 and in more detail in Section 4.2 for Oconee and in Section 4.3 for Ginna. Each of the two logic matrices will serve a separate actuation channel (i.e., the two-of-two logic arrangements are being omitted), and all the logic matrices will be energized to trip and initiate action. One of the actuation channels in the containment isolation system will control the inner valve in a pipe line, and the other actuation channel will control the outer (redundant) valve in the same line.



VALVE CLOSES ON INTERRUPTION OF ACTUATOR POWER SUPPLY

SHOWN) FROM A SECOND PLANT VARIABLE IS COMBINED WITH THE 2-OF-2 SHOWN IN A 1-OF-2
 FEEDER LINE FOR EACH VALVE.
 AND RESET PERMISSIVE LOGIC IS NOT SHOWN.

7. Simplified Logic Diagram for Containment Isolation Actuator at Palisades Plant.

two-of-two logic arrangement in the individual valve control circuits, and the two-of-two signal from either plant variable can close the valves. The instrument channels and the initial two-of-four logic matrices are similar to those in the other engineered safety systems; however, the logic and actuating relays are deenergized to trip and initiate containment isolation. The valves are held open by air pressure against a spring, so they are fail-safe with respect to actuator power. The simplified logic diagram does not show the logic used in resetting the isolation signal.

2.3.5 Dresden Nuclear Power Plant

The actuation systems in Dresden-2 differ somewhat from those in the other three reactors. In some cases, different types of engineered safety subsystems are used to serve the same function in Dresden-2. Thus many of the instrument channels are shared between subsystems serving the same function; however, other instrument channels are unique to one of the subsystems. In general, four instrument channels feed trip signals to a one-of-two-taken-twice logic arrangement similar to the General Electric reactor shutdown system described in the previous section for Browns Ferry. A logic arrangement similar to that shown in Fig. 2.5 is used to initiate the operation of one of the subsystems. Most engineered safety systems have two differences from the reactor shutdown system - the instrument channels and the logic and actuating relays are energized to trip and start engineered safety actions, and most of the logic systems employ local coincidence for each plant variable. The logic arrangements for the coolant admission valves in the low-pressure emergency cooling subsystems are somewhat more complicated in that the initiation of valve opening requires a one-of-two logic arrangement of two reactor low-pressure sensors in addition to the usual one-of-two-taken-twice logic arrangement for the two main plant variables that initiate operation of the remainder of the subsystems.

The containment isolation systems differ from the remainder of the engineered safety systems in Dresden-2 in that the logic and actuating relays are deenergized to initiate action. The two one-of-two logic channels have separate power supplies, so the loss of one logic power supply does not produce spurious isolation. The main steam-line isolation

valves are held open by air pressure against a spring, so they are fail-safe with respect to the loss of actuator power.

2.4 General Comments

All protection instrumentation systems, whether for reactor shutdown or engineered safety features, use electromechanical relays in the logic system and employ coincidence and redundancy for the large majority of the plant variables. The reactor shutdown systems have the system arrangements and features described in the early part of Section 2.2 to achieve a high probability of being able to operate when called upon and at the same time avoid unnecessary actuation of protective devices. There are a few exceptions to the general pattern, since a spurious scram could be caused by the loss of the single compressed air supply in Browns Ferry or a dc logic power supply in either Ginna or Palisades.

All the systems for reactor shutdown have provisions for a certain amount of on-line testing. The procedures in Oconee, Palisades, and Ginna test the transmission of trip signals from two instrument channels or one-of-N logic channels through the majority of the logic system. In Browns Ferry, the only coincidence is made at each rod drive, and the trip signal of a single instrument channel is transmitted to this point. In all these plants, the final devices, such as circuit breakers, power relays, or scram pilot valves, are exercised during on-line testing. Two of the plants, Palisades and Ginna, require some bypasses during on-line testing. In Palisades, bypassing is provided by the energization of a second coil on the mercury-wetted contact relays to inhibit the trip signal during on-line testing. In Ginna, bypass breakers are used to electrically bypass the main trip breakers.

The engineered safety actuation systems use the system arrangements and features described in the early part of Section 2.3. A few notable exceptions to the pattern include the containment-spray system in Ginna, the containment isolation systems in Palisades and Dresden-2, and part of the safety injection system in Palisades.

Most engineered safety systems have provisions for a certain amount of on-line testing, but the approach differs considerably from one design

to another. For instance the operation of the main logic output, or actuation, relays is tested on-line in the Palisades plant, but the instrument channels and logic matrices are not. In contrast, the on-line tests in the Ginna plant include the matrices but not the actuation relays. In Ginna, the pumps and some of the valves in the engineered safety system can be operated individually for testing while the plant is running. In Palisades, the pumps and some of the valves can be test-operated simultaneously as a system while the plant is running. The logic test in Ginna requires that the output of the logic matrix be bypassed, and the pumping system test in Palisades requires that some "inhibit" actions be set up by a test switch.

All these plants have provisions for bypassing or blocking the reactor trip signals and engineered safety actuation signals, as required, to permit normal operation for conditions other than those at rated power. All, except Ginna, have protection system instrumentation that is physically separate from the active controllers in the operation system.

2.5 Summary of Conclusions and Recommendations

The information in the safety analysis reports of the plants reviewed was inadequate for this state-of-the-art review, particularly in the area of engineered safety actuation systems. We recommend accordingly that more comprehensive and uniform descriptions of the features of the plants be provided in the safety analysis reports. Further, we feel that reasonably consistent terminology and drawing symbols should be adopted and used in all descriptions of protection systems.

The protection instrumentation systems for the engineered safety features generally present much more difficult design problems than do those for the reactor shutdown systems. There are wide differences in the designs of the instrumentation systems reviewed that are probably indicative of different design bases, as well as variations in past experience of the designers themselves. During the two-year course of this study, we have seen a number of changes in the designs of these systems, and many of these represent worthwhile improvements. They have included the addition of diversity in plant variables that initiate action, elimination

of some vulnerabilities to potential single failures that could prevent a reactor scram, and improvement in the isolation between redundant elements. We believe that design criteria or functional performance criteria, and possibly some detailed standards, are needed in the protection system field. We recommend that the design criteria include statements on the following: diversity in plant variables used to monitor the approach to one safety limit, diversity in sensors to measure one plant variable, application of the single-failure criterion to complex systems, adequate testability during plant operation, isolation between redundant protection system channels, independence of the operation and protection systems, direct and indirect measurements of safety variables, and the choice of energized or deenergized logic systems to initiate protective actions.

A protection system must provide the necessary functional capability to cope with potential accidents, together with high reliability of individual pieces of equipment. The design of a reliable system includes meeting the general requirement of being able to initiate action despite a single failure. This does not, however, insure adequate functional capability of the instrumentation and the entire protection system. We feel that the functional adequacy of a complete protection system depends heavily on the proper application of a systems engineering approach. In addition, we recommend that protection systems be studied with the intent of finding every possible failure mode, including sources of common mode or systematic failures, and that a rationale regarding the probability of such failures be developed. Again, criteria and standards for all segments of protection systems are needed, and many such criteria and standards are being developed under AEC auspices.

Testing of each type of instrument at least once under realistic accident conditions is needed to gain further assurance that the system will perform as required. The design bases for reliability requirements of protection systems involve consideration of acceptable frequency of occurrence of particular accidents and initiation rates for these accidents. Factual, experimental data are needed on the consequences of potential accidents so that acceptable frequencies of occurrence can be established. Data from operating reactors are needed on the rates at

which the protection systems are challenged in order to establish probable accident initiation rates.

3. TYPICAL INSTRUMENTATION FOR REACTOR SHUTDOWN SYSTEMS

Brief descriptions and discussions of typical protection instrumentation systems for reactor shutdown systems are given in this chapter. The instrumentation reviewed provides signals to initiate emergency reactor shutdowns (scrams). The systems chosen as representative are those in the Oconee Nuclear Station supplied by Babcock & Wilcox, the Palisades Plant by Combustion Engineering, the Ginna Nuclear Power Plant by Westinghouse, and Browns Ferry Nuclear Power Station by General Electric. We attach no significance to the order in which these plants are discussed and wish to point out that the descriptions may not reflect the latest information because all these plants are in the design stage and some details may vary.

3.1 Oconee Nuclear Station

3.1.1 Instrument Channels*

The Babcock & Wilcox Company is providing four instrument channels for each of the important variables in the reactor shutdown system of the Oconee Nuclear Station.¹⁰⁻¹² A simplified diagram of the instrument channels is shown in Fig. 3.1. There are four channels for each of the following: neutron flux in the power range, reactor coolant pressure, and reactor coolant outlet temperature. There are two logarithmic neutron flux channels that provide trip signals on high rate change in flux over the range from intermediate through 10% of rated power.

Each of the neutron flux channels for the power-range trip signals receives its input from the combination of three out-of-core ion chambers. The three chambers used in one flux channel are arranged in a vertical

*After the preparation of this report, the final safety analysis report was issued, which indicates that the plant variables that initiate a reactor shutdown have been changed. The neutron flux startup rate has been omitted as a trip signal, and a pressure/temperature trip signal has been added that is similar to the thermal-margin/low-pressure trip signal used in the Palisades reactor shutdown system (see Table 3.2). The operational bypass of the low reactor coolant pressure trip signals has been omitted.

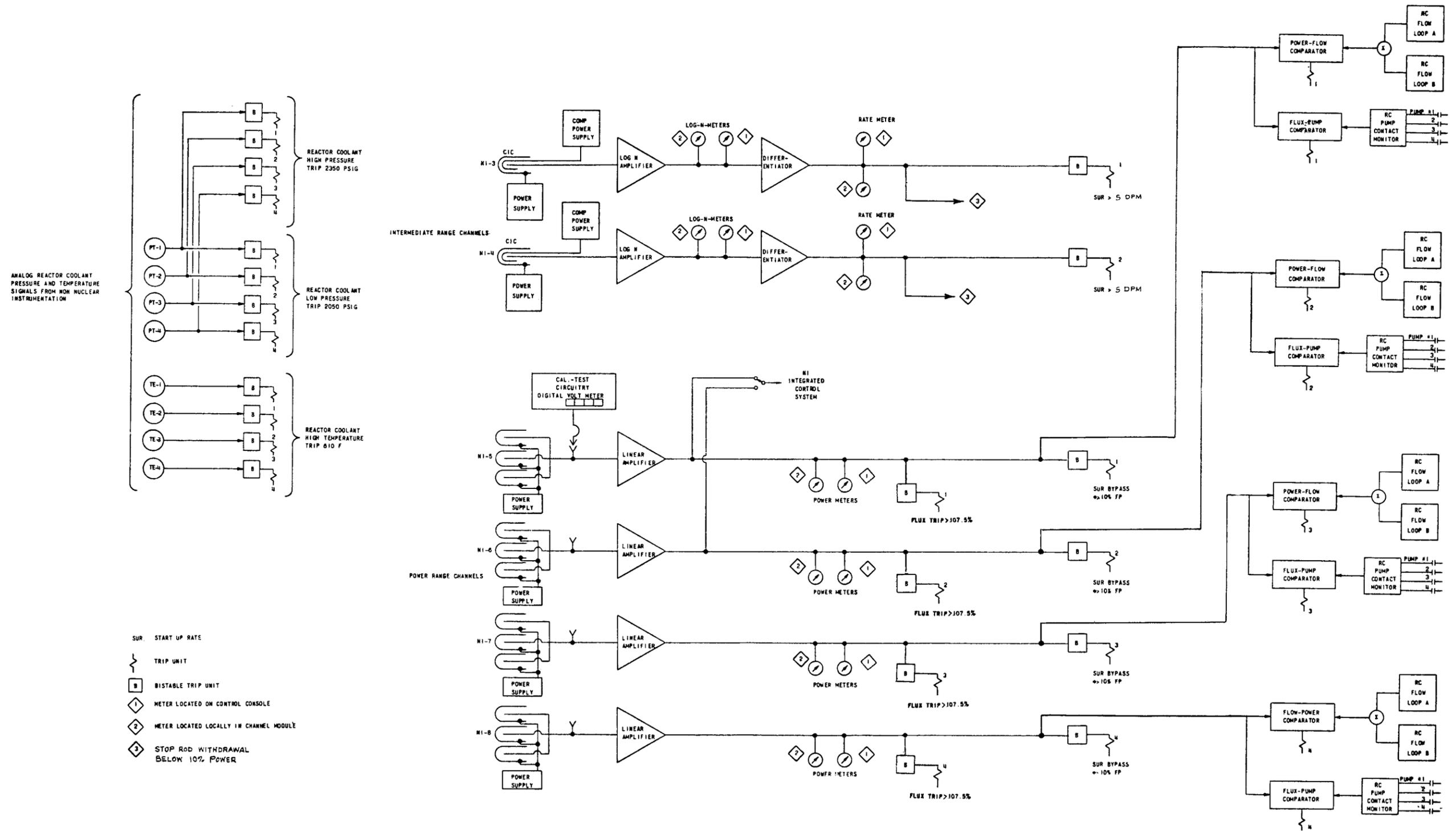


Fig. 3.1. Simplified Instrument Channels for Reactor Shutdown System in Oconee Station. (From Ref. 11 with additions)

column with one chamber near the bottom, one at the center, and one near the top.

Flow measurements from each of the two coolant loops, as well as circuit breaker monitoring signals from each of the four coolant pumps, are used with the power-range neutron flux measurements to provide trip signals related to the ratio of neutron flux to coolant flow and neutron flux to number of coolant pumps in operation. The comparators for power versus flow and flux versus number of operating pumps are basically variable set points for neutron flux trip bistable devices. The comparator of flux versus number of operating pumps gives an immediate trip signal on loss of power to certain combinations of coolant pumps. The circuit-breaker monitoring signals are obtained by means of auxiliary contacts operated by the breakers.

Abnormal conditions that initiate reactor scram signals are listed in Table 3.1. Separate sensors are used for all the trip variables listed, except that the same four flux sensors are used for both neutron flux and the ratio of neutron flux to reactor coolant flow, and both high and low reactor coolant pressure trip signals are taken from the same sensors.*

The bypass of trip signals from high startup rate of neutron flux, indicated in Table 3.1, is applied and removed automatically as a function of neutron flux level.* The trip signals on low reactor coolant pressure can be bypassed manually to prevent a scram during plant startup and during cooldown and depressurization.* This bypass can only be initiated under the conditions indicated in Table 3.1, and the bypass is automatically removed after the coolant pressure exceeds 2100 psig (normal operating pressure range is 2120 to 2250 psig). The bypassing is done on a channel-by-channel basis, with a separate bypass circuit for each low-pressure bistable unit and with the startup rate trip contacts bypassed by the power-range neutron flux channel associated with the same one-of-N logic channel. This is illustrated in Figs. 3.1 and 3.2.

3.1.2 Logic Arrangement

The overall two-of-four logic arrangement of the reactor shutdown system is shown in Fig. 3.2. Contacts from the trip units in the instrument

*See footnote on p. 28.

Table 3.1. Automatic Scram Trip Signals at Oconee Nuclear Station

Plant Variable	Number of Sensors	Trip Set Point or Condition for Trip	Bypasses
1. Neutron flux	4 (shared)	107.5% of full (rated) power	None
2. Ratio of neutron flux to reactor coolant flow	4 flux (shared) 16 reactor coolant pump monitors 2 flow tubes	<ol style="list-style-type: none"> 1. Loss of power to one operating coolant pump motor and reactor neutron power in excess of a predetermined level 2. Loss of power to one operating reactor coolant pump motor in each loop and reactor neutron power in excess of 50% of rated power 3. Loss of power to two operating reactor coolant pumps in one loop 4. Ratio of reactor neutron power to total reactor coolant flow in excess of 1.07 	None
3. Startup rate	2	5 decades/min	Bypassed above 10% neutron flux
4. Low reactor coolant pressure	4 (shared)	2050 psig	Manual bypass permitted between 2050 to 2100 psig and at startup pressure; bypass removed by coolant pressure above 2100 psig
5. High reactor coolant pressure	4 (shared)	2350 psig	None
6. Reactor outlet temperature	4	610°F	None

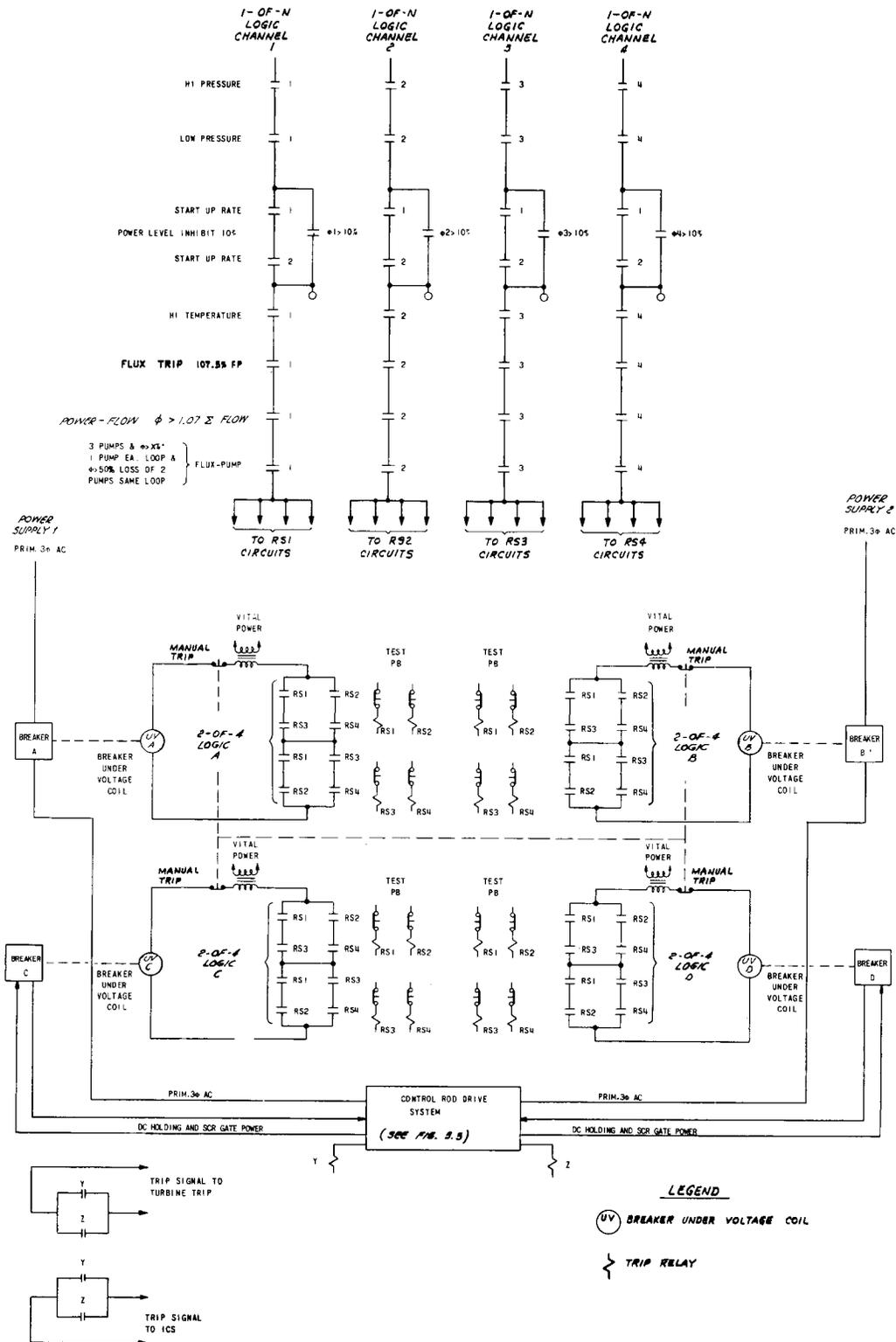


Fig. 3.2. Logic Circuits for Reactor Shutdown System in Oconee Station. (From Ref. 11 with additions)

channels are arranged in four one-of-N logic channels. Each logic channel controls the power to a set of four reactor trip relays, designated RS1 for logic channel 1, etc. The instrument channels are deenergized to trip. Opening a logic channel by opening one or more trip contacts deenergizes the four reactor trip relays associated with that channel.

The contacts from the reactor trip relays in each logic channel are used in four two-of-four logic matrices. These four matrices are identical, and the system uses general coincidence of all plant variables. The logic matrices control the undervoltage coils of the four circuit breakers, and the matrices and coils are deenergized to trip and open the circuit breakers.

The circuit breakers are used to interrupt two parallel sources of three-phase ac power that feed the dc holding power supplies for the four safety groups of control rods and the silicon controlled-rectifier (SCR) switching power supplies for the four regulating groups of control rods. Loss of actuator power causes the rods of both groupings to fall into the core under the influence of gravity. The actuator power control system for the rod drives is shown in more detail in Fig. 3.3. All 69 rods have a roller nut type of drive, but they are divided into four groups (1 through 4) of safety rods and four groups (5 through 8) of regulating rods that have somewhat different actuator control circuits. The rods are moved by applying dc stepped power through the SCR switching power supplies. The SCR gate signals are generated by a motor-driven programmer motor. The regulating rods are held in position by dc current from the SCR switching power supplies. The auxiliary SCR switching power supply is provided to withdraw the safety rods, one group at a time. When fully withdrawn, each safety group is transferred to the hold bus.

Each rod group is powered by two parallel ac feeder lines. These in turn supply either the dual dc holding supplies for the safety rod groups or the dual units of the SCR switching power supplies. Two of the breakers (A and C) interrupt one of the power supply paths (i.e., a one-of-two logic arrangement). The first breaker in the series interrupts the ac feeder line, and the second breaker interrupts either the dc holding power or the SCR gating signal (which turns off the SCR's). The other breakers (B and D) interrupt the parallel power supply path in a

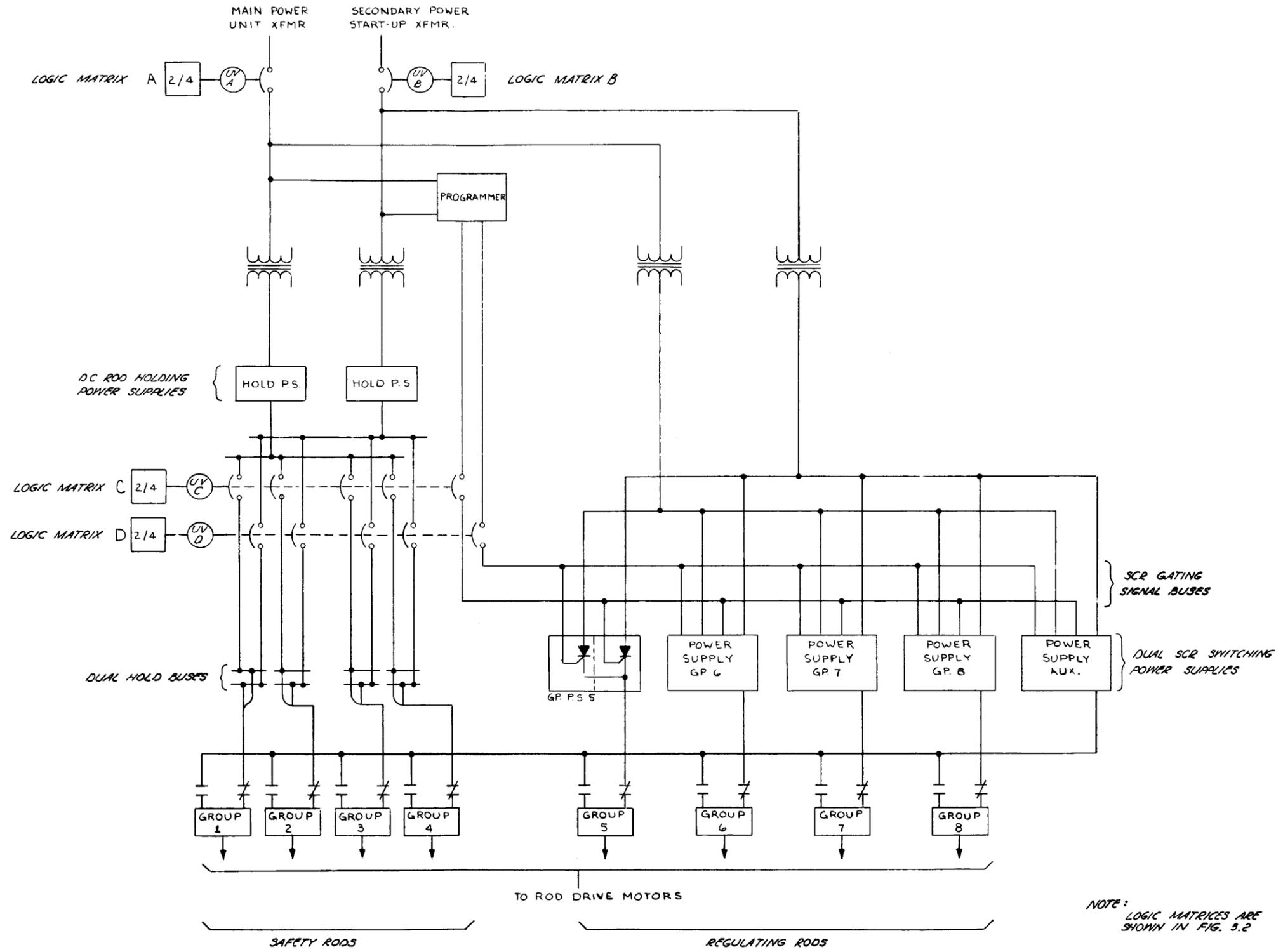


Fig. 3.3. Control-Rod Release Circuits for Reactor Shutdown System in Oconee Station. (From Ref. 11 with additions)

similar fashion. Either of the parallel power supply paths is capable of holding up all control rods, so both paths must be interrupted to produce a scram (i.e., a two-of-two logic arrangement). With this arrangement, deenergizing one circuit breaker, say A or C, will turn off one power supply path, and then deenergizing either of the two circuit breakers, B or D, in the other supply path will give a scram. The use of redundant power supplies avoids spurious scrams from loss of one power supply path or breaker and permits on-line testing of the interruption of the power from these supplies.

The safety rods are divided into four groups with separate sets of dual hold buses for each group, as shown in Fig. 3.3. These groups are controlled by the same set of two-of-four logic matrices; however, Babcock & Wilcox¹¹ has stated that the five-pole breakers shown in Fig. 3.3 may become four or more individual breakers. The regulating rods are also divided into four groups, but the SCR gating signals are driven by dual buses that are common to all four groups.

In summary, a scram requires trip signals from any two instrument channels, trip signals from two one-of-N logic channels, a trip signal from one two-of-four logic matrix in each pair, and the opening of at least one circuit breaker in the pair in each of the parallel power supply paths to interrupt power to the control rod drives.

3.1.3 Power Sources¹²

Power to the reactor shutdown system instrumentation is from a single-phase 120-v 60-cycle supply through four vital instrument buses. Each bus supplies power to one of the four instrument channels of Fig. 3.1, as well as to the corresponding logic channel of Fig. 3.2. We presume that each of the four two-of-four logic matrices is powered separately from these vital instrument buses.

A static inverter supplies the ac power to each vital instrument bus from one of four 125-v dc power panelboards. If power is lost on a dc power panelboard, circuit breakers can be used to disconnect the static inverter and reconnect the vital instrument bus to a regulated 120-v ac instrument bus. The connection to the alternate 120-v ac regulated bus may also be used to permit the inverters to be serviced.

The dc system (for the three-reactor station) includes six 125-v dc batteries connected to provide three 125/250-v dc independent sources. There is a normally open tie with dual circuit breakers between each of the three 125/250-v dc buses. Each of the 125-v sections of a battery bank normally floats on the line with dc power supplied by a battery charger. Nine chargers are used, six for normal service and one for each pair of 125-v battery sections as a spare.

There are six 125-v dc control power panelboards, each being fed from two of the three 125-v dc independent sources. Each panelboard is connected through two diodes in series in each leg to the 125/250-v dc independent sources. A combination of four of the six panelboards is used for each reactor in the three-reactor station.

Alternating-current power for the control rod drive dc power supplies is taken from two separate ac sources. Each source is supplied from a transformer that is connected to a separate 4.16-kv supply.

3.1.4 Testing Arrangement

The analog portions of the instrument channels are checked during reactor operation by visually comparing the output of similar channels. The bistable devices and part of the amplifiers in the analog portions of the channels are tested on-line by substituting an analog test signal at the input of the first active channel element in the protection system cabinets. The test signal is carried over the dynamic range to test the trip-point setting, zero drift, etc.

Coincidence allows on-line tests to deenergize the RS relays connected to each one-of-N logic channel in Fig. 3.2. In addition, the test push button (PB) in series with each RS relay permits each circuit breaker to be tripped individually by deenergizing appropriate pairs of RS relays. Thus, each power source for the control rod drives can be interrupted during on-line testing. The second parallel power supply to the rods prevents the rods from actually being released while the first is being interrupted. Once a circuit breaker has been tripped during a test, all remaining pairs of combinations of RS relays are deenergized in sequence. A monitoring relay in parallel with the undervoltage coil on each breaker indicates whether the undervoltage coil has been turned off. This provision is

included to prevent the need for circuit breaker operation at each portion of the test and subsequent rapid wear out.¹¹

3.1.5 Isolation of Circuits

The circuits of the reactor shutdown instrumentation system are isolated from those of the operation system and use equipment physically separate from the active control part of the operation system, except for unidirectional control actions (such as rod withdrawal prohibits) that can only move the plant away from the safety limits.^{11, 12} The output signal, shown in Fig. 3.1, from the power-range flux channels N1-5 and N1-6 to the integrated control system has been replaced by the output from an additional flux channel that is only used in the active control system. One protection instrument channel for each of three of the plant variables - neutron flux, coolant flow, and coolant pressure - can be used as an alternate input to the active control system. Isolation amplifiers, not shown in Fig. 3.1, supply each signal taken from an instrument channel, whether the signal is used for protection or unidirectional control.

Devices in the four instrument channels and in the four logic channels are physically isolated.¹¹ Either four separate cabinets or two cabinets divided by a barrier are used. Four relays, rather than one, are used on each protection channel in order to allow for more isolation between channels in the circuit breaker tripping circuits. Cable runs are routed and protected to maintain separation of the four channels.

The control rods and release mechanisms are divided into the equivalent of five rod groups of rod release circuits (or buses) below the first breaker in each power supply path.

3.2 Palisades Plant

3.2.1 Instrument Channels

Combustion Engineering, Inc., is designing a reactor shutdown system¹³⁻¹⁵ for the Palisades plant that in general provides four instrument channels for each of the important plant variables. The automatic scram trip signals and the bypasses are listed in Table 3.2, and a diagram of a typical instrument channel is shown in Fig. 3.4.

Table 3.2. Automatic Reactor Shutdown Trip Signals at Palisades Plant

Plant Variable	Trip Set Point	Bypasses
1. High rate of change of neutron flux	2.6 decades/min	Bypassed below $10^{-4}\%$ and above 15% neutron flux
2. High neutron flux		None
Four-pump operation	106.5%	
Three-pump operation	82.25%	
Two-pump operation	53.5%	
3. Low reactor coolant flow		Manual bypass permitted below $10^{-4}\%$ neutron flux; bypass removed by neutron flux above $10^{-4}\%$
Four-pump operation	95%	
Three-pump operation	71%	
Two-pump operation	48%	
4. High pressurizer pressure	2400 psia	None
5. Thermal margin/low pressure	1750 psia to 2500 psia (depending on the primary coolant temperature) ^a	Same as item 3 above
6. Low steam generator water level (either steam generator)	Top of feedwater ring (6 ft below normal water level)	Same as item 3 above
7. Low steam generator pressure (either steam generator)	500 psia	Same as item 3 above
8. Loss of load		Bypassed below 15% neutron flux

^a $P_{\text{set}} = 57T_{\text{h}} - 30T_{\text{c}} - 15,800$, where P_{set} is the thermal-margin/low-pressure set point in psia, T_{h} is outlet coolant temperature, and T_{c} is inlet coolant temperature.

Each of the neutron flux channels for the high flux trip in the power range receives its input from the sum of the outputs of the upper and lower half-sections of an out-of-core ion chamber that monitors the full height of the core. The high-power trip set points can be lowered by a factor of 10 with a range-selector switch in each channel.

Provisions are made in the reactor shutdown system to permit operation at reduced power if one or more coolant pumps are taken out of

service. For operation with one or two pumps inoperative, both the low-flow trip set points and the high-neutron-flux trip set points are simultaneously changed by a manual switch to the allowable values for the selected pump condition (see Table 3.2).

The thermal-margin/low-pressure trip is used to prevent reactor conditions from allowing the departure-from-nuclear-boiling ratio to fall below 1.3. As indicated in Fig. 3.4 and the footnote to Table 3.2, this is accomplished with a low-pressure trip whose set point is continuously computed from measured reactor inlet and outlet coolant temperatures. There is an additional limit that prevents the trip set point from falling below 1750 psia.

Four instrument channels are used to generate the signals necessary to initiate automatic reactor shutdown, except for the loss-of-load and high rate-of-change of neutron flux trip signals, for which two measuring channels are used. Both these plant variables are considered to be anticipatory trip signals, and they are not required to prevent the safety limits from being exceeded. Two trip signals are developed in each of these instrument channels so that the two channels for each of these variables can serve the overall four-channel logic system. The rate-of-change signals are developed in two wide-range logarithmic neutron flux channels. The loss-of-load channels are unique in that they use energize-to-trip relays; whereas, the remainder of the reactor shutdown system instrument channels use deenergize-to-trip relays.

The bypasses of trip signals from two plant variables - high rate of change of neutron flux and loss of load - are applied and removed automatically as a function of neutron flux level, as indicated in Table 3.2. This is done on a channel-by-channel basis by the flux instrument channel that is in the same basic set of instrument channels (i.e., protection channel) as the trip signal being bypassed. Four other plant variables listed in Table 3.2 (items 3, 5, 6, and 7) can be bypassed manually with key-operated switches to permit subcritical testing and low-power operation. One bypass switch removes one instrument channel trip for each of these four plant variables in one of the four basic sets of instrument channels. Thus four bypass switches are employed. These bypasses are automatically removed when the neutron flux level exceeds $10^{-4}\%$. This is

also done on a channel-by-channel basis by the flux instrument channel that is in the same basic set of instrument channels (protection channel) as the trip signals being bypassed.

The bypasses mentioned above have the feature of automatic removal. In addition, key-operated switches are provided to bypass the trip signal from individual instrument channels for maintenance (see Fig. 3.4). Since this type of bypass is not automatically removed with increasing reactor power, these bypasses are limited to only one channel of the four provided for any one plant variable by providing only one key for the four bypass switches for that variable.

Most instrumentation channels for the nonnuclear plant variables have electronic transmitters that generate dc analog-type signals.

3.2.2 Logic Arrangement

The overall two-of-four logic arrangement of the reactor shutdown system instrumentation is shown in simplified form in Fig. 3.5 and in more detail in Fig. 3.6. The four instrument channels for each plant variable are designated A through D. The trip module in each instrument channel has three module trip relays for use in the reactor shutdown system logic arrangement. These relays are the mercury-wetted-contact type and are deenergized to trip. The contacts of the module trip relays are connected to form six logic ladder matrices that give a two-of-two logic trip signal for all combinations of four instrument channels. These logic ladder matrices are designated A-B, A-C, A-D, B-C, B-D, and C-D, and they are deenergized to trip. The contacts of a given module trip relay are used in only one logic ladder matrix (for isolation purposes). As shown in Fig. 3.6, the coincidence is required on an individual basis for each plant variable. Thus, the reactor shutdown system employs local coincidence (or individual logic), and a scram is initiated only if there are a minimum of two trip signals pertaining to a given plant variable.

The output of each logic ladder matrix controls a set of four relays, designated logic trip relays, that deenergize to trip. The contacts from the four relays of the set from each logic ladder matrix output are placed in series with corresponding contacts from the remaining five logic-ladder-matrix sets to form four one-of-six logic matrices. These four one-of-six

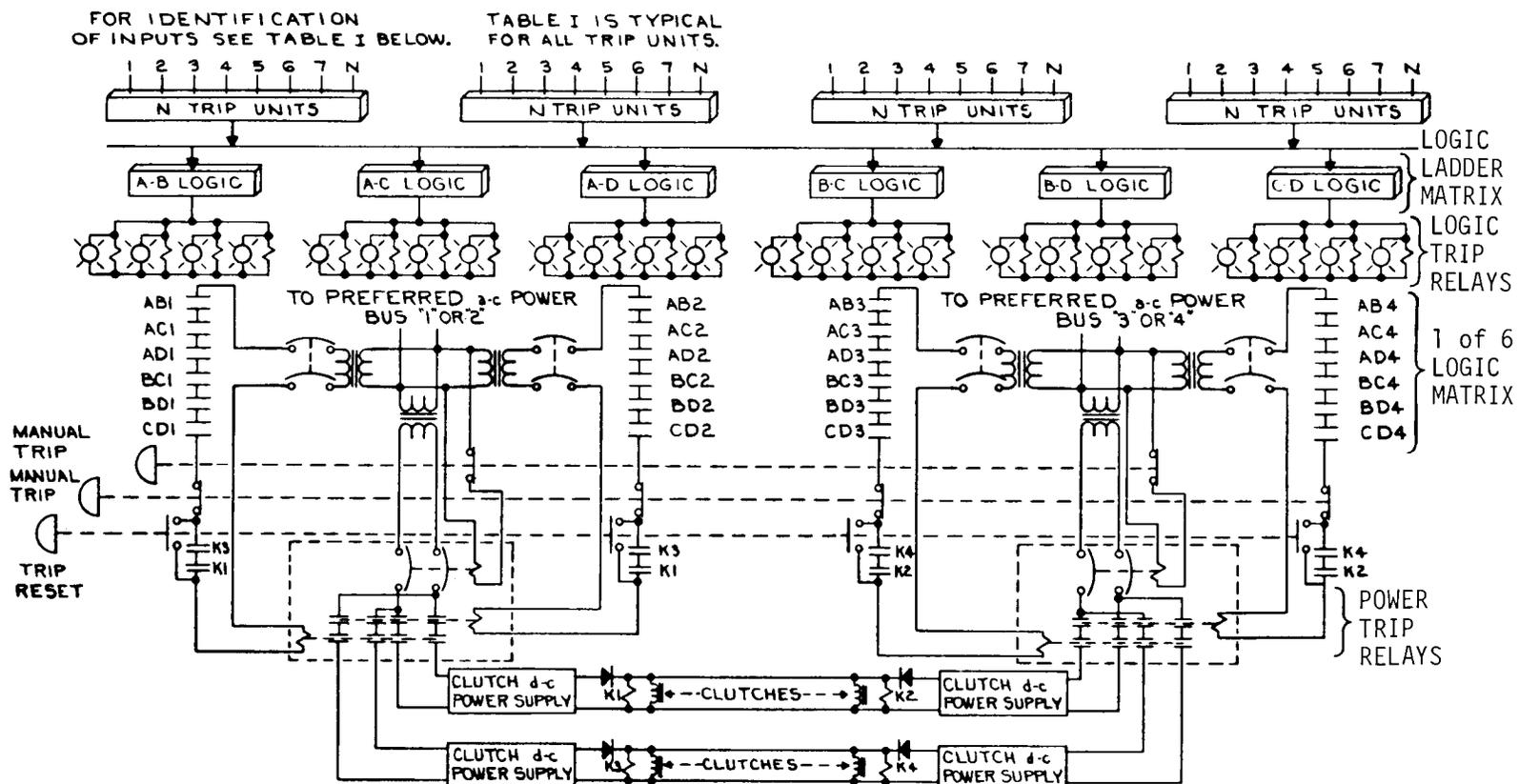


TABLE I	
1	HIGH POWER LEVEL
2	HIGH POWER RATE OF CHANGE
3	LOW FLOW, REACTOR COOLANT
4	LOW WATER LEVEL, STEAM GENERATOR 1
5	LOW WATER LEVEL, STEAM GENERATOR 2
6	LOW PRESSURE, STEAM GENERATOR 1
7	LOW PRESSURE, STEAM GENERATOR 2
8	HIGH PRESSURIZER PRESSURE
9	THERMAL MARGIN/LOW PRESSURE
10	LOSS OF LOAD, TURBINE TRIP

Fig. 3.5. Simplified Logic Circuits and Control-Rod Release Circuits for Reactor Shutdown System in Palisades Plant. (From Ref. 13 with additions)

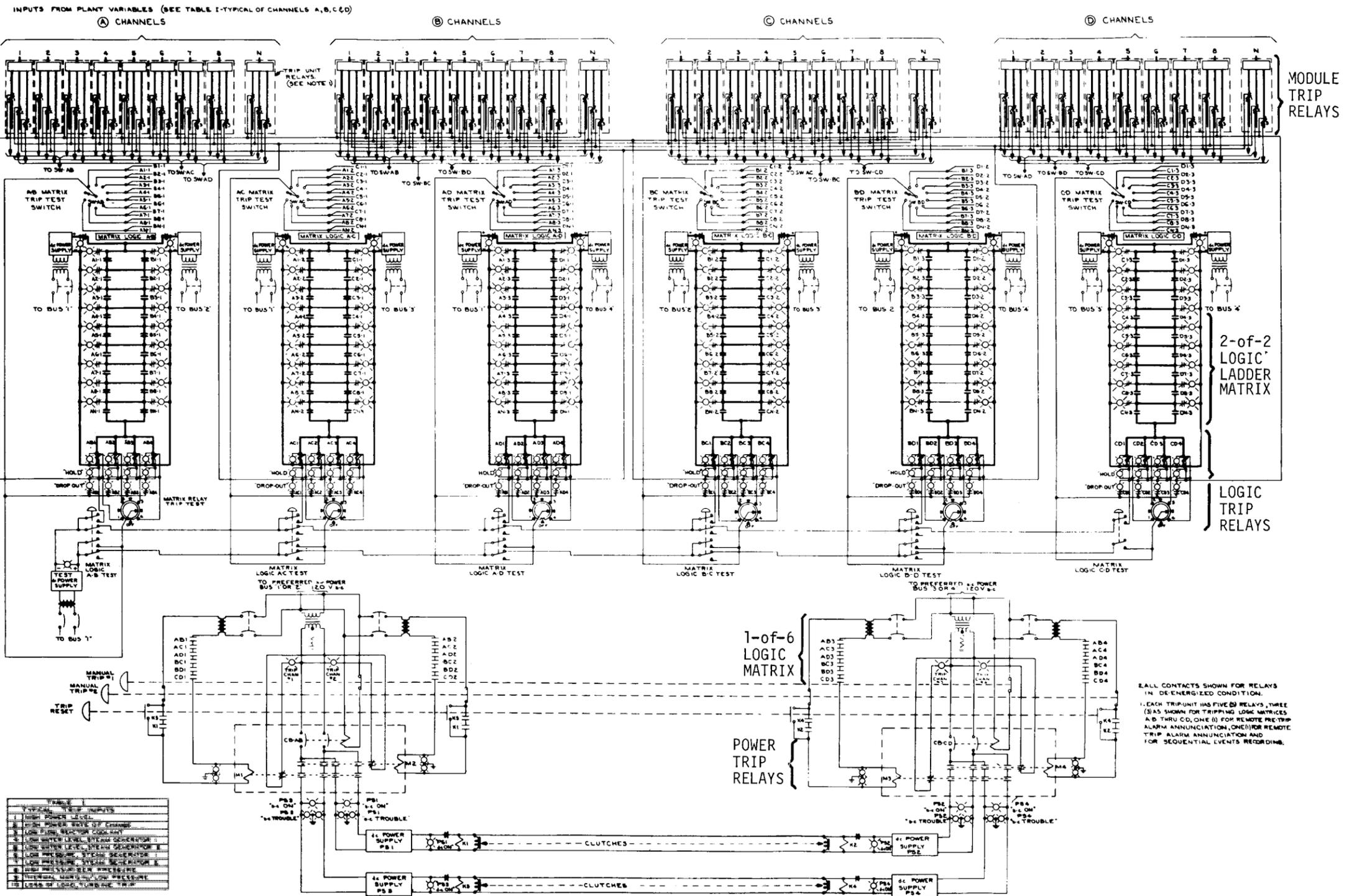


Fig. 3.6. Detailed Logic Circuits and Control-Rod Release Circuits for Reactor Shutdown System in Palisades Plant. (From Ref. 13 with additions.)

logic matrices control four power relays that are deenergized to trip. Thus, a trip signal from one of the logic ladder matrices trips all four power trip relays (or contactors).

The power trip relays are used to interrupt two parallel sources of 120-v ac power that feed the dc power supplies and buses that energize the clutches of the control rod drives. Loss of this dc power releases the clutches and allows the control rods to drop into the core under the influence of gravity. The contacts of two of the power trip relays are placed in series in one of the ac feeder lines (i.e., one-of-two logic), and the other two power relays control the parallel feeder. Either of the parallel power supplies is capable of holding up all control rods as a group, so both feeders must be interrupted to produce a scram (i.e., a two-of-two logic arrangement). With this arrangement, deenergizing one power trip relay turns off one dc supply, and then deenergizing either of the two power trip relays for the other dc supply gives a scram. The use of redundant power supplies avoids spurious scrams from loss of one power supply and permits on-line testing of the interruption of the power from these supplies. The control rods are divided between two sets of dc supplies and buses; however, each clutch bus is controlled by the same set of power trip relays.

In summary, a scram requires trip signals from two instrument channels for the same plant variable, a trip signal from one logic ladder matrix, a trip signal from one one-of-six logic matrix in each pair, and the opening of at least one power trip relay in the pair in each of the parallel feeders to interrupt power to the clutch buses.

3.2.3 Power Sources

The power for the four sets of instrumentation channels is supplied from four separate "preferred" 120-v ac buses. The preferred buses are powered by four inverters from two independent 125-v dc buses. These dc buses are supplied from the 480-v system through battery chargers. A station battery floats on each dc bus to give continuity in power.

Each of the six logic ladder matrices is supplied through two rectifiers in parallel from separate preferred 120-v ac buses (to avoid a spurious scram from the loss of power in one logic ladder matrix). The

parallel power supplies for the control rod clutches are fed from separate preferred 120-v ac buses.

It appears that loss of one of the two 125-v dc buses would produce a scram by tripping two of the instrument channels and also by interrupting both preferred 120-v ac buses serving one or more logic ladder matrices. However, loss of one of the four preferred 120-v ac buses would open one of the parallel feeders to the clutch buses but would not produce a scram.

The control rod drives are separated into two groups with a set of two parallel dc power supplies for each of the groups, as shown in Fig. 3.5. The preferred 120-v ac buses are fed from an isolation transformer having a grounded center tap. The dc clutch power circuits are ungrounded.

3.2.4 Testing Arrangement

The on-line testing arrangements employ a combination of some common and some unique features. The analog portions of the instrument channels are checked during reactor operation by visually comparing the output signals of similar channels. The trip modules are tested by inserting a voltmeter in the circuit, noting the signal level, and initiating a test input (from an external test generator) that is also indicated on the voltmeter. The trip action is indicated by lights on the trip module. The wide-range logarithmic and power-range neutron flux channels have internal pulse and current generators for channel test and calibration.

The logic ladder matrices, logic trip relays, and power trip relays are tested, one at a time, with the arrangement shown in Fig. 3.6. The module trip relays and logic trip relays have dual coils (a normal operation coil and a test coil) for use in the on-line testing of the logic system. In testing a logic ladder matrix (e.g., AB), a holding current is initiated in the test coils of the logic trip relays by turning the MATRIX RELAY TRIP TEST switch to "OFF" and depressing the MATRIX LOGIC AB TEST push button switch. Operation of the AB MATRIX TRIP TEST switch initiates a deenergizing current in the test coils of a parallel pair of module trip relays (in logic ladder matrix AB only). The operation of all pairs of contacts in the logic ladder matrix are tested individually by rotating the AB MATRIX TRIP TEST switch. With the ladder logic relay contacts

open, the operation of logic trip relays and power trip relays may be tested, one at a time, by rotating the MATRIX RELAY TRIP TEST switch. This deenergizes one logic trip relay and one power trip relay. Several sets of indicator lights provide verification that the appropriate logic trip relay and power trip relay have deenergized and the contacts opened to interrupt one of the parallel feeder lines to the rod clutch buses. Since the test procedures require that the trip action of one of the logic ladder matrices be defeated with holding coils, the test circuits in the logic permit only one logic ladder to be opened and one set of relays to be "held" at a time; the application of hold power to one set denies the power source to the other sets.

3.2.5 Isolation of Circuits

The circuits of the reactor shutdown instrumentation system are isolated from those of the operation system and use equipment physically separate from the active control part of the operation system, except for unidirectional control actions (such as turbine runback) that can only move the plant away from the safety limits.

The process transducers located in the containment building are housed in cabinets designed to provide sufficient mechanical and environmental protection following a design-basis accident that the assigned function can be completed. The cables from these cabinets are routed in raceways and in containment penetrations that are separate from each other and from power cables. In the control room, the instrumentation channels are located in four compartments (or cabinets) with mechanical and thermal barriers between them.

The circuits for testing the logic trip relays may provide a path for possible interconnection of some of the six logic ladder matrices (see Fig. 3.6).

The control rods and release mechanisms are divided into two groups of rod release circuits (or buses). The two release circuits are controlled by the same set of power trip relays, so they will be in close proximity.

3.3 Robert Emmett Ginna Nuclear Plant No. 1

3.3.1 Instrument Channels

Westinghouse Electric Corporation is designing a reactor shutdown system^{16, 17} for the Ginna Nuclear Power Plant that provides up to four instrument channels for the plant variables. The reasons for the selection of this system and much of the design basis are discussed in a report by Burnett of Westinghouse.¹⁸ Different logic arrangements are used for different plant variables. The automatic scram trip signals, the type of logic arrangement, and the permissives or blocks (bypasses) are listed in Table 3.3.

Each of the neutron flux channels for the high-flux trip signal in the power ranges receives its input from the sum of the outputs of the upper and lower half-sections of a long out-of-core ion chamber that monitors the full height of the core. The outputs of the half-sections are used in the temperature difference (ΔT) trip signals discussed below.

The purpose of the overtemperature ΔT trip signal (item 2 in Table 3.3) is to protect the core against a departure from nucleate boiling. It also protects the core against an unsafe axial distribution of neutron flux. A difference between the coolant outlet and inlet temperatures (ΔT) in excess of the set point initiates a trip signal. The set point is continuously calculated according to the following equation:

$$\text{Set point} = K_1 + K_2 P - K_3 T_{av} - F(\Delta q) ,$$

where K_1 , K_2 , and K_3 are constants, P is coolant pressure, T_{av} is coolant average temperature in the core, and $F(\Delta q)$ is a function of the flux difference measured by the upper and lower half-sections of the ion chambers.

The purpose of the overpower ΔT trip signal (item 3) is to limit the maximum overpower. It also protects the core against unsafe spatial distribution of flux. The measured differential temperature (ΔT) used for the overtemperature ΔT trip signal is compared for this trip signal against a set point that is continuously computed according to the following equation:

$$\text{Set point} = K_4 - F(\Delta q) ,$$

Table 3.3. Automatic Scram Trip Signals at Robert Emmett Ginna Nuclear Plant No. 2

Plant Variable	Logic Arrangement	Blocks and Permissives
1. High neutron flux (power range)	Two-of-four	None
2. Overtemperature ΔT (see text)	Two-of-four	None
3. Overpower ΔT (see text)	Two-of-four	None
4. Low coolant pressure	Two-of-four	Blocked by three-of-four signals of low-low ($\sim 10\%$) nuclear flux in coincidence with one-of-two low-electrical-load signals
5. High coolant pressure	Two-of-three	None
6. High water level in pressurizer	Two-of-three	Blocked by three-of-four signals of low-low ($\sim 10\%$) nuclear flux in coincidence with one-of-two low-electrical-load signals
7. a. Low coolant flow ($\sim 90\%$)	Two-of-three signals of low flow in both coolant loops	Blocked by three-of-four signals of low-low ($\sim 10\%$) nuclear flux in coincidence with one-of-two low-electrical-load signals
	Two-of-three signals of low flow in any coolant loop	Blocked by three-of-four signals of low ($\sim 50\%$) nuclear power
b. Pump breaker trip	One-of-one signal in both coolant loops	Blocked by three-of-four signals of low-low nuclear flux in coincidence with one-of-two low-electrical-load signals
	One-of-one signal in either coolant loop	Blocked by three-of-four signals of low nuclear power
c. Underfrequency	One-of-two signals from both coolant pump buses	Blocked by three-of-four signals of low-low nuclear flux in coincidence with one-of-two low-electrical-load signals
d. Undervoltage	One-of-two signals from both coolant pump buses	Blocked by three-of-four signals of low-low nuclear flux in coincidence with one-of-two low-electrical-load signals
8. Safety injection actuation	One-of-three pairs of low coolant pressure signals coincident with low pressurizer water level signals, or two-of-three signals of high containment pressure or two-of-three signals of low steam pressure in either steam generator	Manual block permitted by two-of-three signals of low coolant pressure; block removed by two-of-three signals of high coolant pressure
9. Turbine trip	Two-of-three low auto-stop oil pressure signals or two-of-two stop valve position signals	Blocked by three-of-four signals of low-low nuclear flux in coincidence with one-of-two low-electrical-load signals, or three-of-four signals of low nuclear flux and steam bypass unblocked
10. Low feedwater flow	One-of-two signals of steam-feedwater mismatch in coincidence with one-of-two signals of low steam generator water level in any loop	None
11. Low-low steam generator water level	Two-of-three signals from any loop	None
12. High neutron flux (intermediate range)	One-of-two	Manual block permitted by two-of-four signals of high power range flux; block removed by three-of-four signals of low power range flux
13. High neutron flux (source range)	One-of-two	Manual block permitted by one-of-two signals of high intermediate range flux or two-of-four signals of high power range flux; block removed by two-of-two signals of low intermediate range flux or three-of-four signals of low power range flux

where K_4 is a constant, and $F(\Delta q)$ is a function of the flux difference measured by the upper and lower half sections of the ion chambers.

The arrangement of the bypasses for the low-flow trip signals requires that the following number of coolant loops be in operation in different power ranges to avoid a scram: both coolant loops above approximately 50% power, one coolant loop between approximately 10% and 50% power, and no coolant loops below approximately 10% power.

The reactor scram caused by safety injection actuation initiated by low steam pressure is an interesting case (item 9 of Table 3.3). A sudden loss of steam pressure as the result of a failure of the secondary coolant system would be accompanied by excessive heat removal from the primary coolant passing through the affected steam generator. This would cause a rapid drop in the average temperature of the primary coolant and result in low pressure and water levels in the pressurizer, as well as an increase in reactivity from the reduced coolant temperature. Safety injection would be initiated to add makeup water rapidly and to supply borated water to the primary system to aid the control rods in combating the reactivity increase caused by excessively cooling the primary system water.

Some of the blocks (or bypasses) of trip signals listed in Table 3.3 are applied and removed automatically as a function of the plant variables listed. Other blocks are initiated manually if the permissive conditions listed are satisfied. These blocks are automatically removed when the plant variables no longer meet the permissive conditions. All blocking or permissive signals are generated in logic matrices that take signals from each set of instrument channels. The logic arrangements used in developing these blocking or permissive signals are listed in Table 3.3.

Most instrumentation channels for the nonnuclear plant variables have electronic transmitters that generate dc analog-type signals.

3.3.2 Logic Arrangement

The reactor shutdown system has several different logic arrangements for different plant variables. As indicated in Table 3.3, these include one-of-one, one-of-two, two-of-three, and two-of-four logic arrangements.

An example of a dual two-of-four logic arrangement is shown in Fig. 3.7. There are four process sensors, or transmitters, in this arrangement,

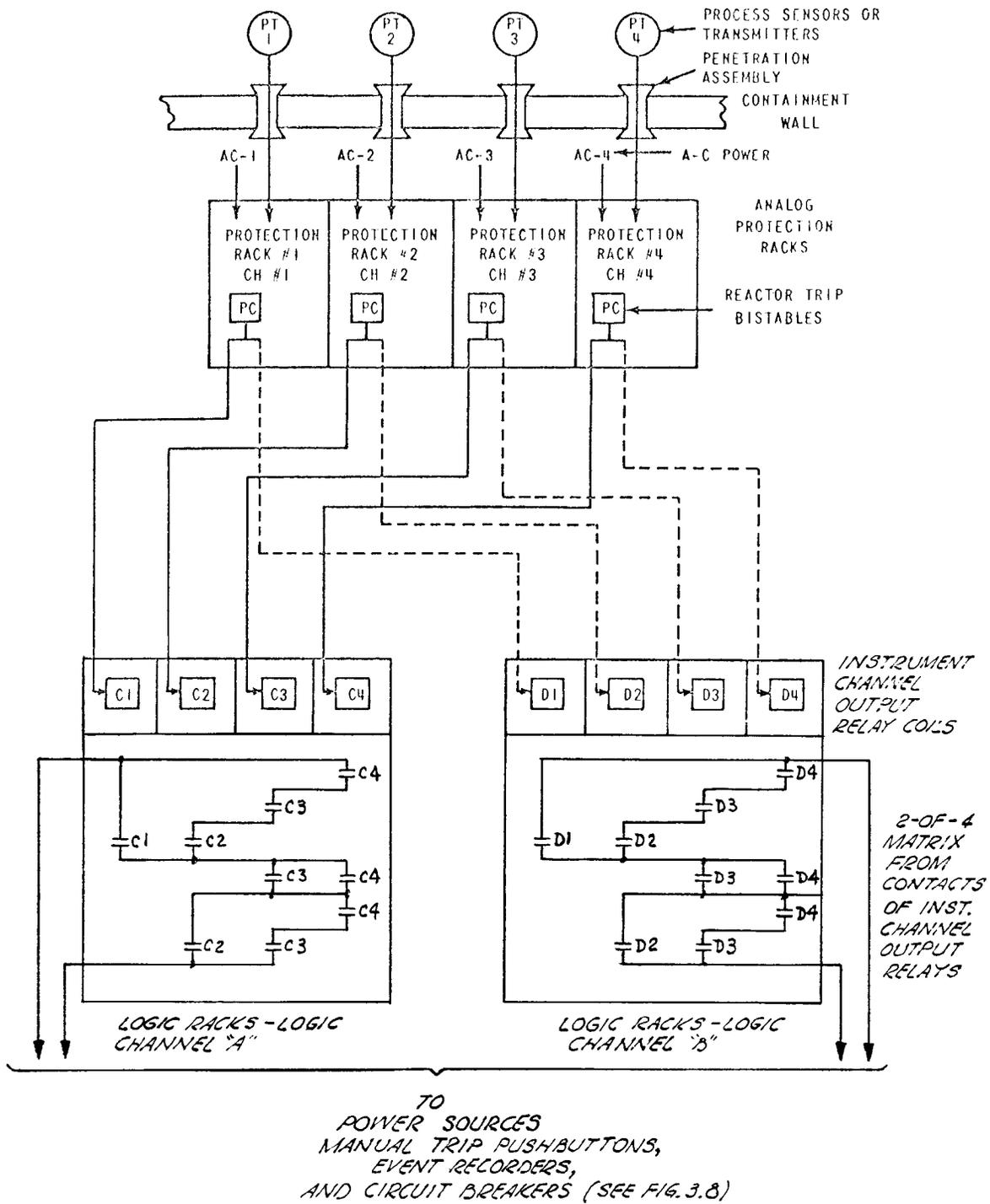


Fig. 3.7. Typical Instrument Channel and Logic Matrices for Reactor Shutdown System in Ginna Plant. (From Ref. 16 with additions)

with four separate power supplies and four reactor trip bistable devices. Each trip bistable device controls the power to two instrument-channel output-relay coils that operate contacts in the two duplicate logic matrices.

The logic matrices for different plant variables are connected in series in two separate circuits, or logic channels, as shown in Fig. 3.8. The instrument channels are deenergized to produce a trip signal. A logic channel is opened up, or deenergized, when contacts from two or more of the instrument-channel output relays in a matrix associated with one plant variable are opened. The logic channels control the undervoltage coils of the circuit breakers, which open the circuit breakers when deenergized. The reactor shutdown system has local coincidence wherein a scram is initiated only if there are at least two trip signals pertaining to one plant variable.

The two "trip" circuit breakers are arranged in series to interrupt the single three-phase ac feeder circuit that supplies power to the control rod drives. The opening of either of the two trip circuit breaker interrupts the power and allows the control rods to drop into the core (i.e., a one-of-two logic arrangement). The system thus can be described as having two sets of logic matrices (i.e., logic channels) from one set of sensors, with either set of matrices capable of producing a reactor scram. The circuit breakers have three poles, although only one pole is indicated on each breaker in the figure. (Some interposing relays are omitted in Fig. 3.8).¹⁷ The bypass breakers are used only in carrying out tests of the circuit breakers and are not normally connected into the rod drive power circuit.

In summary, a scram requires trip signals from two instrument channels for the same plant variable, a trip signal from one logic channel (or series of matrices), and the opening of one circuit breaker to interrupt power to the control rod drives.

3.3.3 Power Sources

There are four 120-v ac buses for instrument power. Two are supplied through dc-to-ac inverters from the two 125-v dc station batteries. The other two are supplied through transformers from two separate 480-v buses.

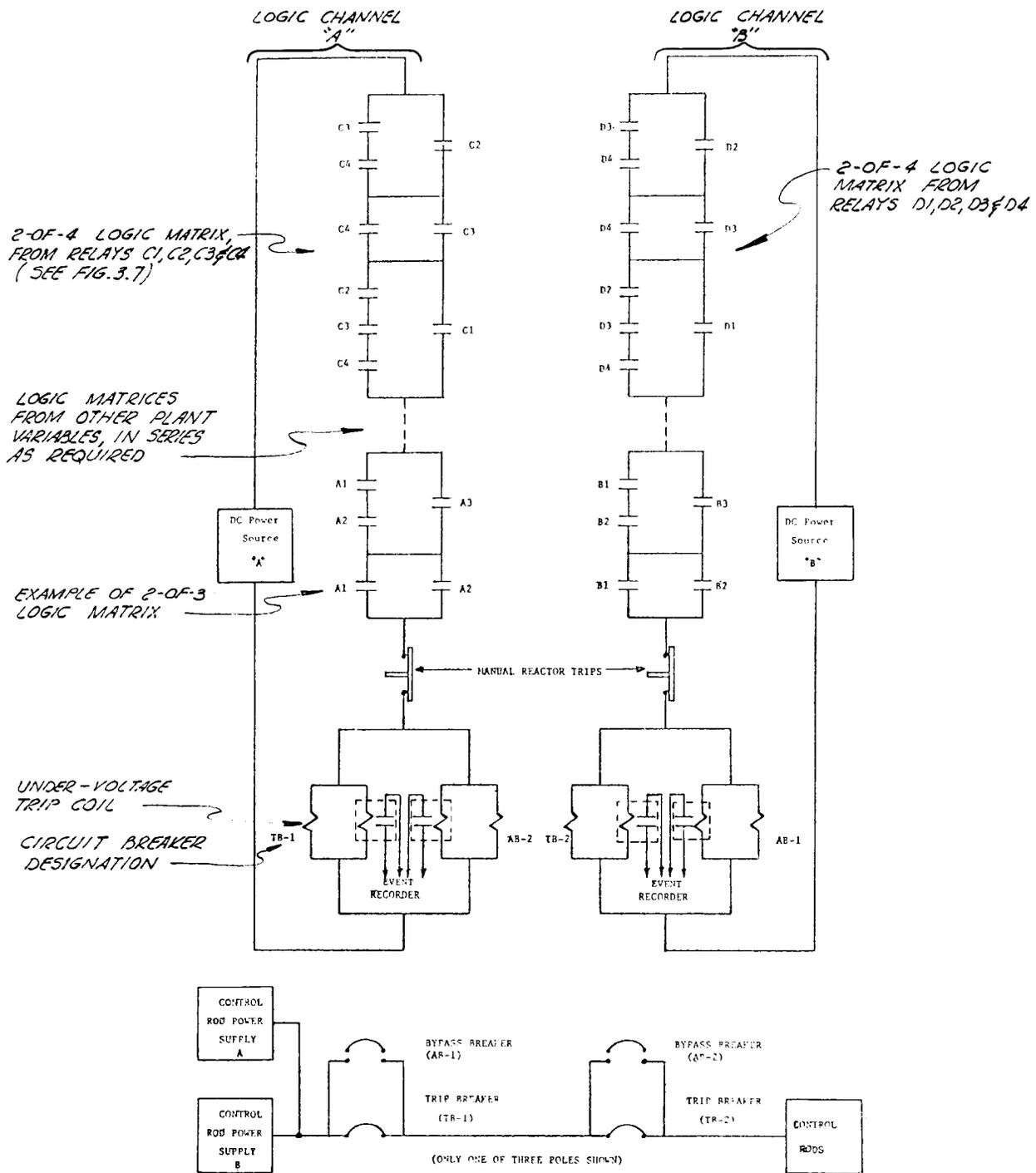


Fig. 3.8. Simplified Logic Circuits and Control-Rod Release Circuits for Reactor Shutdown System in Ginna Plant. (From Ref. 16 with additions)

The two sets of logic matrices in the two logic channels in Figs. 3.7 and 3.8 are separately supplied with dc power from the two station batteries.

The control rod drive power is supplied by two motor-generator sets connected in parallel. These sets provide 260-v line-to-line three-phase four-wire ac power. This power is routed through the circuit breakers as shown in Fig. 3.8 and then to the solid-state power cabinets that convert the ac to "profiled" dc to operate the mechanism coils in the rod drives.

3.3.4 Testing Arrangement

Provisions for testing the analog portion and the bistable unit of each instrument channel are shown in Fig. 3.9. A calibrating signal can be inserted at the SIGNAL INJECTION jack with the TEST-OPERATE switch in the test position to verify operation of the bistable unit. The PROVING LAMP indicates operation of the bistable device. The calibrating signal can be measured at the TEST POINT terminals. The LOGIC TEST switches are used to deenergize individual instrument channel output relays.

Testing of circuit breakers TB-1 and TB-2, shown in Fig. 3.8, is carried out by using bypass breakers AB-1 and AB-2. During normal operation, breakers AB-1 and AB-2 are both open (racked out). In order to test breaker TB-1, bypass breaker AB-1 is closed to allow breaker TB-1 to be opened without shutting down the reactor. Bypass breaker AB-1 is tripped by the same signal that trips breaker TB-2; thus operation of both logic channels in Fig. 3.8 would deenergize the trip coils of the bypass breaker (AB-1), the breaker being bypassed for test (TB-1), and the other breaker (TB-2). The event recorder operated by monitoring coils in parallel with the undervoltage trip coils of the breakers allows verification that the required combinations of instrument-channel trip signals will deenergize the under voltage coils without the necessity of operating a breaker at each test combination. The breaker under test is left open during testing of the logic combinations.

Bypassing the circuit breakers allows on-line tests to be conducted of each of the logic channels separately. Operation of the logic test switches indicated in Fig. 3.9 to deenergize two of the instrument-channel

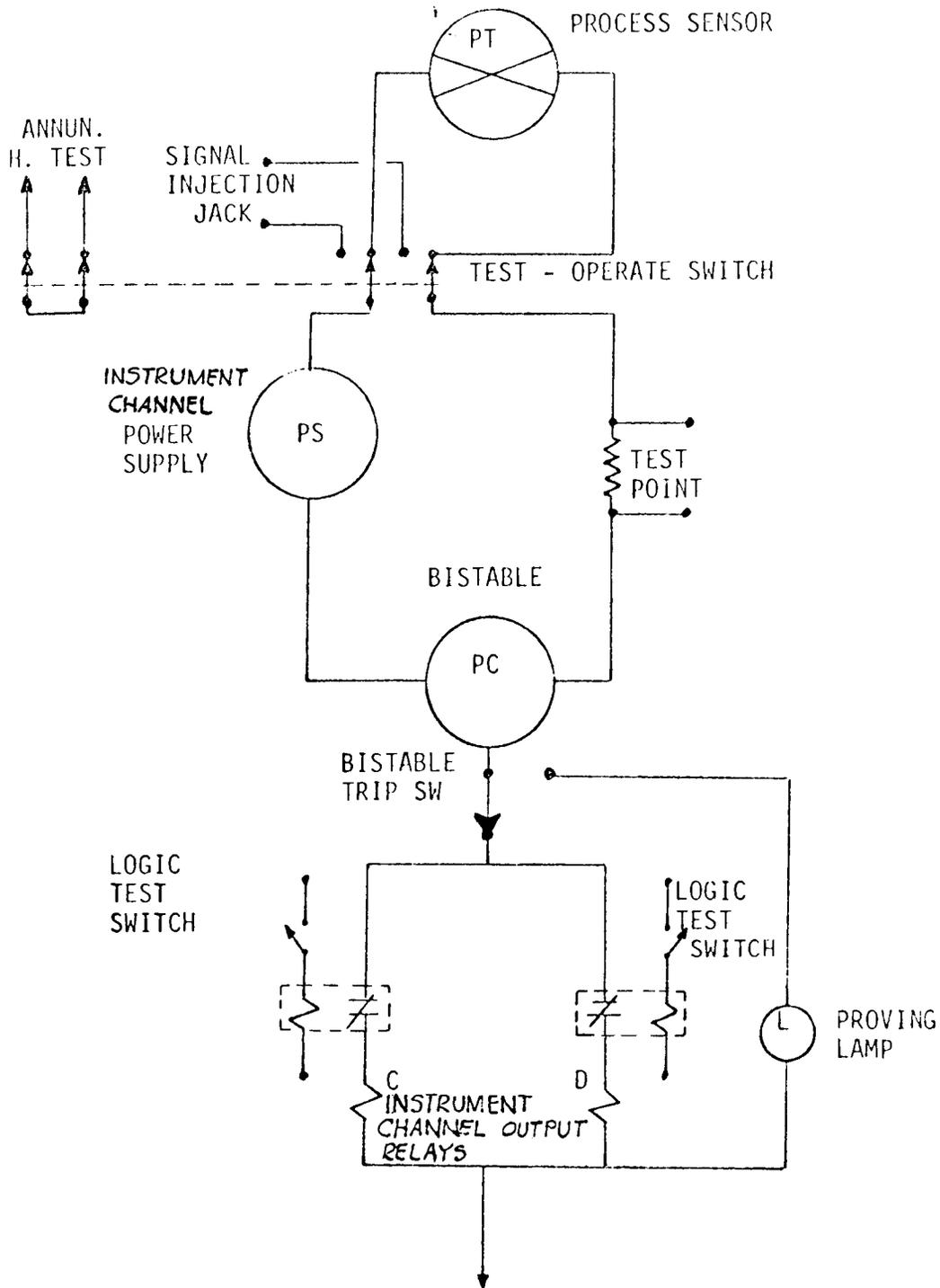


Fig. 3.9. Typical Instrument Channel Testing Arrangement for Reactor Shutdown System in Ginna Plant. (From Ref. 16 with additions)

output relay coils in one matrix opens the circuit to the under-voltage trip coil of the selected circuit breaker and operates the event recorder. For example, deenergizing instrument-channel output relay coils C1 and C2 in Fig. 3.7 deenergizes the trip coil of breaker TB-1 and the act is recorded by the event recorder. This type of test determines whether the matrices actually operate and is a test of the transmission capability of the logic system.

3.3.5 Isolation of Circuits

The same process sensors are used for both operation and protection.¹⁸ Control signals are taken from the protection system through isolation amplifiers. Generally, two-of-four logic is used to cope with a single random failure in the part of the instrumentation common to both protection and operation that can cause a process excursion that requires protective action. In addition, a different plant variable is used as an input to the reactor shutdown system to provide a backup, or diverse, trip signal to cope with common-mode failures that affect all channels for a plant variable that is used for both protection and active control in the operation system.¹⁸

Redundant instrument channels are isolated from each other, as indicated in Fig. 3.7, and are energized from separate ac power sources. Isolation continues from the sensors through the containment penetrations and into the analog protection racks.

The two sets of matrix relays in the two logic channels are located in separate logic racks. Separate dc power sources provide power for the two logic channels and circuit breaker undervoltage trip coils, as shown in Fig. 3.8.

The control rods and release mechanisms are divided into several groups below the two trip circuit breakers. Each group is powered from a separate solid-state power cabinet that converts the ac input to a profiled dc source.

3.4 Browns Ferry Nuclear Power Station

3.4.1 Instrument Channels

The General Electric Company is designing a reactor shutdown system for the Browns Ferry Nuclear Power Station that, in general, provides four instrument channels for each of the important plant variables.^{19,20} The automatic scram trip signals and the bypasses are listed in Table 3.4.

The neutron flux level instrumentation is unique in that it includes a large number of miniature in-core detectors to provide an indication of

Table 3.4. Automatic Scram Trip Signals at Browns Ferry Power Station

Plant Variables	Bypasses
1. High neutron flux in intermediate range	Bypassed in RUN mode
2. High neutron flux in power range	
3. High reactor pressure	
4. High containment (drywell) pressure	
5. Low reactor water level	
6. High water level in scram discharge volume	Bypassed to reset scram
7. High radiation from main steam lines	
8. Low main condenser vacuum	Bypassed in STARTUP and STANDBY modes; bypass removed by reactor pressure in operating range
9. Partial closure of main steam isolation valves	Bypassed in STARTUP and STANDBY modes; bypass removed by reactor pressure in operating range
10. Turbine stop valve closure	Bypassed by low pressure in first stage of turbine
11. Generator load rejection	Bypassed by low pressure in first stage of turbine
12. Mode switch in SHUTDOWN mode	

average reactor power. The flux instruments used from criticality to 10% of full power are termed the intermediate-range monitors (IRM). Eight IRM units are provided, and a maximum of two of these can be bypassed at any one time in the STARTUP, HOT STANDBY, and REFUELING modes of reactor operation and yet leave a sufficient number to execute the four-channel logic. In the power range, the average-power-range monitors (APRM) average the outputs of a number of flux detectors called local-power-range monitors (LPRM). Six APRM units are provided, and a maximum of two of these can be bypassed at any one time, again leaving a sufficient number of channels. The APRM units have an optional provision for varying the trip set point as a function of recirculation flow.

Most instrument channels used in the protection system for measuring pressures, water level, and vacuum consist of nonindicating pressure switches. The reactor water level channel, however, has indicating pressure switches.

Three of the bypasses (items 1, 8, and 9) in Table 3.4 are actuated manually with the reactor-mode selector switch. Two of these (items 8 and 9) are automatically removed when the pressure reaches the power operating range. Two other bypasses (items 10 and 11) are applied and removed automatically as a function of pressure in the first stage of the turbine. This bypassing is done on a channel-by-channel basis in the one-of-N logic channels.

3.4.2 Logic Arrangement

General Electric refers to the basic system arrangement as the Dual Logic Channel Reactor Protection System.¹⁹ In general, an automatic scram requires the coincidence of the action of two one-of-two logic channels (or a one-of-two system taken twice). The system employs general coincidence of all plant variables. The reasons for the selection of this system are discussed in a report by Jacobs of General Electric.²¹

A simplified elementary diagram of the circuits associated with control rod scram is shown in Fig. 3.10. The instrument channels that produce automatic scram trip signal 1A of logic channel A operate relay contacts connected in series with the coils of relays KL1A1 and KL1A2 to form a one-of-N logic. Since there are two automatic scram trip circuits

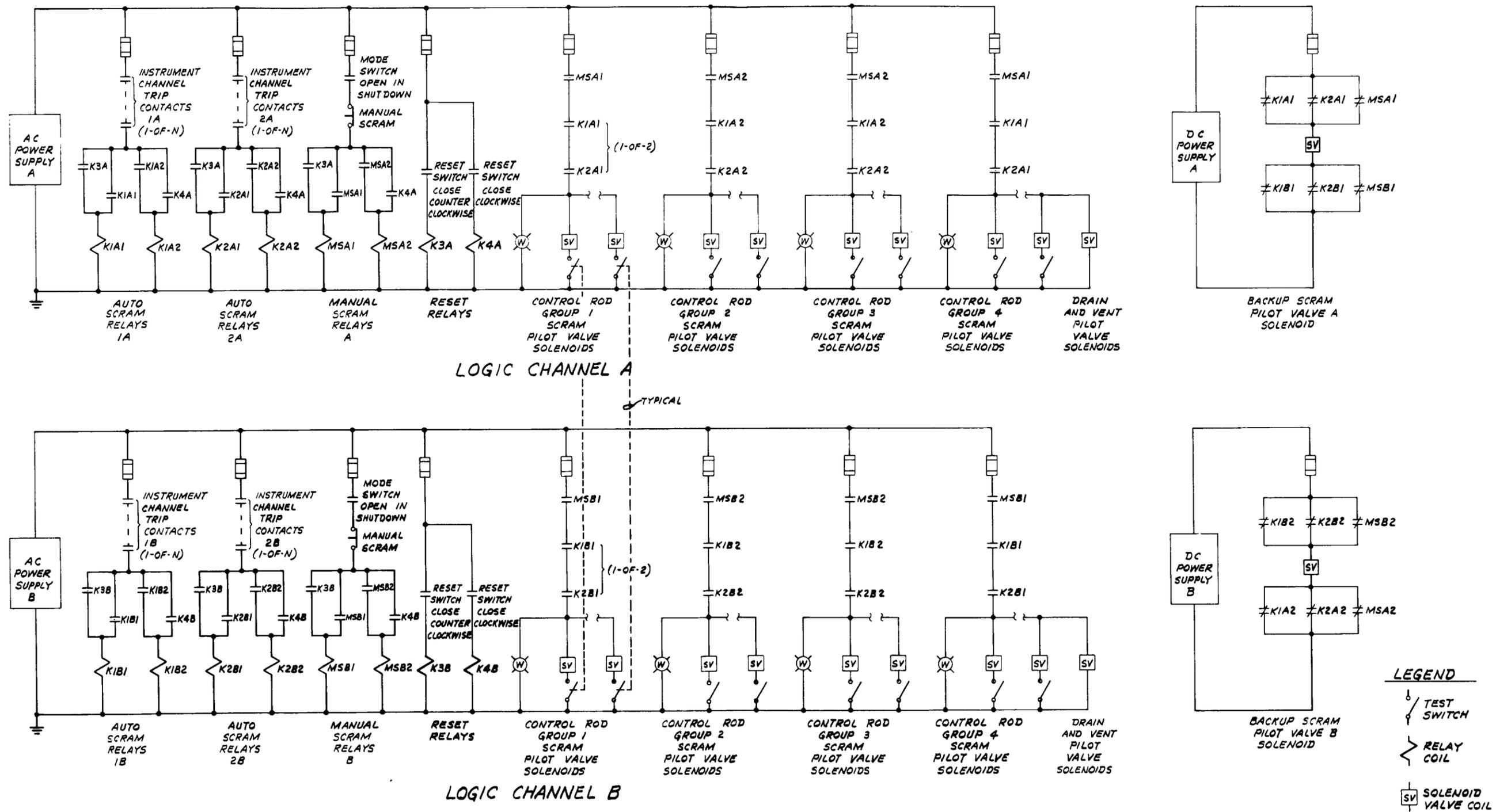


Fig. 3.10. Logic Circuits for Reactor Shutdown System in Browns Ferry Station. (Redrawn from Refs. 19 and 20)

for each logic channel, there are four sets of separate instruments (i.e., protection channels), which are identified as sets 1A, 2A, 1B, and 2B. The instruments for sets 1A and 2A have a common power source, and a similar arrangement prevails for 1B and 2B. A single trip signal from any plant variable in set 1A deenergizes relays K1A1 and K1A2. Similarly, a single trip signal from set 2A deenergizes relays K2A1 and K2A2. The circuits for logic channel B are separate duplicates of those for logic channel A.

Each scram relay is sealed in through one of its own contacts; a trip signal is therefore sealed in until appropriate reset contacts are closed. A manually operated switch resets the trip relays after the individual trip outputs have returned to normal. The RESET switch²⁰ contacts shown in Fig. 3.10 reset a portion of the relays on both buses when turned clockwise, and the remaining relays are reset when the switch is turned counterclockwise. This switch is spring-returned to its center position.

The reactor shutdown system actuates the control rod drives through the solenoids of the scram pilot valves. (The operation of these valves is discussed in the next section.) There are two such valves on each drive, and both must be deenergized to initiate scram action of the individual control rod (i.e., two-of-two logic). The circuits to these valves are divided into four approximately equal groups. For an automatic trip signal only, either relays K1A1 and K1A2 or relays K2A1 and K2A2 of logic channel A, as well as either relays K1B1 and K1B2 or K2B1 and K2B2 of logic channel B, must be deenergized to start a scram. Thus the circuits require a coincidence of two one-of-two logic channels. In order to produce a manual trip, the operator (or operators) must depress a push button for logic channel A and another in logic channel B simultaneously. It is possible, of course, to have an automatic trip of one logic channel and a manual trip of the other, but such a situation would still require a coincidence of trips of both logic channels to produce a scram.

Operation of the drain and vent pilot valves and backup scram pilot valves is discussed following the control rod drive scram subsystem description below.

3.4.3 Control Rod Drive Scram Subsystem

A simplified schematic diagram of a control rod drive scram subsystem is shown in Fig. 3.11. The upward scram motion is produced by admitting water to the lower portion of the double-acting drive cylinder and allowing water to be expelled from the upper portion. The water flow to the drive cylinder is controlled by the inlet and outlet scram valves, which are operated by air diaphragms. The air pressure to these diaphragm operators is controlled by the two scram pilot valves discussed in the previous section. Air pressure is vented from the diaphragm chambers of both the inlet and outlet scram valves when both of the scram pilot valves revert to their deenergized position after the reactor shutdown system logic is tripped. Release of air pressure allows the scram valves to open. Water pressure is in the direction to open these valves. Opening of the inlet scram valve allows water to flow from the accumulator into the lower portion of the drive cylinder to lift the piston. After the outlet scram valve opens, water is free to flow out of the upper portion of the rod drive cylinder into the scram discharge header. As a matter of fact, during power operation, if only the outlet scram valve were opened, the drive piston would be driven upward because the reactor vessel pressure would force water through the check valve and into the cylinder. After the control rod was driven upward into the core, the drive mechanism would clamp the rod in the fully inserted position.

High-pressure water in the accumulator has the purpose of producing rapid control rod insertion when the reactor pressure is low. This water also assists during the initial part of the stroke when the reactor is at pressure. The accumulator water pressure is higher than that of the reactor when the scram begins, and the check valve prevents loss of this high-pressure water into the reactor vessel. As the scram stroke continues, reactor water is admitted to the rod drive cylinder after the pressure of water from the accumulator becomes as low as the reactor pressure. Sufficient water and nitrogen are available in the accumulator to fully insert the control rod when the reactor is at low pressure. The accumulator is charged with water from a high-pressure header. A check

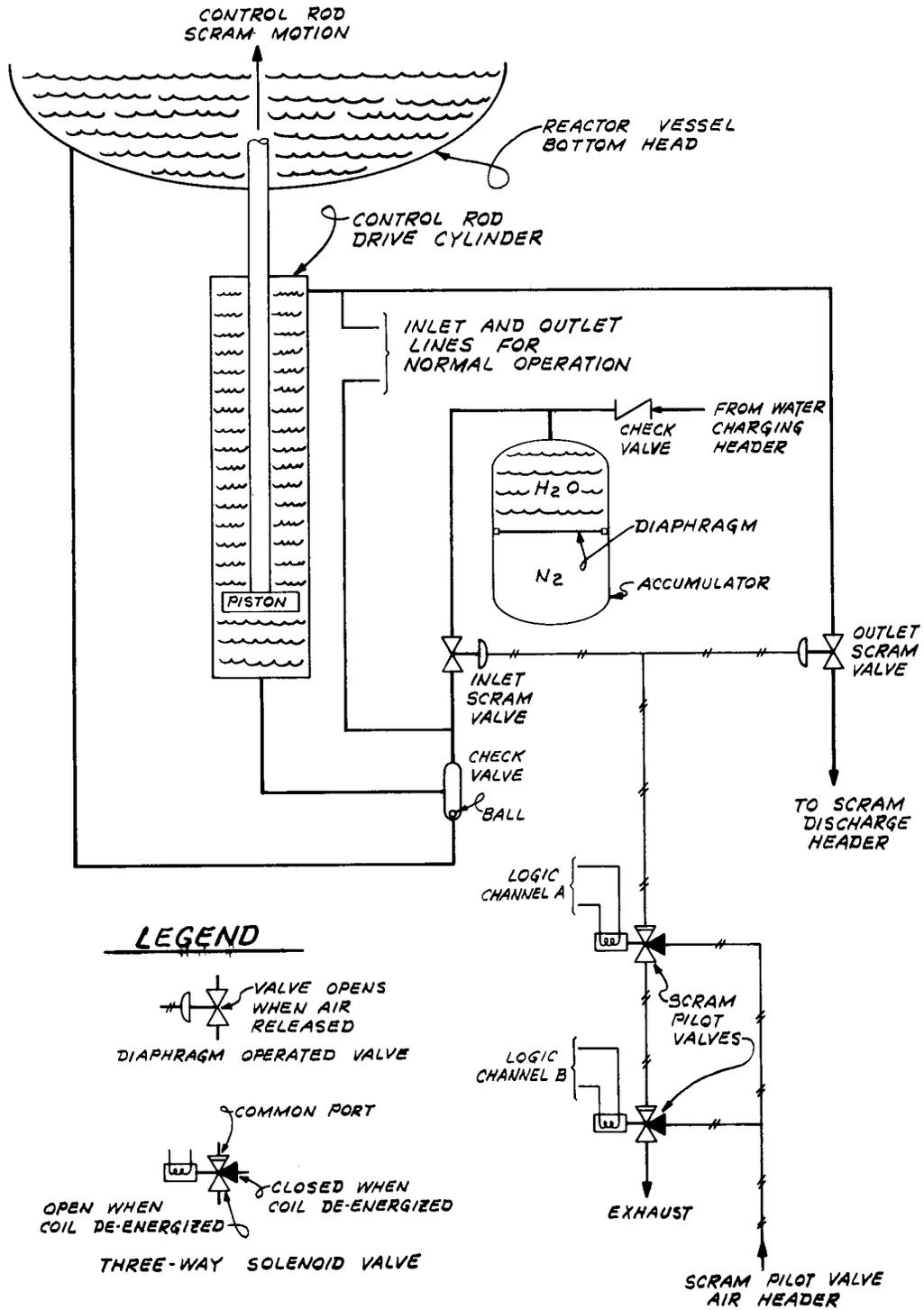


Fig. 3.11. Typical Control-Rod Drive Scram Subsystem for Reactor Shutdown System in Browns Ferry Station. (Redrawn from Ref. 19)

valve prevents loss of accumulator water if the header pressure becomes too low.

3.4.4 Air Supply and Scram Discharge Subsystems

As previously mentioned, the protection system logic in Fig. 3.10 also controls several other solenoid valves. The backup pilot valves and the drain and vent valves are used in the air supply and scram discharge subsystems shown in Fig. 3.12. The header that supplies air to the scram pilot valves of all the control rod drives is connected to the instrument air supply through the two backup scram pilot valves that provide a secondary method of scrambling the drive cylinder. Air is released from this header when the solenoid for either of the two backup valves is energized (i.e., one-of-two logic). The check valve in parallel with backup scram pilot valve A allows both valves to vent the header in parallel when both are energized. The dc solenoid for each backup scram pilot valve is energized when two of the appropriate manual scram relays or either of the two appropriate automatic scram relays are deenergized on both buses of the logic channels (to initiate a scram). Thus coincident trip signals from the two logic channels are required (i.e., two-of-two logic).

Loss of header air pressure through the backup scram pilot valves would allow the inlet and outlet scram valves on any rod drive to open even if both scram pilot valves fail to function on the affected drive. However, the time to initiate rod motion would be somewhat longer than if both scram pilot valves operated because of the larger volume of air to be released.

The two headers and scram discharge volume for collecting the water discharged from the control rod drive cylinders during a scram are shown in Fig. 3.12. Approximately half the drives are connected to each header. The scram discharge volume is empty of water during normal operation; however, it is closed and sealed when a scram occurs to prevent continued leakage of high-pressure reactor water through the control rod drives. A scram signal from both logic channels in Fig. 3.10 deenergizes the solenoids for both of the drain and vent pilot valves shown in Fig. 3.12. This relieves the air pressure from the diaphragm operators for the drain and vent valves. Loss of air pressure allows these valves to close and

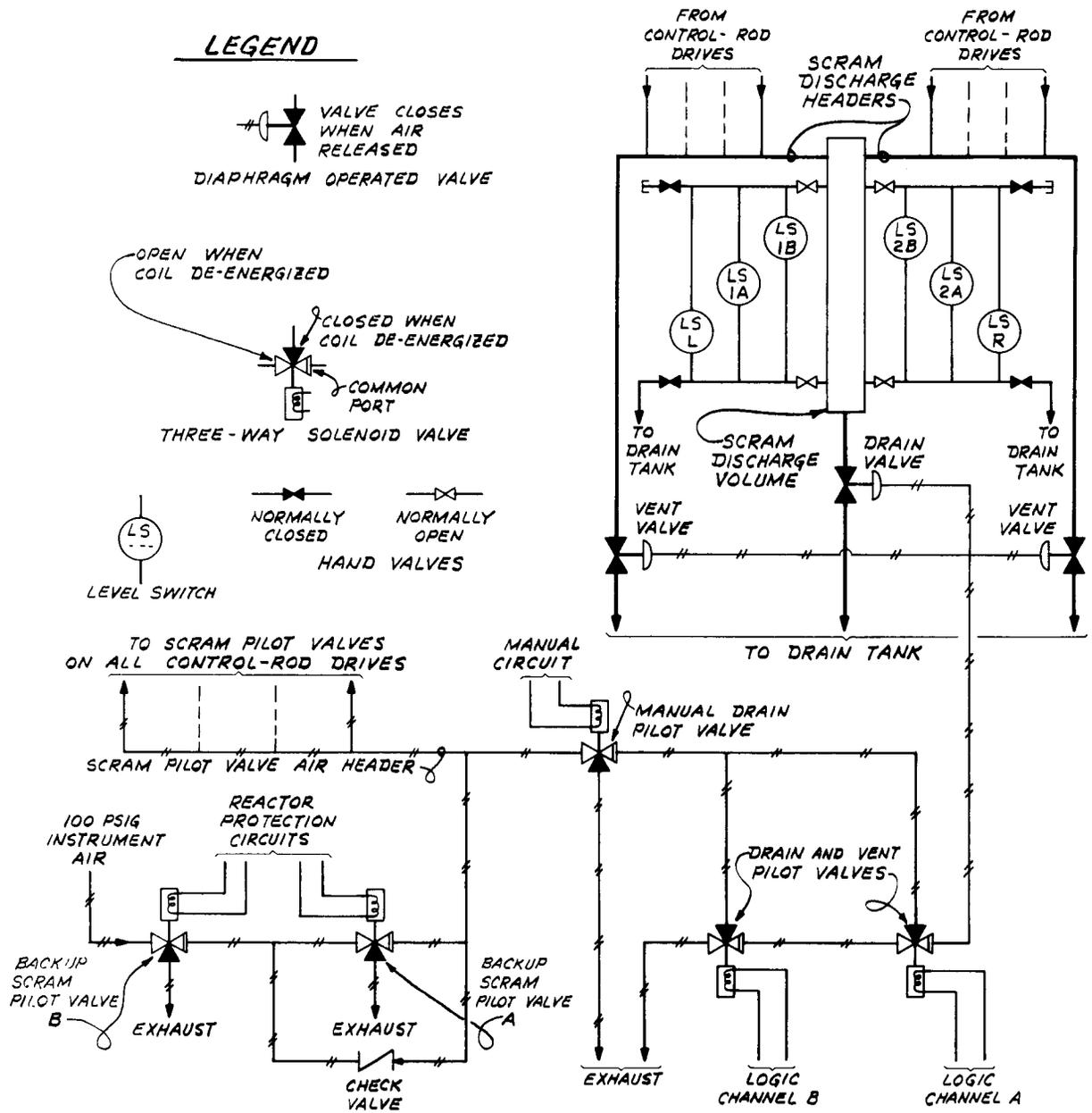


Fig. 3.12. Air Supply and Scram Discharge Subsystems for Control Rod Drives in Reactor Shutdown System in Browns Ferry Station. (Redrawn from Ref. 19)

seal the scram discharge water storage system. Since air for the diaphragm-operated valves is taken from the scram pilot valve air header, energizing either backup scram pilot valve will allow the drain and vent valves to close also. During any time that both scram logic channels are energized, the scram discharge volume can be sealed by energizing a manually controlled valve shown in Fig. 3.12.

The scram discharge volume itself is simply a length of large-diameter pipe, which serves as an instrumented sump, and approximately two-thirds of the system volume is in the header pipes. The scram initiated by the switches on the sump occurs at a level that leaves sufficient space to accept the water discharged from the drives during the subsequent scram. The total capacity of this water-collecting system is approximately 50% larger than the quantity of water discharged from the drives during a scram.²² During a scram, the flow of water into the sealed collecting pipes compresses the air originally in these pipes and pressurizes the scram discharge volume.

3.4.5 Power Sources

Normal power for each logic channel and all instruments associated with each logic channel is supplied individually by two motor-generator sets. Each set is composed of a three-phase 480-v synchronous motor driving a single-phase 120-v ac generator. A flywheel provides additional inertia. This inertia should prevent a momentary interruption of the motor power (as from switching during maintenance) from seriously affecting the voltage and/or frequency of the generator.

An alternate source of single-phase 120-v 60-cps power is available from a stepdown transformer connected to a separate 480-v bus. A manually operated switch can be used to connect this alternate source to either of the two logic channels after the respective normal supply is disconnected. The circuits are arranged to prevent the logic channels from being connected in parallel and to allow the alternate source to be connected to only one logic channel at a given time.

Direct-current power for the two backup scram pilot valves is available from two separate 250-v station batteries. (In some plants these are powered from two 125-v station batteries.²⁰)

Compressed air for the diaphragm-operated valves is obtained from a single 100-psig plant instrument air supply that includes compressors, dryers, storage, etc.

3.4.6 Testing Arrangement

Analog portions of the instrument channels are checked during reactor operation by visually comparing the output of similar channels. The trip units are tested by inserting a substitute electrical test signal and varying its magnitude to produce a trip. Some of the instrument channels are nonindicating on-off devices, such as pressure switches. These are tested by introducing substitute high test pressure at the pressure switch sensor. The test procedure includes steps to verify that the pressure switch has been reconnected correctly after the test.²²

The system design allows a certain amount of testing to be performed on each logic channel separately without shutting down the reactor, since trip signals in both logic channels are required to produce a scram. A test that deenergizes any or all relays and/or scram pilot valves of one logic channel will not shut down the reactor unless safe failures have already occurred in the circuits or pilot valves associated with the other logic channel.

A test that deenergizes any one of the scram relays should, in turn, deenergize all pilot valves connected to the logic channel. The indicating lamps shown in Fig. 3.10 will show whether power is turned off to the groups of valve solenoids. Such a test will disclose the presence of short circuits that prevent the operation of pilot valves in groups.

TEST switches are provided as shown in Fig. 3.10 to allow the pilot valves on each rod to be deenergized to scram each rod individually.

3.4.7 Isolation of Circuits

Circuits of the reactor shutdown system are isolated from the operation system and use equipment physically separate from the active control part of the operation system, except for unidirectional control actions (such as the rod block monitor system) that can only move the plant away from the safety limits.

Circuits involved in automatic scram signal 1A of logic channel A are isolated from those of automatic scram trip signal 2A. Penetrations of cables through the containment barrier are separated into four groups to maintain separation of the four trip circuits. Each scram relay is totally enclosed in a separate compartment. The RESET switch brings the circuits of logic channels A and B into close proximity.

The control rods and drive cylinders are divided into four groups of rod release circuits with a separate set of one-of-two logic matrices for each group.

4. TYPICAL INSTRUMENTATION SYSTEMS FOR ENGINEERED SAFETY FEATURES

In this chapter we describe and discuss the design features of protection instrumentation systems provided to initiate the action of engineered safety features, which in the past were designated "engineered safeguards." For the purposes of this report, we are primarily concerned with the protection instrumentation systems from which the pumps, valves, etc., receive their signals to operate rather than with the mechanical components themselves. The systems covered include the typical reactors whose reactor shutdown protection instrument systems are discussed in Chapter 3, except that Dresden-2 rather than Browns Ferry is discussed.

The engineered safety features for a typical plant include a fairly large number of complex systems, such as high-pressure safety (coolant) injection, automatic pressure relief, low-pressure safety (coolant) injection, core spray, containment isolation, containment spray, containment air cooler, secondary cooling water, and emergency power systems. Typical examples of such systems are described in other papers in this series by Lawson³ and Zapp.⁴ Many of these engineered safety features are actuated by separate protection instrumentation systems.

We do not describe these engineered safety instrumentation systems in as much detail as the reactor shutdown instrumentation systems for several reasons. First, the various engineered safety instrumentation systems for a given plant are usually designed with the same basic approach, and also they are usually more complex because many valves and cooling systems must be operated in the correct sequence, the cooling systems must be connected to several possible sources of water and electrical power, and the cooling systems must be operated for extended periods of time. Finally, it is difficult to obtain detailed information on these systems during the early design stages of the plants. We do discuss the engineered safety systems of the Palisades plant in more detail than those of the other plants because more information was available.

Several plant variables are connected in different logic arrangements to actuate the various engineered safety features. These include variables such as low reactor pressure, low reactor water level, high containment

pressure, high containment radiation, low steam-line pressure, high steam-line radiation, loss of external electrical power, etc. We do not describe these for each plant because of their complexity.

A simplified logic diagram for the actuation of most of the engineered safety features of a fairly typical reactor plant is shown in Fig. 4.1. This diagram applies to the Palisades plant; however, it is illustrative of the plant variables and logic decisions used in controlling the different types of engineered safety features. The details of these systems vary somewhat from one designer to another.

4.1 Palisades Plant

4.1.1 Instrument Channels and Major Functional Requirements

The Bechtel Company is designing the engineered safety features (Refs. 13-15, 23, 24) for the Palisades plant of the Consumers Power Company, whereas Combustion Engineering, Inc., is designing the shutdown system. A four-channel instrumentation system is used for each plant variable. The plant variables used and the major engineered safety functions they actuate are shown in the overall logic diagram in Fig. 4.1. This diagram does not show the additional features of (1) automatic startup of the third pump in a set if the others do not start and (2) automatic transfer to the containment building sump of the suction of the safety injection pumps from the safety injection and refueling water (SIRW) tank upon low tank level.

4.1.2 Typical Logic Arrangement and Actuation Channel*

The logic arrangement and actuation channel for the safety injection system (SIS) that controls most of the engineered safety equipment, such as that provided for core and containment cooling, and the automatic controls of the low-pressure (LP) safety injection pumps for the Palisades plant are typical of the design used for most of the other engineered

*Since the completion of this report in June 1969, G. S. Keeley of Consumer's Power Company has informed us that the designs of the safety injection and containment isolation actuation systems of the Palisades Plant are being revised. The constraints of time did not permit modification of the descriptions; however, in general, both of these actuation

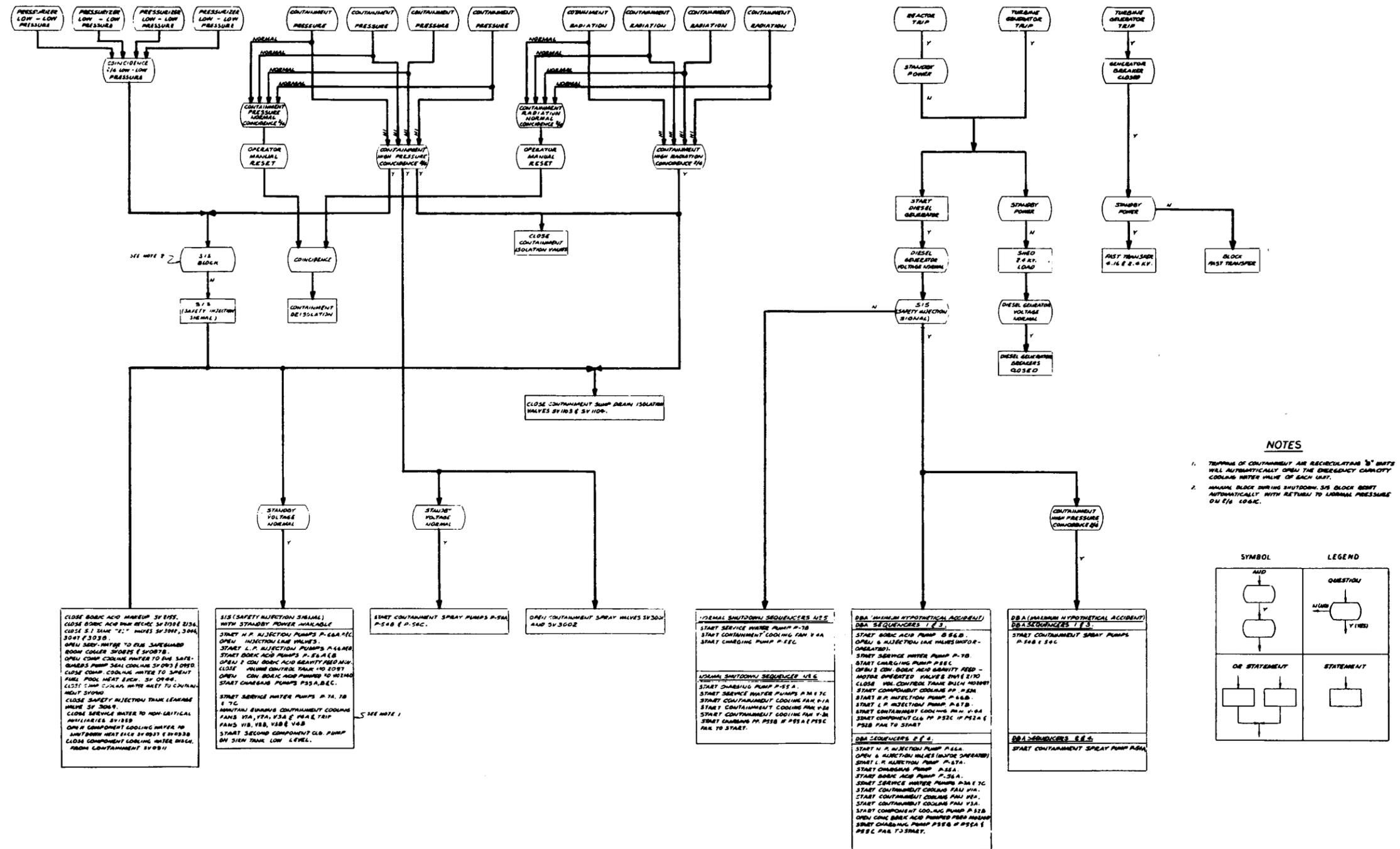


Fig. 4.1. Overall Logic Diagram for Actuation System for Engineered Safety Features in Palisades Plant. (From Ref. 13)

safety systems in the plant. The four instrument channels for each plant variable are usually employed in two-of-four logic arrangements, with local coincidence for each plant variable. The safety injection signal is initiated from either two-of-four pressurizer low-low pressure signals or from two-of-four containment high-pressure signals, as shown in the more detailed logic diagram²⁴ in Fig. 4.2. The four instrument channels for each variable are used in two duplicate sets of logic matrices to generate two safety injection signals that are designated A and B SIS actuation signals. The two matrices for low-low-pressure signals are used separately in the two actuation channels; however, the two matrices for containment high-pressure signals are both used in both actuation channels. (The circuits used to block the safety injection signal are discussed later.) The two actuation channels are part of the two-channel concept used throughout the engineered safety systems. The A SIS signal is used to actuate one of the two redundant full-capacity sets of engineered safety systems. The B SIS signal is used to actuate the other set. The two SIS actuation channels and engineered safety system load groups are supplied from separate sources of normal power and separate sources of emergency power.

The schematic diagram¹³ for one of the two matrices for containment high-pressure signals is shown in Fig. 4.3. The four instrument channels operate the contacts PSX/1801 through PSX/1804 that make up the two-of-four matrix. The instrument channels and the logic matrix are deenergized to produce a trip signal that deenergizes the logic output relays 5P-1 through 5P-9. The duplicate logic channel is not shown, but its logic output relays have even-numbered designations 5P-2 through 5-10.

The schematic diagrams^{14,24} for the B SIS actuation channel logic circuits and part of the A circuits are shown in Figs. 4.4 and 4.5. The

systems are being revised to follow the general pattern used in the other two pressurized-water reactors reviewed, which are described briefly in Section 2.3.1 and Fig. 2.6 and in more detail in Section 4.2 for Oconee and in Section 4.3 for Ginna. Each of the two logic matrices will serve a separate actuation channel (i.e., the two-of-two logic arrangements are being omitted), and all the logic matrices will be energized to trip and initiate action. One of the actuation channels in the containment isolation system will control the inner valve in a pipe line, and the other actuation channel will control the outer (redundant) valve in the same line.

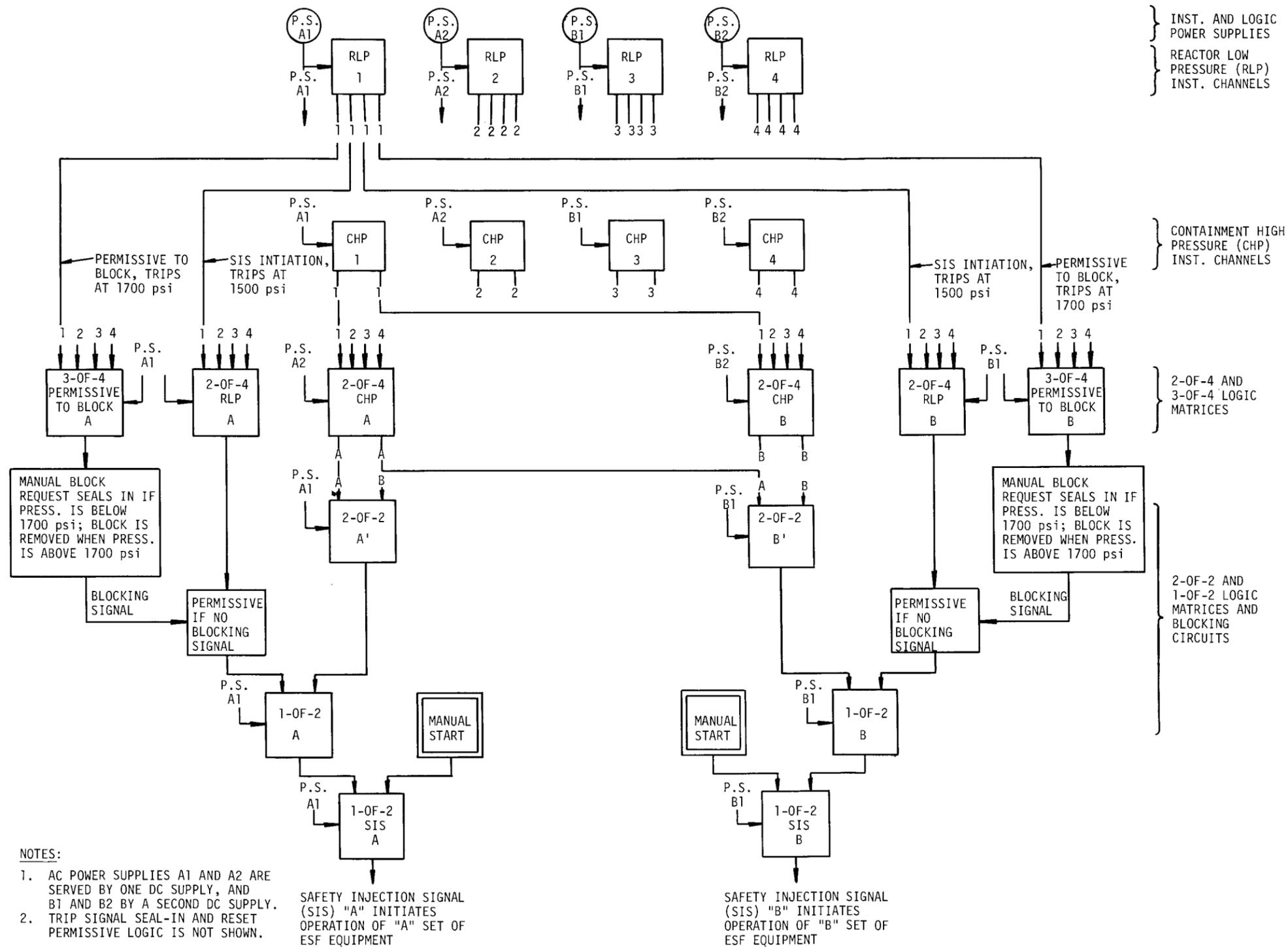
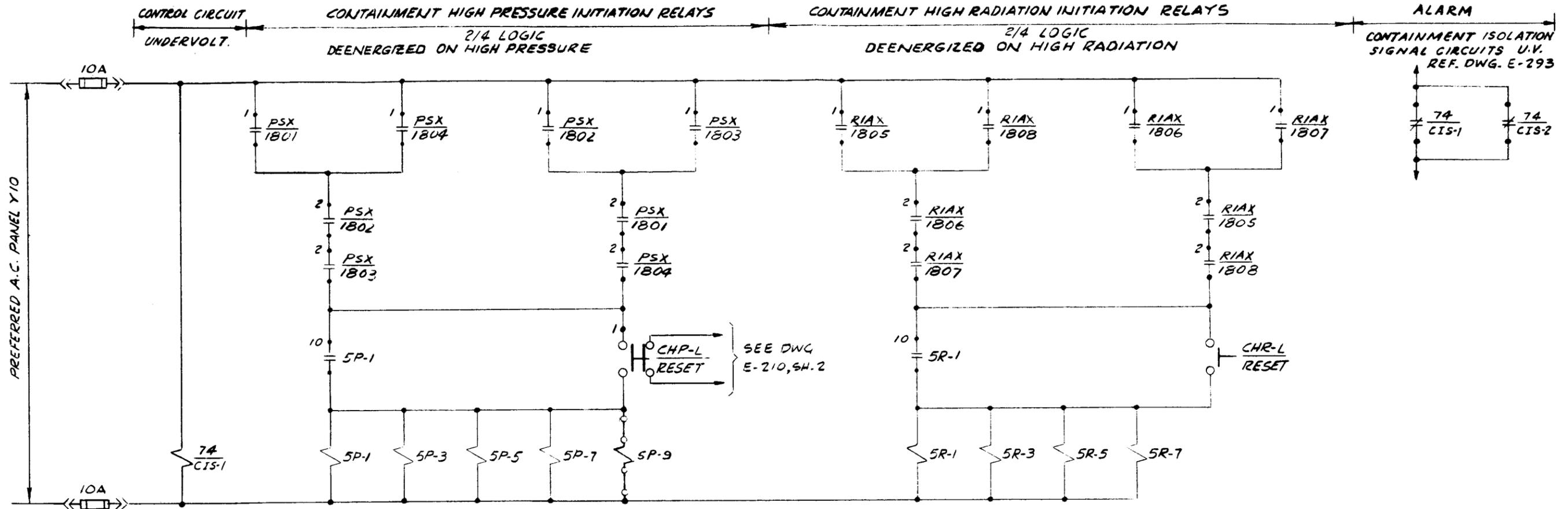


Fig. 4.2. Logic Diagram for the Safety Injection Signal Circuits of Engineered Safety Features in Palisades Plant. (Based on Refs. 13 and 24)

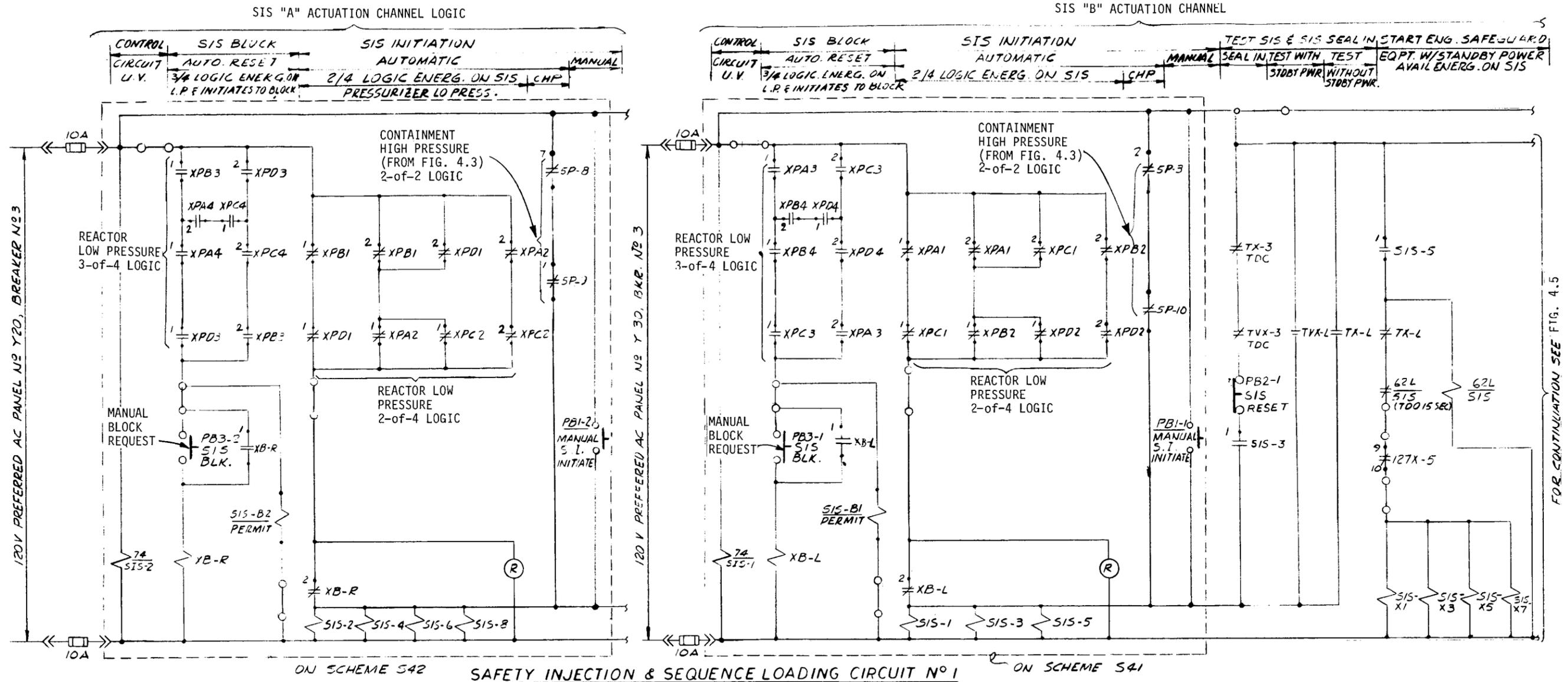


CONTAINMENT HIGH PRESSURE OR HIGH RADIATION ISOLATION CIRCUIT N^o 1
SCHEME N^o 503
ONE OF TWO IDENTICAL CIRCUITS

ADAPTER TABLE

CIRCUIT	SCHEME N ^o	PREF. AC.		RELAYS		PSX, RIAx CONTACTS	P.B.		LOCATIONS	U.V. RELAY 741	RELAY	
		PV	3KR	NO	SECTION		CHP-L	CHP-R			NO.	LOC.
1	503	Y10	3	5P-1, 5P-3, 5P-5, 5P-7 5R-1, 5R-3, 5R-5 & 5R-7.	C13-4	1 & 2	CHP-L RESET	CHP-L RESET	C13L	CIS-1	5P-9	C13R
2	504	Y40	3	5P-2, 5P-4, 5P-6, 5P-8, 5R-2, 5R-4, 5R-6 & 5R-8.	C13-5	3 & 4	CHP-R RESET	CHP-R RESET	C13R	CIS-2	5P-10	C13L

Fig. 4.3. Containment High Pressure and Containment High Radiation Logic Matrices for Engineered Safety Features in Palisades Plant. (From Ref. 24 with additions)



SAFETY INJECTION & SEQUENCE LOADING CIRCUIT N°1

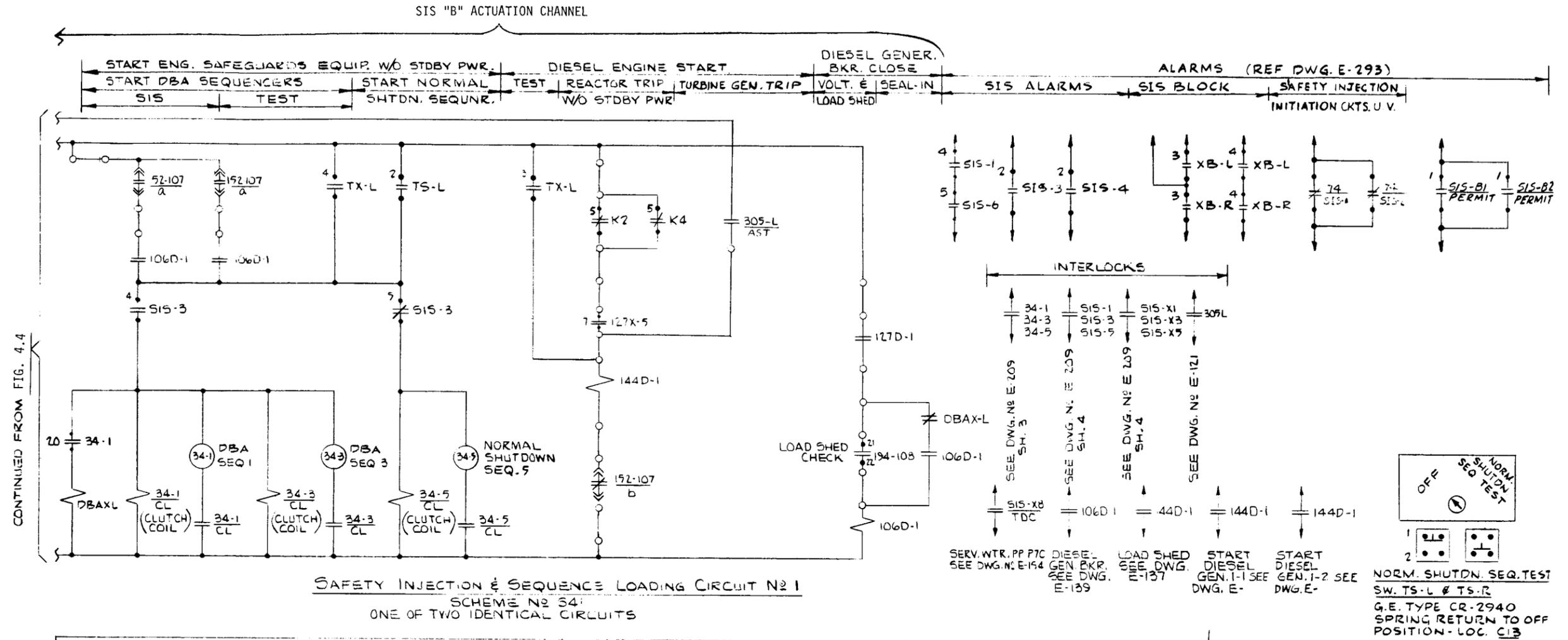
SCHEME N° S41
ONE OF TWO IDENTICAL CIRCUITS

ADAPTER TABLE

DESCRIPTION	SCHEME N°	PREF. AC. BKR. BKR.	AUXILIARY RELAYS			MAINTAINED SI INITIATION RELAYS	MOMENTARY RELAYS				SIS T/D RELAY	L.V. RELAY	TIME DELAY RELAY			
			L.P.S.I.	CHPX-3	SIS BLOCK		LOCATION	SIS WITHSTANDBY POWER RELAYS	SIS-X1	SIS-X3				SIS-X5	SIS-X7	
S.I. & SEQ. LOADING CKT. N°1	S41	Y30	3	XPA1, XPB2, XPC1, XPD2	L	XPA3, XPB4, XPC3, XPD4	C12L	SIS-1, 3, 5	—	SIS-X1	SIS-X3	SIS-X5	SIS-X7	62L SIS	SIS-1	CHPX-3L TDC
S.I. & SEQ. LOADING CKT. N°2	S42	Y20	3	XPA2, XPB1, XPC2, XPD1	R	XPA4, XPB3, XPC4, XPD3	C12R	SIS-2, 4, 6	SIS-8	SIS-X2	SIS-X4	SIS-X6	SIS-X9	62R SIS	SIS-2	CHPX-3R TDC

Fig. 4.4. Actuation Channel Circuits for Safety Injection and Sequence Loading of Engineered Safety Features in Palisades Plant - Part A.
(From Ref. 24 with additions)

FOR CONTINUATION SEE FIG. 4.5



CONTINUED FROM FIG. 4.4

ADAPTER TABLE															
DESCRIPTION	SCHEME NO	LOCATION	REF. AC.	SEQ.	REACTOR TRIP RELAY CONTACTS	DBA RESET	DIESEL ENGINE		DIESEL GEN. BKR.		S.I. PB.			NO STDBY PWR CONT.	LOAD SHED RELAY
							U.V.	START RELAY	CLOSE RELAY	"b" CONT.	MAN. INIT.	RESET	BLOCK		
S.I. & SEQ LOADING CKT. NO 1	S41	A11 C06L C04L C13L C22	Y10	34-1,3,5	K2/5#K4/5	DBAXL	127D-1	144D-1	106D-1	152-107 b	PB1-1	PB2-1	PB3-1	127X-5/5#7	194-108
S.I. & SEQ LOADING CKT. NO 2	S42	A12 C06R C04R C13R C26	Y20	34-2,4,6	K1/5#K3/5	DBAXR	127D-2	144D-2	106D-2	152-213 b	PB1-2	PB2-2	PB3-2	127X-6/5#7	194-211

NORM. SHUT-DN SEQ TEST PUSHBUTTON	CHP RELAY CONTACTS
TS-L	5P-3/2, 5P-10/1
TS-R	5P-4/2, 5P-9/1

Fig. 4.5. Actuation Channel Circuits for Safety Injection and Sequence Loading of Engineered Safety Features in Palisades Plant - Part B. (From Ref. 24 with additions)

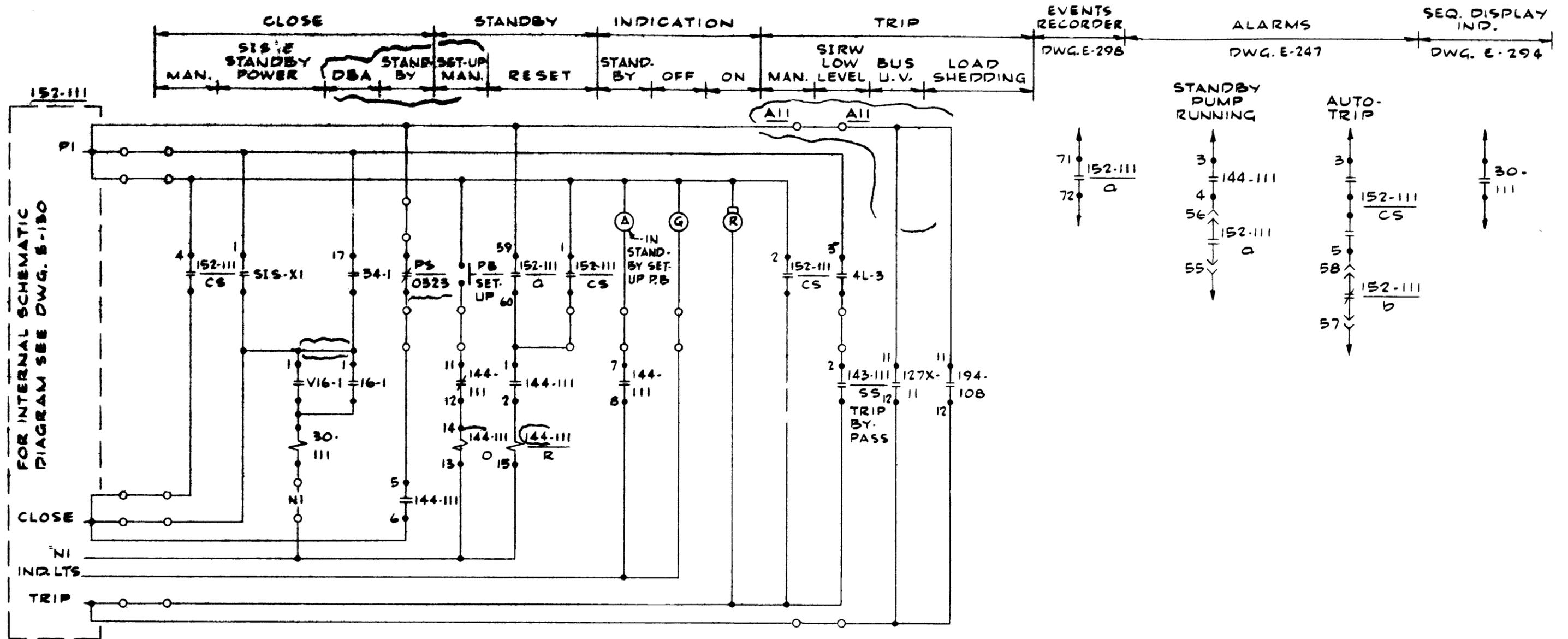
pressurizer low-low pressure instrument channels operate the contacts XPA1 through XPD1 and XPA2 through XPD2 that make up the two-of-four matrices. These instrument channels and output relays are deenergized to trip. Output relays from the two containment high-pressure matrices, shown in Fig. 4.3, are used in both the A and B actuation channels. These operate contacts 5P-8 and 5P-9 in the A actuation channel and contacts 5P-3 and 5P-10 in the B channel. The SIS relays, designated SIS-1, -3, and -5 in the B actuation channel, are energized to actuate the B set of engineered safety systems if either the low-low pressure matrix gives a trip signal or both containment high-pressure matrices give trip signals. The two containment high-pressure matrices are both used in each actuation channel in a two-of-two logic arrangement of their output relays to avoid a spurious initiation of the engineered safety actions, particularly the containment spray system, upon loss of the logic power supply or a relay failure in one of the containment high-pressure matrices, which are deenergized to trip. The containment high-pressure matrices were designed²⁴ to be deenergized to trip because they are also used to actuate the containment isolation system where it is necessary to use this fail-safe feature upon loss of power. An earlier design²³ was somewhat simpler in that it used a different plant variable that was used only in the safety injection actuation system, and a single energize-to-trip matrix was used for each actuation channel, as is now done for the low-low pressure signals.

The manner in which the SIS relays put the engineered safety equipment into operation depends on the type of power available to drive the equipment. If standby electrical power is available from off-site sources, all engineered safety systems are started at one time by momentarily energizing the SIS-X sets of relays. If standby power is not available, DBA (design-basis-accident) sequencers are used for load shedding and connecting the engineered safety loads (that can be operated by the Diesels) to the emergency power buses in a timed sequence so that the Diesels will not be overloaded during motor starting. The B set of loads is split between DBA sequencers 34-1 and 34-3 in the B actuation channel in Fig. 4.5. Not all engineered safety feature loads are started automatically when Diesel power is being used; however, each Diesel generator is sized to supply the minimum engineered safety feature load requirements following

a safety injection signal. The high-pressure injection pumps, component cooling pumps, and charging pumps are supplied in sets of three each.¹⁴ Two in each set are started automatically and are powered by separate Diesels. The third pump in each set of component cooling pumps and charging pumps is interrogated momentarily by the DBA sequencer and is started only if the pressure in the pump header is low, indicating that the other pumps failed to start. The third pump in each set can also be started manually.

The actuation channel circuits of the safety injection system must be blocked to avoid initiating operation of the safety injection equipment when the reactor is shut down for refueling or maintenance and the primary system is depressurized. The safety injection system circuits may be blocked manually (with push buttons PB 3-1 and -2), but this blocking action is effective only when three of the four pressure instrument channels indicate a pressure below 1700 psi. This permissive is developed with the three-of-four logic matrix made up of contacts XPA3 through XPD3 and XPA4 through XPD4 in the A and B actuation channels of Fig. 4.4. Relay XB-L is used to block safety injection in the B actuation channel by preventing the SIS relays from being energized. If the block is not initiated manually, the safety injection equipment is actuated when the pressure falls below 1525 psi by the two-of-four matrices described earlier. The relays that give the block permissive and the relays that initiate safety injection are controlled from separate contacts that operate at the pressures mentioned above in meter relays in each of the four main pressure-measurement channels (illustrated in Fig. 3.4). After the primary system is placed back in service and the pressurizer pressure is restored to normal, the SIS blocks are automatically removed when two of the four pressure instrument channels indicate pressure above 1700 psi.

The schematic diagram for the motor control circuit for one of the low-pressure safety injection pumps shown in Fig. 4.6 is a typical example of how the safety injection signals are used to actuate the various engineered safety-feature loads. This motor control circuit actuates the "close" and "trip" coils of the breaker supplying power to the pump motor. These coils are not shown in Fig. 4.6, but they are part of the breaker indicated by the dashed box (designated as 152-111). The breaker latches



LOW PRESSURE SAFETY INJECTION PUMP P67B
SCHEME A1111

Fig. 4.6. Control Circuit for a Low-Pressure Safety Injection Pump in Engineered Safety Features in Palisades Plant. (From Ref. 14 with additions)

into the closed position when its close coil is energized, and the trip coil must be energized to open the breaker. If standby power is available, the low-pressure pump is started when the SIS-X1 relay in the B actuation channel is momentarily energized. If only Diesel power is available, the low-pressure pump is started when the contact from DBA sequencer 34-1 momentarily closes. Since the actuation signals are momentary, the pump can be stopped manually during the course of the accident to allow the operator to realign the pumping systems as the flow requirements decrease. The control circuit also has provisions for manually placing the pump in a standby setup condition. In this condition, the pump is automatically started if pressure switch PS/0323 opens to indicate low pressure in the header served by the two low-pressure pumps. (This feature could be used in the latter stages of an accident to automatically restart one low-pressure pump if the other one then in operation should fail.)

The other engineered safety systems that employ pumps and motors and the containment isolation valves^{13,24} for the component cooling water discharge are actuated in a manner similar to that used for the low-pressure pumps. However, the system that actuates the containment spray equipment is arranged in a somewhat different fashion. The starting of the containment spray pumps requires the agreement of an SIS signal from one of the actuation channels (Fig. 4.4) and the output signal from one of the two-of-four logic matrices for containment high pressure (Fig. 4.3), that is, a final two-of-two logic arrangement. With this arrangement the containment spray can be initiated with a containment high-pressure signal but not a reactor low-low pressure signal (that can also initiate most other engineered safety actions). Since the SIS actuation channels include a two-of-two logic arrangement of the outputs of both containment high-pressure matrices, the spurious loss of logic power for one of the containment logic matrices (actuating channels) will not initiate an unwanted containment spray. Each of the containment spray valves is controlled by the output of one of the containment high-pressure matrices. As mentioned earlier, these matrices are deenergized to initiate action, so a spurious loss of power for one of the logic matrices will open a containment spray valve; however, the pumps will not start.

The system^{13,23,24} that actuates the majority of the containment isolation valves is also arranged in a somewhat different fashion. Again, dual sets of two-of-four logic signals from four sensors for each plant variable are employed, but both the A and B sets of logic (actuating channels) are combined in the individual solenoid control circuits for each isolation valve. The A and B actuating channels must both be deenergized (in a final two-of-two logic arrangement) to deenergize the solenoid, which, in turn, cuts off the air pressure holding the isolation valve actuator open against a spring force and allows the isolation valve to close. The spurious loss of logic power in one of the two actuating channels will not close the isolation valve; however, spurious loss of electric power to the solenoid on loss of air pressure will close that isolation valve.

4.1.3 Power Supplies

The four instrument channels are supplied²³ separately from the four preferred 120-v ac buses. The preferred buses are powered by four inverters from two independent 125-v dc buses. These dc buses are supplied from two independent 480-v ac buses through battery charges. A station battery floats on each dc bus to give continuity in power. The 480-v buses are in turn supplied from two independent 2400-v ac buses, each of which can be powered separately by its own Diesel generator.

The sets of logic in the A and B actuation channels used to actuate the engineered safety systems are supplied separately from two of the preferred 120-v ac buses, which are in turn supplied separately from the two 125-v dc buses. One Diesel generator supplies emergency power for the B set of engineered safety systems in keeping with the "two-channel concept." The engineered safety equipment is connected to the emergency power by the DBA sequencers.

It appears that the spurious loss of one of the dc buses will trip two instrument channels and will start some of the engineered safety sub-systems.

4.1.4 Testing Arrangements

The logic matrices for all engineered safety features and the containment isolation systems can be tested only^{14, 23, 24} while the plant is shut down, but the remaining engineered safety system components can be tested while the plant is in operation. The actuating relays, such as the SIS relays and DBA sequencers, are energized through test circuits, and the various engineered safety system pumps are started and the automatic valves in most systems are opened. The safety injection systems do not have sufficient head to pump coolant into the primary system at operating pressure.²⁴

The containment spray system is one of the few exceptions to the testing approach, since the pumps are test-operated only when the spray admission valves are closed, and spray admission valves are only test opened when the pumps are not running. Interlocks are used to enforce this testing sequence to prevent actually spraying the containment vessel during a test.

The test push button for the A or B portions of the engineered safety system must be depressed for the duration of the test. When the push buttons are released the engineered safety circuits reset to their normal condition. With this push-button arrangement, the designers²⁴ did not feel that it was necessary to provide any automatic override for the portions of the engineered safety system that are defeated during the test cycle.

4.1.5 Isolation of Circuits

The engineered safety instrumentation system and the operation system use separate instruments and circuits.¹⁴ The four instrument channels for each plant variable in the engineered safety system are physically isolated²³ from each other, but some instrument channels are shared¹⁴ with the reactor shutdown system, as shown in Fig. 3.4. The A and B actuation channel circuits appear to be isolated from each other with separate logic matrices, power sources, and actuating relays.

4.2 Oconee Nuclear Station, Units 1 and 2

4.2.1 Instrument Channels and Major Function Requirements*

The Babcock & Wilcox Company is designing a three-channel instrumentation system^{10,11} for the Oconee Station of the Duke Power Company. The plant variables used in the engineered safety systems and the major engineered safety functions that they actuate are listed in Table 4.1. Some other necessary (and complicating) features, such as the alignment of valves in the systems and the control of emergency power, are not listed in this simplified table. The coolant injection pumps, for example, initially take suction from the borated water storage tank. When the tank is empty the operator manually realigns the valves in the system so that the low-pressure pumps can take suction from the sump in the containment building.

For most variables used in the engineered safety instrumentation system, three process sensors are provided, together with their associated transmitters, bistable units, and channel output relays, as shown in Fig. 4.7. The high reactor building pressure channels used to actuate the reactor building spray system are different in that pressure switches are used instead of the analog transmitter-bistable-relay type of instrument channel used in the rest of the engineered safety system. Also, six pressure switches (three for each of the two actuation channel matrices) are employed, rather than three. The reactor building cooling units and the reactor building isolation systems are also actuated by high reactor building pressure signals; however, the analog type of instrument channel is employed for this application.

The trip signals on low reactor coolant pressure can be bypassed manually to prevent high-pressure and low-pressure safety injection during plant startup and during cooldown and depressurization. These bypasses can only be initiated under the conditions indicated in Table 4.1, and the bypasses are automatically removed after the coolant pressure exceeds the

*After the preparation of this report, the final safety analysis report was issued, which indicates that several of the trip points have been changed.

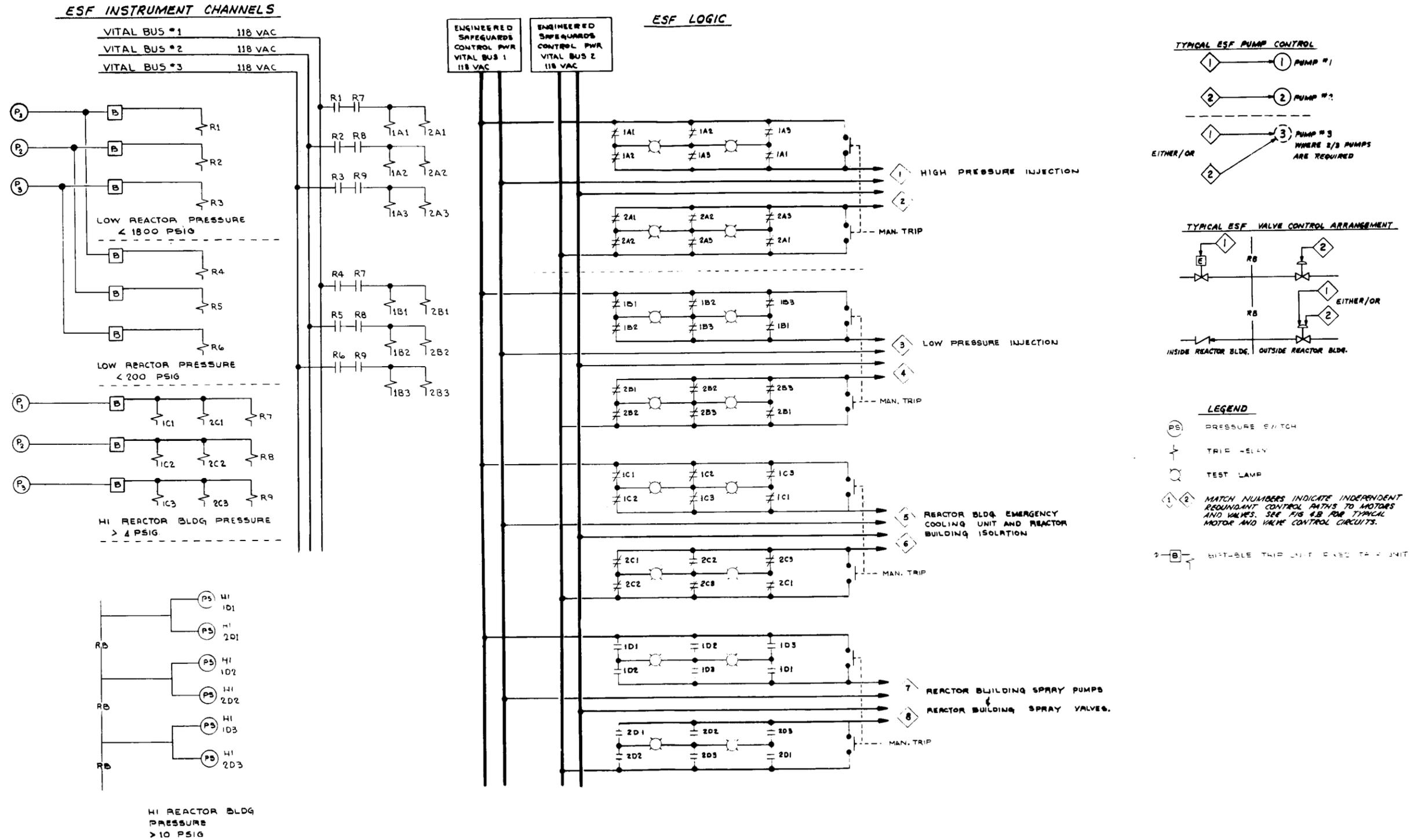


Fig. 4.7. Simplified Instrument Channels and Actuation Channel Circuits for Engineered Safety Features in Oconee Station. (From Ref. 11 with additions)

Table 4.1. Plant Variables and Major Functional Requirements of Engineered Safety Features at Oconee Nuclear Station

Function	Plant Variables	Trip Set Point (psig)	Bypasses
High-pressure injection	Low reactor coolant pressure	1800	Manual bypass permitted between 1800 to 1900 psig and at startup pressure; bypass removed by coolant pressure above 1900 psig
	or		
Low-pressure injection	High reactor building pressure	10	None
	Very low reactor pressure	200	
Start reactor building emergency cooling unit and reactor building isolation	or		Manual bypass permitted between 200 and 400 psig and at startup pressure; bypass removed by coolant pressure above 600 psig
	High reactor building pressure	10	
Reactor building spray	High reactor building pressure	4	None
		10	

value indicated. The bypassing is done on a channel-by-channel basis with a separate bypass circuit for each low-pressure bistable unit.

4.2.2 Typical Logic Arrangement and Actuation Channel

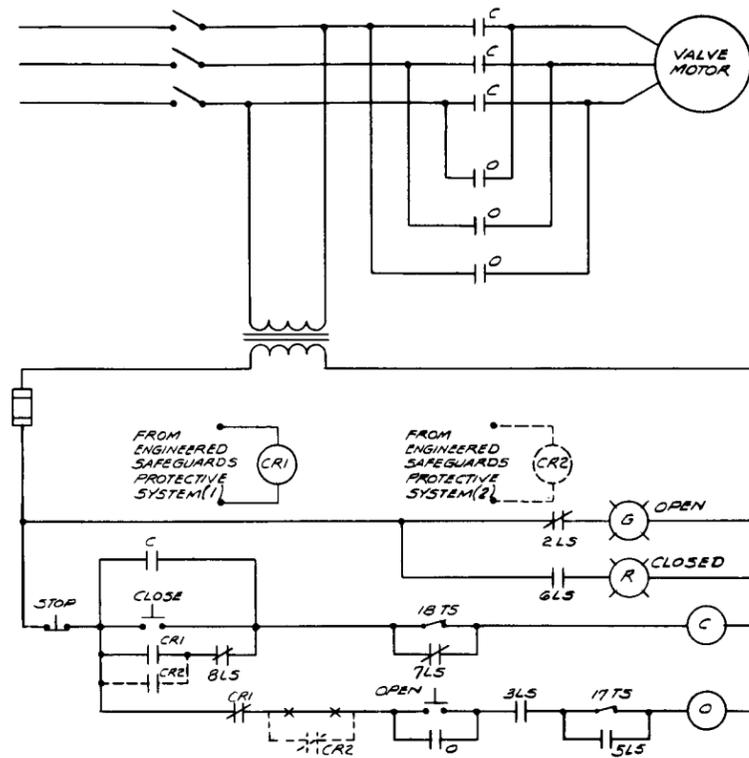
The logic arrangement for the Oconee Station is shown in the simplified diagram in Fig. 4.7. The outputs of the three bistable devices associated with most of the plant variables are used in two sets of identical and independent two-of-three logic matrices, termed actuation channels.

The high- and low-pressure coolant injection systems employ one-of-N logic channels to combine the trip signals from two plant variables in a general coincidence logic. The reactor building spray system is actuated by three separate pressure switches for each of the actuation channels. The engineered safety equipment is divided between the two redundant actuation channels illustrated by the typical control schemes for pumps and valves in Fig. 4.7. The division of equipment between the two actuating channels is based on the redundancy of equipment and functions, and it is done in such a way that the failure of one of the actuating channels and the associated engineered safety equipment will not inhibit the overall engineered safety function. Where active and passive (check valve) engineered safety valves are used redundantly, the active valve will be equipped with two OR control elements, each driven by one of the engineered safety actuation channels. Redundant engineered safety pumps will be controlled in the same manner as redundant active valves.

The bistable units and output relays in the instrument channels are deenergized to trip, and the logic matrices are energized to trip and actuate the engineered safety equipment. Separate power supplies are used for each actuation channel.

Figure 4.8 shows typical control circuits for equipment serving engineered safety functions. One logic circuit shown in Fig. 4.7 serves as a common input to all engineered safety equipment in that actuation channel. A separate TEST-AND-BLOCK module is provided for each pump and valve operator. The logic power energizes the R_0 relay in the output of the TEST-AND-BLOCK module. A contact of the R_0 relay controls a control relay (CR1 or CR2) in the motor or valve control circuit. The CR relays received their power from the associated motor control circuit. Both R_0 and CR are energized to actuate the engineered safety equipment. The individual motor control circuits for pumps employ either mechanical latch-in or electrical seal-in features, so the pumps continue to run after receiving the initial automatic actuation signal when the individual control relays (CR1 and CR2) are energized. In a similar manner, the motor-driven valves continue to move until stopped by limit switches after the valves receive an initial actuation signal. Once the logic system has given a trip signal and the engineered safety equipment is operating, the block

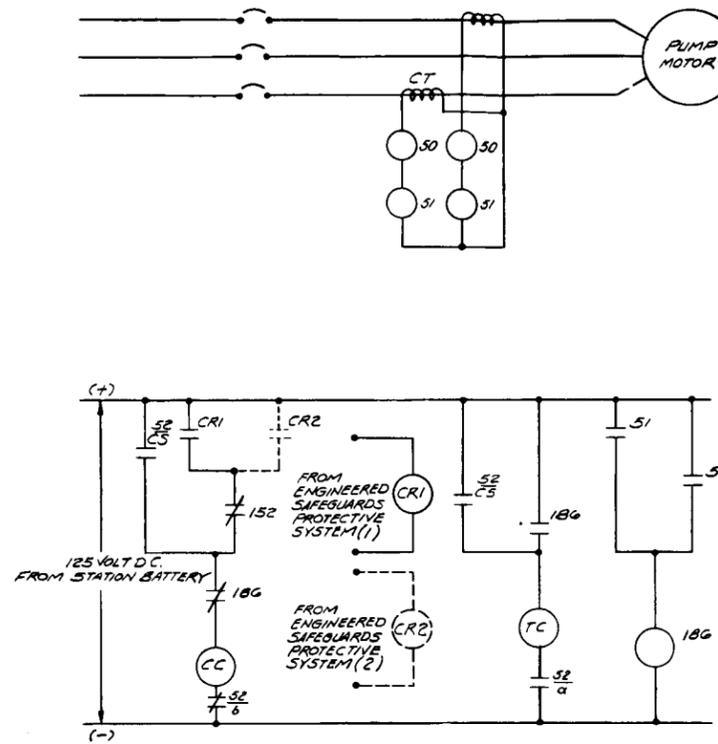
TYPICAL REACTOR BUILDING ISOLATION VALVE



SWITCHES AND CONTACTS SHOWN WITH VALVE IN FULL OPEN POSITION
 C - MAIN CONTACTOR, CLOSING
 O - MAIN CONTACTOR, OPENING
 CR1 - CONTROL RELAY
 CR2 - CONTROL RELAY
 TS - TORQUE SWITCH
 LS - LIMIT SWITCH

LIMIT SWITCH CONTACT DEVELOPMENT				
CONTACT	VALVE FULL OPEN	INTERMEDIATE VALVE POSITION	VALVE FULL CLOSED	CONTACT FUNCTION
1	CLOSED	OPEN	OPEN	SPARE
2	CLOSED	OPEN	OPEN	OPEN IND LT
3	OPEN	CLOSED	CLOSED	OPEN LIMIT
4	OPEN	CLOSED	CLOSED	SPARE
5	OPEN	OPEN	CLOSED	TORQUE SW BYPASS
6	OPEN	OPEN	CLOSED	CLOSED IND LIGHT
7	CLOSED	CLOSED	OPEN	TORQUE SW BYPASS
8	CLOSED	CLOSED	OPEN	HOLD IN CIRCUIT
17	OPENING TORQUE SWITCH - OPENS ON MECHANICAL OVERLOAD IN OPENING DIRECTION			
18	CLOSING TORQUE SWITCH - OPENS ON MECHANICAL OVERLOAD IN CLOSING DIRECTION			

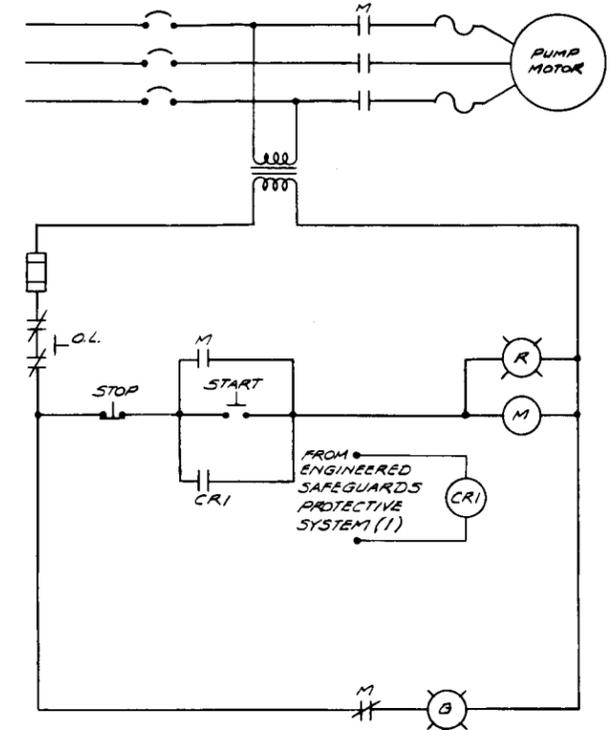
CONTROL CIRCUIT FOR LOW PRESSURE INJECTION PUMP (CIRCUIT BREAKER CONTROL)



CONTACTS SHOWN IN DEENERGIZED POSITION
 CR1 - CONTROL RELAY
 CR2 - CONTROL RELAY
 CC - CIRCUIT BREAKER CLOSING COIL
 TC - CIRCUIT BREAKER TRIP COIL
 50 - INSTANTANEOUS OVERCURRENT RELAY
 51 - TIME OVERCURRENT RELAY
 CS - CIRCUIT BREAKER CONTROL SWITCH
 152 - CIRCUIT BREAKER AUXILIARY SWITCH
 186 - AUXILIARY TRIPPING RELAY

NOTE: CR2, SHOWN DOTTED, IS USED ONLY WHEN REDUNDANT CONTROL IS REQUIRED

CONTROL CIRCUIT FOR REACTOR BUILDING SPRAY PUMP (MOTOR STARTER CONTROL)



CONTACTS SHOWN IN DEENERGIZED POSITION
 CR1 - CONTROL RELAY
 M - MAIN CONTACTOR

TYPICAL CONNECTION OF CR RELAYS TO ESF LOGIC (FIG. 4.7) (FROM REF. 11)

FROM ESF LOGIC MATRIX (1) (FIG. 4.7)

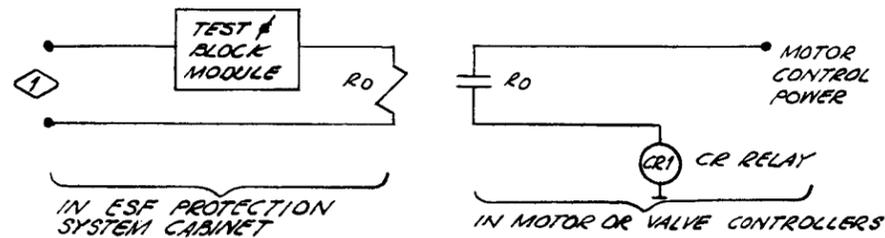


Fig. 4.8. Typical Control Circuits for Engineered Safety Equipment in Oconee Station. (From Refs. 10 and 11)

function of the TEST-AND-BLOCK modules may be used to remove individual engineered safety components from the control of the actuation channel and allow the operator to take manual control of the individual component.¹¹ The block function cannot be activated prior to a logic system trip, so it does not provide a means for negating the initial engineered safety action of the component. Air-operated engineered safety valves automatically go to their safe position upon loss of control air.

4.2.3 Power Sources

The three instrument channels are supplied separately from three of the four 120-v ac vital instrument buses described in Section 3.1.3. The two sets of logic used in the dual engineered safety feature actuating channels are also supplied separately from two of these vital instrument buses. As discussed in Section 3.1.3 the vital instrument buses are supplied through static inverters from a complex arrangement of dc buses, which include batteries floating on the line. We did not examine the sources of power for the engineered safety system pumps and motor operators. (Emergency power sources for heavy loads are somewhat more complicated in a station having three reactor units and using a hydro station rather than Diesels.)

4.2.4 Testing Arrangements

The instrument channels and logic matrices can be tested while the plant is in operation. The analog portions of channels for reactor variables are checked by manually comparing outputs of similar channels. The bistable units are tested by substituting a signal generator for the sensor. The indicating lamps in the logic matrices permit testing of the matrix contacts and the power sources for the logic matrices.

The pump and valve motors are tested separately from the instrument channels and logic. The TEST-AND-BLOCK modules, illustrated in Fig. 4.7, are used to test-operate individual pumps and valves during reactor operation. A test command signal energizes the R_0 relay and the CR relay to start the pump or valve motor. The valves are tested separately from the pumps in a given engineered safety system.

4.2.5 Isolation of Circuits

The engineered safety instrumentation system has instruments and circuits that are separate from both the reactor shutdown and operation systems. Additionally the instrument channels for plant variables are physically isolated from each other.

A single set of three reactor pressure sensors serves the actuation channels for both the high- and low-pressure coolant injection systems. A single set of three reactor building pressure sensors serves the actuation channels for the two coolant injection systems and the reactor building cooling units and isolation systems. Separate relays serve the different actuation channels to provide isolation (see Fig. 4.6). In the case of the reactor building spray system, three separate pressure switches are used for each of the actuation channels.

The duplicate matrices used in the two engineered safety feature actuation channels and the control circuits for the redundant sets of engineered safety equipment are isolated from each other and have separate power sources. A separate test-and-block module and an R_0 relay, illustrated in Fig. 4.7, are used for each pump and valve motor. These serve to isolate the individual motor control circuits from each other and from the logic matrix and logic power supply, which controls one of the redundant sets of engineered safety equipment.

4.3 Robert Emmett Ginna Nuclear Plant No. 1

4.3.1 Instrumentation Channels and Major Functional Requirements

The Westinghouse Electric Corporation is designing a multichannel instrumentation system^{16, 17} for the Ginna plant of the Rochester Gas and Electric Corporation. The reasons for the selection of part of this system and much of the design basis are discussed in a report by Burnett.¹⁸ Table 4.2 lists the plant variables used in the engineered safety systems, the number of channels of instrumentation, and the major engineered safety functions they actuate. Some other necessary (and complicating) features, such as the alignment of the valves in the system and the control of emergency power loading, are not listed in this simplified table. An automatic

Table 4.2. Plant Variables and Major Functional Requirements of Engineered Safety Features at Ginna Nuclear Power Plant

Function	Plant Variables and Logic Arrangement	Blocks and Permissives
1. Safety injection	One-of-three pairs of low coolant pressure signals coincident with low pressurizer water level signal, or two-of-three high containment pressure signals, or two-of-three signals of low steam pressure in either steam generator	Manual block permitted by two-of-three signals of low coolant pressure; block removed by two-of-three high coolant pressure signals
2. Containment spray	Coincidence of two sets of two-of-three high containment pressure signals	
3. Containment fans	Any safety injection signal or containment spray signal (starts idle fans)	
4. Containment isolation	Any safety injection signal or containment spray signal	
5. Steam-line isolation	Two-of-three high containment pressure signals, or one-of-two high steam flow signals in that steam line in coincidence with any safety injection signal and in coincidence with two-of-four low T_{av} signals, or one-of-two high-high steam flow signals in that line in coincidence with any safety injection signal	
6. Feedwater-line isolation and trip of main feedwater pumps	Any safety injection signal	
7. Start auxiliary motor-driven feedwater pumps	Two-of-three signals of low level in either steam generator, or opening of both main feedwater pump circuit breakers, or any safety injection signal	
8. Start auxiliary turbine-driven feedwater pumps	Coincidence of two-of-three signals of low level in both steam generators, or loss of voltage on both 4160-v buses	
9. Start Diesel generators and engineered safety feature loading	Any safety injection signal or undervoltage on either emergency 480-v bus served by one of the Diesels	

system is provided to switch the high-head safety injection pump suction from the boric acid tanks to the refueling water storage tank after the boric acid tanks have emptied. The operator must later manually realign the valves in the system so that the pumps can take suction from the sump in the containment building.

The containment isolation systems in newer Westinghouse designs¹⁷ have two stages of operation for the containment pressure trip signals. A high containment pressure signal ($\sim 10\%$ of design pressure) or a safety injection signal will isolate all containment lines except those needed to maintain normal shutdown cooling. A high-high containment pressure signal ($\sim 50\%$ of design pressure) will give isolation of all lines except those used in engineered safety systems. The containment spray will be activated at this high-high level of containment pressure.

The Westinghouse plants with four coolant loops will employ¹⁷ different plant variables to initiate steam-line isolation than those used in two-loop plants like Ginna.

4.3.2 Typical Logic Arrangement and Actuation Channel

The instrument channel output relays are arranged in local coincidence matrices for each plant variable. Figure 4.9 illustrates a typical logic arrangement¹⁷ for one plant variable. The outputs of the bistable devices PC in the four instrument channels are formed into two identical and independent two-of-four coincident logic networks or actuation channels (A and B). The engineered safety equipment is divided between the two redundant actuation channels. This division of equipment between the two actuating channels is based on the redundancy of equipment and functions, and it is done in such a way that the failure of one of the actuating channels and the associated engineered safety equipment will not inhibit the overall engineered safety function. The redundant engineered safety equipment is connected to the two actuation channels in a manner similar to that described in Section 4.2.2 for the Oconee Station.

Some of the more complex of the logic arrangements listed in Table 4.2 for engineered safety feature actuation are illustrated in the simplified logic diagram in Fig. 4.10. (This figure shows only part of the plant variables that can actuate the safety injection and containment spray

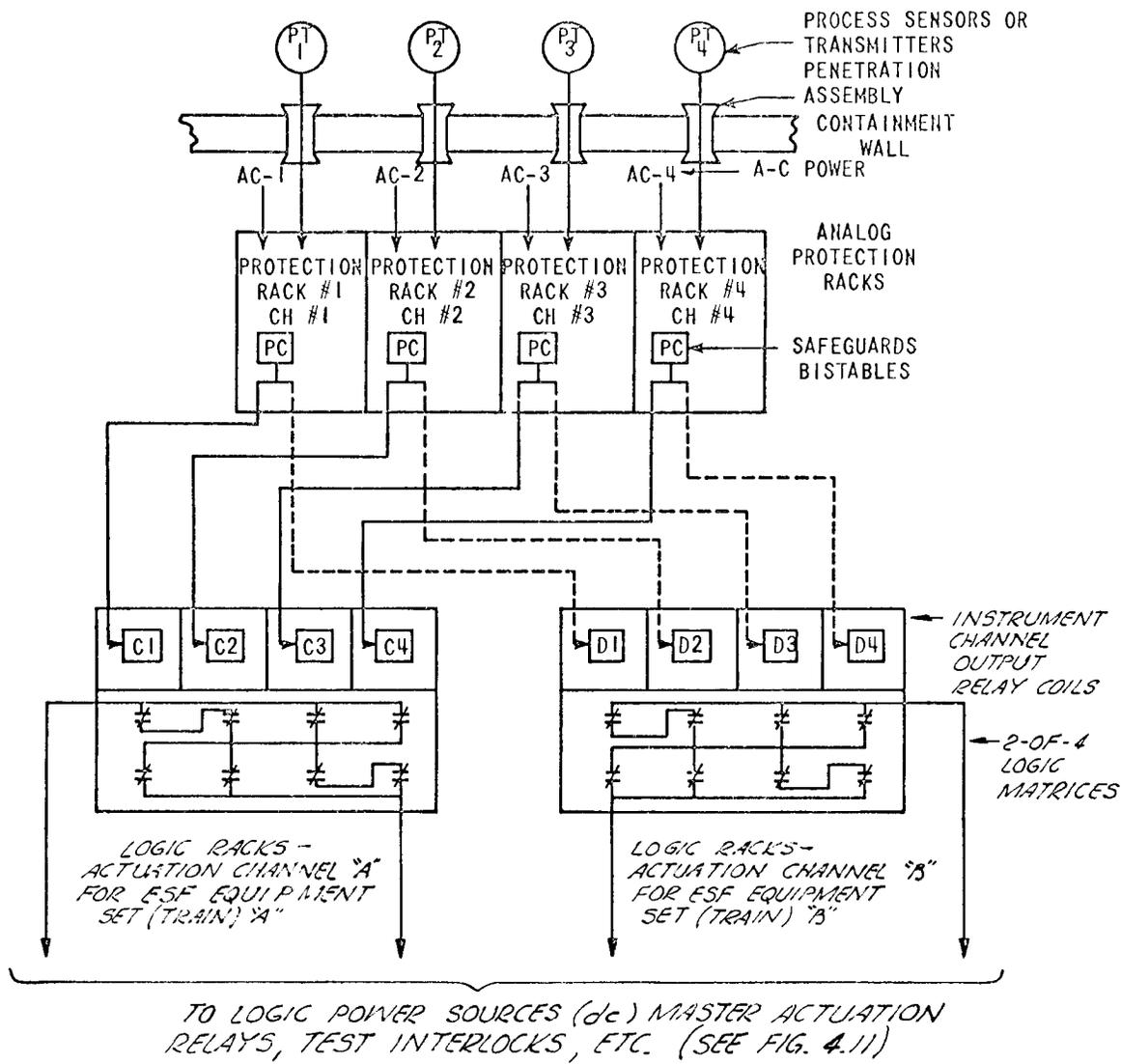
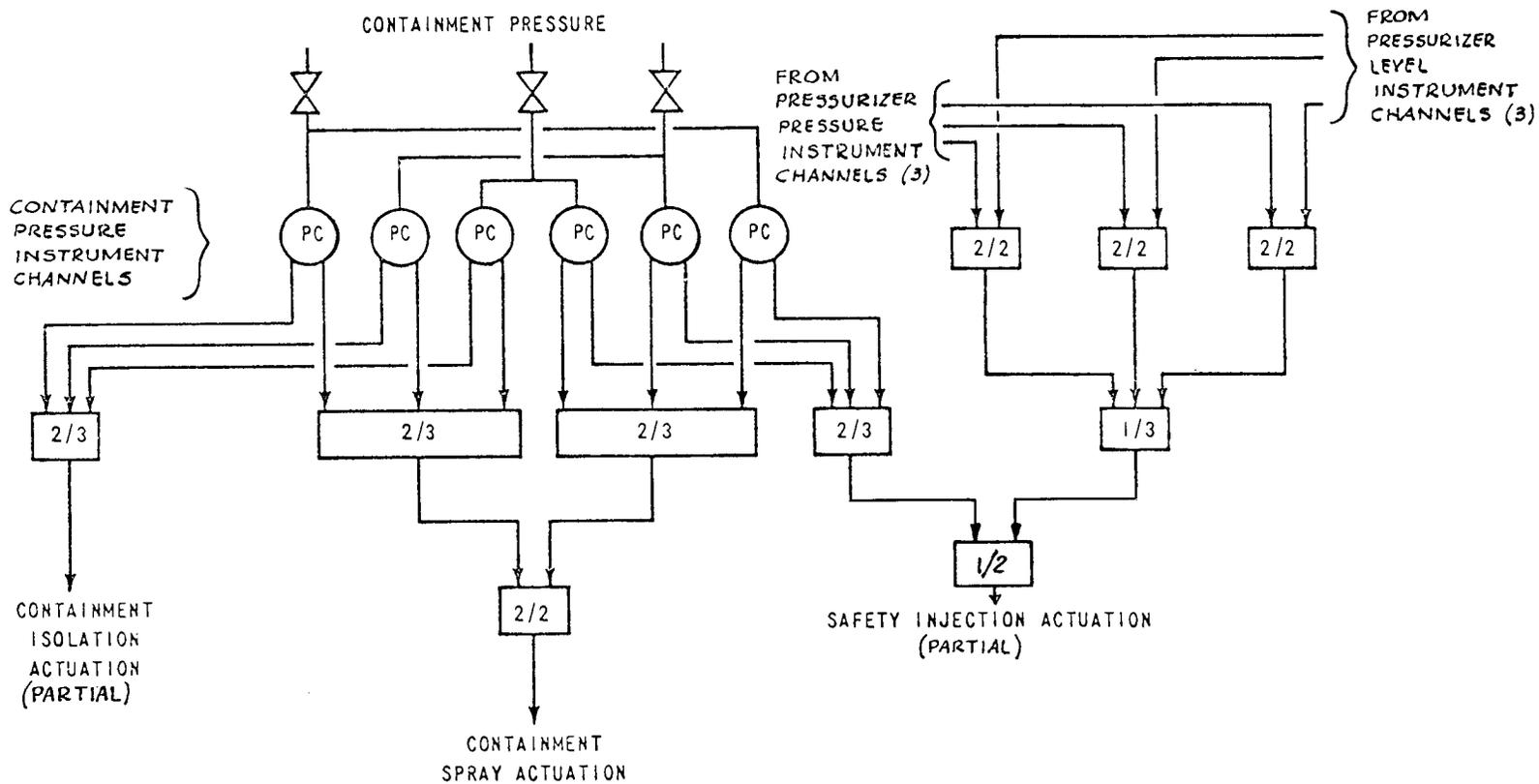


Fig. 4.9. Typical Instrument Channels and Logic Matrices for Engineered Safety Features in Ginna Plant. (From Ref. 17 with additions)

equipment, and it does not show the signals used to block the trip signals.) These logic matrices actuate one of the redundant sets of engineered safety equipment (i.e., train A) for the functions shown. These logic matrices are duplicated in the B set of actuation channels that actuate the other set of engineered safety equipment (i.e., train B). The six containment-pressure instrument channels, the three pressurizer-pressure instrument channels, and the three pressurizer-level instrument channels are shared between the logic matrices in the duplicate actuation channels. The actuation of the containment spray requires the coincidence of



Notes

1. Logic matrices are shown for Actuation Channel "A."
2. Above matrices are duplicated for Actuation Channel "B."
3. Instrument channels shown are shared between Actuation Channels "A" and "B" (per Fig. 4.9).
4. Other trip signals for safety injection and containment isolation are listed in Table 4.2.

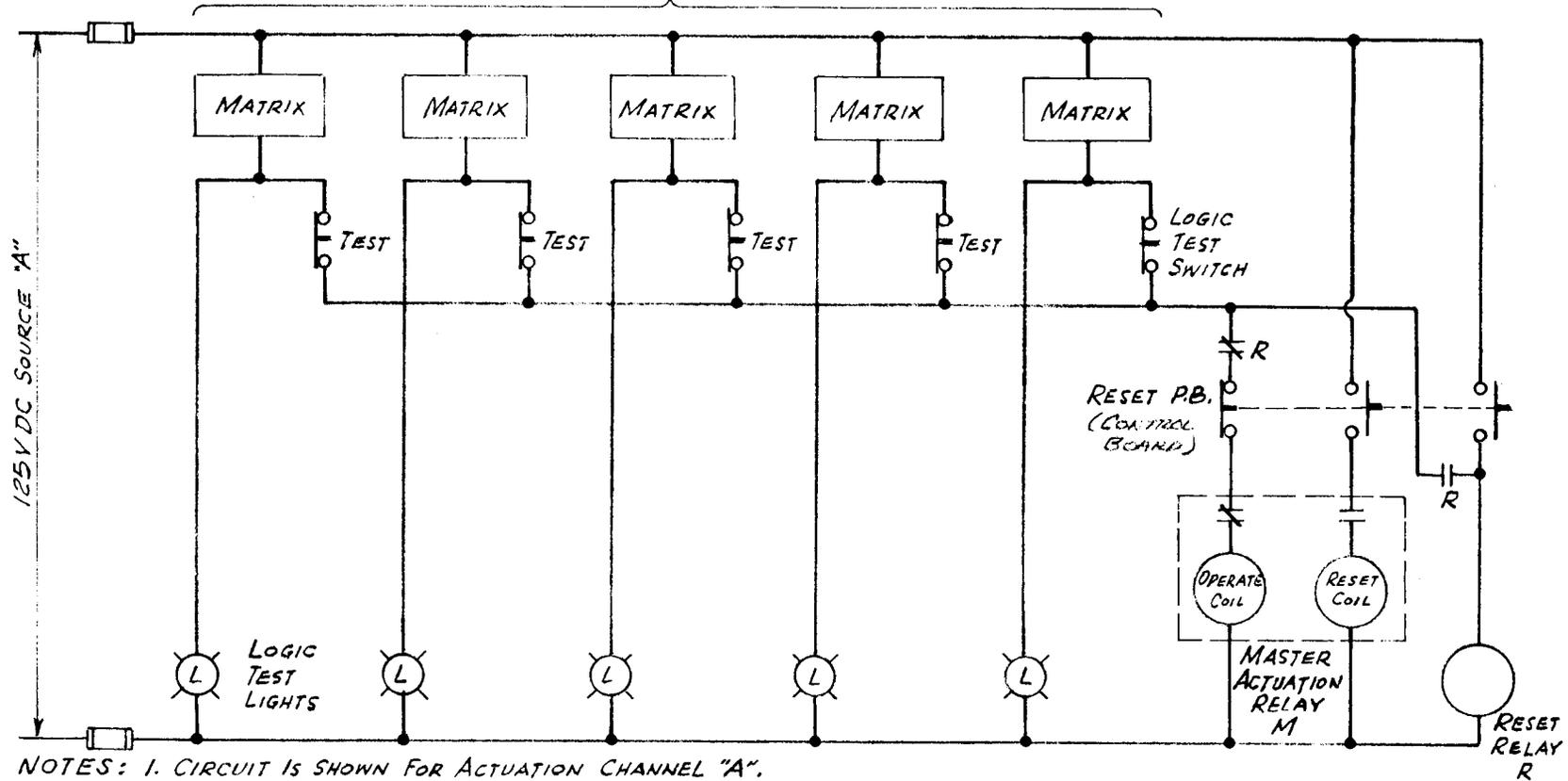
Fig. 4.10. Logic Diagram (Partial) for the Actuation of Safety Injection, Containment Spray, and Containment Isolation Systems in Ginna Plant. (From Ref. 16 with additions)

two sets of two-of-three logic matrices (or a selected four-of-six-logic arrangement). This somewhat complex logic system was developed¹⁷ to provide reliable initiation of containment spray equipment when it is actually needed and to also avoid spurious initiation, since the borated spray would cause damage to the extent that it would represent an economic penalty. The actuation of the safety injection system requires coincidence of a low pressurizer-pressure signal and a low pressurizer-level signal. This coincidence arrangement is used¹⁷ to prevent false actuation in the event of a spurious pressure or level signal. As shown in Fig. 4.10, any one of three redundant sets of these two-of-two logic matrices can initiate safety injection and thus provide reliable initiation when actually needed.

The bistable devices and output relays in most instrument channels are deenergized¹⁷ to trip. The instrument channels that actuate the containment spray equipment are exceptions in that they energize to trip (to avoid spurious actuations, as mentioned above). The logic matrices for the various plant variables controlling an engineered safety function are arranged in local coincidence to actuate a master relay M in the duplicate actuation channels for that engineered safety function, as illustrated in Fig. 4.11. The master relays for all engineered safety functions are energized¹⁷ to initiate action, so the matrices for different plant variables are arranged in parallel, as shown in Fig. 4.11. Separate dc power supplies are used for each of the two actuation channels. The master relays mechanically latch into the closed position once they are energized, so the dc power is needed only to start the engineered safety equipment.

Each device in the engineered safety system below the master relays in the actuation channels is arranged to remain in its operating condition until manually stopped or changed by the operator. The individual motor control circuits for pumps employ either mechanical latch-in or electrical seal-in features for this purpose. In a similar manner, the motor-driven valves continue to move until stopped by limit switches after the valves receive an initial actuation signal. The operator may take manual control of the engineered safety systems to realign them during the course of the accident by deenergizing the master relay with the manual RESET push

TYPICAL LOGIC MATRICES FOR PLANT VARIABLES USED
TO INITIATE OPERATION OF ENGINEERED SAFETY
FEATURES - ARRANGED IN LOCAL COINCIDENCE



- NOTES: 1. CIRCUIT IS SHOWN FOR ACTUATION CHANNEL "A".
2. ABOVE CIRCUIT DUPLICATED FOR ACTUATION CHANNEL "B".
3. MASTER RELAY IS ENERGIZED TO INITIATE OPERATION OF ENGINEERED SAFETY FEATURES FOR SET "A" BY MEANS OF SLAVE RELAYS.

Fig. 4.11. Typical Actuation Channel Circuit for Engineered Safety Features in Ginna Plant. (Redrawn from Ref. 17)

button shown in Fig. 4.11. The actuation channel circuit is restored to its original condition when the trip signal from the logic matrices clears and the separate reset relay R is deenergized.

The valves that are air operated by electrical solenoid pilot valves are arranged to move to the "safe" position on loss of air or solenoid power.¹⁷ The master relays controlling the solenoids are energized to trip as in the other portions of the engineered safety system.

4.3.3 Power Sources

The instrument channels are supplied separately from four 120-v ac buses, as described in Section 3.3.3. The dual sets of logic matrices in the two actuation channels are supplied separately with dc power from the two station batteries.

One Diesel generator provides emergency power for the A set of engineered safety equipment, and the B set is supplied separately from a second Diesel generator. A separate timer¹⁷ is provided for each motor to sequentially connect the loads to the emergency power buses.

4.3.4 Testing Arrangements

The on-line provisions for testing the analog and bistable portions of each instrument channel are shown in Fig. 4.12. The method is similar to that described in Section 3.3.4 for the reactor shutdown system instrument channels.

The logic matrices are tested while the plant is in operation. The LOGIC TEST switches (or push buttons) are depressed in two instrument channels to test the transmission of the coincident trip signal through the matrix. This is monitored by the test lights shown in Figs. 4.11 and 4.12, which also show how the LOGIC TEST switch opens the output of the matrix to prevent the master relay from actually being energized.

The operation of the master relay is not tested while the plant is in operation; however, the integrity of the master relay coil is checked with a continuity monitor.¹⁷ The engineered safety feature pumps and valves can be operated individually during plant operation. The valves appear to be tested separately from the pumps in a given system, and the

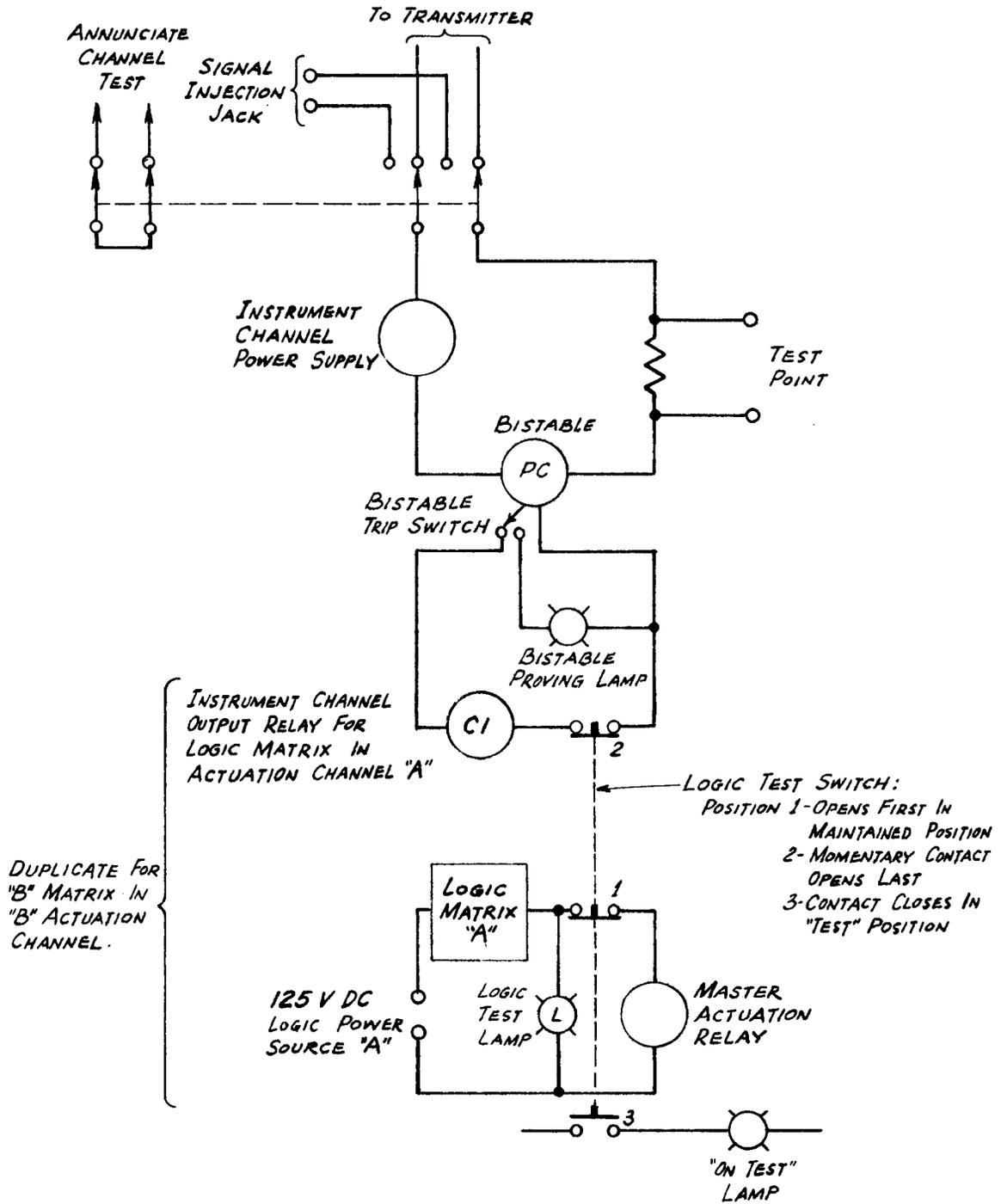


Fig. 4.12. Testing Arrangement of Instrument Channel and Logic Matrix for Engineered Safety Features in Ginna Plant. (Redrawn from Ref. 17)

engineered safety features are tested in an integrated manner during plant shutdowns.

4.3.5 Isolation of Circuits

Several of the same process sensors are used in the engineered safety, reactor shutdown, and plant operation instrumentation systems. The signals used in the plant control and supervisory systems are taken from the protection system through isolation amplifiers.¹⁸

Redundant instrumentation channels for each of the plant variables are physically isolated from each other, as shown in Fig. 4.9. The two sets of matrix relays for each of the two actuation channels are located in separate logic racks. Separate dc sources serve the logic matrices and master relays in the two engineered safety feature actuation channels.

4.4 Dresden Nuclear Power Station, Unit 2

4.4.1 Instrument Channels and Major Functional Requirements

The General Electric Company is designing the protection instrumentation system for Unit 2 of the Dresden Nuclear Power Station for the Commonwealth Edison Company.^{20,25,26} Four instrument channels are used for most of the main variables. (The Dresden-2 station is discussed rather than Browns Ferry because more information is available. The protection systems for the two plants will be similar in design.) The main plant variables used in the engineered safety systems and the automatic functions they actuate are listed in Table 4.3. Some other necessary features, such as the alignment of valves to make a flow path, identification of a damaged recirculation loop, control of minimum flow bypass, stopping of unnecessary pumps, means for cancelling the initiation signals, and the control of emergency power, are not listed in this simplified table.

The plant variables listed for the initiation of the opening of the automatic pressure-relief valves are different from those given in the safety analysis report. General Electric²⁰ has indicated that this revised set of variables will be used in Dresden-2 and in future boiling-water reactor designs.

Table 4.3. Plant Variables and Major Functional Requirements of Engineered Safety Features at Dresden-2 Nuclear Station

Function	Plant Variables and Logic Arrangement
1. High-pressure coolant injection (HPCI)	One-of-two taken-twice logic arrangement of either low-low reactor water level or high containment (drywell) pressure
2. Automatic pressure relief (see text)	One-of-two taken-twice logic arrangement of four pairs of low-low reactor water level coincident with high containment (drywell) pressure
3. Core spray	
3.1 Start system	One-of-two taken-twice logic arrangement of either low-low reactor water level or high containment (drywell) pressure
3.2 Open admission valve to reactor	Start system signal from item 3.1 in coincidence with one-of-two low reactor pressure signals
4. Low-pressure coolant injection (LPCI)	
4.1 Start system	Same as for core spray
4.2 Open admission valves to reactor	Same as for core spray
5. Containment isolation	See block diagram in Fig. 4.13

The various plant variables used in the containment isolation portion of the engineered safety system are shown in detail in Fig. 4.13. At least five different protection instrumentation systems will be used for containment isolation.

Most instrument channels used in the protection system for pressure and water level measurements consist of nonindicating pressure switches. The reactor water level channels, however, have indicating pressure switches. Many of the sensors are shared between different subsystems that carry out different protective functions.

During plant startup or normal shutdown, it is necessary to bypass only one of the trip signals that initiate operation of the engineered safety features. The trip signal for low steam-line pressure in one of

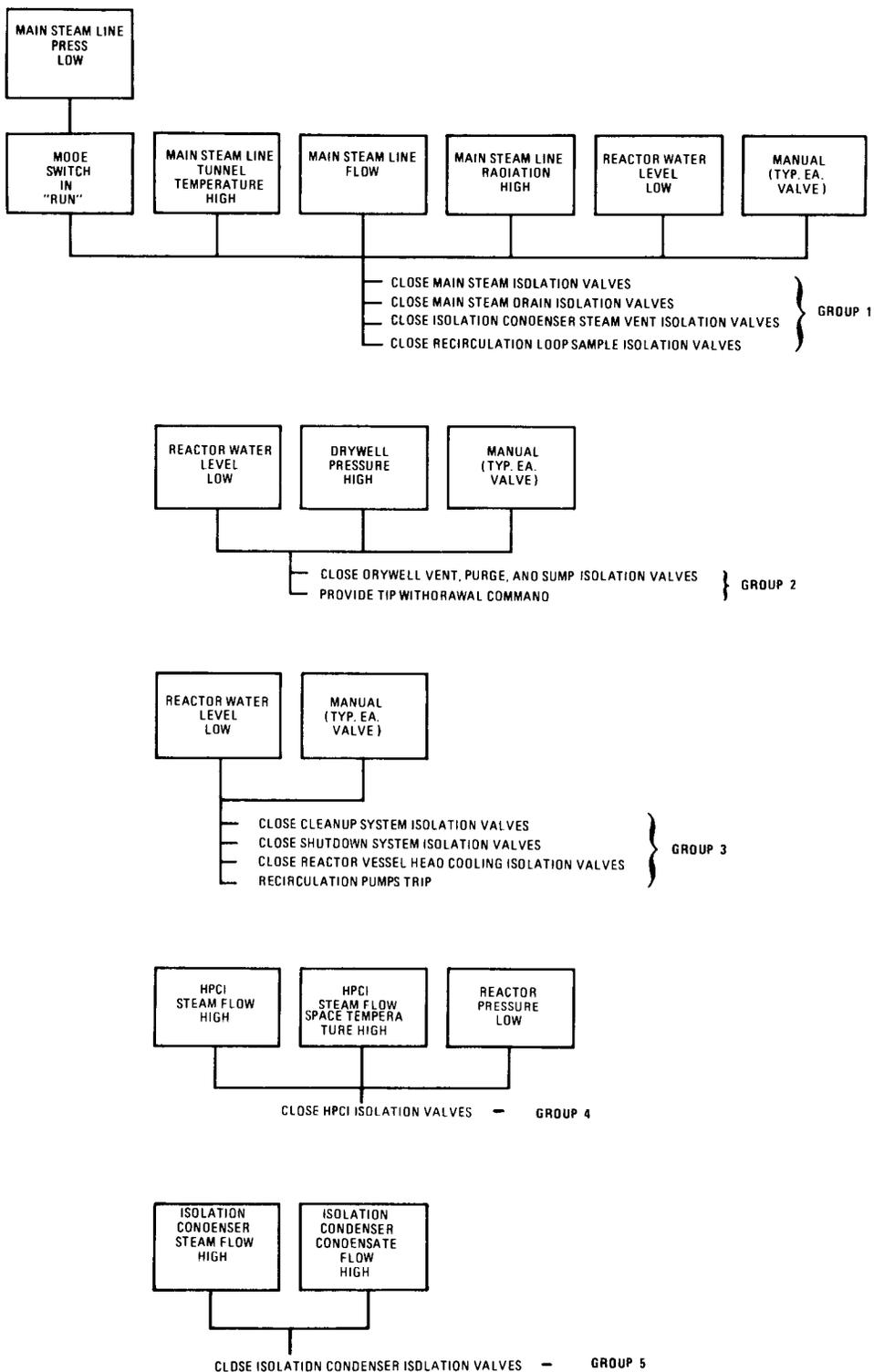


Fig. 4.13. Block Diagram for Signals that Actuate Containment Isolation Engineered Safety Features in Dresden-2 Station. (From Ref. 25)

the containment isolation systems is bypassed with the reactor mode selector switch in all modes except the RUN mode.

4.4.2 Typical Logic Arrangements

We were not able to obtain much detailed information, such as circuit diagrams, on the design of these engineered safety systems because of the preliminary status of the designs. In most cases, the instrumentation systems will have a dual logic channel arrangement (one-of-two taken twice) similar to the General Electric reactor shutdown system described in Section 3.4.2, except that most of these systems will be energized to trip to initiate operation of the engineered safety features. Most engineered safety feature logic systems have local coincidence for each plant variable rather than the general coincidence of all plant variables used in the reactor shutdown logic system.

The emergency core cooling system consists of a number of subsystems to cover a range of loss-of-coolant accidents. There are at least two independent full-capacity subsystems to cope with each range. The failure of one of the subsystems will not inhibit the overall engineered safety function. For this reason the single-failure criterion is applied on a subsystem basis rather than internally within one of the individual subsystems. The two subsystems used to cope with each of the different ranges of accident conditions are different in design.

The plant has two different types of subsystems for emergency cooling at high pressure. The high-pressure coolant injection (HCPI) subsystem consists of steam-turbine-driven pumps that take water from two sources and pump it into the reactor at high pressure (1125 psig). The turbine is driven with steam extracted from the reactor, so the system does not require ac power for operation. The motor-driven valves in the system and the oil pumps for the turbine are powered by a 250-v dc system. The controls and logic system are powered by a 125-v dc system. Four instrument channels are employed for each of the two plant variables that can initiate operation of the system. These are arranged in two one-of-two logic channels. The initiation of high-pressure coolant injection requires the coincidence (i.e., two-of-two logic arrangement) of trip action from both one-of-two logic channels (or one-of-two taken-twice logic arrangement). The

instrument channels and logic channels (or matrices) are all energized to trip and initiate operation. The logic drawings indicate that the system employs local coincidence where a selected set of two instrument channels for the same plant variable must trip to initiate system operation. In summary the actuation of the high-pressure coolant injection system requires a trip signal from one instrument channel in each of the two pairs for the same plant variable, a trip signal from both one-of-two logic channels, and a trip signal from the final two-of-two logic arrangement.

In addition to the initiation logic, the high-pressure coolant injection subsystem employs a number of other logic circuits for controlling and protecting the steam turbine, control of minimum flow bypass, and for automatically switching the pump suction from the condensate storage tank to the suppression chamber pool (in the event of low water level in storage tank or high level in suppression chamber). These controls employ various types of logic arrangements; for example, one-of-two, two-of-two, and the one-of-two taken-twice logic arrangements.

The automatic pressure-relief subsystem is provided as a backup to the high-pressure coolant injection subsystem during a loss-of-coolant accident. If the high-pressure coolant injection subsystem fails to work or if it cannot maintain the water level in the reactor, the automatic pressure-relief subsystem opens the relief valves to vent steam from the reactor to the suppression pool. This blowdown depressurizes the reactor vessel to a pressure that is low enough for the low-pressure emergency cooling systems to pump water into the vessel. The automatic pressure-relief subsystem is tripped at a lower water level than the high-pressure coolant injection subsystem to allow the latter system to have the first opportunity to cope with the accident. The logic diagram shown in the safety analysis report for an earlier set of plant variables indicates that a slightly different logic arrangement was employed. The change in logic arrangement was probably made to reduce the probability of spurious actuation, since rapid depressurization would place unwarranted stress on the reactor and its internals. The outputs from the four instrument channels are used in four one-of-N logic channels. Two of the one-of-N logic channels are combined to form a two-of-two logic arrangement, and the other two are combined in a similar fashion. The outputs of the two two-

of-two logic channels are combined in a final one-of-two logic arrangement to open the relief valves. The instrument channels are deenergized to trip, but the logic matrices and the dc solenoids controlling the relief valves are energized to trip and open the relief valves. The logic drawings indicate that the earlier system used general coincidence (like the reactor shutdown system), where the trip of a selected two-instrument channel for either the same or different plant variables initiates automatic relief action. In summary, the initiation of automatic relief requires a trip signal from two instrument channels for the same or different plant variables but associated with the same two-of-two logic channel, a trip signal from two one-of-N logic channels used in the same two-of-two logic channel, a trip signal from one two-of-two logic channel, and a trip signal from the final one-of-two logic arrangement.

The plant has three full-capacity systems for emergency cooling at low pressure (below ~ 275 psig) for loss-of-coolant accidents. Two of these are independent full-capacity core spray subsystems, and the third is the low-pressure coolant injection (LPCI) subsystem in which three of four pumps can supply full-capacity cooling (without core spray).

All four instrument channels for each plant variable are used in two sets of independent logic systems or actuation channels to initiate the operation of the two core spray subsystems. The logic diagram for one of the core spray subsystems is shown in Fig. 4.14. The logic arrangement for the initiation of system operation is similar to that described above for the high-pressure coolant injection subsystem (i.e., a one-of-two taken-twice logic arrangement that is energized to initiate system operation). The logic for the admission valves (designated core spray inboard and outboard valves in Fig. 4.14) is somewhat more complicated in that they are controlled by a low reactor pressure (~ 350 psig) signal in addition to either low-low water level or high containment (drywell) pressure signals that initiate the operation of the remainder of the core spray system. Two reactor pressure sensors (rather than the usual four) are arranged in a one-of-two logic as an additional signal that is required to open these valves and allow the emergency coolant to enter the reactor. The logic system shown in Fig. 4.14 also includes provisions for starting both core spray systems if normal auxiliary ac power is available or starting only

one system (I) if only power from Diesel generators is available. The second system (II) will start automatically if the spray pump in the first system fails to start or if the discharge pressure is low.

The individual motor control circuits for the pumps have either mechanical latch-in or electrical seal-in features so that once they receive an initial actuation signal, they continue to operate until manually stopped by the operator. (The latches of seal-ins are also released by undervoltage trips or low pressure in the pump header.) The valves in the system are driven by ac motors and continue to move until stopped by limit switches after the valves receive an initial actuation signal.

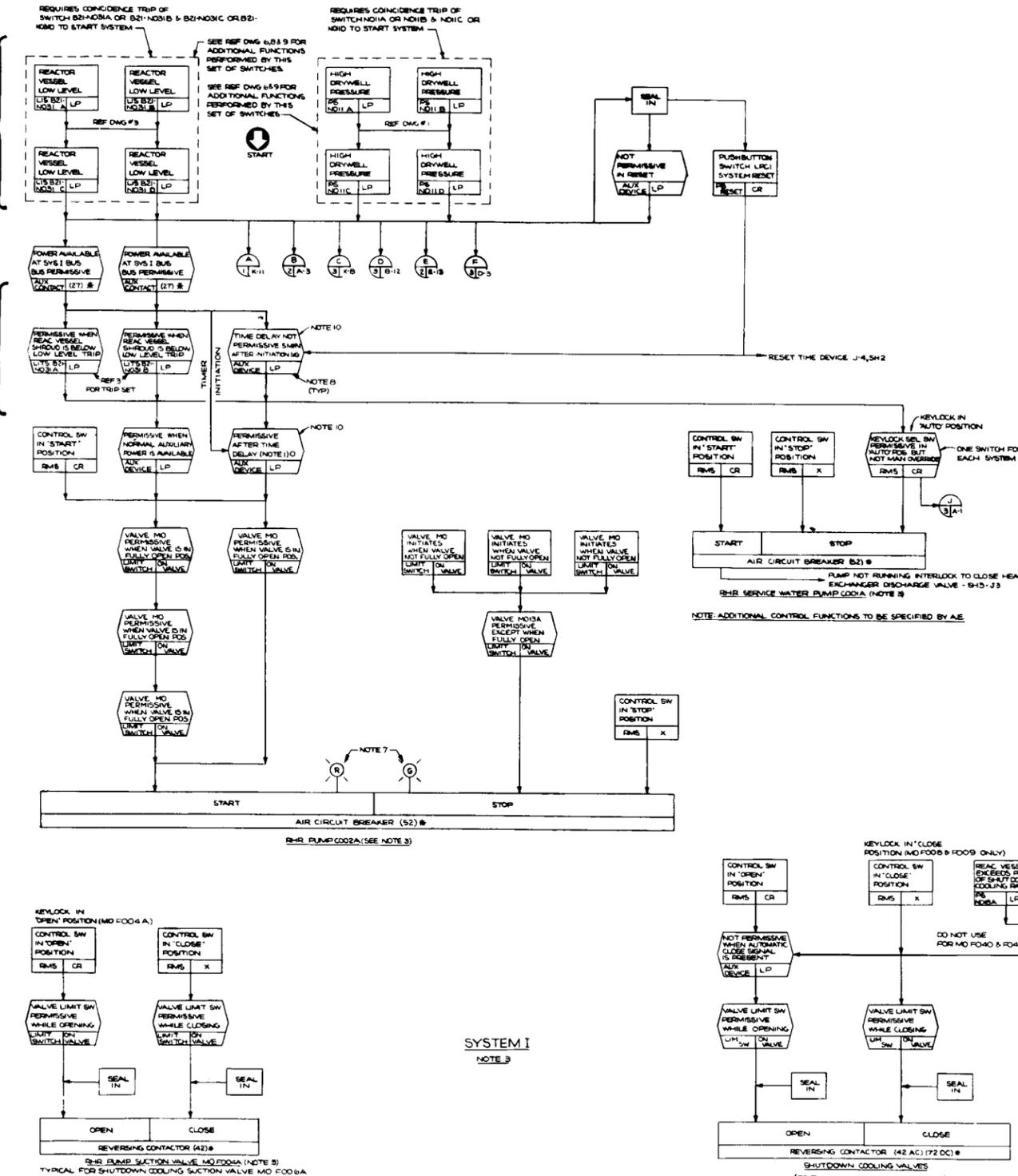
The low-pressure coolant injection system serves as a third source of low-pressure emergency cooling for the core. The logic diagrams for the low-pressure coolant injection and containment cooling systems are shown in Figs. 4.15, 4.16, and 4.17. These diagrams are taken from the preliminary safety analysis report for the Duane Arnold Energy Center²⁷ plant, since General Electric²⁰ indicates that this diagram is more representative. The logic used to initiate system operation and open the admission valves is similar to that described above for the core spray system.

The remainder of the low-pressure coolant injection system is considerably more complex than that for the core spray system because components in this system are also used for normal shutdown cooling, for cooling the suppression chamber pool, and for cooling the containment (drywell) with sprays. These latter functions are manually initiated during the latter stages of a loss-of-coolant accident. The low-pressure coolant injection protection system logic stops the reactor recirculation pumps and the containment cooling service water pumps that are running initially.

The low-pressure coolant injection system logic arrangement must also automatically operate a number of valves to open the flow path for emergency core cooling and to block flow to equipment not needed initially. For instance the pump suction lines from the recirculation lines (used in the normal shutdown cooling mode) must be closed and suction lines from the suppression pool must be opened. This system includes an interesting feature that comes into play if a pipe break occurs in a recirculation loop. A low-pressure coolant injection flow-path sensing

SYSTEM STARTUP LOGIC
(1-of-2 TAKEN-TWICE LOGIC)

WATER LEVEL PERMISSIVE TO STOP PUMPS AFTER 5 min AFTER (1-of-2 LOGIC)

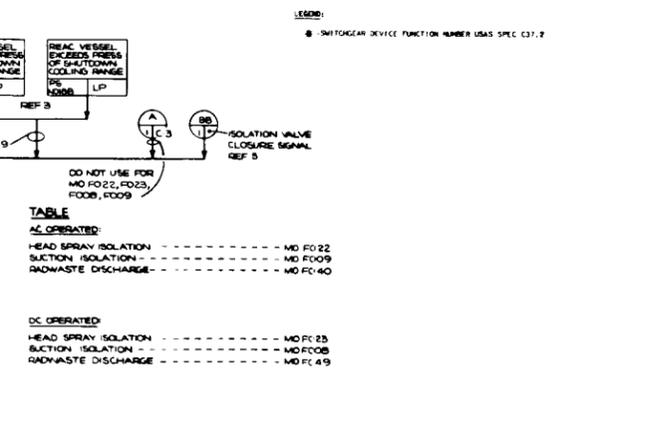


FCF 236X300 (STANDARD PLANT) 7E11-000
236X300A (S&T 7E) 7E11-000
236X300B (S&T 7E) 7E11-000
236X300C (S&T 7E) 7E11-000

- NOTES:
- THE OPERATING SEQUENCE, AFTER LOW WATER LEVEL SIGNAL OF HIGH DRYWELL PRESSURE IS AS FOLLOWS:
- CONDITIONS PLANT ON NORMAL AUXILIARY POWER
- | | | |
|-------------|--------|----------|
| PUMP - 002A | STARTS | NO DELAY |
| PUMP - 002B | STARTS | NO DELAY |
| PUMP - 002C | STARTS | NO DELAY |
| PUMP - 002D | STARTS | NO DELAY |
- VALUES:
- | | |
|------|---|
| F01A | OPENS AFTER REACTOR LOW PRESSURE PERMISSIVE |
| F01B | OPENS AFTER REACTOR LOW PRESSURE PERMISSIVE |
- CONF. CONTACTS:
- | | |
|-----|--|
| 23A | |
| 23B | |
| 23C | |
| 23D | |
- CLOSE, IF OPEN, (NORMALLY MAINTAINED CLOSED)
- HEAT EXCH. VALVE 99A - CLOSES
- SERVICE PUMPS 1A, C, D, STOP IF RUNNING
- CONDITIONS PLANT ON STANDBY DIESEL POWER
- | | |
|------|------------------|
| PUMP | SET TIME DELAY |
| | DEVICE INITIALLY |
| | TIME ALLOWED |
| | TO REACTOR |
| | LOW WATER LEVEL |
| | OR FROM TO BE |
| | AVAILABLE |
- | | |
|-------------|----------|
| PUMP - 002A | 0 SECS. |
| PUMP - 002B | 10 SECS. |
| PUMP - 002C | 0 SECS. |
| PUMP - 002D | 0 SECS. |
- VALUES - SEQUENCE SAME AS CONDITION A
- SERVICE PUMPS - SAME AS CONDITION A
- MANUAL CONTROL SYS FOR THROTTLING TYPE VALVES SHALL BE DESIGNED TO ALLOW VALVES TO BE STOPPED AT ANY DESIRED POSITION.
 - TOP 1000S & 1000S ARE NORMAL SYS 11 CRYS. & EQUIP ARE IDENTICAL EXCEPT CORRESPONDING CRYP. NO. SWITCHES ARE AS FOLLOWS:
SYS 1 - A, C, E, G, & J
SYS 11 - B, D, F, H, I, K
 - PUMP MOTORS SHALL BE PROTECTED WITH OVERLOAD & UNDERVOLTAGE TRIPS OVERLOAD TRIPS TO BE APPLIED SO AS TO INITIATE POWER ON MOTOR AS SOON AS POSSIBLE WITHOUT IMMEDIATE DAMAGE TO MOTOR OR MAIN TO GENERATOR POWER SYSTEM. UNDERVOLTAGE TRIPS SHALL BE SUFFICIENT TO PERMIT POWER TRANSFER FROM AVAILABLE TRIP SOURCES TO START OF TRANSDUCER SIGNAL WITHIN SHIPPING OR VALVE MOTORS SHALL BE PROTECTED BY OVERLOAD TRIP SIGNAL.
 - AUXILIARY RELAYS & DEVICES ARE NOT SHOWN ON THE FUNCTIONAL CONTROL DIAGRAM EXCEPT WHERE NEEDED TO CLARIFY THE FUNCTIONAL REQUIREMENTS.
 - NOTE: PUMP FOR SYS 1 PUMPS SHALL ORIGINATE FROM A DIFFERENT AC BUS THAN THE PUMPS OF SYSTEM 11.
 - NOTE: PUMP FOR VALVES IN BOTH SYSTEMS SHALL ORIGINATE FROM A COMMON BUS WHICH IS AUTOMATICALLY CONNECTIBLE TO A TERNARY ENERGY BUS SOURCE. CONTROL POWER SHALL BE FROM A COMMON BUS DERIVING POWER BY AUTOMATIC TRANSFER FROM EITHER OF TWO INDEPENDENT SOURCES. SEE REFERENCE 3.
 - STATUS LIGHTS SHALL BE AS FOLLOWS:
VALVES: GREEN ON FOR CLOSED POSITION
RED ON FOR OPEN POSITION
BOTH ON FOR INTERMEDIATE POSITION
PUMPS: RED ON FOR PUMP RUNNING
GREEN ON FOR PUMP STOP
 - ALL DEL. TIME DEVICES SHALL BE ADJUSTABLE FROM 0 TO FULL SCALE. FULL SCALE SHALL BE AT LEAST 3:30, UNLESS SPECIFIED OTHERWISE.
 - ALL EQUIPMENT & INSTRUMENTS ARE PREFIXED BY 10, WHICH IS PART 10 ON THE INSTRUMENT PARTS LIST.
 - THE DELAY DEVICE TO AUTOMATICALLY RESET AND BECOME PERMISSIVE ON IMMEDIATE LOSS OF POWER TO MOTOR BUS OR SYSTEM RESET. DEVICE SHALL HAVE REDUNDANT PARALLEL CONTACTS IN THE PERMISSIVE LOGIC.
 - THE FOUR PRESSURE SWITCHES ARE ARRANGED FOR ONE OUT OF TWO TRIPLE LOGIC, SIMILAR TO WHEAT 9 LOGIC SHOWN SHEET 7, C-3.

- REFERENCE DOCUMENTS:
- | | |
|---------------------------------------|----------|
| 1. REFERENCE HEAT REMOVAL SYSTEM PAID | 101-1010 |
| 2. CRIC SYMBOLS | 10984756 |
| 3. NUCLEAR BOILER PAID | 821-1010 |
| 4. PLANT D.C. & INST A.C./D.C. SYS | 821-1030 |
| 5. NUCLEAR BOILER HEAT SYS FCD | 821-1030 |
| 6. CORE SPRAY FCD | 821-1030 |
| 7. HEAVY FLOW CONTROL FCD | 821-1030 |
| 8. MFL SYS FCD | 841-1030 |
| 9. RC 6 SYS FCD | 851-1030 |

LEGEND:
SWITCHGEAR DEVICE FUNCTION NUMBER USAS SPEC C37.2



TABLE

AC OPERATED:

HEAD SPRAY ISOLATION	MO F022
SUCTION ISOLATION	MO F009
RADIWASTE DISCHARGE	MO F040

DC OPERATED:

HEAD SPRAY ISOLATION	MO F023
SUCTION ISOLATION	MO F008
RADIWASTE DISCHARGE	MO F049

Fig. 4.15. Logic Diagram for Low-Pressure Coolant Injection and Containment Cooling Actuation System in Duane Arnold Energy Center - Part A. (From Ref. 27 with additions)

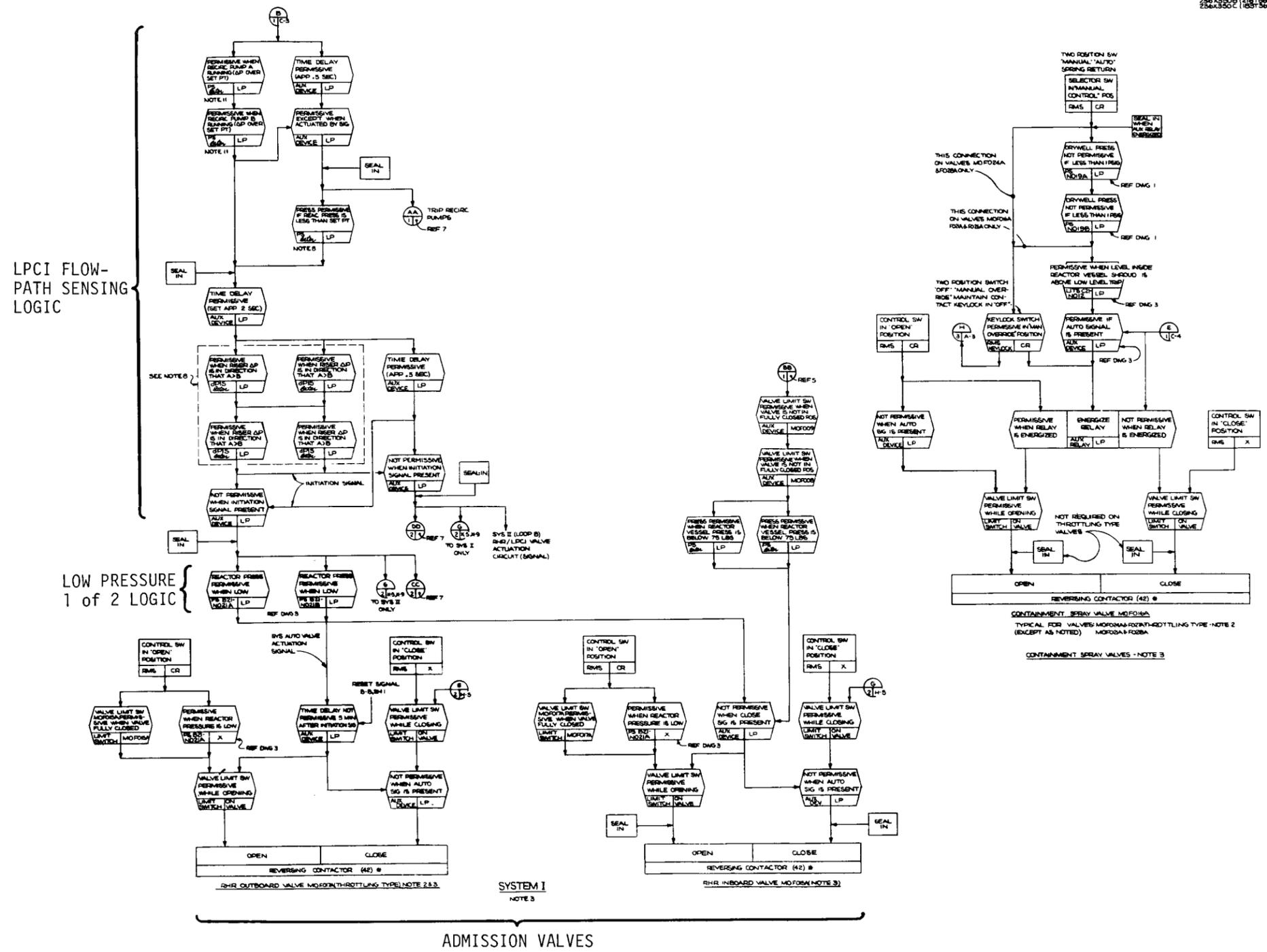


Fig. 4.16. Logic Diagram for Low-Pressure Coolant Injection and Containment Cooling Actuation System in Duane Arnold Energy Center - Part B. (From Ref. 27 with additions)

logic system is used to select and isolate portions of the undamaged recirculation loop and to route all low-pressure coolant injection water into the bottom plenum of the reactor vessel through portions of the undamaged recirculation loop piping. The incorrect selection of the broken recirculation loop instead of the undamaged loop might significantly reduce the amount of low-pressure coolant injection flow entering the interior of the core shroud region in the bottom plenum of the reactor vessel. This portion of the low-pressure coolant injection uses the one-of-two taken-twice logic arrangement.

The logic system includes timers that start the pumps in sequence if normal ac power is not available and the pumps are powered by the Diesel generators. A time delay device is also used to block the automatic start signal for the pumps 5 min after the initiation signal or a system reset. This block is effective only when both of two level switches monitoring water level inside the core shroud indicate that the vessel is flooded to approximately two-thirds of the core height. This blocking of the initiation signal allows the operator to take control and manually stop the pumps that are no longer needed for core cooling or manually start the containment cooling pumps. If the water level in the core falls below that monitored by these two level switches, the block is removed with a one-of-two logic signal and the system reverts to the setup for emergency core cooling.

Some of the low-pressure coolant injection flow can be manually diverted to the spray headers in the drywell and/or the suppression chamber to cool the containment vessel if two permissives exist: (1) the water level in the shroud is above approximately two-thirds of the core height, as indicated by a one-of-one logic signal, and (2) the drywell pressure is high, as indicated by a two-of-two logic signal.

Several different sets of plant variables are used to initiate closure of the different groups of containment isolation valves, as indicated in Fig. 4.13. In general, four instrument channels are employed for each variable, and the systems use a dual logic channel arrangement (one-of-two taken twice) similar to that for the reactor shutdown system. The instrument channels, one-of-N logic channels, one-of-two logic channels, and the final two-of-two logic arrangements are all deenergized to trip

and initiate closure of the valves. Thus the containment isolation system employs more fail-safe features than the remainder of the engineered safety features. The logic for main steam-line isolation employs general coincidence of different plant variables; whereas, the logic for some of the other isolation valves employs local coincidence for each plant variable.

The main steam-line isolation valve system employs several types of power supplies. One pair of instrument channels (used in a one-of-two logic) is powered by one of the motor-generator sets used to power one of the reactor shutdown logic channels. The other pair is powered from a vital ac bus, which is fed by both normal ac and through a dc/ac inverter from the station battery system. A dc solenoid is used as the output of one one-of-two logic channel and an ac solenoid is the output of the other. The two solenoids are arranged in the air supply that holds the isolation valves open so that both solenoids must be deenergized to produce valve closure to form the final two-of-two logic arrangement. The isolation valves can be closed by either air pressure from the normal air supply, or from the individual storage accumulators, or by the closing spring. Loss of air pressure causes valve closure. The other valves in the containment isolation system are either solenoid operated or motor driven. The motor-driven valves require actuator power for closure. All motor-driven valves inside the containment vessel are powered by ac; whereas, the redundant valves in the same pipe lines outside the containment vessel are powered by dc. These arrangements of various power supplies prevent spurious closure of isolation valves or failure to close on demand after the loss of one of the power supplies.

Separate sets of one-of-two logic matrices are provided for the inner and outer (redundant) valves in one pipe line so that the failure of one one-of-two logic matrix would not prevent all isolation valves in that group from closing.²⁰ These two separate sets of one-of-two logic matrices resemble the four separate sets of one-of-two logic matrices used for the four groups of control rods in the reactor shutdown system (see Sect. 3.4.2).

4.4.3 Power Sources

The instrument channels are usually grouped in pairs to serve the one-of-two logic channels. For the cases where power is required for the instrument channels, the two pairs are powered from separate sources. (Some instruments are simple pressure switches that may not require power.) For instance, in the containment isolation system, one pair is supplied by one of the motor-generator sets used for one of the reactor shutdown logic channels (see Sect. 3.4.5), and the other pair is powered from a vital (uninterruptible) ac bus that is fed by both normal ac and through a dc/ac inverter from the station battery system.

Most logic matrices are supplied from the 125-v dc station battery system that serves the multiple reactor units in the station. The logic systems for the two independent core spray subsystems are supplied from two separate buses in the 125-v dc system. The four low-pressure coolant injection pumps are split into two groups, and the logic power for each group of two pumps is supplied from two separate buses in the 125-v dc system. The two two-of-two logic channels used in the automatic pressure-relief system are supplied separately from two buses in the 125-v dc system. One of the one-of-two logic channels in the containment isolation system is supplied by the dc system and the other by an ac system.

The solenoids controlling the relief valves and the isolation valves are powered by the same sources that power the associated logic channels. The motor-driven containment isolation valves are split between ac and dc sources, as described in the previous section. Compressed air for the air-operated valves is obtained from a single 100-psig instrument air supply that includes compressors, dryers, storage, etc.

The valves and turbine-lubrication pumps in the high-pressure coolant injection subsystem are powered by a 250-v dc system. The pumps in the two core spray subsystems are connected to separate emergency ac buses that can be powered by the Diesel generators. The valves in the two core spray subsystems are motor driven and are powered by the same ac bus that supplies the pump in that subsystem. The two groups of two pumps each in the low-pressure coolant injection subsystem are also connected to these separate emergency ac buses. The motor-driven valves in the low-pressure

coolant injection subsystem are connected to one of these ac buses. Three Diesel generators serve the Dresden-2 and -3 units; one is shared between the two units.

4.4.4 Testing Arrangements

The instrument channels and logic systems may be tested during reactor operation in a manner similar to that described in Section 3.4.6 for the reactor shutdown system.

The pumps and valves in the emergency core cooling systems are tested separately from the actuation logic systems during reactor operation. The pumps are test operated separately from the admission valves by pumping water back to the suppression pool. The two admission valves in series in each subsystem are interlocked so that they can only be opened one at a time for testing. The emergency core cooling systems are tested in a more integrated fashion during the refueling plant outages by initiating system operation through the automatic actuation logic.

The main steam-line isolation valves are slowly closed partially (to 90% open) and reopened for on-line exercising. The other motor or diaphragm-operated valves are fully closed and reopened individually for on-line testing. The automatic actuation of the containment isolation system is tested during refueling outages.

The operability of the automatic pressure-relief valves and automatic actuation is tested only during refueling outages. Tests during reactor operation are not practical, since actuation during operation would result in rapid depressurization of the reactor, which would place unwarranted stress on the reactor and its internals.

4.4.5 Isolation of Circuits

Circuits of the engineered safety features are isolated from the operation system and have physically separate equipment from the active control part of the operation system, except for parts of the low-pressure coolant injection subsystem used for normal shutdown cooling.

The four instrument channels or, in some cases, the two sets of two instrument channels are isolated from each other. The emergency core cooling subsystems share some of the same sensors; however, the logic

circuits are isolated from each other on a subsystem basis. The logic circuits for the individual core spray subsystems, the low-pressure coolant injection subsystem, the high-pressure coolant injection subsystem, and the automatic pressure-relief subsystems are isolated from each other. Also the logic circuits for the inner and outer (redundant) isolation valves are isolated from each other.

5. COMPARISON AND DISCUSSION OF INSTRUMENTATION FOR REACTOR PROTECTION SYSTEMS

The comparisons in this chapter are not complete in that not all the reactors and systems considered are discussed in each comparison.

5.1 General Features

Many types of logic arrangements are used in the protection systems for both reactor shutdown systems and engineered safety features. These include one-of-one, one-of-two, one-of-three, two-of-two, two-of-three, and two-of-four logic arrangements, with two-of-three and two-of-four arrangements being the most common. The logic arrangements are summarized in Chapter 2. It appears that all reactor shutdown system and engineered safety feature logic systems can be tested during plant operation, except part of the logic systems for engineered safety features in the Palisades plant.

The relays in the reactor shutdown systems of all the reactors are de-energized and power to the control rod drives is turned off to initiate a scram. Thus, these systems are fail-safe with respect to loss of power supplies for either the instruments, logic channels, or actuators. In the engineered safety systems the relays associated with the instrument channels are usually deenergized to initiate action, and the logic matrices and the logic output, or actuation, relays are energized to initiate action. As discussed in Section 5.5, most of the engineered safety systems are based on the use of two redundant subsystems, where either subsystem for a particular function is capable of independently carrying out that function. For this reason, it is not essential that the engineered safety feature logic (actuation) channels be fail-safe with respect to loss of power.

Bypassing or blocking of reactor scram signals to permit normal operation for conditions other than rated power conditions is carried out in several ways. For example, a manual mode switch is used to bypass some of the plant variables used to produce a scram for different power ranges or modes at Browns Ferry. In addition to the mode switch selection, some of the bypasses in this design also require that the reactor pressure be

low before the trip action is bypassed, and other bypasses are applied and removed automatically by low pressure in the first stage of the turbine. The other three plants have two methods of bypassing: some of the bypasses are applied and removed automatically under the control of another plant variable and, for other cases, manual action is required in coincidence with permissive actions by the instruments to bypass the trip signal, with the bypass automatically removed when the permissive conditions are not met. The bypasses in the Oconee* and Palisades plants are controlled on a channel-by-channel basis, as illustrated in Figs. 3.1 and 3.2. In this scheme, a bypass control signal from one instrument channel (usually neutron flux) is used to control the bypasses of instrument channel trip signals for the plant variables (being bypassed) in only that same basic set of instrument channels (i.e., in the same protection channel). This scheme is simple and avoids interconnections between the sets of channels, but all bypasses in one set of channels are affected directly by a failure in the instrument controlling the bypass. The signals for the bypasses or blocks in Ginna are generated in logic matrices from outputs of the required instruments (such as neutron flux); thus there is interconnection between channels for this purpose, but a one-channel instrument failure cannot affect any of the blocks.

The bypassing of signals used to initiate engineered safety feature action is usually done in a fashion similar to that in the reactor shutdown system for the particular plant. One exception is in the Palisades plant, where bypassing in the engineered safety feature logic system is done with signals from logic matrices rather than on a channel-by-channel basis, as is done in the logic system for the Palisades plant shutdown system.

Several different methods are used in the treatment of plant variables in the reactor shutdown system for insuring that the reactor power reasonably matches coolant flow and that a departure from nucleate boiling condition or a critical heat flux is not reached. The Oconee system automatically changes the flux trip point as a function of coolant flow and employs a high outlet temperature trip signal.* The Palisades system

*See footnote on p. 28.

requires the operator to manually select the number of operating pumps to set the trip set points on both flow and flux, but it has a thermal margin trip signal that automatically varies the low-pressure trip set point as a function of the measured differential temperature across the core. The Ginna system has a low-flow set point that is varied stepwise (with bypasses) as a function of flux and a fixed set point for high flux. In addition, set points for trip signals of high differential temperature across the core are automatically varied as functions of coolant pressure and average temperature. The Browns Ferry system presently has a fixed flux trip set point, but the equipment provides the option of varying the trip set point automatically as a function of recirculation flow.²²

Different input variables for the same protective function are used on similar plants. One example is the different methods mentioned above for preventing the core from approaching the departure from nucleate boiling condition or a critical heat flux. In addition, only Ginna of the three pressurized-water plants (Oconee, Palisades, and Ginna) has a flux-tilt signal in the reactor shutdown system or initiates safety injection of borated water into the reactor as the result of a steam-line break. Palisades, Ginna, and Browns Ferry employ scrams based on direct measurement of steam system breaks, whereas Oconee uses disturbances in the primary cooling system variables for protection after a steam system break. There seems to be considerable variation in the plant variables selected to actuate the engineered safety features. This is discussed in Section 5.5.

The emergency core-cooling pumping systems for Palisades, Ginna, and Dresden-2 (high-pressure coolant injection system) have protection logic systems for automatically switching to second sources of water before the first tank runs dry. The Oconee plant depends on manual operations for this action.

5.2 Testability of the Instrumentation of the Reactor Shutdown Systems

Most of the designs have analog instrument channels to measure the main reactor variables, and the analog portions of the channels are

checked by visually comparing the outputs of redundant channels. This does not test the ability of the sensor to reach the trip set point; however, it does indicate that the channel is operating, and this type of surveillance has the advantage of detecting some of the incipient (or impending) types of failures. The Browns Ferry system has a number of nonindicating pressure switches rather than the analog type of instrument channel. These are tested by tripping the switch with a test pressure substituted for the process pressure. The pressure-switch type of instrument channel has the advantage of reliability that is potentially higher than that of an analog type of channel. However, the testing usually requires disconnecting the sensor from the process by means of valving (and then correctly reconnecting it), and the use of nonindicating sensors does not provide a surveillance feature for use in detecting incipient failures.

All reactor shutdown instrumentation systems examined employed the concept of coincidence in various degrees. In every case, each individual trip unit in a channel can be tested by some sort of signal introduced ahead of the trip device. The requirement of a coincidence of trip signals prevents a single signal from shutting down the reactor. Two of the plants (Oconee and Browns Ferry) use general coincidence, and the other two (Palisades and Ginna) use local coincidence. A single-channel trip signal is transmitted further through the general coincidence logic than through the local coincidence logic. Complexity of the testing circuits is dependent somewhat on whether the logic is arranged in local or general coincidence.⁹ The local coincidence arrangement of Ginna appears to have less complexity in testing than that of Palisades.

Both Ginna and Palisades use bypassing of actions to allow testing. The bypassing in the Ginna system is accomplished at the output of the logic channel by placing a bypass circuit breaker around the main trip breaker, as shown in Fig. 3.8. Testing of the logic system is carried out by deenergizing two relays in a particular matrix and observing that the trip signal is transmitted to the final logic level (circuit breaker).

The bypassing required in the reactor shutdown system testing in the Palisades plant is carried out by means of a second coil on each logic trip relay (shown in Fig. 3.6). The second coil is supplied a holding

current to prevent the relay contacts from opening when the operating coil is deenergized by the test of the ladder matrices. This testing of the ladder matrices requires that each two-of-two pair of the module trip relays be supplied in succession with a deenergizing current in the second coil of the mercury-wetted contact relays. The opening of the selected pair of contacts in a matrix is monitored by indicating lights. The circuit arrangement for supplying the necessary deenergizing or holding current to the second coil on each relay requires interconnecting wires between the six groups of logic ladders and trip relays.

The final reactor shutdown system logic in Oconee, Palisades, and Browns Ferry is a two-of-two arrangement. The electric power to the rod drives in Oconee and Palisades must be shut off from two parallel feeders to produce a scram. In Browns Ferry the solenoids for both scram pilot valves for each rod drive must be deenergized or the solenoids for backup scram pilot valves must be energized to initiate a scram. This arrangement of final logic allows each breaker, or power relay, or scram pilot valve, as the case may be, to be exercised during testing. Since the final logic in the Ginna plant is in a one-of-two arrangement, exercising of a circuit breaker requires that a bypass breaker be connected into the circuits, as shown in Fig. 3.8.

Indication of the operation of the final breakers or power relays in Oconee, Ginna, and Palisades is provided. The actual operation of the individual scram pilot valves in Browns Ferry is not indicated; however, power to the solenoids is monitored with lamps.

The test procedures in Oconee, Palisades, and Ginna test the transmission of trip signals from two instrument channels or one-of-N logic channels through the majority of the logic. This is done in Oconee by deenergizing the output relays (designated RS relays in Fig. 3.2) from two of the one-of-N logic channels to make one of the main circuit breakers open. This is done in Palisades and Ginna by deenergizing two instrument channel output relays to produce a trip signal at the output of one logic matrix, which in turn makes one of the main circuit breakers open. (As mentioned earlier, these tests require some bypassing in Palisades and Ginna.) In Browns Ferry, the only coincidence is made at each rod drive in the two-of-two logic arrangement of the two scram pilot

valves, and the trip of a single instrument channel is transmitted to this point.

None of the tests during plant operation actually interrupt the electric power or relieve the pneumatic pressure, as the case may be, to the control rod actuators. Thus the tests do not actually determine that the final logic devices are capable of initiating rod insertion to produce a reactor scram. It may be possible, in some plants, to initiate insertion of individual rods during operation, but individual actuation is not identical to interrupting electric power or relieving air pressure to all the rod drives simultaneously. This difficulty is common to all tests conducted during plant operation. A complete scram test cannot be made on a frequent basis and still maintain acceptable plant load factors (serviceability). Consequently, attention should be given to the components that can only be tested during an outage to insure that they have the long mean life (low failure rate) needed to achieve their required reliability with a testing frequency determined by the interval between normal shutdowns.

Ginna has common instrument channels for protection and active control in the operation system, and the introduction of a test signal into an instrument channel may affect plant operation by blocking normal control actions. The other three plants use signals from the protection system for unidirectional control actions (such as rod withdrawal prohibits or turbine runbacks) that can only move the plant away from the safety limits. Thus the testing of the protection system in these other three plants might also introduce disturbances in the plant.

5.3 Effects of Circuit and Component Failures in the Instrumentation of the Reactor Shutdown Systems

The relays in the reactor shutdown systems of all the reactors are deenergized, and power to the control rod drives is turned off to initiate a scram. Thus, these systems are fail-safe with respect to loss of power supplies for either the instruments, logic channels, or actuators. One exception is the nonessential trip signal for loss of load in Palisades that employs energize-to-trip action for the instrument channels. Several

system arrangements are used to reduce the chances of a spurious scram caused by the loss of a single power supply (and other single failures). In general, all designs have separate power supplies for the individual instrument channels; most designs have separate power supplies for the multiple logic channels (or multiple sets of logic matrices); and most designs have two parallel (and separate) sources of power serving the control rod drives, so the loss of any of these individual power supplies will not produce a spurious scram. There are a few exceptions to this general pattern. In the Browns Ferry system, the loss of the single plant instrument supply of compressed air would produce a scram. In the Ginna system, the loss of one of the dc power supplies that serves one of two logic channels would produce a scram, since these two logic channels control the trip circuit breakers that are arranged in one-of-two logic in the single feeder line that serves all control rod drives. In the Palisades system, the loss of one of the two 125-v dc supplies for the plant could produce a spurious scram by causing a loss of power to one of the logic ladder matrices and also by tripping two of the instrument channels.

None of the logic arrangements in the four plants appear to have obvious deficiencies regarding the single-failure criterion^{8,28} for unsafe failures. However, the number of interconnecting wires necessary for testing the logic relays in Palisades increases the difficulty of packaging the six sets of logic matrices separately in isolated compartments and the possibility of maintenance errors affecting several logic relays in different matrices.

Bypassing for testing, such as in Ginna and Palisades, presents problems.²⁹ During the time interval that a bypass breaker is closed in parallel in the Ginna system, the logic channel not associated with the paralleled trip breaker must operate to provide protection. Thus there is only one logic channel that can produce a scram during the interval required to carry out the particular tests involved. Criterion 4.11 of IEEE allows bypassing for testing of one-of-two logic systems,⁸ but we are concerned that the time interval cannot be as short as desired because of such factors as the test not going as smoothly as anticipated and because of unexpected repair times. The operator may be faced with a difficult decision

as to whether to continue to operate with the bypass in place or to shut down the plant in case the time interval for the test is longer than the designer anticipated. Also, in the Palisades plant there is some possibility that a failure in a matrix logic test push button could maintain the current in the holding coils on at least a portion of the logic trip relays after the test was completed. The amount of redundancy would be reduced by failure of the bypassing device. This is a universal type of problem with bypasses for testing.

None of the plants have single buses³⁰ to the control rod scram actuators in the literal sense of "single"; however, the actuators in the Ginna station are on a single three-phase ac four-wire circuit. The other three plants divide the control rods and release mechanisms into groupings of control rod release circuits (or buses). Palisades has two groups of control rod release circuits, Browns Ferry has four groups, and Oconee employs the equivalent of five groups. A single short circuit cannot prevent scram operation of all control rod release circuits in these plants, but it could prevent scram of one group of rods. A sufficient number of short circuits could prevent control rod release in any of the plants. In Ginna this would require the short circuiting of a large amount of three-phase four-wire power around the trip breakers in a circuit with small physical exposure. In the other three plants, there is no single control rod release circuit; however, the multiple release circuits could be tied together. If this went undetected, a single short circuit around one set of contacts could prevent the release of all rods.

The connection of enough sources of power to the control rod release circuits at the proper points could also prevent a scram. It would be necessary for such a source to have a rather unusual voltage (260 v, three phase) in Ginna, and in the other three plants it would be necessary to make connections from a power source to each of the groups of control rod release circuits.

A single failure in any of the rod drive mechanisms could prevent insertion of one rod, but sufficient redundancy in the number of control rods is provided to shut down the reactor with one or more rods stuck out of the core. In the Browns Ferry station, the single volume for collecting the discharge water from all the control rod drives during a scram is

a common point in the protection system. In addition, this volume is sealed when a scram is initiated. The reason for sealing the discharge volume, we understand, is to prevent excessive loss of water from the reactor through leakage around the seals in the control rod drives if the system is not reset and the scram valves are not closed. Insufficient free volume would prevent full insertion of the control rods. The probability of insufficient free volume in the discharge volume is reduced by the scram trip signal initiated by level switches in the sump of the discharge volume, as discussed in Section 3.4.4.

Some method of bypassing or inhibiting particular trip signals under various conditions is applied in all plants. For example, the system in Palisades has a bypass signal generated on a channel-by-channel basis, as noted in Section 3.2.1. As discussed in Section 5.1, the failure of a neutron flux instrument would affect all the other trip signals associated with the bypass signal from the neutron flux instrument that failed. The Ginna plant has logic matrices associated with all the channels of a particular variable to generate a signal to bypass or block the trip action of all the channels of another variable, as indicated in Table 3.3. A single failure in a channel supplying a signal to a block matrix would not affect any of the blocking signals, but the logic arrangement provides interconnections between all the associated channels and increases the complexity. Similarly, a mode switch, such as that used in Browns Ferry, can be a source of interconnections between channels.³⁰

The Ginna plant has common instruments for both protection and some of the active control part of the operation system. Control signals are taken from the protection system through isolation amplifiers, and different plant variables are used as inputs to the reactor shutdown system to provide a backup trip signal for the shared plant variables, as discussed in Section 3.3.5. The other three plants use protection system instrumentation that is physically separate from the active control systems. Failures in the common instruments in Ginna would affect both the protection system and the active control system; however, the two-of-four logic arrangements provide an extra redundant channel¹⁸ to meet the requirements of Section 4.7 of the IEEE Criteria⁸ on the basis of no common

mode failures. We feel that physically separate systems would be better. This is discussed further in Section 7.7.4.

All the plants utilize signals taken from the protection system channels for such things as data logging, alarms, comparison of signals of similar channels, and unidirectional control actions, such as rod withdrawal prohibits or turbine runbacks, that can only move the plant away from the safety limits. We feel that this class of uses of signals from the protection instrumentation is acceptable³¹ if failures of the circuits will not induce or inhibit protective actions. The resulting circuits create the problem of interconnections between channels of the protection system, and adequate isolation must be provided between the protection system and the external system, as stated in Section 7.7.5.

5.4 Testability of the Instrumentation of the Engineered Safety Features

All engineered safety feature instrumentation systems examined employed the concepts of coincidence in various degrees. Provisions were made for testing the instrument channels and logic matrices in Oconee, Ginna, and Dresden-2 while the plant was operating; however, the instrument channels and logic matrices in Palisades can be tested only during plant shutdowns. The instrument channels in the first three plants are tested with the general methods described in Section 5.2 for the reactor shutdown system instrument channels. In the Oconee station, monitoring lamps in the matrices indicate the operation of the contacts of output relays of the instrument channels and one-of-N logic channels as the instrument channels are tripped individually. Two instrument channels are tripped at the same time in the matrix tests in Ginna for matrices employing coincidence, and the transmission of the coincident trip signals through the matrix is observed with a monitoring lamp at the matrix output. This feature of testing coincident trip signal transmission through the matrix requires, however, that the output of the matrix be disconnected (i.e., bypassed) from the master relay to prevent the master relay from being energized and initiating engineered safety feature actions. The one-of-two taken-twice logic used in Dresden-2 will be tested up to

the final two-of-two logic channels by tripping individual instrument channels.

The main logic output or actuation relays that initiate engineered safety feature actions are tested in different manners in the various plants. A test circuit is used in Palisades to energize the main safety injection relays (SIS and SIS-X) and the DBA sequencers during plant operation. Since these relays and timers actuate the engineered safety cooling systems, a few of the functions are automatically blocked during the test. The actuation relays in the containment isolation systems in Palisades will not be tested during plant operation. The actuation or main control relays (R₀, CR1, and CR2) in Oconee will be energized while the plant is in operation for the tests of individual pumps and motors. The master relays in the engineered safety feature actuation channels in the Ginna plant will be tested only during plant shutdowns; however, the integrity of the master relay coil will be checked with a continuity monitor.

The integrated operation of the various engineered safety systems is tested in different degrees in all the plants during operation. The test circuits in Palisades allow most of the systems to be placed in operation at any given time while the plant is in operation. In the on-line tests in Oconee, Ginna, and Dresden-2, the motors and valves are individually operated for testing. In general, the pumps and valves in a given system are tested separately in these three plants. Bypass flow circuits are set up to allow the pumps to be operated without injecting water into the high-pressure primary system. The on-line testing of the pumps and valves is discussed in more detail in other papers in this series by Lawson³ and Zapp.⁴ The engineered safety features can be tested in a more integrated fashion during refueling outages by initiating system operation through the automatic actuation logic.

5.5 Effects of Circuit and Component Failures in the Instrumentation of the Engineered Safety Features

Analysis of failures of circuits and components is difficult because of the complexity of the systems. The single-failure criterion^{8,28} often used in the failure analysis of reactor shutdown circuits must usually be

adapted to functions or subsystems rather than to circuits for the engineered safety systems.

Many of the emergency core-cooling systems are activated by two or more plant variables, such as low coolant level, low coolant pressure, high containment pressure, or low steam pressure (Ginna). In most cases this gives some desirable diversity in input measurements;³² however, there are a few cases where only one plant variable is used. The containment spray systems in Palisades, Oconee, and Ginna are initiated with only one plant variable - containment system high pressure. The containment air coolers, which provide another form (fans and heat exchangers) of containment cooling, employ other initiating signals in addition to containment high pressure for the systems in Palisades and Ginna,¹⁸ but not in Oconee. There may be need for an independent variable to give some diversity³² in the initiation of the containment spray and possibly the containment air coolers in Oconee. (It should be noted that the containment spray and suppression chamber cooling in Dresden-2 are initiated manually rather than automatically.)

The containment isolation system in Oconee also employs only containment high pressure as an automatic initiation signal, and the same set of three sensors actuates the emergency core cooling and containment air cooling, as well as the containment isolation. This appears to be another area where diversity in the initiating signals would afford better protection.

The measured reactor pressure is a crucial parameter for Dresden-2 because the initiation of emergency core cooling requires either coincidence of low reactor pressure and low coolant level or coincidence of low reactor pressure and high containment pressure. The automatic pressure-relief system in Dresden-2 is actuated by only the coincidence of low-low water level and high containment pressure. The use of a separate diverse initiating signal may not be warranted, since this coincidence requirement is probably based on the need to reduce the probability of a spurious depressurization, and this subsystem is actually a backup for the high-pressure coolant injection system.

Several of the systems have interesting diversity features, with somewhat unique plant variables used as additional initiating signals.

For example, high radiation is used as one of the initiating variables for some of the containment isolation systems in Palisades and Dresden-2. The set of initiation signals for emergency core cooling in Ginna includes low steam pressure in a steam generator.

Most of the engineered safety systems are based on the use of two redundant subsystems, where either subsystem for a particular function is capable of independently carrying out that function. A single set of redundant sensors for each plant variable serves a duplicate logic matrix in the actuation channels for each engineered safety subsystem for a given function. Since failure of one subsystem and its associated actuating system and power supply will not inhibit the overall function, ordinary relay and motor-control design techniques are used in each of the actuation channels beyond the logic matrix of initiating or inhibiting signals. In general, single relays, contacts, timers, interlocks, etc., are used in the actuation channels, and consequently each of the dual subsystems is subject to single failures disabling that subsystem.

The relays associated with the instrument channels are usually de-energized to initiate action of engineered safety features. Most logic matrices and the logic output, or actuation, relays in the actuation channels must be energized to initiate the function. The pumps (except those in the high-pressure coolant injection subsystem in Dresden-2) and most of the valves, including those for containment isolation, are motor driven and require electric power to operate. This "trip aspect" for the logic and logic output relays is used to prevent spurious initiation of safety functions upon the loss of the power supply for the logic in an actuation channel, since spurious operation of some of the systems could produce either safety problems or economic penalties, as summarized in Section 6.5. Most of the equipment below the logic output relays in the actuation channels is arranged to remain in its "operating condition" after an initial actuating signal is received, so the logic power is needed only to start the engineered safety equipment. As mentioned earlier, failure of the logic power supply in one actuation channel will prevent one of the subsystems (i.e., one-half of the equipment) from being put into operation (even if actuator power is available); however, this will not prevent the overall function from being carried out by the other subsystem.

There are a few notable exceptions to this overall pattern. The logic and actuating relays in the containment isolation systems for most of the valves in Palisades and Dresden-2 are deenergized to initiate action.* Also the logic matrices for one plant variable used in the safety injection systems in Palisades are deenergized to initiate core and containment cooling.* These systems employ a two-of-two final logic fed from two power supplies, so the loss of one logic power supply does not produce a spurious isolation or actuation of engineered safety features. Most isolation valves in Palisades and the main steam-line isolation valves in Dresden-2 are held open by air pressure against a spring, so they are fail-safe with respect to loss of actuator power. Another exception is in Ginna, where the instrument channels for containment spray are energized to initiate operation; this reduces the chances of spurious operation of the containment spray.

Bypassing for testing, as is done in parts of the Ginna and Palisades actuation channels, presents problems.²⁹ In Ginna, the output of the matrix for the plant variable being tested is momentarily disconnected during the on-line test. In Palisades, the SIS-X relays are momentarily blocked while the DBA sequencers are tested.

Each of the two actuation channels that serve all the containment isolation valves in Palisades contains one two-of-four logic matrix for each plant variable used as an initiating signal. These two actuation channels are combined in a two-of-two logic for each isolation valve. It appears that a single failure (such as a short circuit around a matrix) in the output of either of the two matrices for a plant variable could prevent the closure of all isolation valves if that plant variable exceeded its trip point. The same two matrices that handle the containment high-pressure signals are used in the actuation channels for both

*As discussed in the note on p. 68, the designs of the safety injection and containment isolation actuation systems in Palisades are being revised. The two-of-two logic arrangements are being omitted, and all logic matrices will be energized to trip and initiate action. Elimination of the two-of-two logic arrangements will remove the possibility of a single failure of a single matrix preventing the initiation of protective action from trip signals from one plant variable.

the containment isolation and the core and containment cooling systems controlled by the safety injection signal. As shown in Figs. 4.2, 4.3, and 4.4 in Section 4.1.2, the signals from these two matrices are also combined in a two-of-two logic in each of the safety injection actuation channels. With this arrangement, a single short circuit around one of the two-of-four matrices would prevent the initiation of both containment isolation and core and containment cooling from this particular plant variable.* The designers²⁴ indicate that this two-of-two logic was employed to prevent the more likely condition of a spurious loss of a logic power supply from causing unwanted initiation of containment spray and containment isolation, as discussed in Section 4.1.2. The design has a degree of diversification of plant variables in separate logic circuits and matrices for initiating these functions. Core and containment cooling will be initiated by pressurizer low-pressure logic matrices, and containment isolation will be initiated by containment high radiation logic matrices, as discussed in Sections 4.1.1 and 4.1.2. The logic system employs an ungrounded ac power system with ground detectors, so two short circuits to ground would be needed to prevent operation of a matrix, and the first would be alarmed. The containment isolation system in Dresden-2 has a somewhat similar final two-of-two logic that combines the output of two one-of-two logic channels; however, separate sets of one-of-two logic matrices are used for the inner and outer isolation valves in the same pipe line. With this arrangement a single short circuit around a one-of-two logic matrix could prevent either the inner or outer valves from closing, but not both.

Some of the designs, such as in Palisades, use two or four main timers (DBA sequencers) to sequentially connect the loads to the emergency Diesel generators. Other designs, such as in Ginna, use separate timers for each of the individual engineered safety feature loads for this purpose. It appears that the use of individual timers would reduce the amount of equipment that might be disabled if a timer should fail.

The low-pressure coolant injection subsystem in Dresden-2 is very complex. For instance, the logic system must control the operation of

*See footnote on p. 125.

a number of valves to establish the flow path used for the initial emergency core cooling stage and bypass components that are used for normal shutdown cooling or for cooling the suppression pool and spraying the containment vessel. In addition, a flow-path sensing logic system is used to select and isolate portions of the undamaged recirculation loop and to route all injected water into the bottom plenum of the reactor through portions of the undamaged recirculation loop piping. The core spray subsystems are considerably simpler, and they each serve as functional backups for the low-pressure coolant injection system, since either of the two core spray subsystems or the coolant injection system can independently provide sufficient core cooling at low pressure.

6. CONCLUSIONS

6.1 Information Availability

This report was prepared during the time period in which the detailed designs for the plants examined were being formulated. This may, in part, account for the descriptions and discussions in the safety analysis reports for these plants being generally insufficient for this review. The final safety analysis reports that were available for some of the plants naturally contained more detail than the preliminary reports because of the evolution of the plant design. However, in every case, it was necessary to obtain information directly from design or operating groups. In particular, it was difficult to obtain complete descriptions of the engineered safety features, since they tend to be designed last and are interrelated with many areas of the plant.

The safety analysis reports were sometimes difficult to interpret because of wide variations in terminology and in symbols and formats used for drawings by the different reactor manufacturers. In many instances, we found it difficult to use drawings taken directly from manufacturer's material without adding clarifying notes and sketches.

Detailed criteria beyond general statements such as those in the IEEE and AEC documents^{6,8} are just now becoming available in reference material in the public domain. Some of the design groups provided us with copies of internal reports and specifications related to their particular design approach.

6.2 System Performance

A protection system must provide the necessary functional capability to cope with potential accidents, together with high reliability of individual pieces of equipment, as discussed in Section 1.2. The functional adequacy of a complete protection system involves systems engineering consideration of such things as the potential accidents, plant variables used as inputs, trip settings, dynamic response of the system, capability of the actuators, magnitude of the protective action, efforts to eliminate

sources of common mode or systematic failures, etc. This systems engineering approach is the most important consideration in achieving an adequate protection system. Since the instrumentation is only a portion of the protection system,^{2,8} high reliability and adequate capability of the instrumentation system is not sufficient to insure that the protection system can cope with accidents that may occur. Overall plant protection requires integration of the instrumentation with the other components of the protection systems, primarily the emergency equipment and power systems. The designers of the instrumentation system must be thoroughly familiar with all the mechanical devices used in the system and all the protection system requirements.

In this report, we limited our review of system performance to an examination of the effects of failures within the instrumentation system. The failures examined were of the "single" type and were related to random events rather than to a common mode wherein one event causes the failure of several devices.³³ (The examination of systems for sources of common mode failures is difficult at best and impossible from the information available to us.) As a minimum, protection systems must be capable of providing protection after sustaining a single failure.⁸ It should be noted that random single failures have not been the cause of recorded reactor accidents.³⁴ The majority of the designs have, in general, met the single-failure criterion.⁸

6.3 Design Variances

It is rather obvious from the descriptions of instrumentation for reactor shutdown systems and engineered safety features given in Chapters 3 and 4, compared and discussed in Chapter 5, and summarized in Chapter 2 that current practice varies widely. As yet there are no commonly recognized "best ways" of solving many of the problems in protection system instrumentation. Some of the differences found in the designs of instrumentation systems are surely dictated by differences in the plants themselves, but they also reflect different approaches by different designers to apparently similar problems. Examples of different designs to carry

out similar functions include (1) arrangement of logic circuits, (2) energizing or deenergizing to initiate action, (3) methods for testing, (4) methods for bypassing trip signals, and (5) the use of analog instrument channels or simple nonindicating switches (such as pressure switches). In addition the design for a given plant may undergo rather basic changes during the design period. There is certainly no firm or constant condition of the state of the art of instrumentation for protection systems.

6.3.1 Safety and Serviceability

We have no doubt that the major objective of every design examined was to achieve a low probability of failure to initiate a protective action. We are equally certain that another objective was to obtain a low probability of the occurrence of any spurious protective action that could interfere with normal plant operation and reduce serviceability or possibly create safety problems by inducing the need for a second protection system to operate or by producing thermal shocks in the plant. The use of parallel power supplies to control rod actuators and the use of logic circuits that must be energized to initiate most of the engineered safety features, as well as the usual use of coincidence in logic circuits, are examples of methods used to reduce interference of normal operation from spurious failures of single components. In many instances the methods used to improve serviceability reduce the safety of the system and vice versa. Consequently the design must involve a reasonable compromise between these two goals; that is, the protection system design must provide an adequate degree of both safety and serviceability if the plant is to provide an economic source of energy. The four designs examined employed different techniques, particularly in the engineered safety features, to achieve these goals.

6.3.2 Plant Variables

The use of different plant variables as input signals for similar functions in different designs and the use of a different number of plant variables indicate that there may be different design bases or functional requirements. Examples of these differences are given in Sections 5.1

and 5.5. We are not commenting on the adequacy of these arrangements, but we do note their differences.

During the two-year course of this study, the choices of plant variables used for some of the protection signals changed several times. These changes indicate that the selection of variables for these functions is probably difficult. Areas or functions where changes have been made include (1) the sets of variables used to detect the approach to the condition of the departure from nucleate boiling for pressurized-water reactors,* (2) sets of variables used to detect a steam-line break in a pressurized-water reactor, and (3) sets of variables used to initiate and control many of the engineered safety feature actions for both pressurized- and boiling-water reactors.

6.4 Optimization of Design Features

The different designs seem to emphasize the equipment in different areas of similar protective functions. For example, on-line tests of the engineered safety features in Ginna include the logic matrices but not the master relays that start the pumps; while in Palisades, integrated on-line tests are made of the master relays, sequencers, and pumps but not of the logic matrices. The differences in designs, we believe, are largely the result of differences of opinions of the designers regarding the likelihood of failures in various equipment or portions of the instrumentation, coupled with the expected results of such failures. The past record of failures known by the individual engineers responsible for these designs must certainly influence the areas they emphasize.

It may not be possible to combine the best features of all the designs because each "good" feature may create problems in other areas. For example, testing the logic matrices by actually transmitting a trip signal through the logic system always requires some sort of bypassing to prevent initiation of protective action. Also, testing circuits and provisions may compromise the independence of channels.

*See footnote on p. 128.

6.5 Design of Engineered Safety Features

The engineered safety features present much more difficult design problems than the reactor shutdown systems for the following reasons:

1. The engineered safety features must operate for long periods in contrast to the short time required for a reactor scram.
2. Rather complex logic decisions may be involved, such as availability of cooling water and electric power.
3. Spurious operation of some of the engineered safety systems may create safety problems. For example, spurious actuation of the automatic pressure-relief system in a boiling-water reactor or containment isolation system in pressurized- or boiling-water reactors would require operation of other protection subsystems to protect the plant. Such spurious actuations would increase the accident initiation rate (challenge rate) with which these other protection systems would have to cope. Spurious actuation of the automatic pressure-relief system in a boiling-water reactor could cause damage to some of the fuel cladding.
4. Spurious operation of some of the engineered safety features could have economic penalties by causing a plant shutdown and the accompanying loss in revenue or by causing some damage to the plant. For example, spurious actuation of containment sprays, particularly those with chemicals for fission-product reduction, could cause expensive damage to the interior of the containment building.

Most engineered safety features use a concept of two independent subsystems, either of which is sufficient to provide protection. Each subsystem has its own logic system, logic power supply, pumps, heavy electric power, etc. The designs employ ordinary circuits and machinery and contain many opportunities for failure of an individual subsystem from a single cause.

6.6 Recent Improvements in Designs

During the two-year course of this study, a number of worthwhile improvements were made in most of the designs.

6.6.1 Plant Variables Used to Initiate Engineered Safety Feature Action

Some of the sets of variables used to initiate action of engineered safety features in the earlier designs required the coincident agreement of two or three different plant variables. All the designs have been changed to eliminate this requirement of the agreement of several plant variables. Also, in several cases, notably the initiation of emergency core cooling, diversity in input signals has been added where either of two different plant variables can start the operation of the engineered safety features.

6.6.2 Control Rod Release Circuits

A few of the early designs seemed to be vulnerable to a single failure that could prevent a reactor scram. The arrangement of control rod release circuits was changed to eliminate this problem.

6.6.3 Separation of Redundant Actuation Channels

Several changes were made in the engineered safety feature actuation circuits that improve the physical separation, or isolation, of the dual and redundant actuation channels.*

*See footnotes on pp. 68 and 125.

7. RECOMMENDATIONS

Our recommendations concerning the state of the art of instrumentation for reactor protection systems fall naturally into three areas. The first of these (Sect. 7.1) is concerned with the documentation of factual design information, the second (Sects. 7.2 through 7.6) with obtaining factual data on the performance and requirements of protection system instrumentation, and the last (Sect. 7.7) with the development of solutions to instrumentation problems.

7.1 Documentation of Designs

We would like to see more lucid, comprehensive, and accessible presentations of factual information than are available at present. We recognize that it would be difficult, in general, to provide detailed descriptions at the stage of the design when the preliminary safety analysis reports are prepared; however, fairly detailed descriptions could be provided for reactors in which the protection system is almost a duplicate of that used in a previous plant.

We feel that a standard format for presenting the description of the instrumentation system design should be adopted. A standard outline with a uniform set of section headings and drawing titles is needed. Also, reasonably consistent terminology and drawing symbols and formats should be adopted and used in all descriptions of protection systems. These improvements in documentation techniques and terminology would help to eliminate the difficulties discussed in Sections 1.3 and 6.1, they would aid the utilities that operate reactors built by different manufacturers, and they would aid the designers of future systems, as well as the regulatory reviewers.

7.2 Information Needed to Develop Design Bases for Protection Systems

A logical approach to the determination of the reliability requirements of protection systems would involve consideration of (1) the acceptable frequency of occurrence of particular accidents and (2) an

initiation rate for these accidents. The determination of this acceptable frequency of occurrence of accidents depends heavily on predicting the consequences of accidents in which the protection system does not function.

7.2.1 Experimental Tests of Accident Consequences

The analysis of potentially damaging accidents is a difficult task because of the lack of applicable experimental data or accident experience and because of the complexity of calculations used to predict the behavior. With the current state of knowledge, the sequence of events, nature, and consequences of severe accidents are indeterminate and subject to much speculation and conjecture.^{35,36} This often forces the designer to take limiting cases that are more severe than would ever be experienced. Factual data are needed on the consequences of potential accidents. Full-scale, realistic experiments that determine the consequences of unprotected accidents should be conducted to assess the magnitude of the actual consequences.

7.2.2 Experimental Tests of Spurious Operation of Protection Systems

Experimental information is also needed on the actual effects of spurious operation of protection systems, particularly some of the engineered safety subsystems. As mentioned in Section 6.5, the spurious operation of some of the subsystems may create safety or economic problems, so the consequences of spurious operation become part of the design basis for the reliability requirements for the protection systems.

7.2.3 Accident Initiation Rates

Data from operating reactors are needed on the rates at which the various subsystems of the protection system are challenged (i.e., the accident initiation rates). Such data should include cases of successful operation of the protection system, as well as the more obvious but much less frequent cases of unsuccessful operation. Some work is already being done in this area.^{37,38}

7.3 Performance Testing Under Accident Conditions

The performance of each type of instrumentation system (or subsystem) should be determined at least once by a test under accident conditions that are as realistic as possible.³⁹ In particular the ability of the sensors and signal-handling equipment to produce a trip signal under transient conditions of the plant variables and environment that approach those of potential accidents should be ascertained. Such tests should be performed prior to installation in the plant in specialized experimental facilities such as SPERT and LOFT and could be part of tests of the overall protection system (including actuators).

7.4 Instrument and Component Tests

One of the more perplexing problems involves the kind and frequency of tests that should be performed on installed instruments and components. Data are needed on the mean life and failure mode of each device in the protection system instrumentation for determining whether the required interval between testing will be less than the normal time between normal plant shutdowns and thus whether there should be capability for on-line testing during plant operation. Devices of interest include the sensors, amplifiers and signal modifiers, relays, and final logic devices, such as circuit breakers, solenoid valves, valve actuators, control rod actuators, and motor control gear. A recent report⁴⁰ on failures of a number of important engineered safety feature valves indicates the need for sound testing and maintenance practices. Some components of the protection system, such as the mechanisms that release control rods and circuit breakers that open under load, can be tested only during plant shutdowns. Consequently, special attention should be given to these components to insure that they have the long mean life (low failure rate) needed to achieve the required reliability with a testing frequency determined by the interval between normal shutdowns.

It is possible, perhaps, that a short time interval between tests might create new problems. We have been told, for example, that the circuit breakers used in the reactor shutdown systems of two of the

plants reviewed must not be exercised too frequently because they will wear out and fail.

Another problem related to sensors and amplifiers, in fact to any analog device, is that of drift. Life tests on these devices would determine the frequency of the need for calibration tests.

7.5 Direct Measurement of Safety Variables

In many instances, plant variables that must be prevented from reaching safety limits cannot be measured directly, and the values of these safety limit variables must be inferred from measurements of other variables. Although neutron and gamma fluxes can be measured as a function of position in the core (usually in the core coolant channels), techniques for measuring local heat flux, cladding temperature, fuel center-line temperature, local coolant boiling, and local flow velocity are not presently available for in-core use. The values of safety limit variables such as these must therefore be inferred from other measurements, together with known or assumed parameters (cross sections, heat transfer coefficients, etc.). We feel that research and development is needed on methods for directly measuring the safety variables and thus reducing the need for using the somewhat tenuous chains of inference.

7.6 Safe Failure Modes⁴¹

The design of protection instrumentation systems could be eased if the plant could accept any and all protective actions without safety penalties or large economic penalties (such as those mentioned in Sect. 6.5). If the plant can easily tolerate spurious action of the protective systems, more fail-safe techniques can be employed, and the decisions involved in making compromises between safety and serviceability (discussed in Sects. 6.3.1 and 7.7.6) are considerably easier to make.

7.7 Design of Instrumentation Systems

Clear, detailed criteria are needed for the design of instrumentation systems. The following items are examples of the type that should be examined in the development of satisfactory requirements.

7.7.1 Single Failure

Systems should be truly immune to "single" failures. We believe it to be axiomatic that potential failure modes that are recognized and acknowledged can be protected against. It is therefore the unrecognized or unacknowledged potential failures that will manifest themselves in a test (hopefully) or in an accident. Protection systems should be studied "perversely" to ferret out potential failure modes.

The crux of the problem is in defining a single failure. One difficulty in this regard is the use of two highly complex subsystems to accomplish a single vital function, such as emergency core cooling. In present designs, each of these subsystems is susceptible to many single failures that would prevent its operation. It is necessary to examine these systems closely to determine where "subset" redundancy is required internally within one of the individual subsystems.

7.7.2 Testing Provisions

Complete, detailed, safe testing should be feasible, and yet most present designs do not incorporate all the testing precepts we believe should be followed.²⁹ New studies and designs are needed, with the objective of demonstrating adequately that no failure has occurred and thus providing the necessary validation of the single-failure criterion. This is particularly important with respect to control rod release circuits. As discussed in Section 5.3, multiple short circuits are required to prevent scram operation of all control rod release circuits; however, provisions must be included in the designs for detecting the first of this type of short circuit to prevent accumulation of short circuits to the point of system failure.³⁰

A rationale needs to be developed regarding the testing of sensors. As discussed in Section 5.2, blind instruments, such as pressure switches, are tested periodically during reactor operation, but they are not amenable to surveillance. On the other hand, indicating analog-type instruments may be checked by visually comparing the outputs of redundant channels, but the sensors are not tested during reactor operation.

Another problem area exists in the testing of circuit breakers (or "circuit makers") that are closed to initiate engineered safety feature protective actions. In the case of some breakers, stored energy mechanisms must be recharged after the breaker is opened following a test of its closing to provide energy for the next closure. Hence, a simple test of breaker closure does not demonstrate that the breaker is capable of closing the circuit the next time the request is made.⁴²

We feel that integrated tests of the operation of subsystems for individual protective functions should be performed occasionally during the life of the plant. This involves the introduction of a sufficient number of signals into the instrument channels, as near the sensors as possible, to trip the logic and actually initiate operation of the actuators to carry out the protective action (i.e., scram the rods, pump emergency cooling water into the reactor, or close isolation valves).

7.7.3 Diversity

A rationale is needed for the application of diversity. This applies particularly to (1) the measurement of different variables associated with the same accident or the same plant condition, (2) the measurement of the same variable with different types of sensors, and (3) the application of different types of actuators to carry out the protective actions. Of less concern is the application of diversity to amplifiers, bistable devices, relays, circuit breakers, etc., that are more standardized and better protected than the sensors and actuators close to the reactor. The use of diversity has a potential advantage for reducing the chance of unanticipated common mode failures.^{18,32,33} It has a disadvantage of increasing the number of trip variables and thus increasing the chances of spurious actuation if additional measurements are added for the sake of diversity.

7.7.4 Interaction Between the Protection and Operation Systems

The design must preclude a single event from causing an operation system failure that introduces actions requiring protection while at the same time paralyzing the protection system. Such single events include random failures originating within either system that are random relative

to time and individual channels, as well as common mode failures³³ that affect all similar equipment or equipment in the same environment.

Two approaches⁴³ are used to negate the effect of random failures: (1) physically separate systems are used for protection and operation, and (2) shared instrument channels are provided with isolation between the protection and operation systems and extra redundancy in the protection system. We recommend the first approach of physically separating systems.⁴³

Several methods have been considered for coping with the difficult problem of common mode failures. Representative solutions include (1) use of different types³³ and hence physically separate instrument channels for the protection and operation systems, (2) use of the same type but physically separate instrument channels for the protection and operation systems, with another set of diverse instrument channels in the protection system for backup, and (3) use of shared instrument channels with isolation between the protection and operation systems and another set of diverse instrument channels in the protection system for backup.¹⁸ The first approach may not provide much improvement in combatting common mode failures because of the difficulty or impracticality of attaining complete diversity of the two systems. Therefore the second solution may give more improvement with practical measures. We feel that the second method has an advantage over the third in that the separate systems are more amenable to testing, maintenance, and future modifications in the operations system. The third solution has the advantage of requiring fewer penetrations in the primary system.

7.7.5 Isolation Between Redundant Channels of the Protection System

Redundant channels of the protection system must have physical and electrical separation. All the designs examined were intended to provide this isolation; however, particular attention should be given to the detailed layout of instrument cabinets, connecting cables, logic arrangement, and associated hardware, such as mode switches.

As discussed in Section 5.3, we feel that it is acceptable to take signals from protection system channels to use for such things as data

loggers, annunciators, rod withdrawal prohibit devices, and set-point modifiers for controllers. These types of connections offer paths for possible interconnection of protection system channels, so when used, they must be made carefully and employ isolation amplifiers or other isolation devices.

7.7.6 Energizing to Initiate Protective Action

A rationale is needed regarding the choice of energizing or deenergizing to initiate protective actions, particularly in the engineered safety features. Spurious protective action as the result of loss of power to a single logic matrix can be avoided by methods such as the use of (1) an arrangement of two logic matrices, each with its own power supply, in a two-of-two logic for each group of actuators to be deenergized to initiate action, or (2) an arrangement of one logic matrix, with its own power supply, for each group of actuators to be energized to initiate action. In both cases, failure of an actuator group to take action when protection is needed must be tolerable. Both methods are vulnerable to a single failure that causes the unsafe failure of one actuator group; a short circuit would affect the first method, and an open-circuit would affect the second. The first method is used in most reactor shutdown systems, and there is much discussion in the safety analysis reports of the merits of the "fail-safe" aspect on loss of power supplies. The second method is used in most actuation systems for engineered safety features.



REFERENCES

1. Code of Federal Regulations, Title 10, Part 100, Reactor Site Criteria; see Federal Register, 26(28): 1224 (Feb. 11, 1961).
2. S. H. Hanauer and C. S. Walker, Design Principles of Reactor Protection Instrument Systems, USAEC Report ORNL-NSIC-51, Oak Ridge National Laboratory, September 1968. (See Sects. 2.1, 2.2, 2.4, and App. A for definitions of terms.)
3. C. G. Lawson, Emergency Core-Cooling Systems for Light-Water-Cooled Power Reactors, USAEC Report ORNL-NSIC-24, Oak Ridge National Laboratory, October 1968.
4. F. C. Zapp, Testing of Containment Systems Used with Light-Water-Cooled Power Reactors, USAEC Report ORNL-NSIC-26, Oak Ridge National Laboratory, August 1968.
5. H. A. McLain, Potential Metal-Water Reactions in Light-Water-Cooled Power Reactors, USAEC Report ORNL-NSIC-23, Oak Ridge National Laboratory, August 1968.
6. Code of Federal Regulations, Title 10, Part 50, General Design Criteria for Nuclear Power Plant Construction Permits; see Federal Register, 32(132): 10213-10218 (July 11, 1967).
7. International Electrotechnical Commission, Protection System Draft, Clause 5, February 1967.
8. Institute of Electrical and Electronics Engineers, Proposed Criteria for Nuclear Power Plant Protection Systems, IEEE No. 279, Aug. 30, 1968.
9. S. H. Hanauer and C. S. Walker, Principles of Design of Reactor-Protection Instrument Systems, Nucl. Safety, 9(1): 31-32 (Jan.-Feb. 1968).
10. Duke Power Company, Oconee Nuclear Station, Units 1 and 2, Preliminary Safety Analysis Report, Vols. I and II, undated, Chap. 7, Docket Nos. 50-269 and -270.
11. H. H. Stevens, E. S. Patterson, and R. E. Wascher, Babcock & Wilcox Company, personal communications.
12. W. H. Owen, Duke Power Company, personal communication.
13. Consumers Power Company, Palisades Plant, Final Safety Analysis Report, Vols. I, II, and III, Docket No. 50-255, undated.
14. B. J. Cochran and L. M. Johnson, Combustion Engineering, Inc., personal communication.

15. G. S. Keeley and K. A. Swarts, Consumers Power Company, personal communication.
16. Rochester Gas and Electric Corporation, Robert Emmett Ginna Nuclear Power Plant Unit No. 1, Final Facility Description and Safety Analysis Report - Plant Design Description and Safety Analysis, Docket No. 50-244.
17. J. M. Gallagher, T. W. T. Burnett, R. J. Cooney, R. Hayford, and R. A. Wiesemann, Westinghouse Electric Corporation, personal communications.
18. T. W. T. Burnett, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors, USAEC Report WCAP-7306, Westinghouse Electric Corporation, April 1969.
19. Tennessee Valley Authority, Browns Ferry Nuclear Power Station, Design and Analysis Report, Vols. I and II, Sect. IX-7, Docket Nos. 50-259 and 50-260, undated.
20. J. C. Russ, I. M. Jacobs, M. R. Lane, E. P. Peabody, J. F. Osborn, D. G. Scapini, L. Stanley, and A. J. McCrocklin, General Electric Company, personal communications.
21. I. M. Jacobs, Reactor Protection System, A Reliability Analysis, USAEC Report APED-5179, General Electric Company, June 1966.
22. J. C. Ebersole, G. P. Palo, R. M. Pierce, and G. O. Wessenauer, Tennessee Valley Authority, personal communications.
23. Consumers Power Company, Palisades Plant, Interim Redraft of the Engineered Safeguards Electrical Equipment, Sects. VII and VIII, May 13, 1968.
24. S. A. Guisti, Bechtel Company, personal communication.
25. Commonwealth Edison Company, Dresden Nuclear Power Station Units 2 and 3, Safety Analysis Report, Vols. I and II, Docket No. 50-237/249. (N.b., this is the Dresden-2 and -3 final safety analysis report.)
26. W. B. Behnke, Commonwealth Edison Company, personal communication.
27. Iowa Electric Light & Power Co., Duane Arnold Energy Center, Preliminary Safety Analysis Report, Vols. 1 through 6, Docket 50-331.
28. S. H. Hanauer and C. S. Walker, op. cit. Ref. 2, Sect. 4.4.
29. Ibid., Sect. 4.3.
30. Ibid., Sect. 4.6.1.
31. Ibid., Sect. 5.4.3.

32. Ibid., Sects. 3.3 and 5.4.4.
33. E. P. Epler, Common Mode Failure Considerations in the Design of Systems for Protection and Control, Nucl. Safety, 10(1): 38-45 (Jan.-Feb. 1969).
34. E. P. Epler, Safety System Reliability Versus Performance, Nucl. Safety, 6(4): 411-414 (Summer 1965).
35. G. O. Bright, A Review of Generalized Reactivity Accident for Water-Cooled and Moderated UO₂-Fueled Power Reactors, Nucl. Safety, 8(2): 116-127 (Winter 1966-1967).
36. W. K. Ergen (Ed.), Emergency Core Cooling, Report of Task Force Established by U.S. Atomic Energy Commission to Study Fuel Cooling Systems of Nuclear Power Plants, USAEC Report TID-24226, 1967.
37. B. J. Garrick et al., An Analysis of Nuclear Power Plant Operating and Safety Experience, USAEC Report HN-185, Holmes & Narver, Inc., Dec. 15, 1966.
38. USAEC Reactor Safety Operating Experience Bulletins.
39. S. H. Hanauer and C. S. Walker, op. cit. Ref. 2, Sect. 3.8.
40. Valve Malfunctions, in USAEC Reactor Safety Operating Experience Bulletin ROE 69-8, Apr. 1, 1969.
41. S. H. Hanauer and C. S. Walker, op. cit. Ref. 2, Sect. 4.1.
42. J. V. Stephens, Circuit Makers Need Supervision, Power Eng., 73(2): 33-35 (February 1969).
43. S. H. Hanauer and C. S. Walker, op. cit. Ref. 2, Chap. 5.

9

•

•

•

•

•

•

Appendix A

REVIEWERS, CONSULTANTS, AND INFORMATION SOURCES

Steering Committee

E. P. Epler, Oak Ridge National Laboratory
 J. M. Harrer, Argonne National Laboratory
 T. J. Thompson, Massachusetts Institute of Technology

External Reviewers and Consultants

F. C. Legler, U.S. Atomic Energy Commission
 V. A. Moore, U.S. Atomic Energy Commission
 A. J. Pressesky, U.S. Atomic Energy Commission
 Frank Schroeder, Phillips Petroleum Company

ORNL Reviewers and Consultants

R. H. Bryan	E. W. Hagen
C. M. Burton	L. C. Oakes
W. B. Cottrell	T. G. Robinson
S. J. Ditto	P. Rubel

Information SourcesThe Babcock & Wilcox Company

E. S. Patterson
 H. H. Stevens
 R. E. Wascher

General Electric Company

I. M. Jacobs
 A. J. McCronklin
 J. F. Osborn
 E. P. Peabody
 J. C. Russ
 D. G. Scapini
 L. Stanley

Bechtel Company

S. A. Giusti

Duke Power Company

W. H. Owen

Commonwealth Edison Company

W. B. Behnke

Westinghouse Electric Corporation

T. W. T. Burnett
 R. J. Cooney
 J. M. Gallagher
 R. I. Hayford
 J. S. Moore
 W. F. Schmauss
 R. A. Wiesemann

Combustion Engineering, Inc.

Frank Bevilacqua
 B. J. Cochran
 L. M. Johnson

Consumers Power Company

G. S. Keeley
 K. A. Swarts

Tennessee Valley Authority

J. C. Ebersole
 C. Michelson
 G. P. Palo
 R. M. Pierce
 G. O. Wessenauer