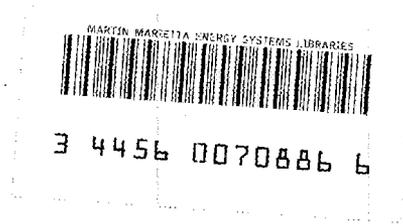


ornl

OAK RIDGE
NATIONAL
LABORATORY

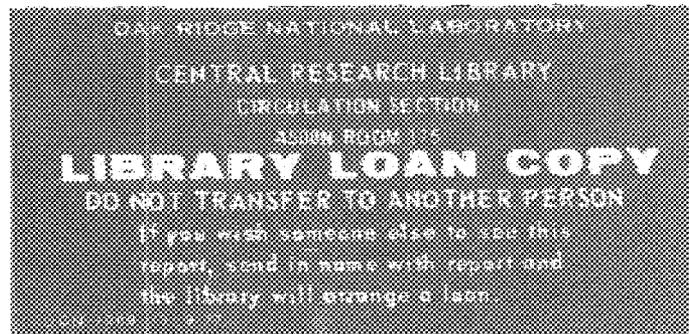
MARTIN MARIETTA



ORNL/TM-10045

A Common Cause Failure Analysis of the Rodded Scram System of the Arkansas Nuclear One-Unit 1 Plant

D. F. Montague
D. J. Campbell
G. F. Flanagan



OPERATED BY
MARTIN MARIETTA ENERGY SYSTEMS, INC.
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

Printed in the United States of America. Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road, Springfield, Virginia 22161
NTIS price codes— Printed Copy: A08; Microfiche A01

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ENGINEERING PHYSICS AND MATHEMATICS DIVISION

A COMMON CAUSE FAILURE ANALYSIS OF THE RODDED SCRAM SYSTEM
OF THE ARKANSAS NUCLEAR ONE-UNIT 1 PLANT*

D. F. Montague⁺
D. J. Campbell⁺
G. F. Flanagan

Date Published - October 1986

*Research sponsored by the U.S. Nuclear Regulatory Commission under Interagency Agreement 40-550-75 with Martin Marietta Energy Systems, Inc.

⁺JBF Associates, Inc., Technology Drive, 1000 Technology Park Center, Knoxville, TN 37932.

Prepared by the
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831
operated by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under Contract No. DE-AC05-84OR21400



3 4456 0070886 6

PREFACE

Probabilistic risk assessments (PRAs) of nuclear power plants frequently identify common cause failures (CCFs) as major contributors to plant risk. However, the methods employed to analyze CCFs in PRAs are usually empirical techniques that do not systematically address all CCF scenarios and do not identify specific causes of CCFs.

This study presents the results of using formal common cause failure analysis (CCFA) methods in a detailed reliability analysis of a nuclear power plant safety system. The study identified both important and unimportant general causes of CCFs for a rodged scram system, as well as specific causes within the important general categories. Through this study we established many of the strengths and practical limitations of performing a detailed, systematic CCFA. As a result of this work, we developed a draft set of guidelines for performing a dependent failure analysis. These newly developed guidelines are now being finalized as a set of recommended procedures.

SUMMARY

This study demonstrates the use of a formal method for common cause failure analysis in a reliability analysis of the Arkansas Nuclear One - Unit 1 rodged scram system. The scram system failure of interest is loss of capability of the system to shut the reactor down when required. The results of this analysis support the ATWS program sponsored by the U.S. Nuclear Regulatory Commission. The methods used in this analysis support the NRC's Risk Methods Integration and Evaluation Program (RMIEP).

Results of interest in this study include:

- an estimate of the average unavailability for the scram system due to independent component failures and the major contributors to this unavailability
- the scram system minimal cut sets that are susceptible to common cause failure
- a list of potential root cause events that are conducive to scram system common cause failure
- estimates of the conditional probability of scram system failure, given the occurrence of each type of root cause event
- a sensitivity analysis of scram system unavailability with respect to each type of root cause event
- estimates of scram system unavailabilities for important types of root cause events.

Our estimate of the average unavailability of the scram system due to independent component failures is 4.1×10^{-6} . This result is consistent with the scram system unavailability estimate in the ANO-1 IREP study. Ninety-nine percent of the time when the scram system is unavailable due to independent hardware failures the cause of failure is an electrical

component failure (as opposed to a mechanical component failure). The major contributors to the scram system average unavailability when considering only independent failures are the two scram breakers used to interrupt ac power to the control rod drive mechanisms (CRDMs).

We determined that common cause failures are potentially dominant contributors to scram system unavailability. Twenty-nine root cause event types (generic causes) that can cause scram system failure (e.g., impact events, power surges, and common links) were identified. The contributions of some of these events to scram system unavailability are greater than the total contribution from independent failures. The most important scram system components--with respect to common cause failures--again are the ac power interrupt breakers for the CRDMs.

Based on the results of this work, we recommend the following:

1. Develop a streamlined procedure for identifying and calculating the frequency of root cause events. In this study, we performed a plant walk-through to identify potential root cause events. Root cause event frequency estimates were based primarily on engineering judgment. A detailed root cause event analysis procedure will ensure a comprehensive treatment of root cause events, with a more refined estimate of the frequency of root cause events.
2. Perform a common cause failure analysis on other scram system designs. Even though results from this ANO-1 scram system analysis are not directly applicable to other scram systems, the analysis indicates there are good reasons to believe the failures of other scram systems are also dominated by common cause failures. Plant-specific analyses will determine the common cause failure characteristics of other scram systems.
3. Investigate the feasibility of collecting component failure data to determine more accurate conditional probabilities of important component failures, given severe generic environments. These data are needed

to calculate the conditional probability of system failure, given a severe generic environment. Component failure probabilities used in this study were synthesized from WASH-1400 data and engineering judgment.

4. Develop methods for performing an uncertainty analysis on the conditional probabilities of scram system failure, given the occurrence of each type of root cause event.
5. Update the importance calculation method in COMCAN III to allow for calculations that are not based on "rare event" approximations.

Implementing these recommendations will result in defensible estimates of scram system failure probabilities and ATWS frequencies for light water reactor designs used in the U.S. commercial nuclear power industry.

ACKNOWLEDGMENTS

We express sincere appreciation to William Cavanaugh III, Gary Kendrick, and Jack Robertson (Arkansas Nuclear One Plant) for their technical assistance on this project. We also thank the many people at the Idaho National Engineering Laboratory who assisted us in using the COMCAN III computer program and the people at Sandia National Laboratories who supplied us with ANO-1 information. We gratefully acknowledge the support given to this work by Ken Murphy (U.S. Nuclear Regulatory Commission).

GLOSSARY

| | |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Barrier | a device that limits the propagation of an adverse environment |
| Basic event | the malfunction of a component in one of its possible failure modes |
| Common cause candidate | a minimal cut set whose basic events could all fail because of a common dependency |
| Common cause failure | the occurrence of a root cause event and subsequent failure of one or more common cause candidates associated with the root cause event |
| Common link | a source of common cause failures that can transgress physical barriers |
| Domain | an area within a plant that contains a root cause event source and is bounded by barriers to the adverse environment produced by the root cause event |
| Generic cause | an event or condition that can result in common cause failures |
| Generic environment | an environmental condition such as impact, grit, or vibration (whose source is unspecified) that can cause component failures |
| Generic susceptibilities | limitations associated with components that can cause them to fail when subjected to adverse environmental conditions |
| Minimal cut set | a group of basic events that are collectively sufficient to cause system failure. The occurrence of each basic event in the minimal cut set is necessary to cause system failure |
| Root cause event | an event that produces conditions (either environmental or operational) that increase component failure frequencies |
| Special conditions | conditions associated with components such as component manufacturer, the maintenance crew charged with component upkeep, or the procedures used for component maintenance. As with common links, special conditions can transgress physical barriers |
| Unavailability | the probability a system is in a failed state at time t |

TABLE OF CONTENTS

| Section | Page |
|---------------------------------------------------------|------|
| PREFACE | iii |
| SUMMARY | iv |
| ACKNOWLEDGMENTS | vii |
| GLOSSARY | viii |
| LIST OF TABLES | xi |
| LIST OF FIGURES | xii |
| 1. INTRODUCTION | 1 |
| 1.1 Purpose | 1 |
| 1.2 Background | 2 |
| 1.3 Scope | 3 |
| 1.4 Report Organization | 4 |
| 2. PROBLEM DEFINITION | 5 |
| 2.1 System Description | 5 |
| 2.1.1 System Design | 5 |
| 2.1.2 Instrumentation and Controls | 15 |
| 2.1.3 Testing and Maintenance | 16 |
| 2.1.4 Interfacing Systems | 17 |
| 2.2 Failure Descriptions | 18 |
| 2.2.1 TOP Event Definition | 18 |
| 2.2.2 Scram System Equipment Failure Modes | 18 |
| 2.3 Transient Initiating Events | 22 |
| 3. QUALITATIVE ANALYSIS | 24 |
| 3.1 Fault Tree Modeling | 24 |
| 3.2 Minimal Cut Set Determination | 27 |
| 3.3 Common Cause Candidate Identification | 28 |
| 3.3.1 Input Data for COMCAN III | 29 |
| 3.3.2 Identification of Common Cause Failures | 33 |
| 3.3.3 Identification of Root Cause Events | 34 |
| 3.4 Qualitative CCFA Results | 35 |
| 4. QUANTITATIVE ANALYSIS | 41 |
| 4.1 Independent Failure Quantification | 41 |
| 4.2 Common Cause Failure Quantification | 44 |

TABLE OF CONTENTS

(continued)

| Section | Page |
|----------------------------------------------------------------------------------------------|------|
| 4.2.1 Conditional Failure Probabilities | 46 |
| 4.2.2 Fault Exposure Times | 55 |
| 4.2.3 Root Cause Event Frequencies | 57 |
| 4.3 Quantitative CCFA Results | 65 |
| 5. CONCLUSIONS AND RECOMMENDATIONS | 68 |
| REFERENCES | 72 |
| RELATED BIBLIOGRAPHY | 73 |
| APPENDICES | |
| A. Detailed Fault Tree of the ANO-1 Scram System | A-1 |
| B. Reduced Fault Tree of the ANO-1 Scram System | B-1 |
| C. Basic Event Descriptions and Data | C-1 |
| D. Conditional Failure Probabilities for Basic Events | D-1 |
| E. Example Calculation of the Conditional Failure Probability for a Basic Event | E-1 |

LIST OF TABLES

| Table | | Page |
|-------|-----------------------------------------------------------------------------------------------|------|
| 2.1 | Reactor Protection System Trip Setting Limits | 8 |
| 2.2 | ANO-1 Rod Group Compositions | 14 |
| 3.1 | CCFA Qualitative Results - Generic Environments | 36 |
| 3.2 | CCFA Qualitative Results - Common Links | 37 |
| 3.3 | CCFA Qualitative Results - Similar Parts | 38 |
| 4.1 | Unavailability Importance of Components in the Scram System - Independent Failures | 43 |
| 4.2 | Scram System Conditional Failure Probabilities - Generic Environments | 48 |
| 4.3 | Scram System Conditional Failure Probabilities - Common Links | 49 |
| 4.4 | Unavailability Importance of Components in the Computer Room - Generic Environments | 53 |
| 4.5 | Unavailability Importance of Components in the Control Room - Generic Environments | 56 |
| 4.6 | Scram System Fault Exposure Times - Generic Environments | 58 |
| 4.7 | Scram System Fault Exposure Times - Common Links | 59 |
| 4.8 | CCFA Quantitative Results - Sensitivity Analysis for Generic Environments | 61 |
| 4.9 | CCFA Quantitative Results - Sensitivity Analysis for Common Links (Similar Parts) | 62 |
| 4.10 | Scram System Unavailability Estimates by Root Cause Event Type | 66 |
| C.1 | Basic Event Descriptions and Failure Data | C-2 |
| C.2 | Reduced Fault Tree Basic Event Locations | C-11 |
| D.1 | Conditional Failure Probabilities for Basic Events | D-3 |

LIST OF FIGURES

| Figure | | Page |
|--------|-------------------------------------------------------------|------|
| 2.1 | Functional Block Diagram of the Reactor Protection System . | 6 |
| 2.2 | RPS Sensor Channels | 10 |
| 2.3 | Two-out-of-four RPS Trip Logic | 11 |
| 3.1 | ANO-1 Scram System Fault Tree Top | 25 |
| 3.2 | ANO-1 Barriers to Generic Types of Environments | 32 |
| A.1 | Detailed Fault Tree of the ANO-1 Scram System | A-2 |
| B.1 | Reduced Fault Tree of the ANO-1 Scram System | B-2 |

1
A COMMON CAUSE FAILURE ANALYSIS OF
THE RODDED SCRAM SYSTEM OF THE ARKANSAS
NUCLEAR ONE - UNIT 1 PLANT

1. INTRODUCTION

1.1 Purpose

The major purpose of this study was to demonstrate the use of a formal method for common cause failure analysis (CCFA) in a detailed reliability analysis of a scram system. The system analyzed herein is the rodded scram system of the Arkansas Nuclear One - Unit 1 Power Plant (ANO-1). The system consists of electrical and electronic equipment (1) that determines when process parameters exceed preset limits and (2) that removes electrical power from the control rod drives (the mechanical portion of the system), allowing the rods to fall into the reactor core and shut down the reactor.

In addition to demonstrating how a CCFA can be performed as part of a scram system reliability analysis, this report includes qualitative and quantitative evaluations of the effects of independent failures and common cause failures on the availability of the scram system to shut down the reactor when required. More specifically, this study provides the following results:

- an estimate of the average unavailability for the scram system due to independent component failures and the major contributors to this unavailability
- the scram system minimal cut sets that are susceptible to common cause failure

- a list of potential root cause events that are conducive to scram system common cause failure
- estimates of the conditional probability of scram system failure, given the occurrence of each type of root cause event
- a sensitivity analysis of scram system unavailability with respect to each type of root cause event
- estimates of scram system unavailabilities for important types of root cause events.

This report also provides recommendations for additional common cause failure analysis research that will enhance future reliability analyses of other nuclear power plants' scram systems.

1.2 Background

The issue of anticipated transients without scram (ATWS) for light water reactors has been, and continues to be, a source of debate for those concerned with nuclear reactor safety. One of the central questions in this debate concerns the probability of failure to scram.¹ Light water reactor scram systems are designed with so much redundancy and with such a tendency to fail safe when component failures do occur that the probability of system failure arising from independent failures of system components is negligible. Instead, important failures of these high reliability systems tend to be the result of common cause failures.²

This study was a pioneer analysis of a light water reactor scram system using a systematic method of common cause failure analysis. While the study was plant-specific to the Arkansas Nuclear One - Unit 1 (ANO-1) scram system, the results are generically applicable to similar Babcock and Wilcox (B&W) scram systems.

1.3 Scope

Three types of scenarios can result in an anticipated transient without scram:¹

1. A transient occurs that causes failure of the scram system.
2. An external event causes a transient and also causes scram system failure.
3. A transient occurs when the scram system is already failed.

According to NUREG/CR-0460, the first type of scenario occurs at a frequency so low that it need not be considered in a reliability analysis. This study found no evidence to the contrary. Scram system components at ANO-1 are located where they will not be adversely affected by any reactor transients before the components would effect a reactor trip.

The second type of scenario occurs if an external event causes scram system failure and causes a failure in the integrated control system (ICS), which produces a transient through improper control action (e.g., closing the main feedwater control valve). The physical locations of ICS and reactor protection system (RPS) equipment at the Arkansas Nuclear One - Unit 1 Plant are such that the occurrence of this type of event is extremely remote. The chances of an event occurring that causes scram system failure and that produces a transient by causing failure of equipment associated with normal plant operation is also extremely remote because of the physical location of RPS equipment. Thus, the second type of scenario was not considered in our detailed analysis.

This analysis focused on the third type of ATWS scenario: the scram system loses capability to scram during reactor operation, the failure is

not corrected, and a transient occurs, which requires that the reactor be scrammed. Scram system failure can be caused by independent hardware failures or by common cause failures; therefore, this report discusses the qualitative and quantitative analyses of the ANO-1 scram system considering both independent hardware failures and common cause failures.

1.4 Report Organization

Section 2 of this report describes the ANO-1 rodded scram system and defines the problem for analysis. Section 3 discusses the methods and results of the qualitative analysis of the scram system, and the methods and results of the quantitative analysis are discussed in Section 4. Section 5 presents the conclusions and recommendations of this study.

2. PROBLEM DEFINITION

2.1 System Description

2.1.1 System Design

The scram system at ANO-1 protects the nuclear fuel cladding from damage and helps prevent transient overpressure events from occurring in the reactor coolant system. It consists of the reactor protection system (RPS), the control rods, and the control rod drive mechanisms (CRDMs). The RPS has redundant channels of sensors and signal processing equipment for monitoring several conditions in the nuclear steam supply system. If any of these monitored conditions, or a combination of these conditions, reaches specified safety system settings, the RPS trips the reactor by interrupting all power to the windings of the control rod assemblies in the safety rod and regulating rod groups. This power interruption allows the control rods to drop into the core and effect a reactor shutdown.

The ANO-1 reactor protection system (Figure 2.1) monitors conditions in the nuclear steam supply system through four independent channels of sensors (channels A, B, C, and D) and trips the reactor upon receiving shutdown votes from any two channels. There are 10 trip parameters that feed a bistable trip string in each of the 4 independent channels:

1. high reactor coolant temperature
2. high reactor coolant pressure
3. low reactor coolant pressure
4. variable low reactor coolant system pressure (based on reactor temperature)
5. overpower
6. power vs. number of reactor coolant pumps operating

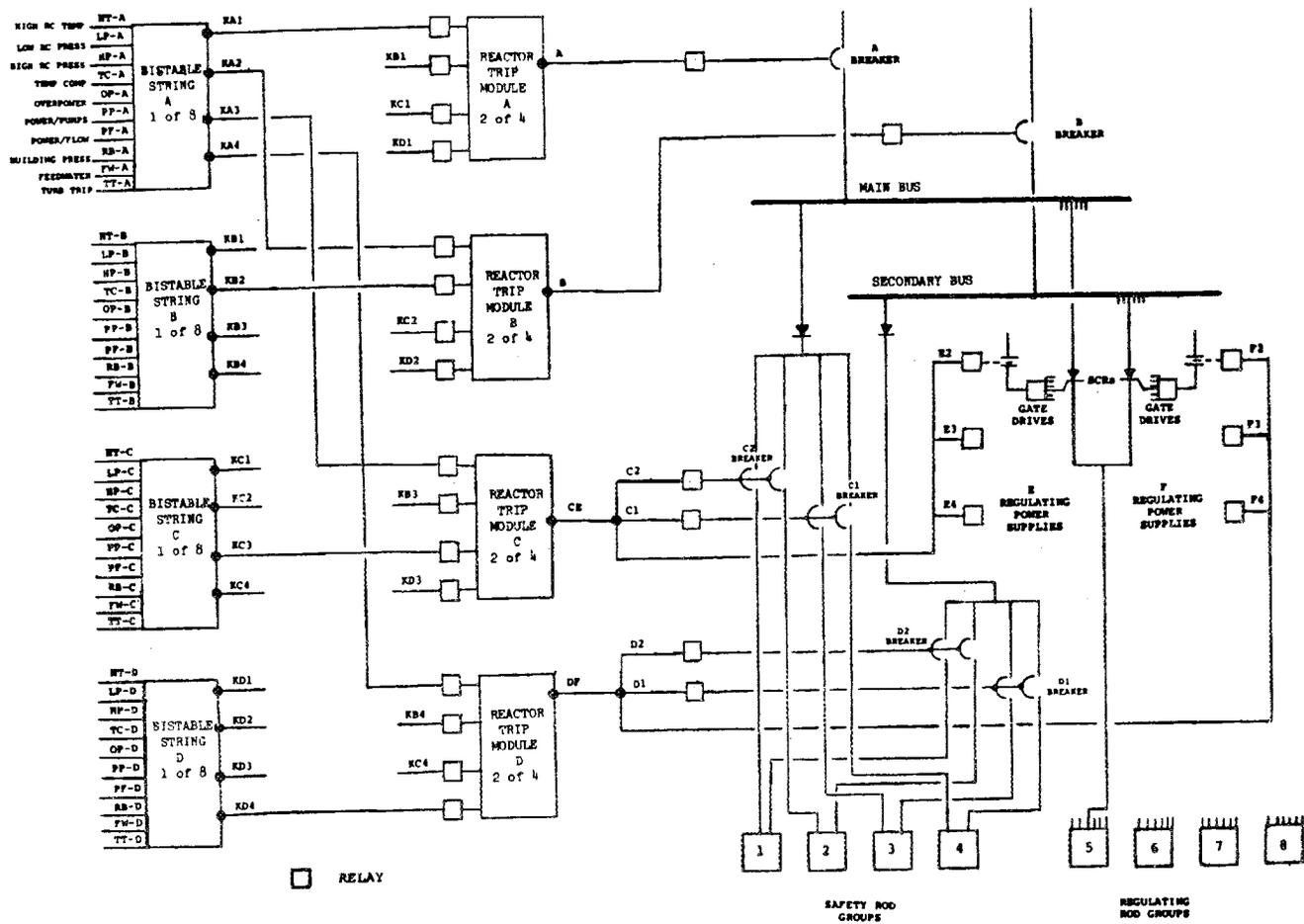


Figure 2.1 Functional Block Diagram of the Reactor Protection System

7. high reactor building pressure
8. power/imbalance/flow
9. anticipatory feedwater pump trip
10. anticipatory turbine trip

Table 2.1 lists the safety system "trip" points for each of these parameters.

The bistable trip string for each channel (Figure 2.2) consists of 10 bistable trip relays and 1 channel trip relay (KA, KB, KC, or KD). All bistable trip relays in each trip string are normally energized and closed. Power for all relays in a channel's bistable trip string is supplied by the channel's 15V dc power supply. Power for the 15V dc source is supplied by the channel's 120V vital ac bus. Loss of power from the channel's 15V dc power supply or from the 120V vital ac bus results in a channel trip (fail safe). Power surges from either of these sources, however, may result in one or more channels failing unsafe. A crowbar on the 15V dc power supply prevents an excessively high voltage output.

Each trip parameter signal in a channel controls one bistable trip relay. When system conditions reach one of the safety system trip points, the associated trip parameter signal commands its bistable trip relay to open. This action de-energizes the bistable trip channel relay, causing it to open and thus providing one of the two channel votes needed to initiate a reactor trip.

The channel trip relays (KA, KB, KC, and KD) are connected in a two-out-of-four trip logic configuration (Figure 2.3). Each channel trip relay de-energizes four auxiliary trip relays--one in each channel (e.g.,

Table 2.1 Reactor Protection System Trip Setting Limits^a

| | Four Reactor Coolant Pumps Operating (Nominal Operating Power - 100%) | Three Reactor Coolant Pumps Operating (Nominal Operating Power - 75%) | One Reactor Pump Operating in Each Loop (Nominal Operating Power - 40%) | Shutdown Bypass |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------|--------------------|
| Nuclear power, % of rated, maximum | 104.9 | 105.5 | 105.5 | 5.0 ^b |
| Nuclear power based on flow ^c and imbalance, % of rated, maximum | 1.054 times flow minus reduction due to imbalance(s) | 1.057 times flow minus reduction due to imbalance(s) | 1.057 times flow minus reduction due to imbalance(s) | Bypassed co |
| Nuclear power based on pump monitors, % of rated, maximum ^d | N/A | N/A | 55% | Bypassed |
| High reactor coolant system pressure, psig, maximum | 2300 | 2300 | 2300 | 1720 ^b |
| Low reactor coolant system pressure, psig, minimum | 1800 | 1800 | 1800 | Bypassed |
| Variable low reactor coolant system pressure, psig, minimum | $(11.75T_{out}-5103)^e$ | $(11.75T_{out}-5103)^e$ | $(11.75T_{out}-5103)^e$ | Bypassed |

Table 2.1 (continued)

| | Four Reactor Coolant Pumps Operating (Nominal Operating Power - 100%) | Three Reactor Coolant Pumps Operating (Nominal Operating Power - 75%) | One Reactor Pump Operating in Each Loop (Nominal Operating Power - 40%) | Shutdown Bypass |
|--------------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------|--------------------|
| Reactor coolant temperature F, maximum | 618 | 618 | 618 | 618 |
| High reactor building pressure, psig, maximum | 4(18.7 psia) | 4(18.7 psia) | 4(18.7 psia) | 4(18.7 psia) |

^a trip setting limits as of fuel cycle #4

^b automatically set when other segments of the RPS (as specified) are bypassed

^c reactor coolant system flow, %

^d the pump monitors also produce a trip on (a) loss of two reactor coolant pumps in one reactor coolant loop and (b) loss of one or two reactor coolant pumps during two-pump operation.

^e T_{out} is in degrees Fahrenheit (F).

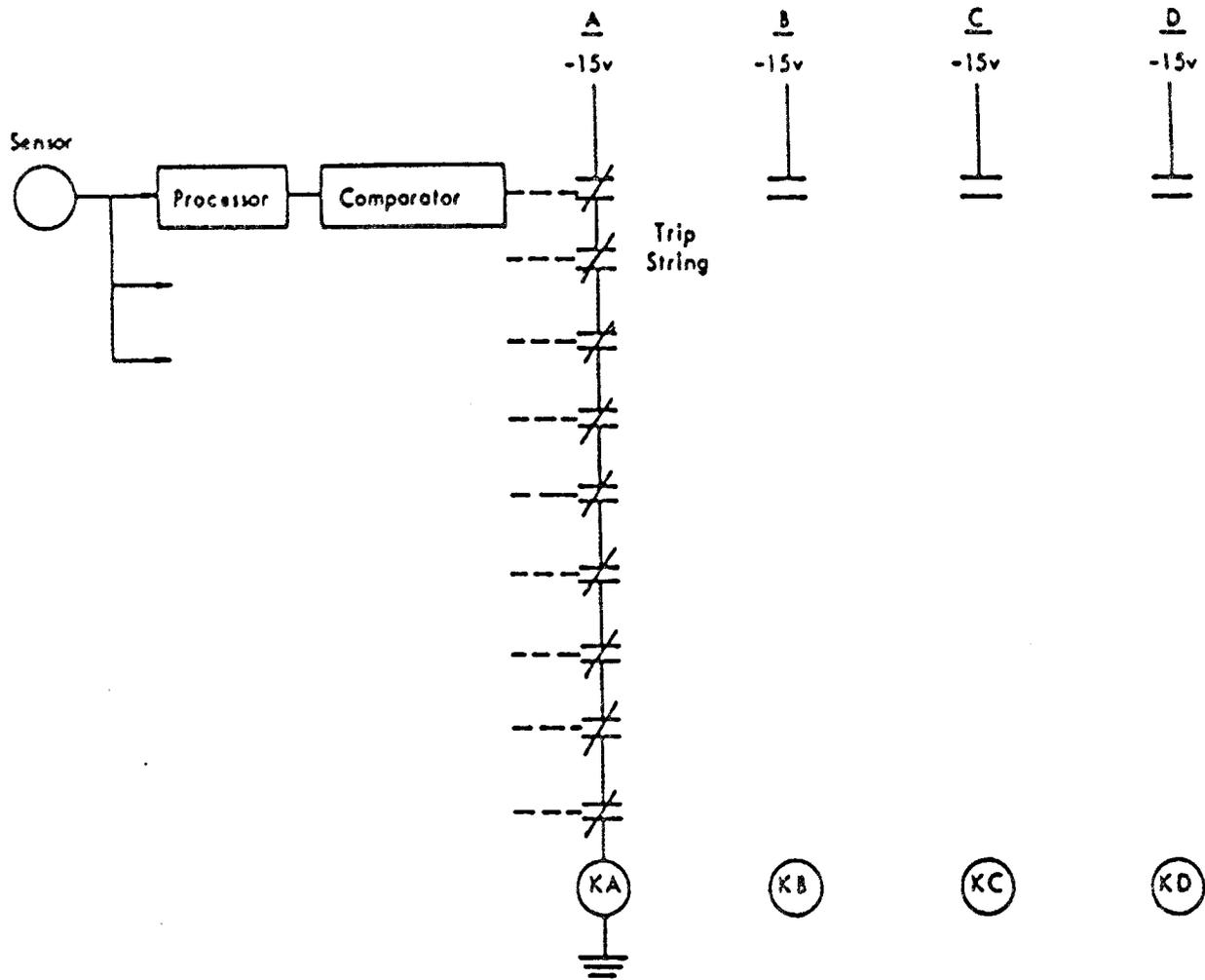


Figure 2.2 RPS Sensor Channels

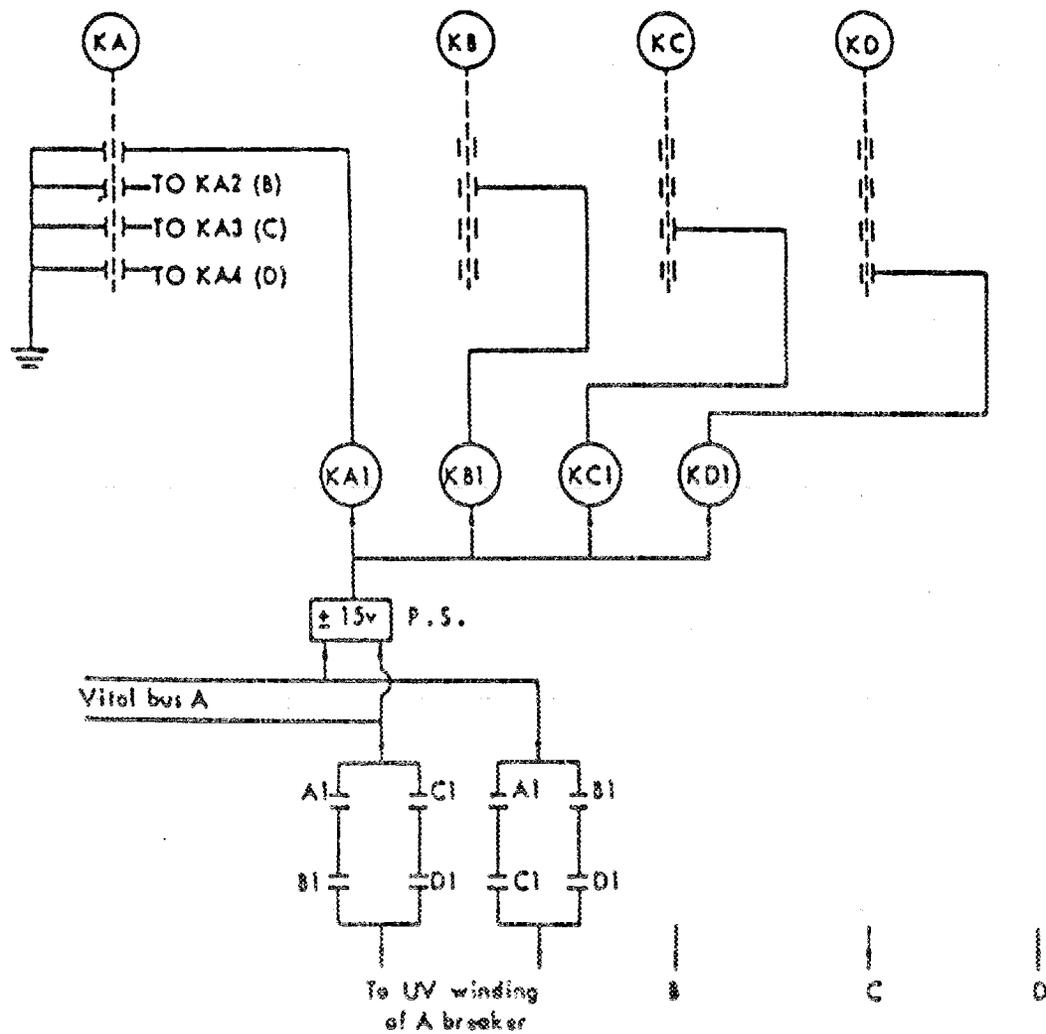


Figure 2.3 Two-out-of-four RPS Trip Logic

KA de-energizes KA1, KA2, KA3, and KA4). De-energizing the four auxiliary trip relays results in a shutdown vote from the channel, which is sent to all four reactor trip modules (Figure 2.1).

The reactor trip modules control circuit breakers on main and secondary power supply lines to the control rod assembly windings. Reactor trip modules A and B control ac scram circuit breakers A and B, respectively (Figure 2.1). Reactor trip module C controls the dual dc scram circuit breakers C1 and C2 and the dc control power scram relays E2, E3, and E4. Reactor trip module D controls a similar set of scram circuit breakers (D1 and D2) and scram relays (F2, F3, and F4).

One of the four 120V vital ac buses (one bus per channel) supplies control power to the undervoltage coil of the scram circuit breakers and scram relays just described through the controlling reactor trip module. Each reactor trip module contains a dual, two-out-of-four matrix of contacts with interrupt control power if any combination of two channels is tripped (Figure 2.3). The auxiliary trip relays control the breakers in the two-out-of-four matrix. Interruption of control power by any one reactor trip module causes the scram circuit breakers or scram relays controlled by that module to open (Figure 2.1). This action results in the interruption of power from one of two buses to the control rod assembly windings. Interruption of power from both buses to the control rod assembly windings is necessary for control rod assemblies to drop into the core.

The operator can also manually interrupt control power to the scram circuit breakers and scram relays. A manual trip switch is located between

each channel's reactor trip module and the undervoltage coil(s) that it controls. A pushbutton in the control room controls all four switches. Actuation of this pushbutton opens all four switches, interrupting control power to all scram circuit breakers and scram relays.

The control rod assemblies at ANO-1 are divided into eight groups: four groups of safety rods and four groups of regulating rods. However, one of the regulating rod groups is used for power shaping and is not inserted when the reactor trips. Table 2.2 lists the current number of rods in the other seven groups.

Each control rod drive assembly has six windings that receive six-phase power from both a main and a secondary bus (Figure 2.1). A delta/star transformer takes three-phase ac power, transforms it into six-phase power, and supplies it to the main and secondary buses through independent 480V ac lines (ac bus #1 and #2). The A circuit breaker interrupts power to the main bus, and the B circuit breaker interrupts power to the secondary bus. Loss of power on both of these buses de-energizes all control rod assembly windings.

The safety rods receive dc power inverted from the ac power of the main and secondary buses via the dual dc breakers (C1 and C2 or D1 and D2), respectively. The dual dc breakers provide a means of interrupting power from the main and secondary buses to the safety rods. The safety rods will drop only if main and secondary power to the safety rods is interrupted. The RPS interrupts power to the rods by opening an appropriate set of scram circuit breakers.

Table 2.2 ANO-1 Rod Group Compositions

| Rod Group | Category | Number of Rods |
|-----------|------------|----------------|
| 1 | Safety | 8 |
| 2 | Safety | 9 |
| 3 | Safety | 4 |
| 4 | Safety | 12 |
| 5 | Regulatory | 8 |
| 6 | Regulatory | 8 |
| 7 | Regulatory | 12 |

Each regulating rod group receives power from the main bus through 36 silicon-controlled rectifiers (6 rectifiers per phase) and power from the secondary bus through 36 parallel silicon-controlled rectifiers. The silicon-controlled rectifiers turn on and off the dc control rod holding power to regulate the rod positions. Only 12 or 18 rectifiers (2 or 3 phases) are on at any time. Gate drives regulate dc control power to the silicon-controlled rectifiers. Each gate drive (2 per regulating rod group) has 6 outputs and controls 36 rectifiers. The E and F scram relays interrupt dc control power to the gate drives and silicon-controlled rectifiers. Like the safety rods, regulating rods will drop only if power is interrupted from both the main and secondary buses.

The ANO-1 plant has roller nut-type control rod drive mechanisms. Each mechanism consists of a motor tube that houses a lead screw and its rotor assembly and an external motor stator that surrounds the motor tube. The motor stator magnetically rotates the rotor assembly, which in turn drives a non-rotating, translating lead screw coupled to a control rod assembly. When the motor stator is de-energized, mechanical springs disengage the roller nuts in the rotor assembly from the lead screw and allow the control rod assembly to drop into the reactor core.

2.1.2 Instrumentation and Controls

Annunciators indicate changes in RPS status to the control room operator. Specifically, these conditions are annunciated:

- reactor trip
- RPS trouble

- RPS shutdown bypass
- RPS channel bypass

Operators can get additional information on the status of each individual channel from the RPS cabinets (located in the control room).

Each channel has two key-operated bypass switches, a channel bypass switch, and a shutdown bypass switch. Operators use these switches to bypass a channel before performing control rod drive tests or channel trip circuitry tests. Interlocks between the channel key switches prevent bypassing two or more protection channels simultaneously.

The signal processing equipment, bistable trip string, and reactor trip module for any one channel are physically isolated from this same equipment for the other channels. The equipment for each channel is contained in two cabinets in the control room. In each of the two cabinets, there is a meter for every analog signal employed by the channel and a visual indication of the state of every logic element. A lamp mounted on top of one of the cabinets indicates the trip status of the channel.

Each CRDM motor stator has a high-temperature alarm, and the intermediate cooling water system (ICWS) that provides CRDM motor stator cooling has low-flow alarms.

2.1.3 Testing and Maintenance

ANO-1 personnel check all RPS channel indications twice during each shift. The surveillance check includes comparing the values of analog variables between channels and observing that equipment status is normal. In addition, each channel power level indicated by nuclear instrumentation is compared with a thermal power calculation.

Plant personnel test each RPS channel monthly. (A different channel is tested each week.) They verify that each portion of the channel trip logic--from the signal processors to the scram breakers--operates properly. A complete test on a channel takes about four hours, during which time the RPS channel is bypassed and the system is in a condition where two out of three channels must trip to cause a scram. Two or more channels are never simultaneously bypassed for testing and maintenance since this would violate administrative control, and interlocks prevent bypassing more than one channel.

Maintenance on an RPS channel, if necessary, is performed during monthly testing or during shutdown. Unless a channel is bypassed, a system of interlocks initiates a channel trip whenever a reactor trip module is removed from the RPS.

2.1.4 Interfacing Systems

The electric power system (EPS) and the intermediate cooling water system (ICWS) interface directly with the scram system. The EPS supplies 120V ac power to the RPS via four vital 120V buses: one bus for each channel. Each vital ac bus supplies power to the channel's 15V dc instrumentation power supply and to the undervoltage windings of the scram breaker(s) and scram relays associated with the channel. Loss of power on any vital ac bus trips the associated channel. Power surges on any vital ac bus or dc power supply may result in one or more channels failing unsafe by welding relay contacts closed.

The ICWS provides cooling water to the CRDM motor stators. Loss of cooling water causes the CRDM motor stators to overheat. Overheating can cause mechanical failure of the CRDMs, which can result in the coupled control rod assemblies not inserting when commanded.

2.2 Failure Descriptions

2.2.1 TOP Event Definition

The TOP event (system failure of interest) analyzed in this study was "Scram System Fails to Achieve a Satisfactory Reactor Shutdown When Required." The scram system consists of eight groups of control rods, seven of which comprise the emergency portion of the system. The TOP event occurs whenever at least one complete emergency control rod group and one other emergency control rod assembly fail to insert into the reactor core when required (based on the ANO-1 IREP success criterion for the RPS). Control rod assemblies can fail to insert because of scram breaker/relay failures, relay failures in the RPS logic, failures in the trip parameter signal processing equipment, mechanical failures in the CRDMs, or combinations of failures of this equipment.

2.2.2 Scram System Equipment Failure Modes

The scram system at ANO-1 consists of the following types of equipment: scram breakers, scram relays, control relays, logic modules, bistable trip strings, trip parameter instrumentation, gate drives, silicon-controlled rectifiers, control rods, and control rod drive mechanisms. This section describes each of these types of equipment and their failure modes of interest for this analysis.

Scram Breakers/Relays

The RPS has two types of scram circuit breakers: ac breakers (breakers A and B, Figure 2.1) and dual dc breakers (breakers C1 and C2 and D1 and D2, Figure 2.1). The RPS also has six dc scram relays to interrupt control power to the gate drives. These breakers/relays consist of a contact set and a normally energized, solenoid-type device that holds the contacts closed. The breakers/relays are spring-loaded to open when de-energized. Failure of a scram breaker/relay occurs whenever the solenoid coil is de-energized and the contacts remain closed.

Control Relays

The RPS uses control relays to transmit shutdown votes from the bistable trip strings to the reactor trip modules. The relays are solenoid-type devices that control the contact sets in the reactor trip modules; they vote for shutdown by transferring open. The control relays are normally energized closed and are spring-loaded to open when de-energized. A control relay failure occurs whenever a relay fails to open when the solenoid is de-energized.

Logic Modules

Each trip logic module for the RPS consists of a dual, two-out-of-four matrix of normally closed contacts (Figure 2.3). Failure of a reactor trip logic module occurs whenever three of the four contacts in both matrices of contacts stick closed.

Bistable Trip Strings

Each bistable trip string consists of 10 trip relays (controlled by trip parameter signals) and 1 channel relay. All 11 relays are of the same design and operate like the scram relays. Failure of a bistable trip string occurs whenever all bistable trip relays that should trip (given an upset condition) stick closed or when the one channel trip relay sticks closed.

Trip Parameter Instrumentation

The trip parameter instrumentation for the RPS consists of sensors, signal conditioning electronics, and signal comparators. Signals from RPS sensors monitoring seven conditions in the nuclear steam supply system--or combinations of these signals--open the bistable trip relays. Failure of trip parameter instrumentation occurs if the signal comparator set point for the trip parameter is out of tolerance or if the signal(s) feeding the signal comparator is incorrectly high or low (depending on the trip parameter). Incorrect high or low signals result from sensors and signal conditioning electronics (detector power supplies, amplifiers, function generators, contact monitors, bridge networks, and signal converters) failing high or low.

Many of the sensors in the RPS send signals to more than one bistable trip relay. The sensors and their associated signal processing equipment that feed more than one bistable trip relay may cause one bistable trip relay to fail in an unsafe mode (closed) and another bistable trip relay to fail in a safe mode (open). For example, the reactor coolant pressure sensor feeds the bistable trip relays for both high and low reactor coolant

pressure. Thus, the pressure sensor failing high results in failure of the trip parameter instrumentation for low reactor coolant pressure, but it also trips the reactor via the bistable trip relay for reactor coolant high pressure. Trip parameter instrumentation failures that cause any bistable trip relay to fail in a safe mode were neglected in this analysis.

Gate Drives

The RPS gate drives distribute dc control power to the silicon-controlled rectifiers. Each gate drive has six output legs, and each output leg controls six silicon-controlled rectifiers. Failure of a gate drive occurs if any output leg transmits an "on" signal to the silicon-controlled rectifiers when all output legs should transmit "off" signals.

Silicon-controlled Rectifiers

The silicon-controlled rectifiers transform ac power to dc power to drive the CRDMs of the regulating rod group assemblies. Failure of the silicon-controlled rectifiers for a regulating rod group occurs if any rectifier supplies power when all rectifiers should be off. This type of failure would result in the energized CRDMs holding a regulating rod group out of the reactor core.

CRDMs/Control Rods

A CRDM provides for controlled withdrawal and insertion of a control rod assembly into the reactor core. The control rods (16 rods in each control rod assembly) contain neutron absorber material and are used to control reactor power. A mechanical fault in a CRDM (or in the control rods) that prevents the control rod assembly from dropping into the reactor core constitutes a failure of the component(s).

2.3 Transient Initiating Events

A transient initiating event is an upset condition in the nuclear steam supply system that requires protective action by the scram system and/or other safety systems. Transient initiating events are important because they can cause reactor core meltdowns if the scram system or other safety systems fail.

There are several important anticipated transient initiating events for pressurized water reactors.³ However, the transient initiating events that isolate the reactor from normal cooling systems are most important to this study because, if not controlled, they can result in a large pressure rise in the reactor that could disable the emergency cooling systems and threaten the integrity of the reactor coolant system pressure boundary. These transient initiating events have the greatest likelihood of occurrence and the most severe potential consequences should the scram system fail.

This study analyzed the reliability of the reactor protection system under the condition that either a turbine trip or loss of main feedwater transient initiating event has occurred. These events are the most frequent transient initiating events for pressurized water reactors.³ Either of these transient initiating events can result in loss of normal cooling to the reactor core.

A turbine trip transient initiating event initially affects the following RPS trip parameters:

- high reactor coolant temperature
- high reactor coolant pressure
- anticipatory turbine trip

And a loss of main feedwater transient initiating event initially affects these trip parameters:

- high reactor coolant temperature
- high reactor coolant pressure
- anticipatory feedwater pump trip

For this study, we assumed that if either a turbine trip or loss of main feedwater transient initiating event occurs, no other RPS trip parameters will be affected soon enough to effect a reactor scram prior to the reactor coolant system overpressurizing.

3. QUALITATIVE ANALYSIS

The qualitative analysis of the ANO-1 scram system involved three steps:

1. fault tree modeling
2. minimal cut set determination
3. common cause candidate identification

The qualitative analysis identified minimal cut sets for hardware failures, and it provided lists of common cause candidates for the TOP event, "Scram System Fails to Achieve a Satisfactory Reactor Shutdown When Required." This information provides insight into how the scram system can fail, and the minimal cut sets and common cause candidates were used as input to the subsequent quantitative analysis. We used the COMCAN III computer program⁴ to perform both the qualitative and quantitative analyses of the scram system fault tree.

3.1 Fault Tree Modeling

A fault tree was used to model the failure logic for the scram system TOP event. Scram system failure can result from an appropriate combination of scram breaker and scram relay failures, from mechanical failures of the control rods or CRDMs, or from a combination of breaker/relay and control rod failures. Figure 3.1 illustrates the top level fault events that can cause scram system failures.

Appendix A is a detailed fault tree of the ANO-1 scram system. This fault tree was developed using the same methodology that was used in the WASH-1400 (Ref. 5) and the ANO-1 IREP studies.⁶ However, it contains

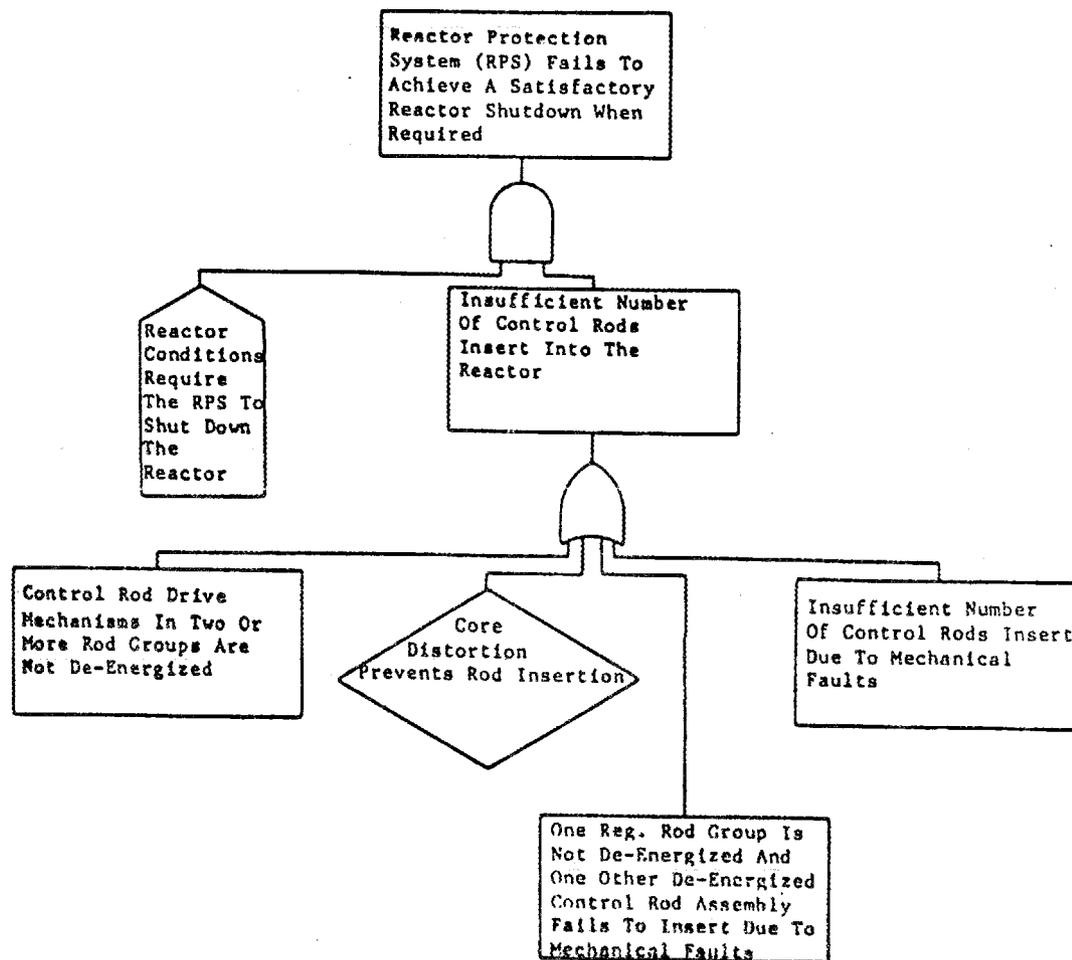


Figure 3.1 ANO-1 Scram System Fault Tree Top

significantly more detail than the ANO-1 IREP fault tree. Component failures have been expanded and new events have also been added to the fault tree. For example, the fault tree in Appendix A includes a logical development of failures of the reactor trip modules (Figure 2.1) and combinations of control rod and scram breaker failures that can contribute to scram system failures.

The extensive modeling of the scram system in Appendix A provided the level of detail needed for performing a thorough independent failure analysis and a thorough common cause failure analysis. However, this detailed fault tree has nearly 10^{32} cut sets and is too large to efficiently process using COMCAN III. Thus, the detailed fault tree required modifications to reduce the number of possible cut sets to be considered in the CCFA. These modifications included streamlining the logic in sections of the fault tree and replacing several sections of fault tree logic with single basic events. Carrying out these modifications required extreme care to ensure no lost information for the common cause failure analysis.

Appendix B is the reduced fault tree of the ANO-1 scram system. This tree reflects the following modifications:

1. Failure of each channel's trip parameter instrumentation (represented in the detailed fault tree by an AND gate with 10 possible inputs) is represented by a single basic event.
2. Multiple basic events input to OR gates are consolidated into single basic events.
3. We assumed that operators would not manually trip the control relays to the SCRs.

4. The two-out-of-three failure logic for the regulating rod group power supplies (E and F scram relays, gate drives, and silicon-controlled rectifiers) is streamlined.

As a result of Modification 1, we modeled only those trip parameter failures that are appropriate for the transient initiating event under consideration. For example, when a loss of main feedwater initiating event was analyzed, a single basic event in the reduced fault tree represents failure of the high reactor coolant temperature, high reactor coolant pressure, and main feedwater pump trip parameter instrumentation. Similarly, Modification 2 combined several basic events whose components are located in the same room into a single, consolidated basic event.

All four modifications resulted in no loss of information for either the qualitative CCFA or the quantitative analysis (independent failures and common cause failures), and they substantially reduced the number of cut sets to be analyzed (to less than 10^5).

3.2 Minimal Cut Set Determination

From the reduced fault tree, the COMCAN III computer program identified 2265 minimal cut sets for the ANO-1 scram system TOP event. The minimal cut sets ranged in size from two-event cut sets to six-event cut sets. All two-event minimal cut sets involve combinations of scram breaker/relay failures. About half of the three-event minimal cut sets contain scram breaker/relay failures. The other three-event minimal cut sets and the higher-order minimal cut sets contain combinations of scram relay, power supply (SCR), cable, and CRDM failures.

Since these minimal cut sets were obtained from the reduced fault tree, the basic events in many of the cut sets represent multiple component failures. These consolidated basic events and the minimal cut sets can be expanded to reflect specific component failures if desired. But expansion will increase the number of minimal cut sets of each order (e.g., 1 two-event cut set could become 10 two-event cut sets). Expanding the cut sets gives no additional common cause failure information; therefore, the cut sets were not expanded for this analysis.

3.3 Common Cause Candidate Identification

A common cause failure analysis identifies single causes, or events, that can produce multiple component failures that can subsequently result in system failure. In highly redundant systems, such as nuclear power plant scram systems, common cause failures are often significant contributors to the system's failure probability.

We used a modified generic cause approach^{2,7-10} and the COMCAN III computer program⁴ to perform the common cause failure analysis of the ANO-1 scram system. Based on this approach, a minimal cut set for the scram system TOP event must meet one of the following criteria to be considered a common cause candidate:

1. All members of the minimal cut set must be susceptible to the same generic type of environment and must be in a common location with respect to that environment (e.g., the scram breakers are all susceptible to vibration and are all located in the computer room).
2. All members of the minimal cut set must have a common link (i.e., a condition associated with the components such as component manufacturer, the

maintenance crew charged with component upkeep, or the procedures used for component maintenance that can transgress physical barriers).

Common cause candidates according to the first criterion are location-dependent, and common cause candidates according to the second criterion are location-independent. The COMCAN III computer program identified common cause candidates according to each of the above criteria.*

Identifying common cause failures for the qualitative analysis of the ANO-1 scram system involved the following three steps:

1. collecting and preparing the data to be input to COMCAN III
2. identifying common cause failures using COMCAN III
3. identifying root cause events

3.3.1 Input Data for COMCAN III

In addition to the fault tree, COMCAN III required input data on component physical locations, component susceptibilities to generic types of environments, plant barriers to generic types of environments, and other factors that can link components. The component physical locations, the component susceptibilities, the plant barriers, and the fault tree are the data needed by COMCAN III for identifying common cause candidates by the

*The COMCAN III computer program identified approximately 30 common cause candidates for the ANO-1 scram system. In the interest of maintaining a tractable analysis, we did not attempt to identify partial common cause candidates.

first criterion (location-dependent). The fault tree and common links for components are the data needed by COMCAN III for identifying common cause candidates by the second criterion (location-independent). The remainder of Section 3.3.1 discusses the data required by COMCAN III in more detail.

Component Locations

ANO-1 scram system components are located in the computer room, the control room, the penetration rooms, and the reactor building. Table C.2, Appendix C, lists each reduced fault tree basic event and the location of the component that is defined by the basic event.

Component Susceptibilities

Component susceptibilities (for this study) are generic types of environments that can cause components to fail. The following aided our identification of generic types of environments that can fail scram system components:

1. a review of several hundred licensee event reports (LERs) on scram system failures
2. a literature review of common cause failure analysis methods
3. discussions with ANO-1 personnel

When multiple component failures were consolidated into single basic events to reduce the complexity of the fault tree, the new single basic event assumed all the susceptibilities of the multiple component failures that it represents if the consolidation was through an OR gate. If the consolidation was through an AND gate, the new basic event assumed only the

susceptibilities shared by all of the component failures that the basic event represents. Appendix D lists each basic event that appears in the reduced fault tree and the secondary failure susceptibilities for the basic event.

Plant Barriers

A plant barrier is a physical obstruction or separation that confines the effects of a generic environment within the boundaries established by the barrier. Plant barriers define the domains of the generic environments. In this analysis, the walls of rooms in the ANO-1 plant act as barriers to most generic environments. Only the exterior door of the computer room is not a barrier to impact and corrosion generic environments; all other doors and walls are barriers to these two generic environments. With one exception, walls are also barriers to plant internal vibration events. (The floor separating the computer room from the control room is not a barrier to plant internal vibration events.) There are, however, no barriers anywhere in the plant to external vibration events (earthquakes). Figure 3.2 identifies the plant barriers defined for this study. (One barrier is not shown in Figure 3.2: a fire wall in the computer room between the ac and dc scram breakers.)

Common Links

The terms "common links" and "special conditions" are used interchangeably throughout the remainder of this report; they refer to any factors that closely link components so the combined probability of the component failures is greater than the product of the independent component

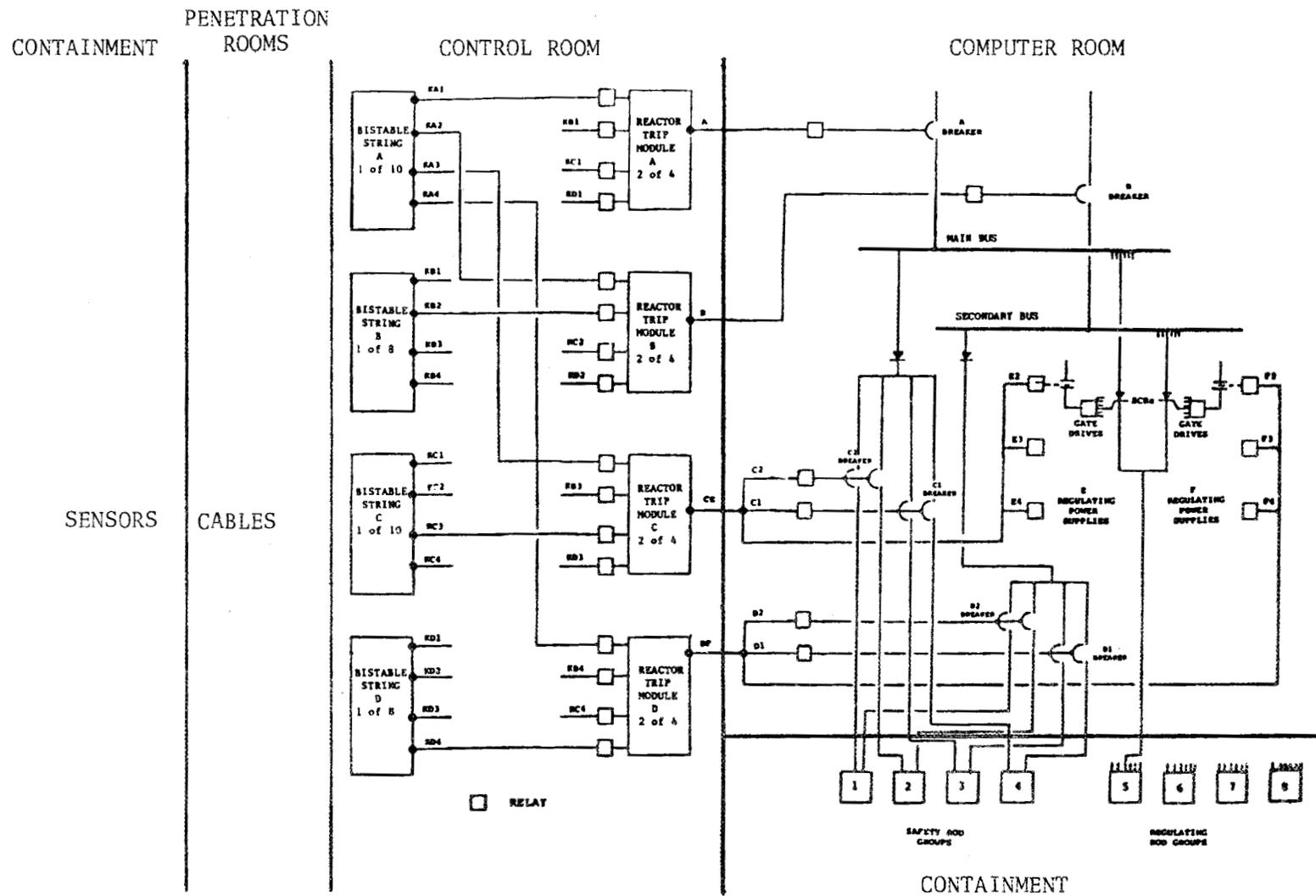


Figure 3.2 ANO-1 Barriers to Generic Types of Environments

failure probabilities. Three common links and special conditions were defined for this study:

1. common power supply
2. common cooling water supply
3. similar parts

If all components in a minimal cut set have a common link or special condition,^{10,11} the minimal cut set is identified as a common cause candidate. Physical barriers between components do not eliminate common links and special conditions; therefore, common links and special conditions define common cause candidates that are location-independent.

The rules for evaluating common links and special conditions when consolidating multiple component failures into single basic events are the same as the rules for evaluating generic susceptibilities. Appendix D lists the common links, or special conditions, for each basic event that appears in the reduced fault tree of the ANO-1 scram system.

3.3.2 Identification of Common Cause Failures

COMCAN III used the following procedure to identify common cause candidates for the ANO-1 scram system analysis:

1. It selected a generic environment/location or a common link for analysis.
2. It identified the basic events in the fault tree that are in the selected location and are susceptible to the generic environment or that have the common link (or special condition). These basic events were treated as failed and all other basic events were treated as not failed.

3. It determined the minimal cut sets. These cut sets are common cause candidates for the specified generic environment/location or common link.

This procedure was repeated until every generic environment/location and common link was analyzed.

3.3.3 Identification of Root Cause Events

The final step in the qualitative CCFA was identifying root cause events. A root cause event is a specific mechanism defining the origin of a generic environment or common link that produces a common cause failure. For example, a root cause event that could lead to a high-temperature environment in a room could be the failure of the room's air conditioner.

A number of different root cause events can produce the same generic environment in a particular location or affect the scram system through the same common link. For example, either turbine imbalance or diesel generator vibration can cause vibration in the control room and the computer room. All root cause events that produce the same generic environment in the same location have the same effect on the scram system. Similarly, all root cause events that affect the system through the same common link have the same effect on the system.

Our common cause failure analysis was streamlined by considering types of root cause events that affect the scram system before we identified and analyzed more specific root cause events. (That is, we considered all events that could cause vibration in the control room as one type of root cause event for analysis.) No time was wasted analyzing root cause events that had no potential to cause scram system failures.

This study investigated potential root cause events associated with ANO-1 scram system failures for both generic environments and common links. We identified potential root cause events by (1) performing walk-throughs of the containment penetration rooms, the computer room, and the control room; (2) inventorying equipment and personnel in each of these areas; and (3) determining whether equipment failures and personnel errors in these areas could produce the generic environment(s) of interest. Equipment failures and personnel errors that could produce the generic environment(s) of concern were listed as root cause events. LER reviews, the plant visit, and discussion with ANO-1 personnel helped determine the potential root cause events that should be considered in the detailed reliability analysis of the scram system.

3.4 Qualitative CCFA Results

The scram system common cause failure analysis identified common cause candidates for 17 generic environment/location combinations and 12 common links (4 of which are similar parts). All common cause candidates contain consolidated basic events that could have been expanded to provide more detail on specific component failures. Expanding the common cause candidates was not necessary for performing the quantitative CCFA; therefore, the candidates were not expanded.

Tables 3.1, 3.2, and 3.3 list the generic environment/location combinations, common links, and similar parts that produce the common cause candidates, and the tables also identify potential root cause events for each of these event types. Most of the root cause events in these tables are ANO-1 plant-specific.

Table 3.1 CCFA Qualitative Results - Generic Environments

| Generic Environment/Locations | Potential Root Cause Events ^a |
|------------------------------------------|-------------------------------------------|
| Fire/control room | Instrumentation overheats |
| Grit/computer room | ABS filters fail, construction activities |
| Grit/control room | Construction activities |
| Grit/containment | ----- |
| Moisture/computer room | A/C fails, roof leaks |
| Moisture/control room | ----- |
| Vibration/computer room and control room | Diesel generators, turbine imbalance |
| Vibration/containment | ----- |
| Vibration/whole plant | Earthquake |
| Temperature/computer room | A/C fails, transformers overheat |
| Temperature/control room | ----- |
| Corrosion/computer room | Hydrazine drums leak |
| Corrosion/control room | ----- |
| Corrosion/containment | ----- |
| Impact/computer room | ----- |
| Impact/control room | ----- |
| Impact/containment | ----- |

^aA dashed line indicates that no likely potential root cause events(s) for the associated generic environment/location was identified during our search for these events. The quantitative common cause failure analysis results in Section 4 of this report reflect no contributions of these generic environment/location combinations to scram system failure frequencies.

Table 3.2 CCFA Qualitative Results - Common Links

| Common Link | Potential Root Cause Events |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Cooling water | ICWS pump failure |
| ac bus #1 | Power surge |
| ac bus #2 | Power surge |
| dc bus #1, Channel A vital ac bus AA, and Channel C vital ac bus AC | Power surge |
| dc bus #2, Channel B vital ac bus AB, and Channel D vital ac bus AD | Power surge |
| ac bus #1, dc bus #1, Channel A vital ac bus AA, Channel C vital ac bus AC, Channel A 15V dc power supply, and Channel C 15V dc power supply | Power surge |
| ac bus #2, dc bus #2, Channel B vital ac bus AB, Channel D vital ac bus AD, Channel B 15V dc power supply, and Channel D 15V dc power supply | Power surge |
| All 15V dc power supplies | Power surge |

Table 3.3 CCFA Qualitative Results - Similar Parts

| Similar Parts | Potential Root Cause Events |
|----------------|---------------------------------------------------------------------------------|
| ac/dc breakers | Design error Installation error Maintenance error Manufacturing defect |
| ac/dc relays | Design error Installation error Maintenance error Manufacturing defect |
| CRDMs | Design error Installation error Manufacturing defect |
| Cables | Design error Installation error Manufacturing defect |

Table 3.1 lists the potential root cause events for generic environments. A dashed line in this table for a particular generic environment/location indicates one of two things: (1) no root cause event was identified for the environment/location or (2) the root cause event(s) identified was considered extremely unlikely. For example, we did not identify any high-speed equipment, high-pressure piping, or explosive materials in the computer room or control room that could produce an impact environment. Thus, we listed no potential root cause events for impact environments for these rooms. We also listed no potential root cause events that could lead to high-temperature environments in the control room. The control room has four independent air conditioning systems, and we considered failure of all these systems extremely unlikely. As indicated in the footnote to Table 3.1, generic environment/locations with no potential root cause events or with unlikely root cause events were not considered in the quantitative CCFA described in the next section of this report.

Table 3.2 lists the common links considered in this analysis that are not similar part common links. Most of these common links are power supplies. This study investigated combinations of power supply failures when the power supplies were tied to each other. For example, a surge on dc bus D1 would affect vital ac buses AA and AC. However, a surge affecting the scram system would require failure of one or more overcurrent protection devices (an unlikely event). For this reason, we did not consider power surges in our quantitative CCFA. A loss of cooling water to the CRDMs was also not included in the quantitative CCFA. A loss of

cooling water would be immediately announced by several alarms. We considered it very unlikely for this type of failure to go undetected (and uncorrected) by operators until after a scram system failure had occurred.

Table 3.3 lists the similar part common links identified in the qualitative CCFA and the root cause events that could be responsible for their failures. Of the root cause events listed for breakers/relays, we consider maintenance errors the most likely contributors to multiple, similar part failures. Past nuclear power plant operating experience with scram breakers/relays supports this observation. The other root cause events listed--design, installation, and manufacturing errors--are less likely contributors to multiple, similar part failures of breakers and relays because these types of errors should be identified and corrected during pre-operational testing or early plant operation. However, similar part failures listed in Table 3.3 can produce common cause failures and are considered in the quantitative analysis.

4. QUANTITATIVE ANALYSIS

The frequency of ATWS is the frequency of transients that produce conditions requiring reactor trip multiplied by the probability of failure to scram (given a transient has occurred). This section describes the procedure for estimating the probability of failure to scram, given a transient. This probability is the time-averaged unavailability of the scram system and it includes contributions from independent failures and from common cause failures.

4.1 Independent Failure Quantification

We used the same approach to quantify the independent hardware contribution to scram system unavailability that was used in the ANO-1 IREP study.⁶ Components that are not periodically tested at ANO-1 were assigned unavailabilities that are average probabilities of failure per demand (constants). Components whose safety functions are periodically tested were assumed to be working immediately after a test and to fail at a specified rate between tests. Failures are not announced until the next test. The test interval is short enough in all cases that a component's unavailability increases linearly with time, and its average unavailability is equal to the component's failure rate times one-half of its test interval.

All ANO-1 periodically tested components are tested once a month, and each of the four channels is out of service for testing and maintenance an average of four hours each month. The channel tests were assumed evenly staggered so the average unavailability of a minimal cut set containing failure of more than one periodically tested component is less than the

product of the average unavailabilities of the components in the cut set. This study approximated the average unavailability of each minimal cut set with the product of the average unavailabilities of the basic events in the cut set.

Failure data (taken from WASH-1400) that were applicable for calculating the independent failure probability of each basic event in the reduced ANO-1 scram system fault tree are presented in Table C.1 of Appendix C. Our average unavailability estimate for the scram system due to independent failures of components is 4.1×10^{-6} . This is approximately equal to the unavailability presented in the ANO-1 IREP study for the scram system. Thus, the detailed fault tree developed for this study produced results that are consistent with the ANO-1 IREP calculations of the average unavailability of the scram system due to independent hardware failures.

Combinations of CRDM mechanical failures, combinations of RPS electrical equipment failures, and combinations of CRDM mechanical failures and RPS electrical failures are responsible for the independent failure contributions to scram system unavailability (Figure 3.1). The estimated contributions to the average unavailability from these three groups are 5.7×10^{-19} , 4.06×10^{-6} , and 4.2×10^{-8} , respectively. About 99% of the scram system independent failure probability is a result of RPS electrical component failures (in particular, scram breaker failures).

Table 4.1 lists the scram system components whose independent failures are important contributors to scram system unavailability. This table includes only components with importances greater than 0.1. A component's unavailability importance is the probability that independent failure of the component contributes to scram system unavailability, given the scram

Table 4.1 Unavailability Importance of Components in the Scram System - Independent Failures

| Component | Importance ^a |
|-----------------------------|-------------------------|
| RPBACPSC - scram breaker A | .499 |
| RPBBCPSC - scram breaker B | .499 |
| RPBRC1SC - scram breaker C1 | .246 |
| RPBRC2SC - scram breaker C2 | .246 |
| RPBRD1SC - scram breaker D1 | .246 |
| RPBRD2SC - scram breaker D2 | .246 |

^aComponent importance is defined as the probability that a component contributes to scram system unavailability, given the scram system is unavailable due to independent failures.

system is unavailable due to independent failures. As indicated in the table, the most important components in the ANO-1 scram system are the A and B scram breakers. The four scram breakers used to interrupt dc power to the CRDMs are next in importance. These six components, individually or in combinations, appear in about half of the three-event minimal cut sets and in all of the two-event minimal cut sets identified for this analysis. They also have high unavailabilities (10^{-3} /breaker) relative to other scram system components.

A sensitivity study on the ac and dc scram breaker unavailabilities determined that the scram system unavailability is almost directly proportional to the percent change in the breaker unavailabilities squared. For example, a 5% increase in breaker unavailability changes in the scram system unavailability to approximately $4.5 \times 10^{-6} [(1.05)^2 \cdot (4.1 \times 10^{-6})]$. This proportionality is due to the 4 two-event minimal cut sets, all of which are composed of scram breaker failures; these cut sets contribute almost 98% to the total scram unavailability.

4.2 Common Cause Failure Quantification

The average unavailability of the ANO-1 scram system due solely to common cause failures was estimated using the following equation:

$$\bar{A}_T = \sum_{I=1}^N (\Lambda_I)(T_I)[P(F|I)] \quad (4.1)$$

where

Λ_I = the failure rate applicable to root cause event type I,

T_I = the average fault exposure time (the average time period between scram system failure and failure detection and correction) for scram system failure resulting from root cause event type I,

$P(F|I)$ = the conditional probability of scram system failure, given root cause event type I

N = the number of root cause event types of interest.

Each type of root cause event with the potential to cause a scram system failure makes a contribution to the system's failure rate that is equal to the product of the root cause event type failure rate (Λ_I) and the appropriate conditional probability of scram system failure, given the occurrence of that type of root cause event $P(F|I)$. This product, $\Lambda_I \cdot P(F|I)$, times the appropriate scram system fault exposure time (T_I) is the time-averaged unavailability of the scram system due to the occurrence of root cause event type I.

For this study, generic environments resulting from the root cause events were defined to be severe enough to cause failures of all scram system equipment in the location of the root cause event. However, the design of the electrical portion of the scram system is such that, if equipment does fail as a result of a root cause event, it is more likely to fail safe than to fail unsafe. Safe failures contribute to inadvertent scrams. Unsafe failures contribute to failure to scram when a scram is required. Thus, $P(F|I)$ is not necessarily 1.0 even for root cause events that produce common cause candidates. The following section describes the methods used to estimate $P(F|I)$. Sections 4.2.2 and 4.2.3 describe the methods used to estimate T_I and Λ_I .

4.2.1 Conditional Failure Probabilities

The conditional probability of a basic event occurrence is the probability the component defined by the basic event fails in the unsafe mode, given the occurrence of an applicable root cause event. No directly applicable data were available to estimate conditional probabilities for the basic events identified for this analysis. Therefore, we used the following procedure to estimate conditional failure probabilities:

1. The WASH-1400 failure probabilities (or failure rates) for all failure modes of a component type (e.g., relays or cables) were summed. This sum is an estimate of the probability (or failure rate) the component type enters a failed state (unsafe failures and safe failures).
2. The probability (or failure rate) a component type will fail in one specific unsafe mode was then divided by the probability the component type enters a failed state. This fraction is the initial estimate of the conditional failure probability for a basic event, given the occurrence of any type root cause event.

In some cases, conditional failure probability estimates were adjusted based on engineering judgment. Adjustments were made in the absence of supporting data. Appendix D presents the conditional failure probability estimate for each basic event, for each type of root cause event, considered in the ANO-1 analysis. Appendix E provides an example that illustrates the procedure for estimating these conditional failure probabilities.

All of the common cause candidates associated with a particular type of root cause event were used as input to the quantitative analysis routine in

COMCAN III. The basic event probabilities used for each calculation were the appropriate conditional failure probabilities. The result of each calculation was an estimate--for a root cause event type--of the conditional probability of failure to scram, given a particular type of root cause event $P(F|I)$. This procedure was repeated for each root cause event type. Tables 4.2 and 4.3 present the results of these calculations.

As indicated in Section 3.4 of this report, several common cause candidates were excluded from the quantitative analysis because there were no likely potential root cause events identified for them. For this reason, Tables 4.2 and 4.3 do not include conditional scram system failure probability estimates for nine generic environments/locations identified in the qualitative CCFA or for eight common links identified in the qualitative CCFA. The excluded generic environments are as follows: moisture, temperature, corrosion, and impact generic environments in the control room; impact generic environments in the computer room; and grit, vibration, corrosion, and impact generic environments in containment. Cooling water failures of the CRDMs and power surges of the ac and dc power supplies account for the eight common links included in the qualitative analysis but excluded from the quantitative analysis.

There are several reasons why the nine generic environments were not quantitatively analyzed. Harsh temperature and moisture environments were considered unlikely for the control room because the room has four independent air conditioners. Corrosion and impact environments for this room were not quantitatively analyzed because no root cause events were identified for this environment/location.

Table 4.2 Scram System Conditional Failure Probabilities - Generic Environments

| Generic Environment/Location | P(F I) ^a |
|------------------------------------------|------------------------|
| Fire/control room | 1.0 x 10 ⁻² |
| Grit/computer room | 1.0 |
| Grit/control room | 1.0 |
| Moisture/computer room | 4.6 x 10 ⁻² |
| Vibration/computer room and control room | .11 |
| Temperature/computer room | 7.5 x 10 ⁻² |
| Corrosion/computer room | .74 |
| Vibration/whole plant | .93 |

^aCOMCAN III calculated these scram system P(F|I)s using estimated failure data for the basic events that were based primarily on engineering judgment. (See Appendices D and E.)

Table 4.3 Scram System Conditional Failure Probabilities - Common Links

| Common Link | P(F I) ^a |
|--------------------------------|---------------------|
| Similar parts - ac/dc breakers | 1.0 |
| Similar parts - ac/dc relays | 1.0 |
| Similar parts - CRDMs | 1.0 |
| Similar parts - cables | 1.0 |

^aThese scram system P(F I)s were calculated using estimated failure data for the basic events that were based primarily on engineering judgment.

We did not estimate a scram system failure probability for impact root cause events in the computer room because we identified no potential root causes for this generic environment in the computer room.

For the containment building, we identified several potential root cause events for grit, vibration, corrosion, and impact generic environments. However, we did not quantitatively analyze these types of generic environments because the root cause events were not considered likely to affect the capability of the scram system to shut down when required. Failures of scram system equipment in containment (CRDMs and sensors) are announced; thus, operators should correct these failures (or shut down the reactor) before scram system failure occurs. Furthermore, the scram system equipment in containment is environmentally qualified, which reduces the likelihood of failure under harsh environment conditions. Also, the amount of redundancy and spatial dispersion of scram system equipment in containment reduce the likelihood of a generic-environment-caused system failure in containment.

Cooling water common links that affect the CRDMs were not quantitatively analyzed because failures in the cooling water system are immediately announced. Loss of cooling water to the CRDMs is announced via low-flow alarms on the intermediate cooling water system and via high-temperature alarms on the CRDM stators. Thus, operators should correct a loss of cooling water situation before this common link could cause CRDM failures.

The other common links excluded from the quantitative analysis, power surges, were not analyzed in detail since there are many devices in the electrical circuitry that protect scram system equipment (relays, breakers,

and logic circuits) from the effects of a power surge. A power surge will cause these protective devices (fuses, crowbars, circuit breakers, and protective relays) to trip open, which in turn will cause a reactor scram.

Based on estimated basic event failure data, the probability estimates of scram system failure--given a root cause event--range from 10^{-4} to 1.0, depending on the type of root cause event. (See Tables 4.2 and 4.3.) For most root cause event types, the conditional probability of scram system failure is greater than 0.5.

The system conditional failure probabilities in these tables are high for two reasons. First, the root cause event, by definition, is severe enough to cause component failures. Secondly, the estimated conditional probabilities of scram system component failures in the unsafe mode, given a root cause event, are relatively large.

The scram system conditional failure probabilities listed in Tables 4.2 and 4.3 contain large uncertainties. Two reasons for uncertainties in these estimates are:

1. The component conditional probabilities of failure used to calculate $P(F|I)$ are estimates.
2. The scram system fault tree may not include all contributors to scram system failure (i.e., we cannot guarantee the fault tree models all mechanisms of scram system failure).

Uncertainties in the components' conditional failure probabilities are large since the conditional failure probabilities are based mainly on engineering judgment. No hard data were available in the literature for

estimating the component conditional failure probabilities. Other sources of uncertainty may also exist.

Component Importance

Tables 4.4 and 4.5 list the more important components identified in the common cause failure analysis for each type of root cause event. Component importance for common cause failures is defined as the probability that a component contributes to scram system unavailability, given the scram system is unavailable due to the occurrence of a particular type of root cause event. Hand calculation methods were used to calculate component importances whenever the scram system $P(F|I)$ for a particular root cause event type was greater than 0.1. (The automated routines in COMCAN III are based on "rare event" approximations, and $P(F|I)$ s greater than 0.1 are not rare events.)

Table 4.4 lists the important components located in the computer room for the types of root cause events (i.e., generic environments) considered in this analysis. For each generic environment considered, the A and B scram breakers are the most important components with respect to the availability of the scram system. And, with the exception of the vibration generic environment, every common cause candidate identified for each type of generic environment in the computer room contains one of these two scram breakers. Depending on the generic environment type, either the regulating rod power supplies or the dc power interrupt scram breakers (C1, C2, D1, and D2) are the next most important components in the computer room, with respect to the availability of the scram system.

Table 4.4 Unavailability Importance of Components in the Computer Room -
Generic Environments

| Generic Environment/Location | Component | Importance ^a |
|------------------------------|------------------------------------------------------------|-------------------------|
| Grit | Scram breaker A | .5 |
| | Scram breaker B | .5 |
| | Scram breaker C1 | .23 |
| | Scram breaker C2 | .23 |
| | Scram breaker D1 | .23 |
| | Scram breaker D2 | .23 |
| Corrosion | Scram breaker A | .5 |
| | Scram breaker B | .5 |
| | Scram breaker C1 | .22 |
| | Scram breaker C2 | .22 |
| | Scram breaker D1 | .22 |
| | Scram breaker D2 | .22 |
| Moisture | Scram breaker A | .50 |
| | Scram breaker B | .50 |
| | Scram breaker C1 | .22 |
| | Scram breaker C2 | .22 |
| | Scram breaker D1 | .22 |
| | Scram breaker D2 | .22 |
| Temperature | Scram breaker A | .50 |
| | Scram breaker B | .50 |
| | Regulating rod power supplies E2, E3, E4, F2, F3, F4 | .17 ^b |
| | Scram breaker C1 | .13 |
| | Scram breaker C2 | .13 |
| | Scram breaker D1 | .13 |
| | Scram breaker D2 | .13 |

Table 4.4 (continued)

| Generic Environment/Location | Component | Importance ^a |
|------------------------------------------|------------------------------------------------------|-------------------------|
| Vibration/computer room and control room | Scram breaker A | .37 |
| | Scram breaker B | .37 |
| | Regulating rod power supplies E2, E3, E4, F2, F3, F4 | .14 ^b |
| | Channel trip relay KA | .12 |
| | Channel trip relay KB | .12 |
| | Channel trip relay KC | .12 |
| | Channel trip relay KD | .12 |
| | Scram breaker C1 | .11 |
| | Scram breaker C2 | .11 |
| | Scram breaker D1 | .11 |
| | Scram breaker D2 | .11 |

^aComponent importance is defined as the probability that a component contributes to scram system unavailability, given the scram system is unavailable due to the occurrence of a particular type of root cause event.

^bUnavailability importance per power supply.

Table 4.5 lists the important components for the two types of root cause events (generic environments) that generated common cause candidates for the control room. The channel trip relays (KA, KB, KC, and KD) are the most important components in both generic environments for the control room.

The important components for one type of root cause event (generic environment) considered in the quantitative analysis are not listed in Tables 4.4 or 4.5. When the entire ANO-1 plant is exposed to a vibration environment, the CRDMs are the most important components with regard to scram system availability. Their importance is 0.97. The A and B scram breakers are next in order of importance; each breaker's importance is 0.26. No other scram system component has an importance above 0.1 (with regard to an entire plant vibration environment that could affect the availability of the scram system).

4.2.2 Fault Exposure Times

The scram system's average fault exposure time is the average amount of time between scram system failure and the time the failure is detected and corrected. The fault exposure time associated with a scram system failure is a function of three things:

1. the probability the failure or the root cause of failure is announced
2. the test policy applicable to the system (including individual channel test intervals and the method of staggering tests)
3. the probability the failure is discovered by a test

Table 4.5 Unavailability Importance of Components in the Control Room -
Generic Environments

| Generic Environment/Location | Component | Importance ^a |
|------------------------------|-----------------------------------------------------------------|-------------------------|
| Grit | Channel trip relay KA | **b |
| | Channel trip relay KB | **b |
| | Channel trip relay KC | **b |
| | Channel trip relay KD | **b |
| | Auxiliary control relays (16 relays) KA1, KA2,...KD3, KD4 | **b |
| Fire | Channel trip relay KA | .57 |
| | Channel trip relay KB | .57 |
| | Channel trip relay KC | .57 |
| | Channel trip relay KD | .57 |

^aComponent importance is defined as the probability that a component contributes to scram system unavailability, given the scram system is unavailable due to the occurrence of a particular type of root cause event.

^bBecause there is a large number of common cause candidates that contained these components and because the rare event approximation does not apply to this problem, we were not able to estimate the importance of these components.

Scram system average fault exposure times (T_I) for the various root cause event types (Tables 4.6 and 4.7) are estimates based on our evaluation of plant operating procedures and discussions with ANO-1 personnel. The uncertainties in the T_I values are not as large as the uncertainties in $P(F|I)$.

4.2.3 Root Cause Event Frequencies

The frequency of any type of root cause event is the sum of the frequencies of all specific root cause events of that type. With the exceptions of fires and similar part failures, no information was available in the open literature concerning frequencies of the types of root cause events identified in this study. In many cases, it was possible to identify very specific root cause events that could produce conditions leading to common cause failure of the scram system. However, it was not possible to quantitatively analyze such events in detail, within the scope of this study.

Consider a scram system failure that results from high vibration in the control and computer rooms. The only identified root cause events that would produce high vibration levels in the control and computer rooms are steam turbine imbalances and emergency diesel generator imbalances. An analysis of these events to determine more specific root cause events and the frequency of the root cause event type would have required (1) a definition of an unacceptably high vibration level, (2) a thorough analysis of the emergency diesel generators and the steam turbine, and (3) an evaluation of potential operator intervention that might preclude an ATWS.

Table 4.6 Scram System Fault Exposure Times - Generic Environments

| Generic Environment/Location | P(F I) | T _I (hr) ^a |
|---------------------------------------------|------------------------|----------------------------------|
| Fire/control room | 1.0 x 10 ⁻² | <1 |
| Grit/computer room | 1.0 | 84 |
| Grit/control room | 1.0 | 84 |
| Moisture/computer room | 4.6 x 10 ⁻² | 84 |
| Vibration/computer room and control room | .11 | 84 |
| Temperature/computer room | 7.5 x 10 ⁻² | 84 |
| Corrosion/computer room | .74 | 84 |
| Vibration/whole plant | .93 | 360 |

^aFault exposure times less than one hour indicate that failure discovery and corrective action would occur almost immediately after the root cause event occurs.

Table 4.7 Scram System Fault Exposure Times - Common Links

| Common Link | P(F I) | T _I (hr) |
|--------------------------------|--------|---------------------|
| Similar parts - ac/dc breakers | 1.0 | 84 |
| Similar parts - ac/dc relays | 1.0 | 84 |
| Similar parts - CRDMs | 1.0 | 84 |
| Similar parts - cables | 1.0 | 84 |

Performing a more detailed quantitative analysis to determine the frequency of root cause event types at ANO-1 would have resulted in a more comprehensive analysis of this plant's scram system. But it would have contributed little to the overall objective of this analysis: to demonstrate the use of a formal method for common cause failure analysis of a scram system. The frequency of a root cause event--such as failure of all control room cooling systems--is plant-specific and the results of an analysis of specific root causes at ANO-1 would not necessarily apply to other scram system CCFAs. All preceding results of the analysis documented here, however, are generic to B&W plants with scram systems like the one at ANO-1.

Because of the difficulties just described and the desire to make analysis results as generally applicable to B&W plants as possible, we used the following approach when analyzing root cause events at ANO-1:

1. We provided qualitative descriptions of the types of root cause events of concern (Tables 3.1-3.3).
2. We performed a sensitivity analysis of scram system unavailability, with respect to root cause event type frequency, to identify important types of root cause events.
3. We estimated frequencies for these important types of root cause events.
4. We calculated scram system unavailabilities for these important types of root cause events.

Tables 4.8 and 4.9 show the results of the sensitivity analysis. These tables contain estimates of the scram system unavailability for each type of root cause event of concern. Scram system unavailability estimates are

Table 4.8 CCFA Quantitative Results - Sensitivity Analysis for Generic Environments

| Generic Environment/Location | Λ_I | | | | |
|---------------------------------------------|--------------------|-------------------|-------------------|-------------------|-------------------|
| | .2/yr | 1/yr | .025/yr | .01/yr | .001/yr |
| Scram System Unavailability | | | | | |
| Fire/control room | 2.2 ^{-7a} | 1.1 ⁻⁷ | 2.8 ⁻⁸ | 1.1 ⁻⁸ | 1.1 ⁻⁹ |
| Grit/computer room | 1.9 ⁻³ | 9.6 ⁻⁴ | 2.4 ⁻⁴ | 9.6 ⁻⁵ | 9.6 ⁻⁶ |
| Grit/control room | 1.9 ⁻³ | 9.6 ⁻⁴ | 2.4 ⁻⁴ | 9.6 ⁻⁵ | 9.6 ⁻⁶ |
| Moisture/computer room | 8.8 ⁻⁵ | 4.4 ⁻⁵ | 1.1 ⁻⁵ | 4.4 ⁻⁶ | 4.4 ⁻⁷ |
| Vibration/computer room and control room | 2.1 ⁻⁴ | 1.1 ⁻⁴ | 2.6 ⁻⁵ | 1.1 ⁻⁵ | 1.1 ⁻⁶ |
| Temperature/computer room | 1.4 ⁻⁴ | 7.2 ⁻⁵ | 1.8 ⁻⁵ | 7.2 ⁻⁶ | 7.2 ⁻⁷ |
| Corrosion/computer room | 1.4 ⁻³ | 7.1 ⁻⁴ | 1.8 ⁻⁴ | 7.1 ⁻⁵ | 7.1 ⁻⁶ |
| Vibration/whole plant | 7.6 ⁻³ | 3.8 ⁻³ | 9.5 ⁻⁴ | 3.8 ⁻⁴ | 3.8 ⁻⁵ |

$$^a 2.3^{-7} = 2.3 \times 10^{-7}$$

Table 4.9 CCFA Quantitative Results - Sensitivity Analysis for Common Links (Similar Parts)

| Similar Part | λ_I | | | | |
|------------------------------------|--------------------|-------------------|-------------------|-------------------|-------------------|
| | .2/yr | .1/yr | .025/yr | .01/yr | .001/yr |
| Scram System Unavailability | | | | | |
| ac/dc breakers | 1.9 ^{-3a} | 9.6 ⁻⁴ | 2.4 ⁻⁴ | 9.6 ⁻⁵ | 9.6 ⁻⁶ |
| ac/dc relays | 1.9 ⁻³ | 9.6 ⁻⁴ | 2.4 ⁻⁴ | 9.6 ⁻⁵ | 9.6 ⁻⁶ |
| CRDMs | 1.9 ⁻³ | 9.6 ⁻⁴ | 2.4 ⁻⁴ | 9.6 ⁻⁵ | 9.6 ⁻⁶ |
| cables | 1.9 ⁻³ | 9.6 ⁻⁴ | 2.4 ⁻⁴ | 9.6 ⁻⁵ | 9.6 ⁻⁶ |

^a1.9 ⁻³ = 1.9 x 10⁻³

based on root cause events occurring at ANO-1 on the average of 1 event every 5 years, every 10 years, every 40 years (plant lifetime), every 100 years, and every 1000 years. For example, the estimated scram system unavailability is 1.8×10^{-5} if high-temperature environments in the computer room severe enough to cause scram system failure (with an average fault exposure time of 84 hours) occur once every 40 years.

A comparison of the scram system unavailability due to independent failures (4.1×10^{-6}) with the results in Tables 4.8 and 4.9 provides some quantitative basis for determining which types of root cause events are important and require further investigation. Based on data in Table 4.8 and documented data on the frequency of fires in nuclear power plants, we believe fires in the control room need not be analyzed in greater detail. Even at an occurrence frequency of 1 fire every 5 years, the estimated scram system unavailability due to a major fire is less than 10% of the scram system unavailability due to a fire caused by independent failures. And according to NUREG/CR-2258, the occurrence frequency of fires in nuclear power plant control rooms is much less than once every five years. (The documented frequency is approximately 3 every 1000 reactor-years.)¹² This lends additional support to our belief that investigating control room fires is not necessary.

Using the only other data documented in the open literature on the frequency of root cause event types, we determined that the similar part common link should be analyzed in detail. The nuclear industry has recorded two scram system failures due to similar part faults during its approximately 1000 reactor-year history. The most recent failure resulted from the UV trip attachment binding on both RPS scram breakers at the Salem

Unit 1 Plant. The binding was attributed to improper maintenance. The other failure resulted from all scram relays in the Kahl reactor sticking closed because a corrosion inhibitor coating on the relays was not properly cured. Based on these two incidents in 1000 reactor years, the scram system unavailability estimates in Table 4.9 indicate that the similar part common link could be a significant contributor to scram system failure and that it requires further investigation.

Since we found no data in the open literature on occurrence frequencies for the other types of root cause events considered in this study, we considered each of these root cause event types potentially important contributors to ANO-1 scram system unavailability. The final two steps in the root cause event analysis, then, involved estimating frequencies for these potentially important types of root cause events and estimating scram system unavailabilities using these frequency estimates.

Specifically, in the third step, we used two methods to estimate occurrence frequencies for root cause event types. For generic environment type root causes, we estimated occurrence frequencies based on the potential root cause events identified during our plant walk-throughs (Table 3.1) and using engineering judgment. The occurrence frequencies for similar parts, on the other hand, were derived using a β -factor method and the following equation:

$$\begin{aligned} \Lambda_{sp,i} = & (.02)(N_{2,i})(\lambda_1) + (.02)(.1)(N_{3,i})(\lambda_1) \quad (4.2) \\ & + (.02)(.1)(.2)(N_{4+,i})(\lambda_1) \end{aligned}$$

where

$\Lambda_{sp,i}$ = the occurrence frequency of multiple failures of similar part i

λ_i = the failure rate of similar part i

$N_{2,i}; N_{3,i}; N_{4+,i}$ = the number of two-event, three-event, and four-event (or larger) minimal cut sets composed of only similar part i

.02, .1, .2 = the β -factors for the second, third, and fourth members of a minimal cut set composed of similar parts.*

We assumed a β -factor of 1.0 for the fifth and sixth members of a minimal cut set. We also assumed the β -factors were the same for all component types.

Table 4.10 lists the frequency estimates for the root cause event types of interest in this analysis and the corresponding scram system unavailability estimates. The frequency estimates range from $5 \times 10^{-2}/\text{yr}$ for moisture and temperature type root cause events in the computer room to $7 \times 10^{-7}/\text{yr}$ for cables (similar parts). The scram system unavailability estimates range from 1.8×10^{-4} to 5.7×10^{-9} . The total estimated scram system unavailability due to common cause failures only is 5.2×10^{-4} .

4.3 Quantitative CCFA Results

Based on the unavailability estimates in Table 4.10, all of the important generic environment and one of the similar part (ac/dc breakers)

*These β -factors were obtained from Attachment A to the report entitled Amendments to 10 CFR 50 Related to Anticipated Transients Without Scram (ATWS) Events. (See Reference 13.)

Table 4.10 Scram System Unavailability Estimates by Root Cause Event Type

| Root Cause Event Type | Λ_I (yr ⁻¹) or Λ_{sp} ^a | Scram System Unavailability |
|------------------------------------------|----------------------------------------------------------------|-----------------------------|
| Grit/computer room | 1.0×10^{-2} | 1.0×10^{-4} |
| Grit/control room | 1.0×10^{-2} | 1.0×10^{-4} |
| Moisture/computer room | 4.9×10^{-2} | 2.2×10^{-5} |
| Vibration/computer room and control room | 2.4×10^{-2} | 2.6×10^{-5} |
| Temperature/computer room | 4.9×10^{-2} | 3.6×10^{-5} |
| Corrosion/computer room | 2.4×10^{-2} | 1.8×10^{-4} |
| Vibration/whole plant | 1.0×10^{-3} | 3.8×10^{-5} |
| ac/dc breakers | 1.7×10^{-3} | 1.7×10^{-5} |
| ac/dc relays | 3.3×10^{-6} | 5.0×10^{-8} |
| CRDM | 3.0×10^{-6} | 3.4×10^{-7} |
| cables | 7.0×10^{-7} | 6.7×10^{-9} |

^aThese frequency estimates are based primarily on engineering judgment; in some cases they were calculated using β -factors.

root cause event types are potentially significant contributors to scram system unavailability. The scram system unavailability estimates for these root cause event types are, in some cases, as much as a factor of 50 larger than the total scram system unavailability estimate due to independent failures. Common cause failures of the scram system due to ac/dc relay, CRDM, and cable failures are not significant contributors to scram system unavailability.

5. CONCLUSIONS AND RECOMMENDATIONS

This study developed a workable method for quantitative common cause failure analysis that produces useful results for formulating recommendations to improve system designs. While the method demonstrated here was for a common cause failure analysis of the ANO-1 scram system, its application illustrates the type of data needed to quantify common cause failures and the general quantitative results that can be expected from analyses of other scram systems.

Some of the data used to perform the quantitative common cause failure analysis of the ANO-1 scram system were based on engineering judgment since supporting data were not readily available. If the input data used here are reasonably accurate, the CCFA quantitative results support several conclusions.

The most important components in the scram system--with respect to system availability--are the A and B scram breakers. Each of these components has the highest importance in the independent failures case and in all the root cause event cases considered for the generic environments that can affect the computer room. These components also have the highest importances for most of the common links identified for this analysis.

Electrical component failures are the dominant contributors (99%) to the scram system's unavailability resulting from independent component failures. Electrical component failures are also dominant contributors to the scram system's unavailability resulting from common cause events.

Results from the common cause failure analysis of the ANO-1 scram system indicate that common cause failures may be dominant contributors to scram system unavailability at other nuclear power plants. This study

identified common cause candidates for 29 generic-environment- and common-link-type root cause events. Eight of these common cause events would individually contribute more to scram system unavailability than the independent failures contribute. Documented nuclear power industry experience, such as the Kahl and Salem reactor scram system failures (similar part failure events), support the significance of these eight events.

We calculated the conditional probabilities of scram system failure, $P(F|I)$, for each of the different root cause event types considered using estimated conditional failure probabilities for the components. The estimated probabilities are based primarily on engineering judgment, and, therefore, these $P(F|I)$ values have large uncertainties. For most root cause event types considered, the system conditional failure probabilities are sensitive to just a few component failure probabilities (in particular, the scram breakers and regulating rod power supplies). The uncertainties and sensitivities associated with the failure probabilities should be taken into consideration when making decisions based on the results of this study.

All results presented in this study, with the exceptions of the potential root cause events and the fault exposure times (T_I), are generic to Babcock and Wilcox nuclear power plants with scram systems designed like the ANO-1 system. These results, combined with a plant-specific root cause analysis, provide the data needed to quantify the unavailability of a Babcock and Wilcox scram system due to common cause failures.

Based on the results of this study, we recommend the following work.

Recommendation 1

Perform common cause failure analyses of scram systems designed by other NSSS vendors. This study identified common cause failures as potential dominant contributors to scram system failure probability. The fact that common cause failures are potentially dominant contributors to scram system failure merits analyzing other scram system designs. The results of analyzing other scram systems will support the NRC's ATWS and RMIEP studies.

Recommendation 2

Develop a procedure for identifying and calculating the frequency of root cause events. In this study, we performed a plant walk-through to identify potential root cause events, and we estimated root cause event frequencies using primarily engineering judgment. A detailed root cause event analysis procedure employing reliability and data analysis methods will ensure a comprehensive treatment of root cause events in other common cause failure analyses.

Recommendation 3

Investigate the feasibility of collecting component data to determine the conditional probability of a component failure, given a severe generic environment. The conditional failure probabilities of components considered in this study are estimates based on engineering judgment. Data collection efforts in other CCFAs should focus on generic component types that frequently appear in nuclear safety systems. Thus, only generic environment data for a few component types need be collected. Sensitivity studies to identify more important scram system components and root cause

event analyses to identify important generic environments would provide the information necessary to limit data collection efforts in future CCFAs.

Recommendation 4

Develop methods for performing an uncertainty analysis on the conditional probabilities of scram system failure, $P(F|I)$, given a root cause event. The uncertainty analysis methods may require the application of specialized Monte Carlo techniques that have the capability of preventing component failure probability samples from exceeding 1.0 when the median failure probability is large (as high as 0.9).

Recommendation 5

Update the importance equations in COMCAN III to allow for calculations that are not based on "rare event" approximations. The importance equations in COMCAN III are based on rare event approximations, and these approximations are not valid when large (>0.1) conditional failure probabilities are used. Manual calculations were performed in this study for more accurate results.

Implementing these five recommendations will enable analysts to more accurately estimate scram system failure probabilities and ATWS frequencies for light water reactor designs used in the U.S. commercial nuclear power industry.

REFERENCES

1. Anticipated Transients Without Scram for Light Water Reactors, NUREG/CR-0460, U.S. Nuclear Regulatory Commission, Office of U.S. Nuclear Reactor Regulation, Washington DC, March 1980.
2. D. M. Rasmuson, G. R. Burdick, and J. R. Wilson, Common Cause Failure Analysis Techniques: A Review and Comparative Evaluation, TREE-1349, EG&G Idaho, Inc., Idaho Falls, ID, September 1979.
3. ATWS: A Reappraisal - Part III, Frequency of Anticipated Transients EPRI NP-801-Project 767, Interim Report, Science Applications, Inc., July 1978.
4. D. M. Rasmuson et al., Using COMCAN III in System Design and Reliability Analysis, EGG-2182, March 1982.
5. Reactor Safety Study, NUREG-75/014 (WASH-1400), U.S. Nuclear Regulatory Commission, Washington, DC, October 1975.
6. Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One - Unit 1 Nuclear Power Plant, NUREG/CR-2787 (SAND82-0978), Sandia National Laboratories, Albuquerque, NM, June 1982.
7. J. B. Fussell et al., A Collection of Methods for Reliability and Safety Engineering, ANCR-1273, Aerojet Nuclear Co., ANCR-1273, April 1976.
8. G. R. Burdick, N. H. Marshall, and J. R. Wilson, COMCAN - A Computer Program for Common Cause Failure Analysis, ANCR-1314, Aerojet Nuclear Co., May 1976.
9. D. M. Rasmuson et al., COMCAN II - A Computer Program for Automated Common Cause Failure Analysis, TREE-1361, EG&G Idaho, Inc., May 1979.
10. C. L. Cate and J. B. Fussell, BACFIRE - A Computer Code for Common Cause Failure Analysis, the University of Tennessee, Knoxville, February 1977.
11. D. P. Wagner et al., FAUST - A Computer Program for Common Cause Failure Analysis of Nuclear Power Plants, JBFA-108-81, JBF Associates, Inc., Knoxville, TN, December 1981.
12. M. Kazarians and G. Apostolakis, Fire Risk Analysis for Nuclear Power Plants, NUREG/CR-2258 (UCLA-ENG-8102), September 1981.
13. W. J. Dircks, Amendments to 10 CFR 50 Related to Anticipated Transients Without Scram (ATWS) Events, Report SECY-83-293, U.S. Nuclear Regulatory Commission, Washington, DC, July 19, 1983.

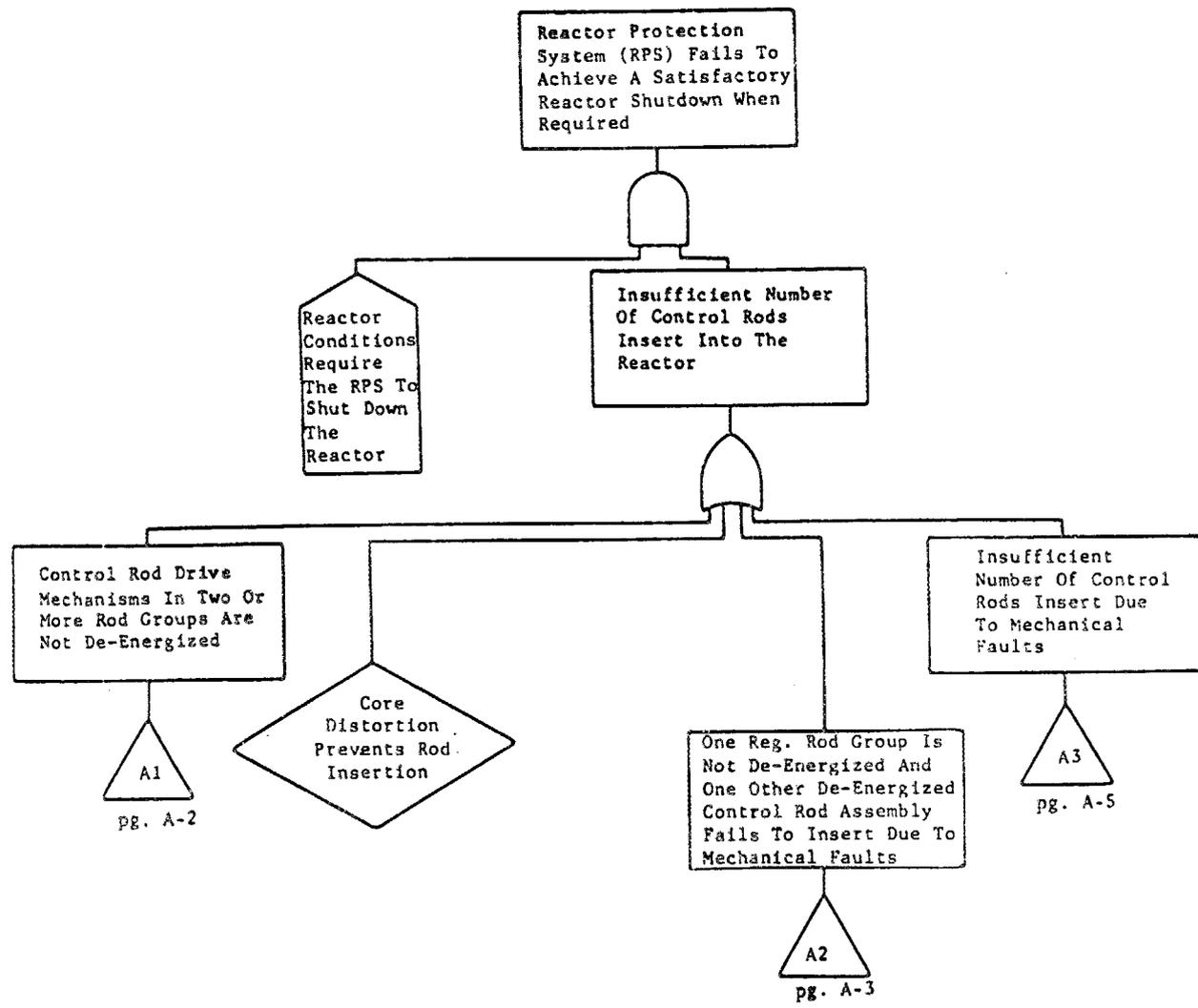
RELATED BIBLIOGRAPHY

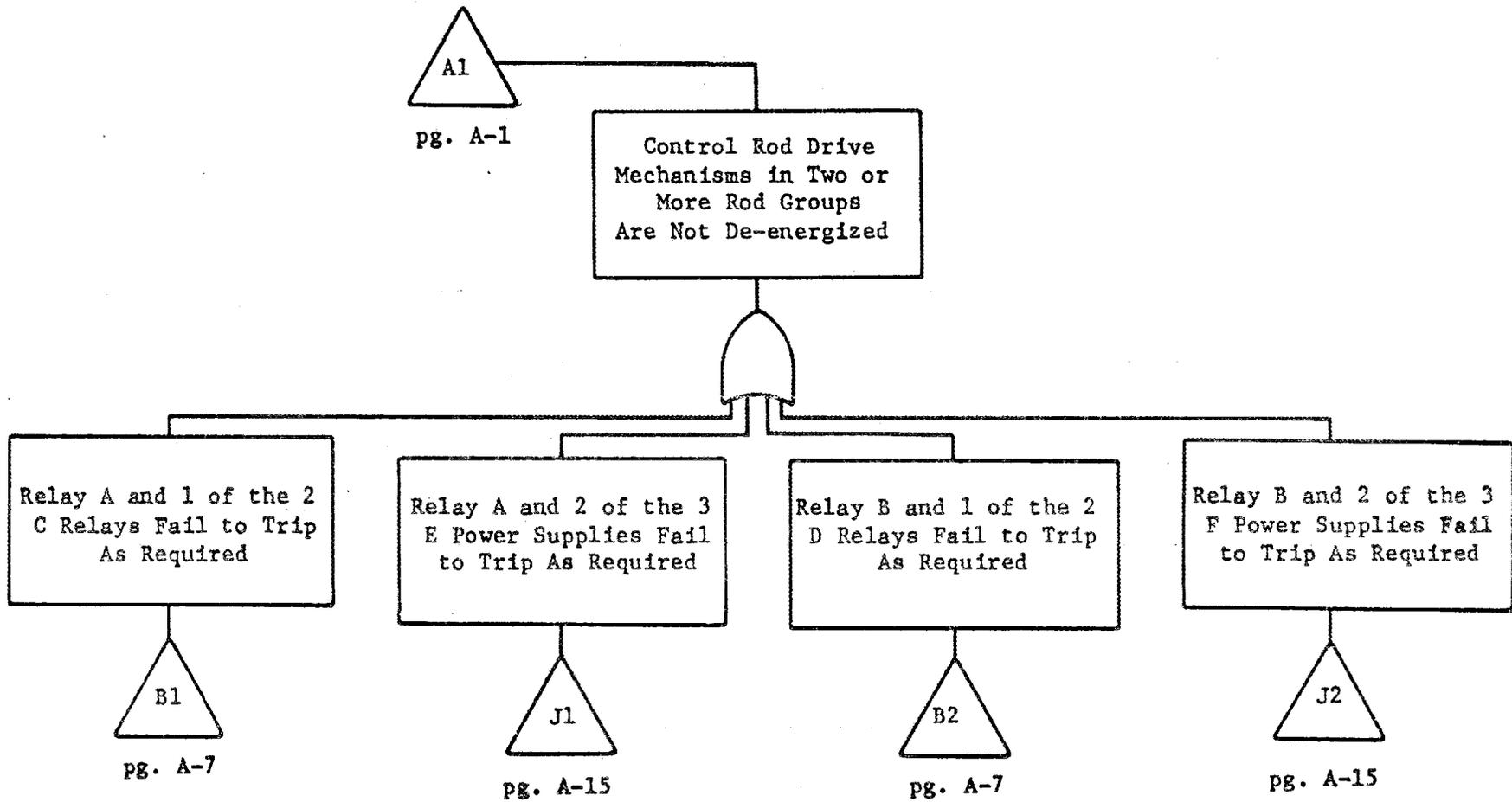
Hammond, C. W. et al., Anticipated Transients Without Scram Program: Common Mode Failure Analysis of Control Rod Drive Mechanism, Topical Report BAW-10101P, Rev. 1, September 1975.

LaBelle, D. W. et al., Babcock and Wilcox Anticipated Transients Without Scram, Topical Report BAW-10099, December 1974.

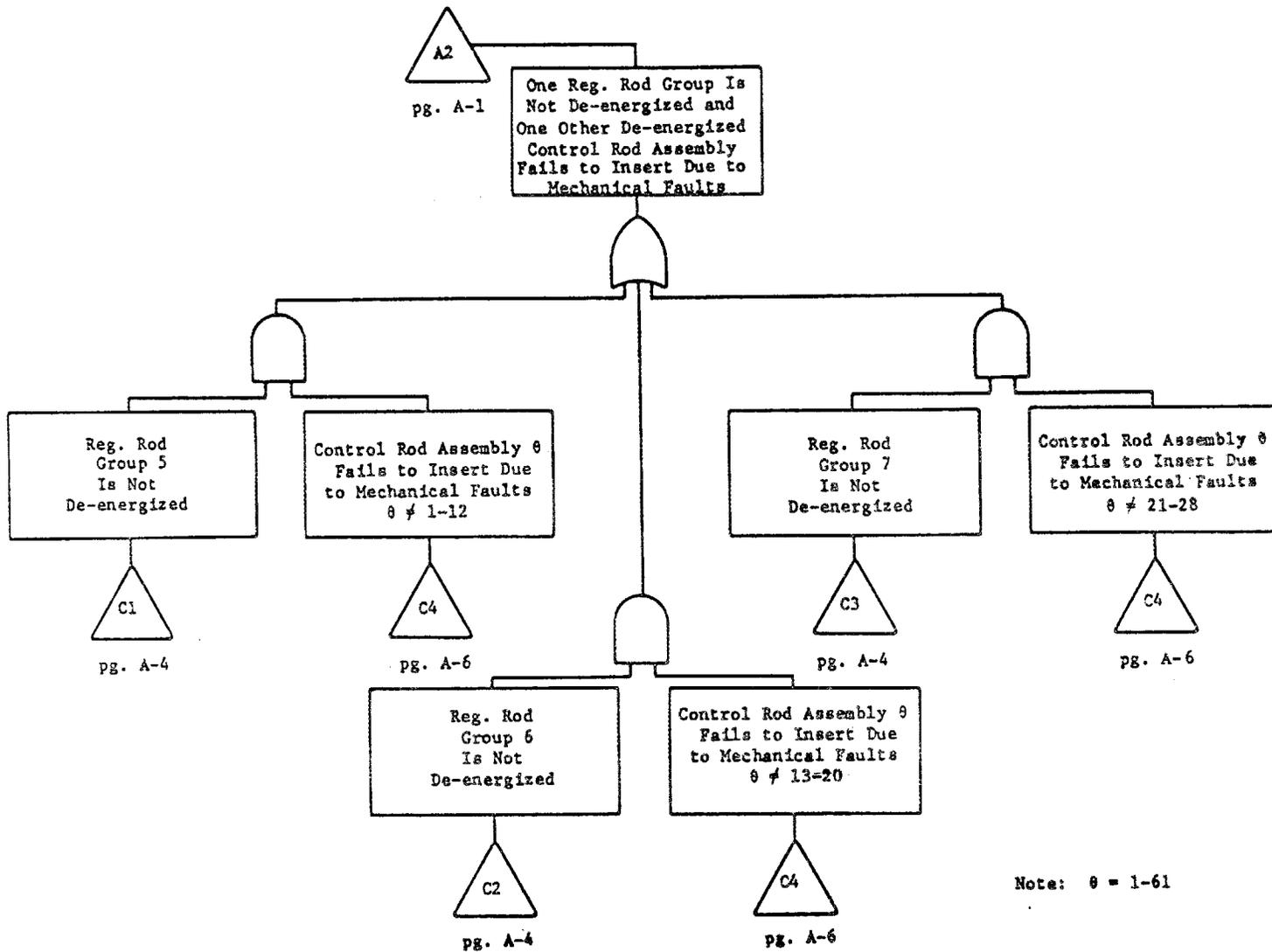
APPENDIX A

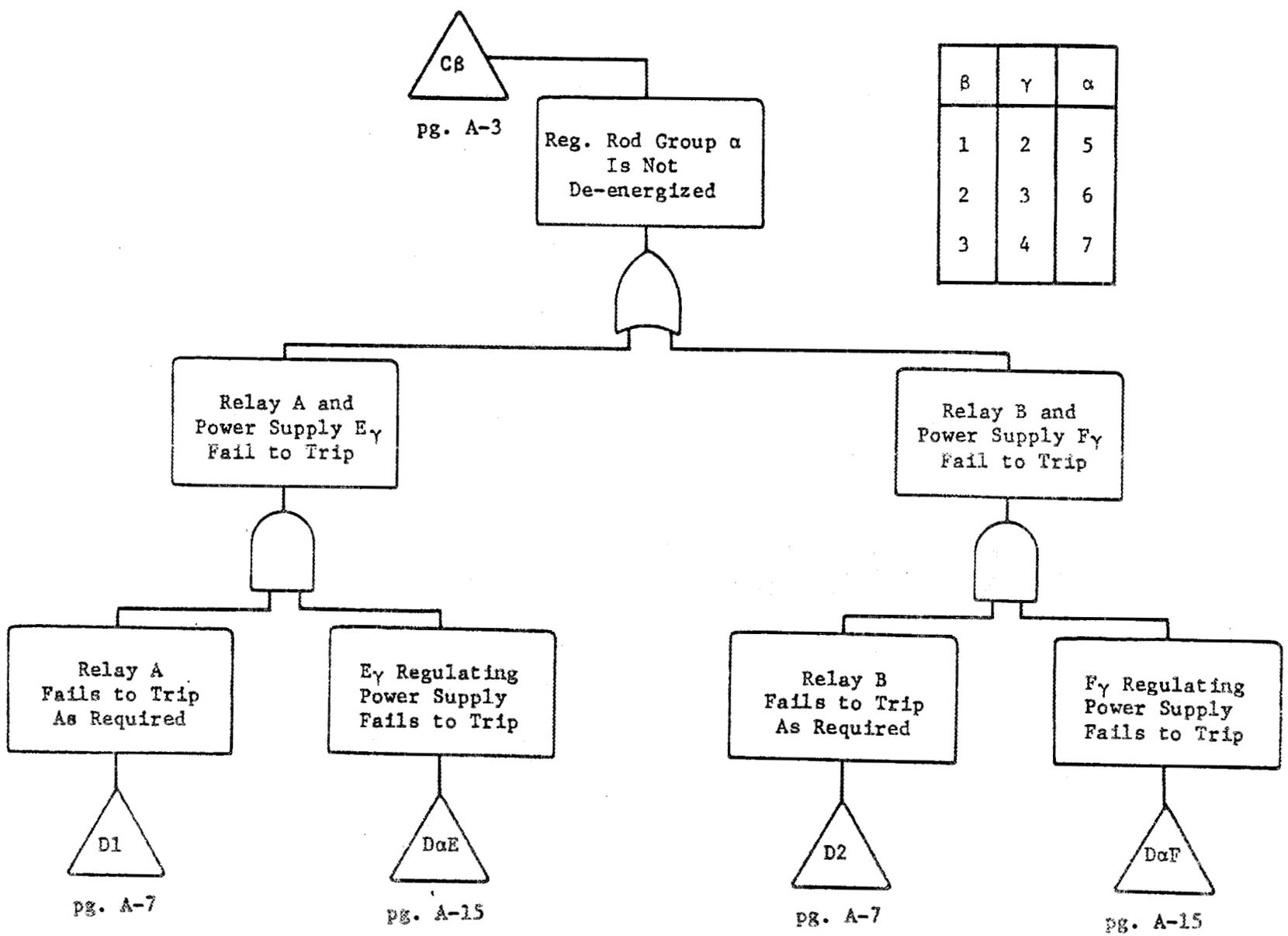
Detailed Fault Tree
of the ANO-1 Scram System





A-3



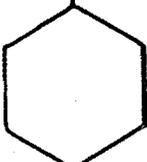


A-5

A3

pg. A-1

Insufficient
Number of Control
Rods Insert Due
to Mechanical
Faults



An Appropriate Set of
5 Control Rod Assemblies
Fails to Insert Given 5
Control Rod Assemblies
Are Failed



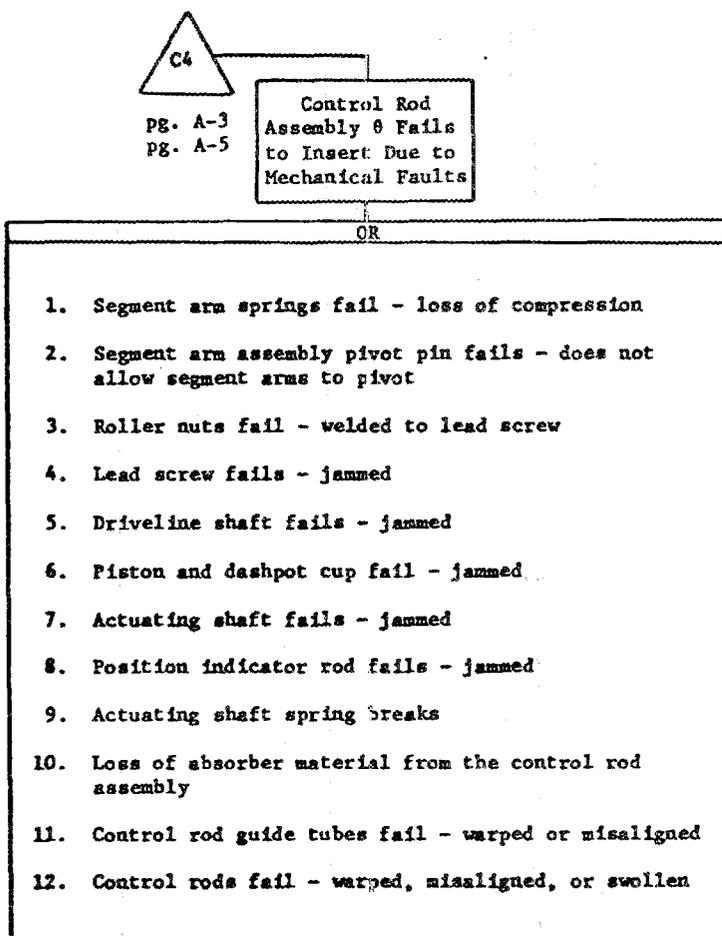
Control Rod
Assembly 0 Fails
to Insert Due to
Mechanical Faults

C4

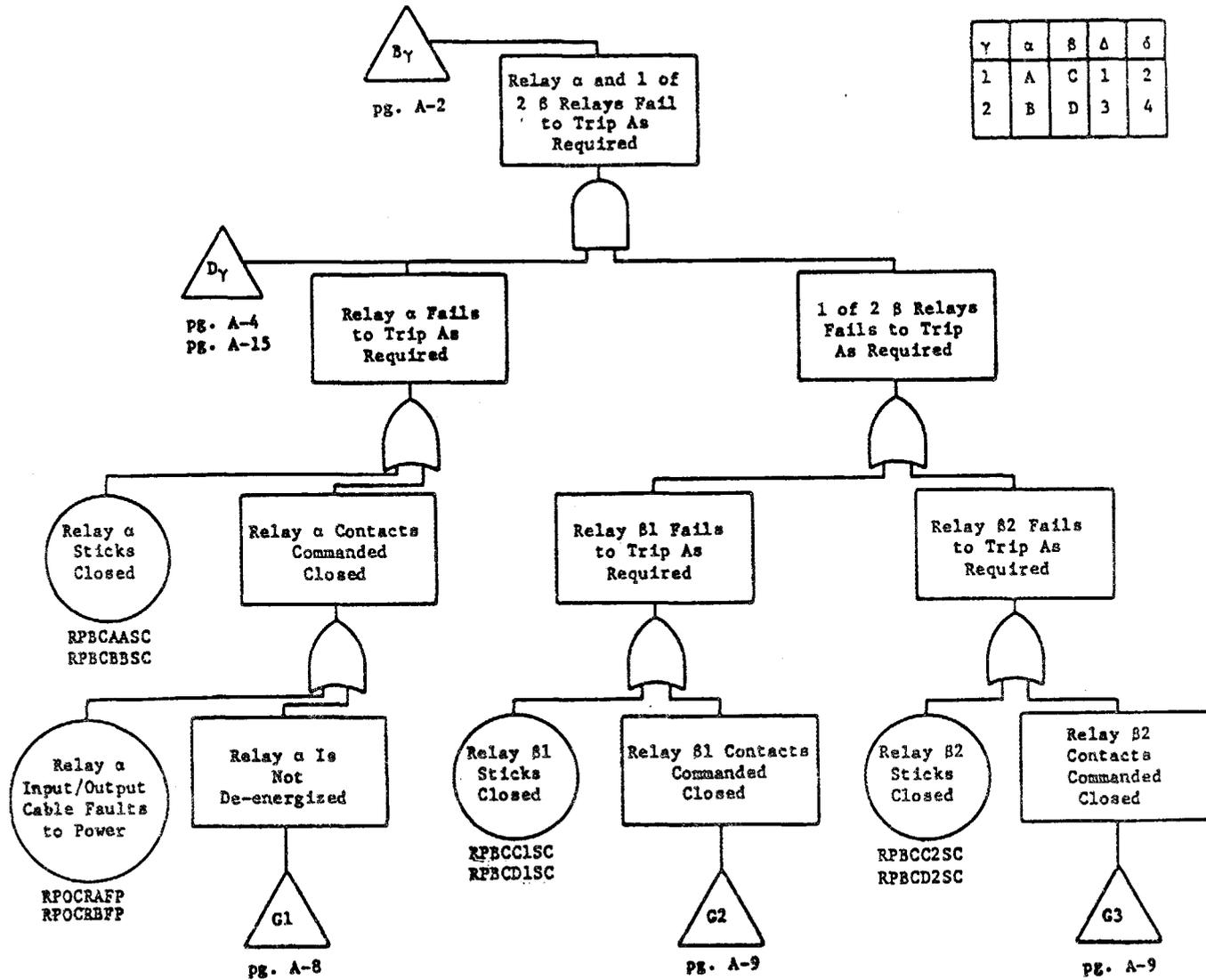
pg. A-6

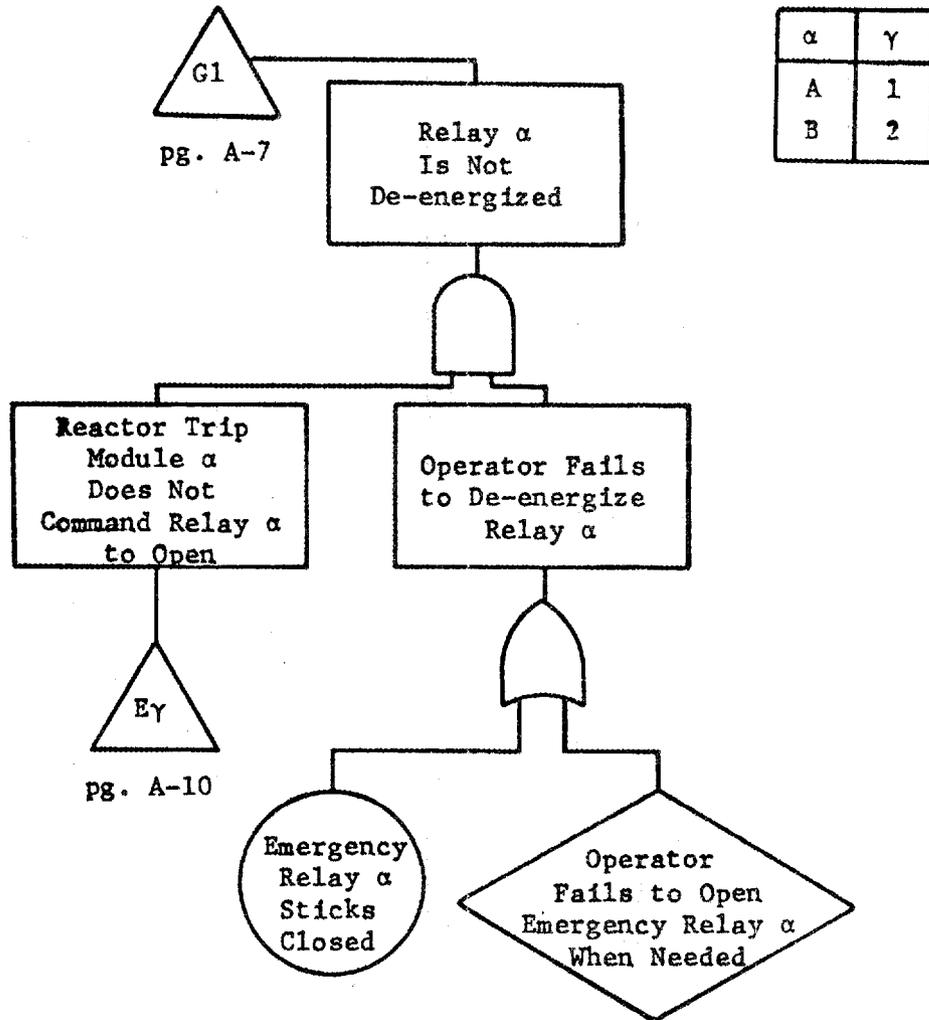
Note: 0 = 1-61

A-6

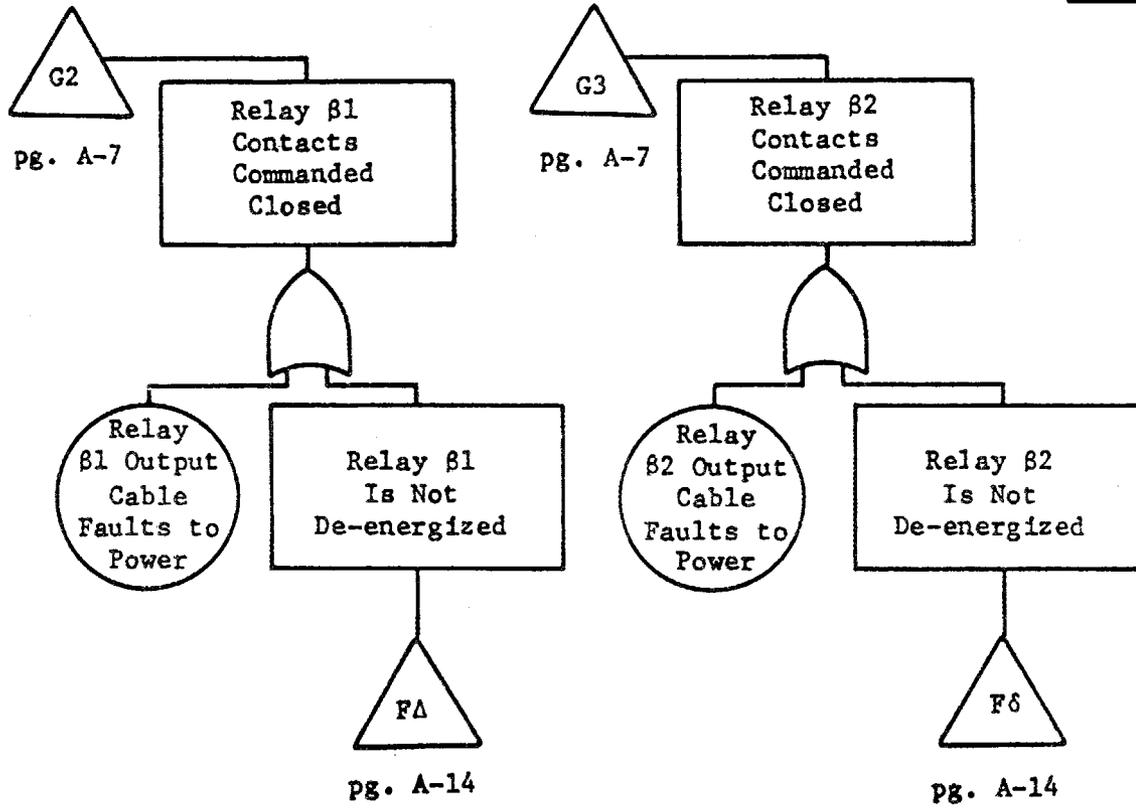


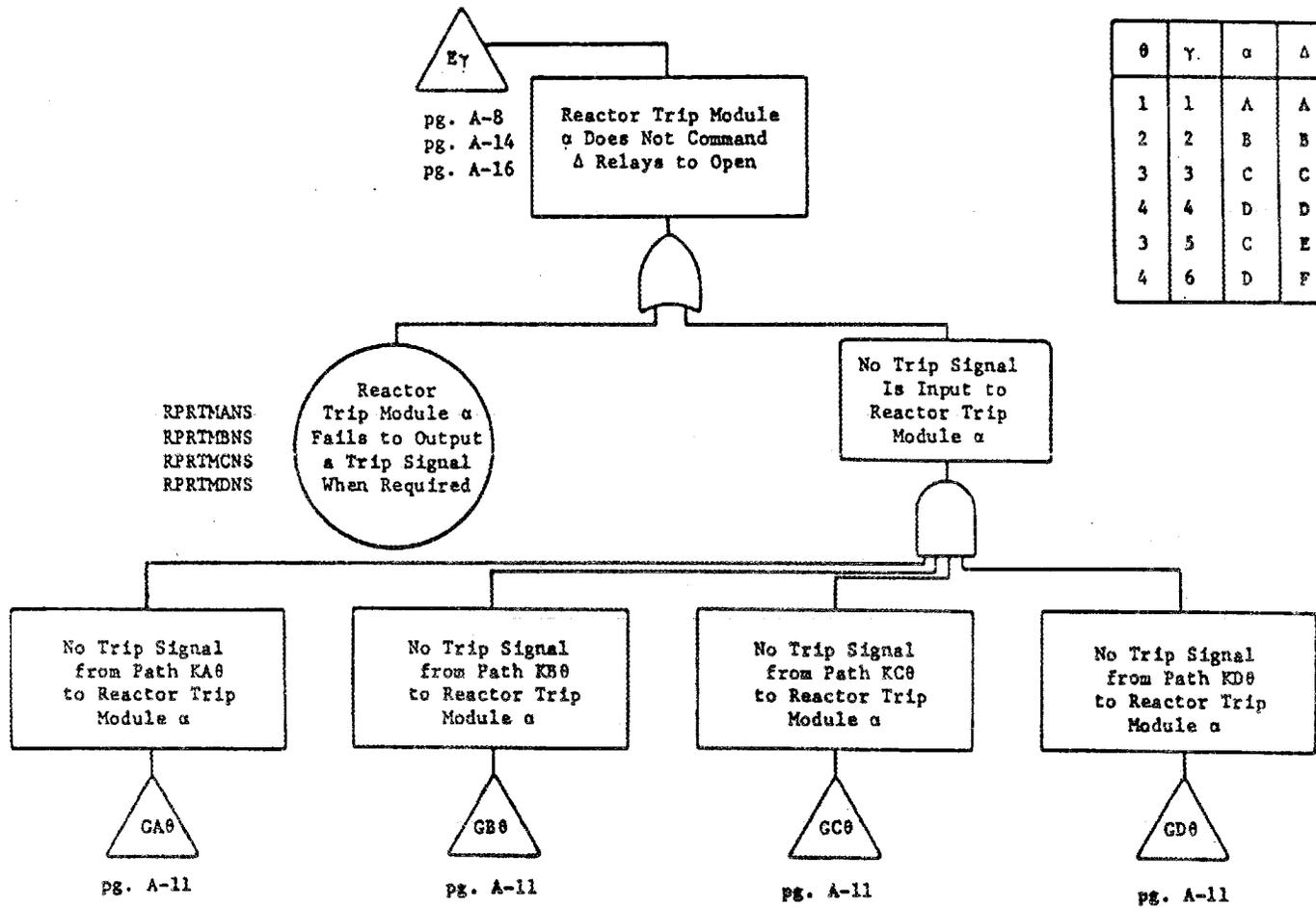
Note: 6 - 1-61



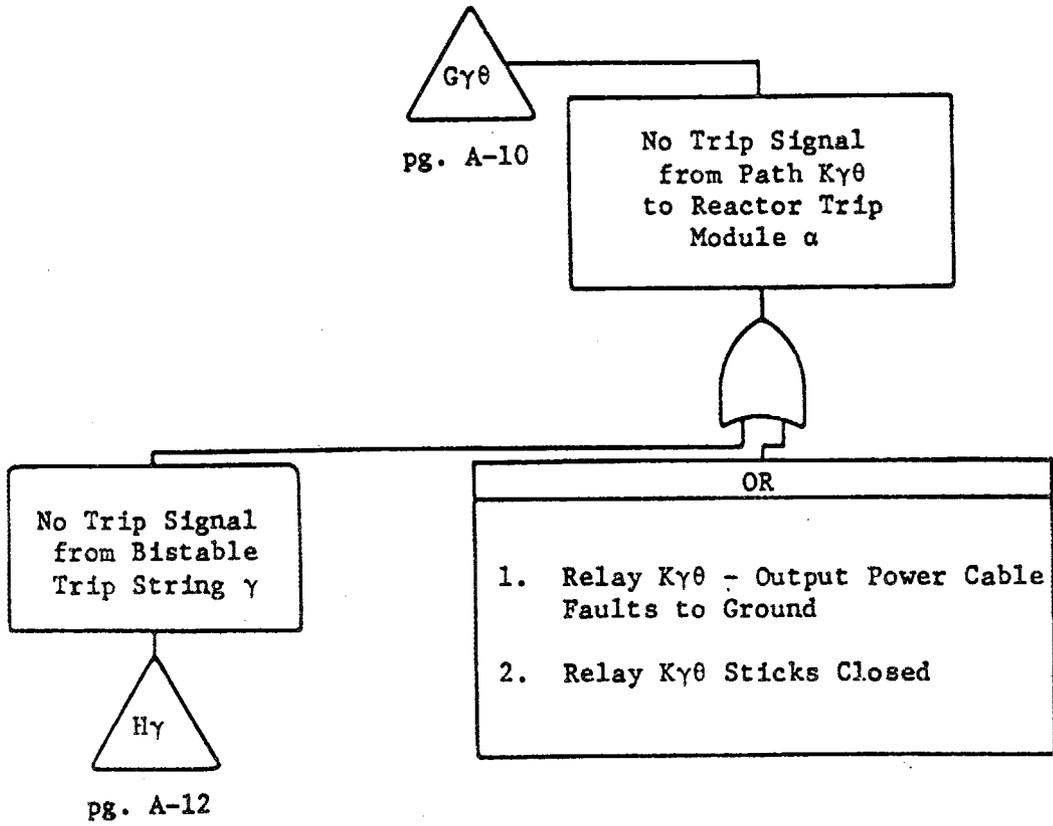


| | | |
|---------|----------|----------|
| β | Δ | δ |
| C | 1 | 2 |
| D | 3 | 4 |

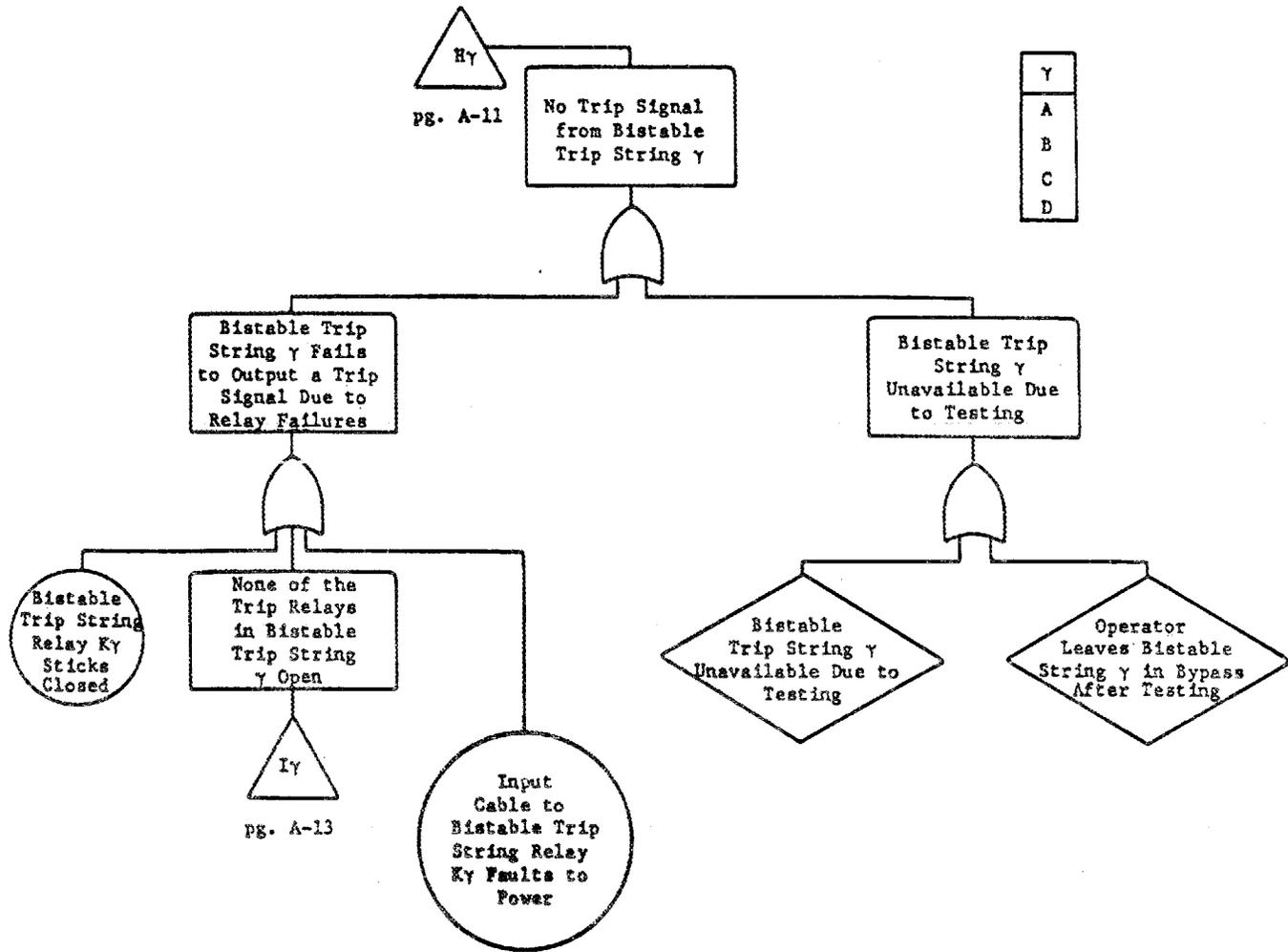


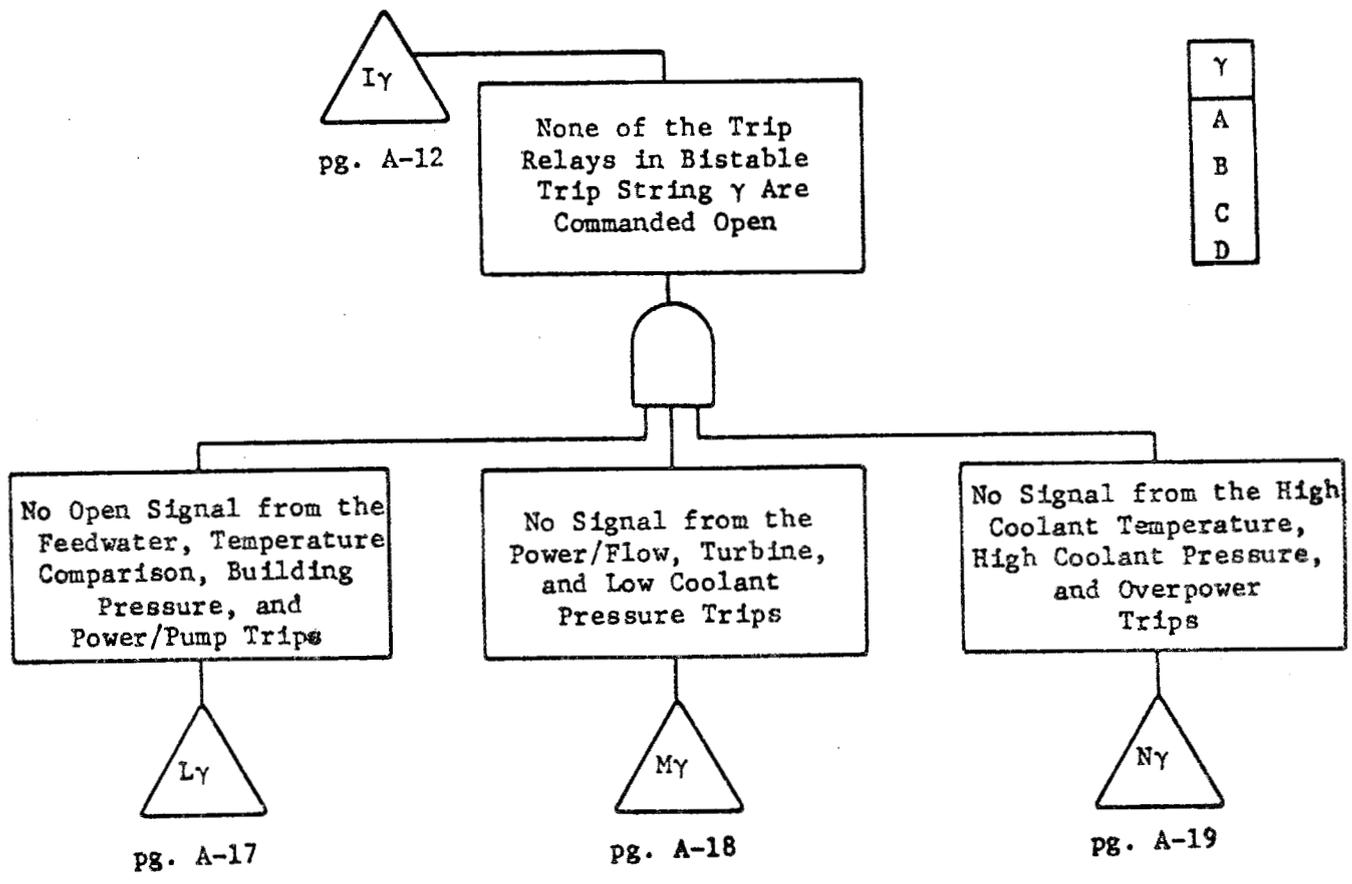


| θ | γ | α | Δ |
|----------|----------|----------|----------|
| 1 | 1 | A | A |
| 2 | 2 | B | B |
| 3 | 3 | C | C |
| 4 | 4 | D | D |
| 3 | 5 | C | E |
| 4 | 6 | D | F |

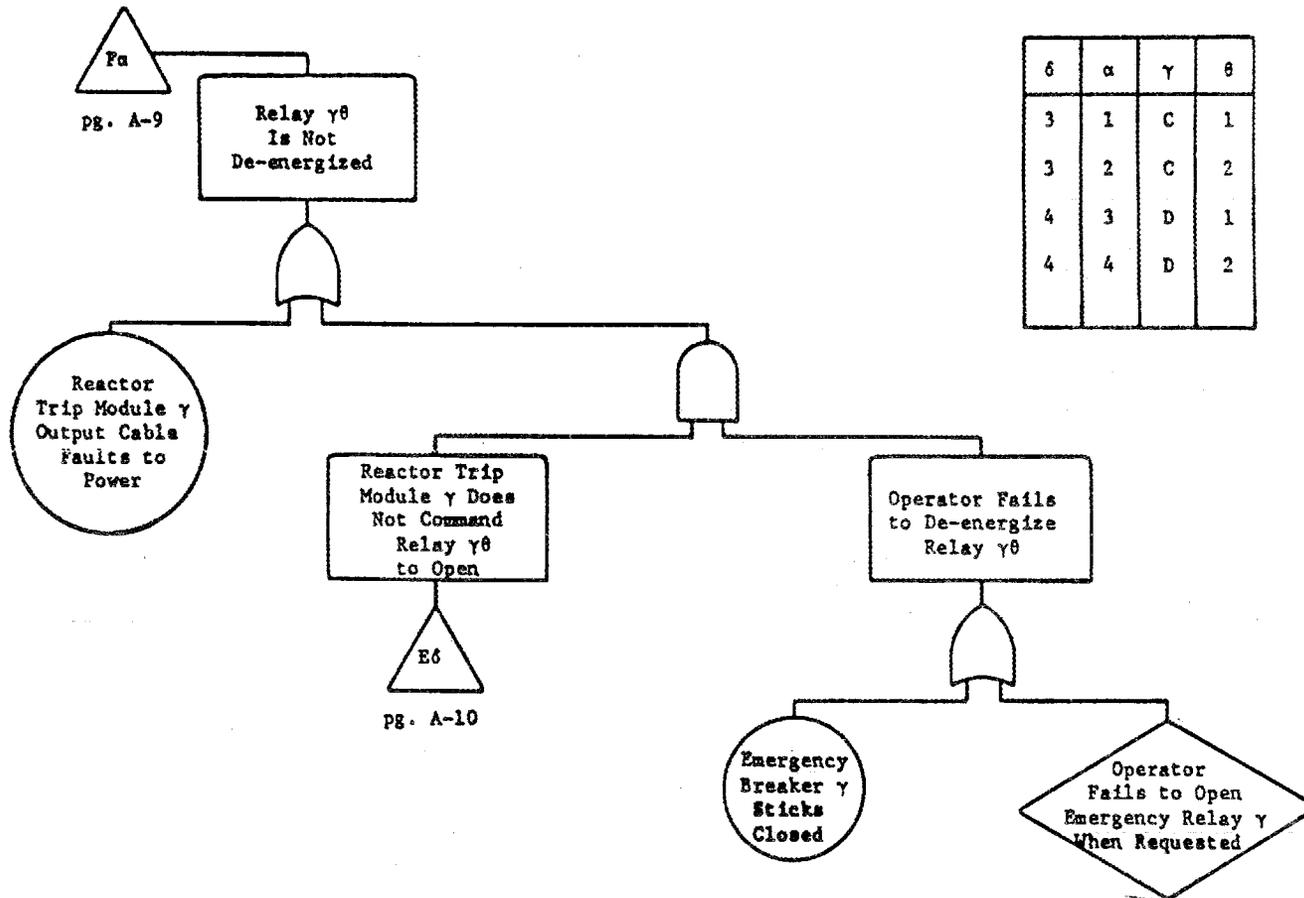


| γ | α | θ |
|----------|----------|----------|
| A | A | 1 |
| B | A | 1 |
| C | A | 1 |
| D | A | 1 |
| A | B | 2 |
| B | B | 2 |
| C | B | 2 |
| D | B | 2 |
| A | C | 3 |
| B | C | 3 |
| C | C | 3 |
| D | C | 3 |
| A | D | 4 |
| B | D | 4 |
| C | D | 4 |
| D | D | 4 |

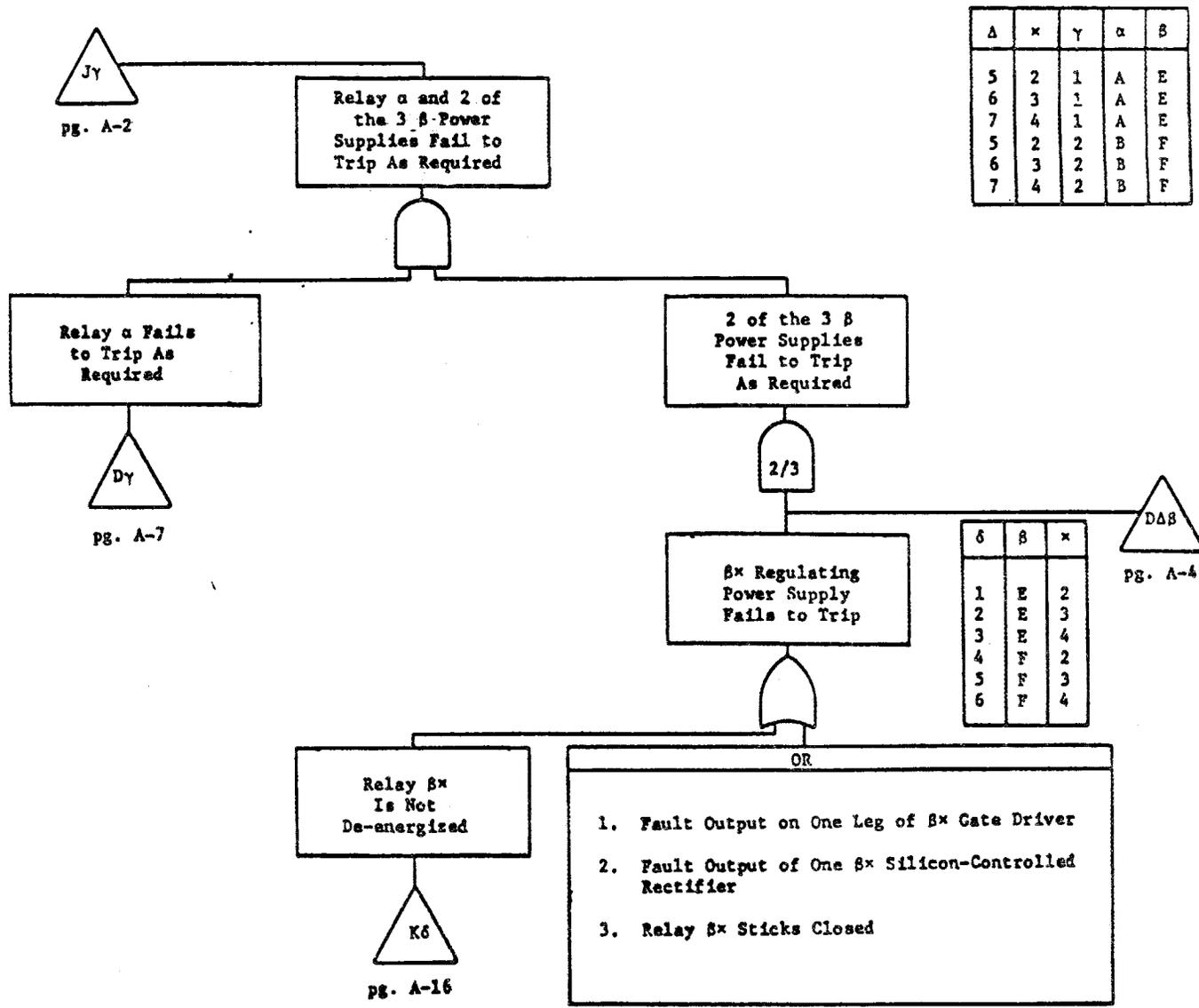


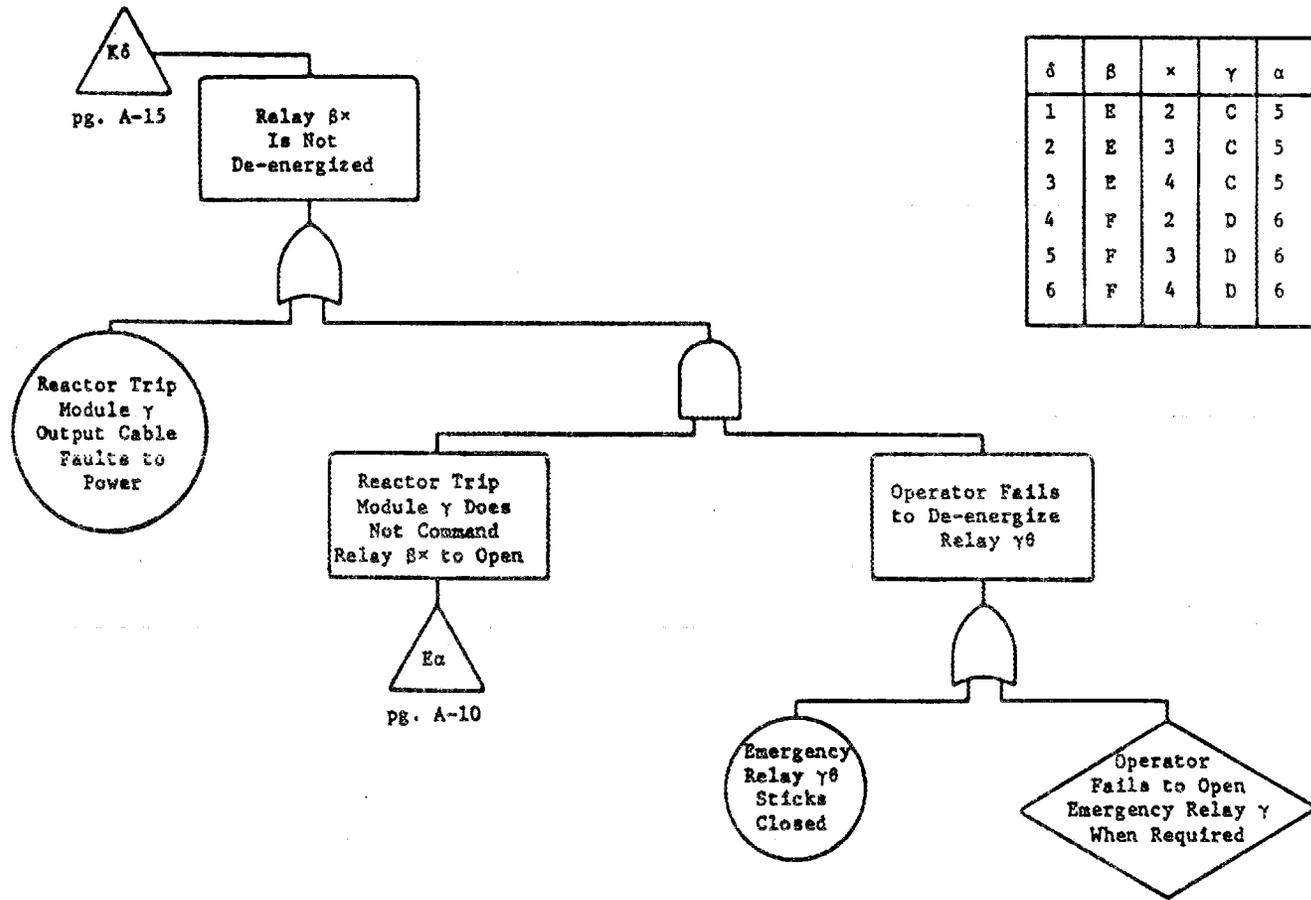


| |
|----------|
| γ |
| A |
| B |
| C |
| D |

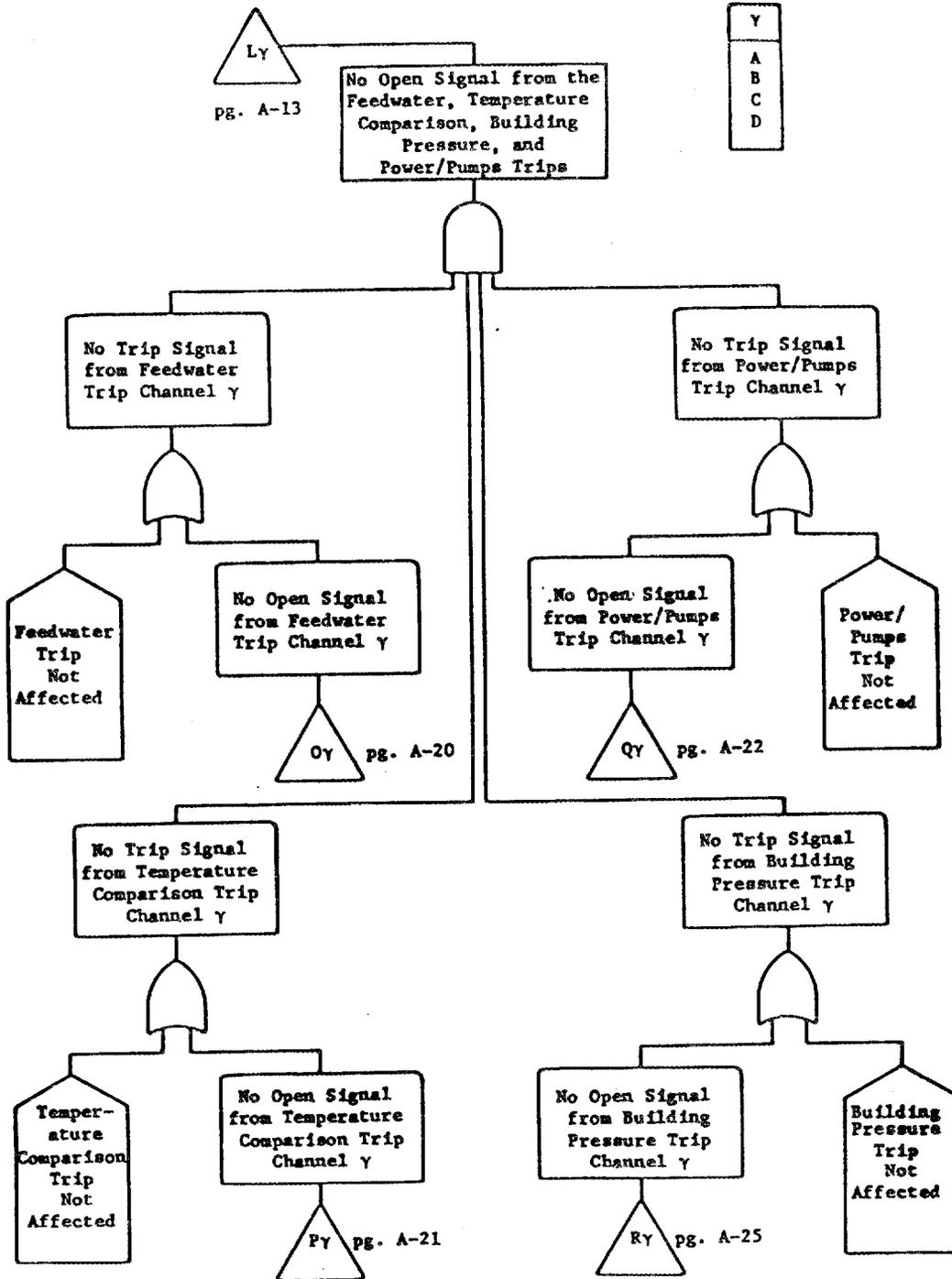


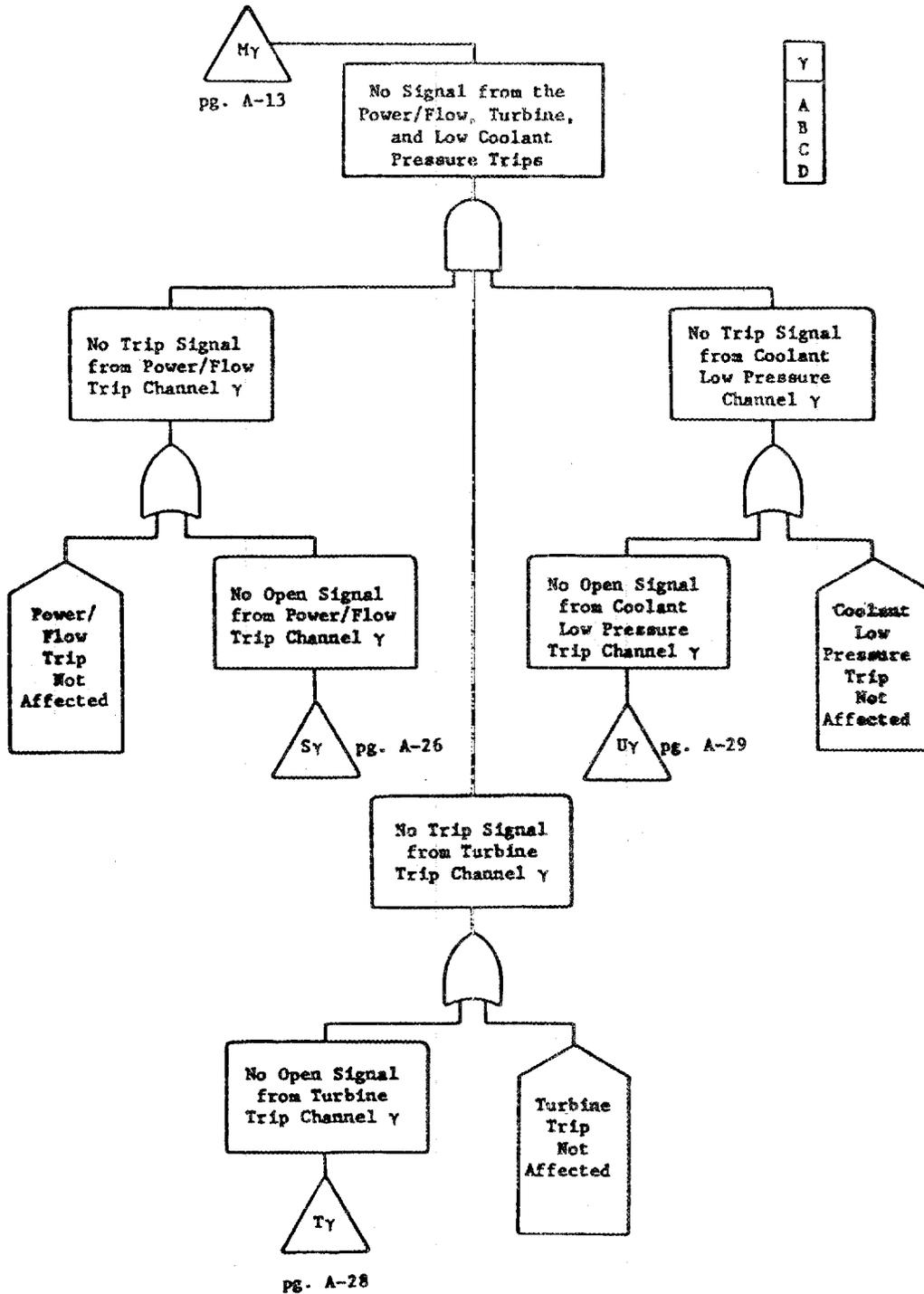
| δ | α | γ | θ |
|----------|----------|----------|----------|
| 3 | 1 | C | 1 |
| 3 | 2 | C | 2 |
| 4 | 3 | D | 1 |
| 4 | 4 | D | 2 |

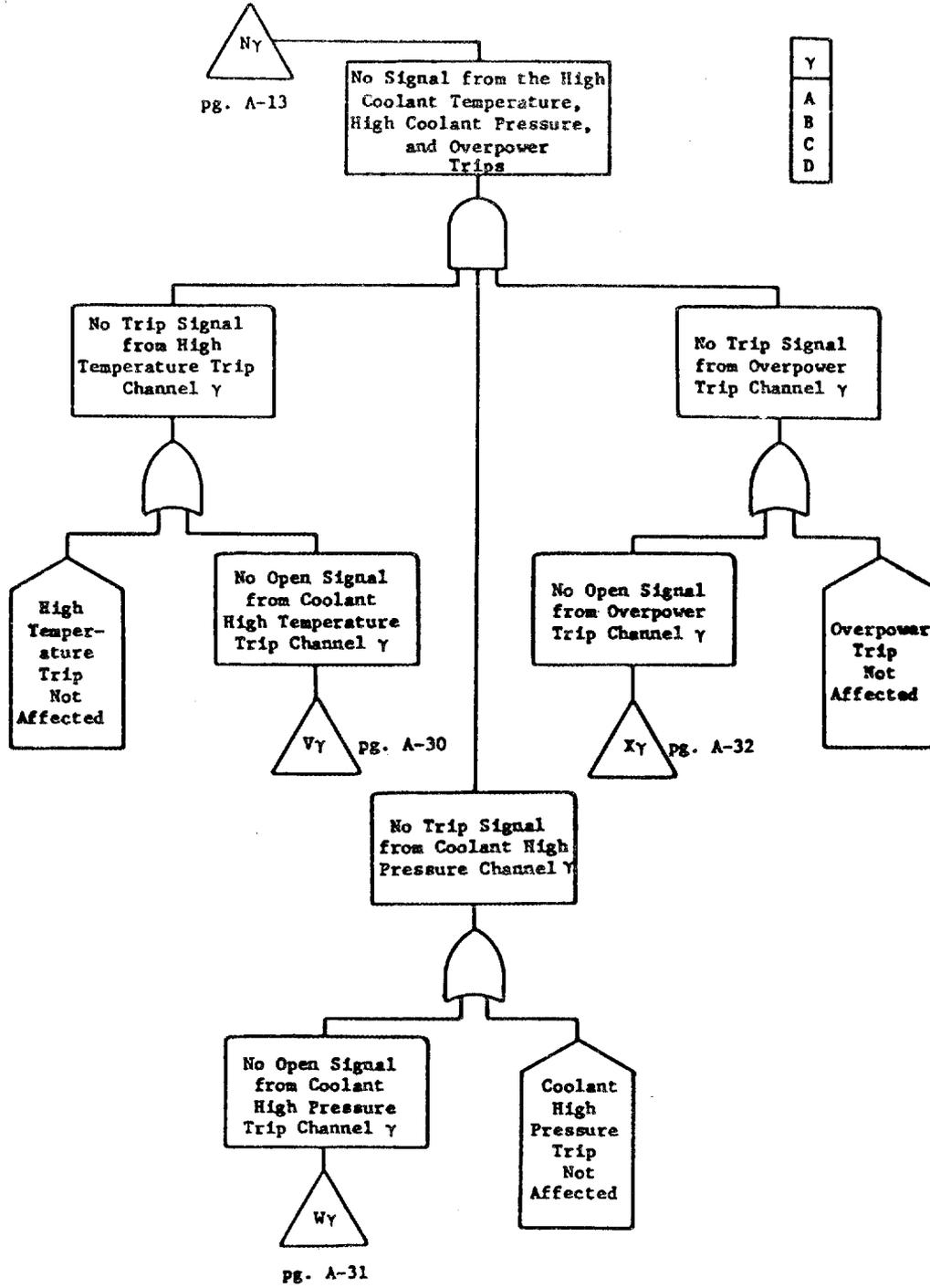


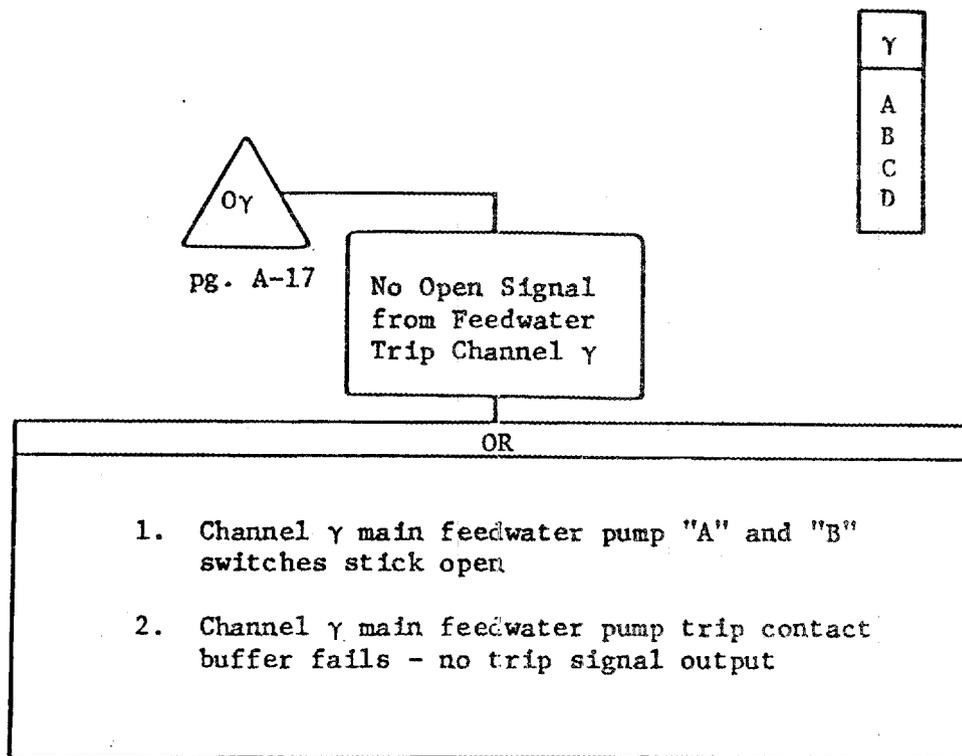


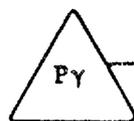
| δ | β | x | γ | α |
|---|---|---|---|---|
| 1 | E | 2 | C | 5 |
| 2 | E | 3 | C | 5 |
| 3 | E | 4 | C | 5 |
| 4 | F | 2 | D | 6 |
| 5 | F | 3 | D | 6 |
| 6 | F | 4 | D | 6 |





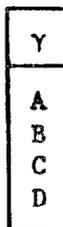






pg. A-17

No Open Signal
from Temperature
Comparison Trip
Channel γ



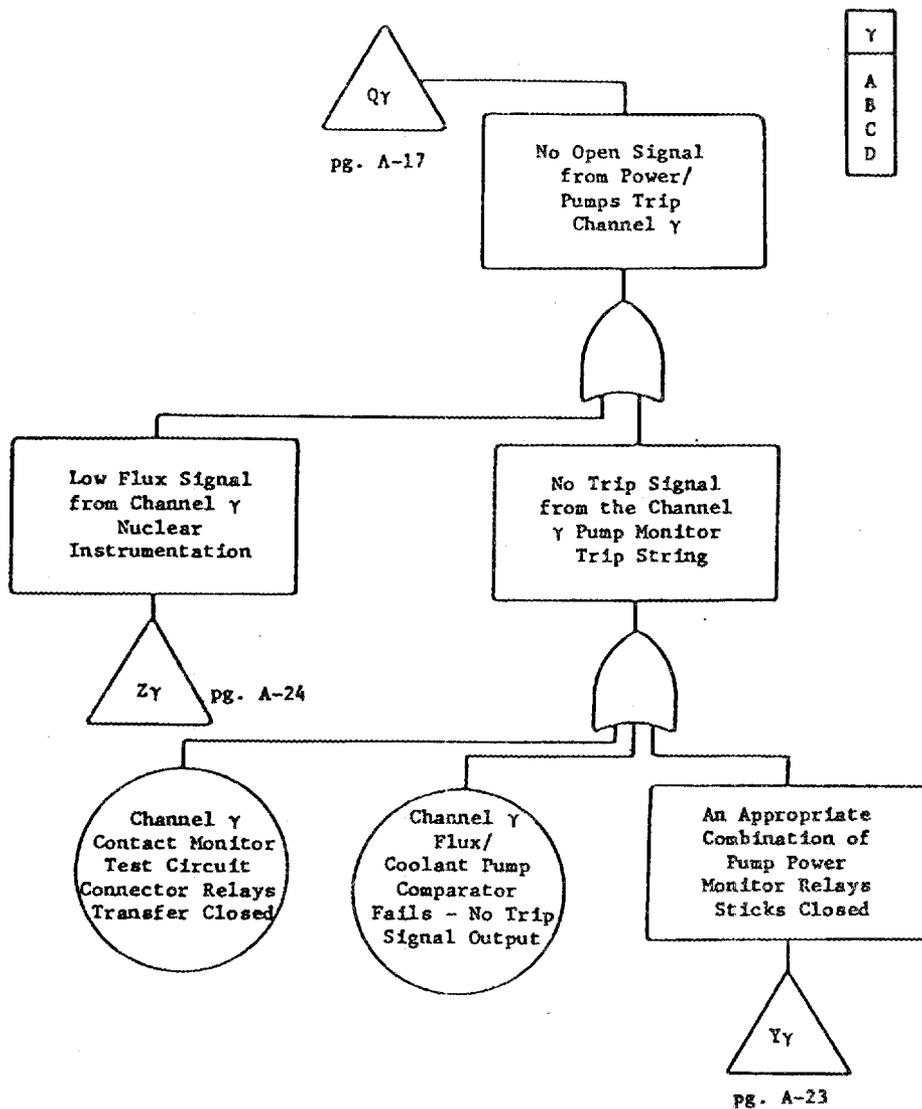
OR

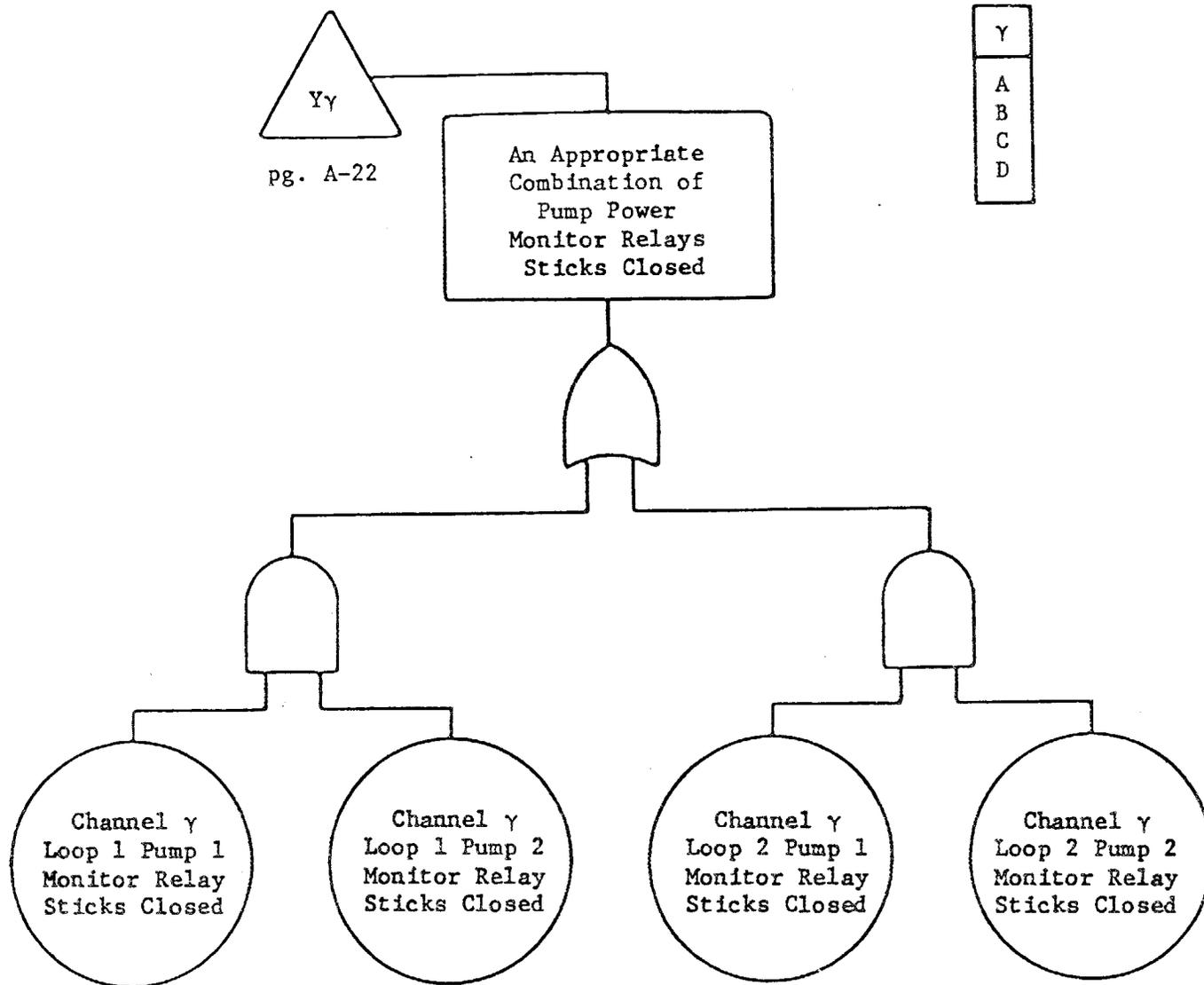
Temperature Signal is Low

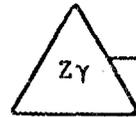
1. Channel γ RTD fails - low temperature signal output
2. Channel γ RTD output cable fails - low signal
3. Channel γ Rosemount linear bridge fails - low temperature signal output
4. Channel γ temperature test circuit - bridge connector relays transfer closed
5. Channel γ temperature test circuit - signal converter cable fails - low signal
6. Channel γ signal converter fails - low temperature signal output
7. Channel γ signal converter output cable to P < T comparator fails - low temperature signal
8. Channel γ power supply into the bridge fails - low voltage

Pressure Signal is High

9. Channel γ pressure sensor fails - high signal
10. Channel γ pressure test circuit - buffer amplifier connector relays transfer closed (false input signal)
11. Channel γ pressure buffer amplifier fails - incorrect signal (high)
12. Channel γ pressure sensor power supply fails - wrong voltage
13. P < T comparator fails - no trip signal output

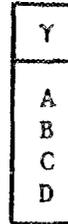






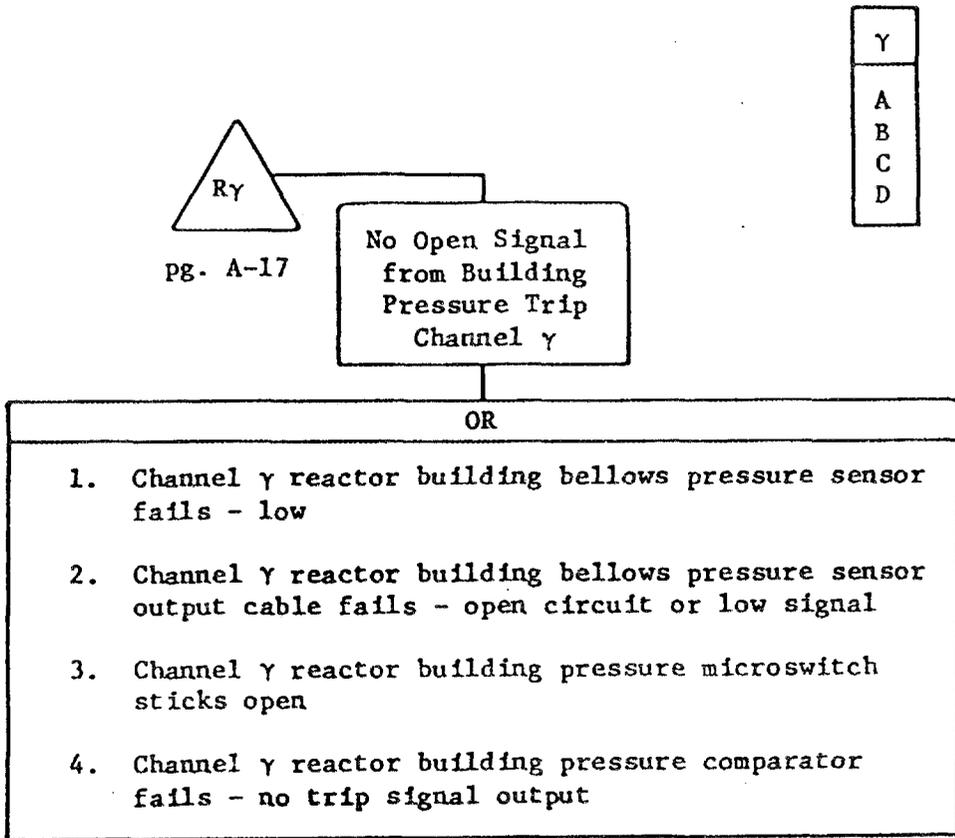
Pg. A-22

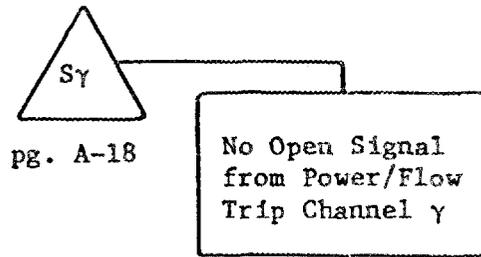
Low Flux Signal
from Channel γ
Nuclear
Instrumentation



OR

1. Channel γ flux detector power supply fails - low voltage
2. Channel γ flux detector power supply output cable fails - open circuit, grounded or degraded
3. Channel γ flux detector (top and bottom) fails - low flux signal
4. Channel γ flux detector output cables fail - degraded
5. Channel γ linear amplifier (top) fails - low flux signal output
6. Channel γ linear amplifier (bottom) fails - low flux signal output
7. Channel γ flux summer amplifier fails - low signal output
8. Channel γ flux summer amplifier output cable fails - open circuit, grounded or degraded
9. Channel γ linear amplifier (top) output cable fails - degraded
10. Channel γ linear amplifier (bottom) output cable fails - degraded





Y

A

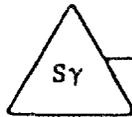
B

C

D

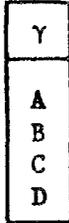
OR

1. Channel γ flux detector power supply fails - low voltage
2. Channel γ flux detector power supply output cable fails - open circuit or low voltage
3. Channel γ flux detector fails (top and bottom) - low flux signal
4. Channel γ flux detector output cables (top and bottom) fail - open circuit or low signal
5. Channel γ linear amplifier (top) fails - low flux signal output
6. Channel γ linear amplifier (bottom) fails - low flux signal output
7. Channel γ linear amplifier (top) output cable fails - low flux signal
8. Channel γ linear amplifier (bottom) output cable fails - low flux signal
9. Channel γ difference amplifier fails - low output signal
10. Channel γ difference amplifier output cable fails - low signal output
11. Channel γ DP#1 sensor fails - high signal
12. Channel γ DP#2 sensor fails - high signal
13. Channel γ flow test circuit: connector relay to extractor transfers closed



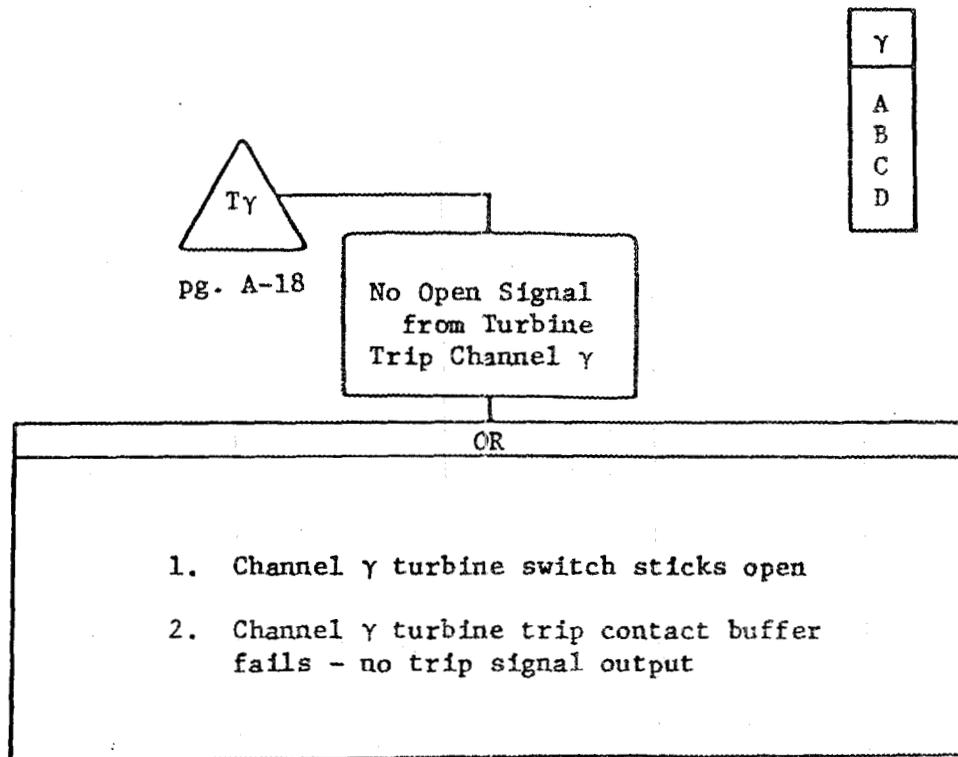
pg. A-18

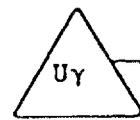
No Open Signal
from Power/Flow
Trip Channel γ



OR

14. Channel γ DP#1 sensor buffer amplifier fails - high signal
15. Channel γ DP#2 sensor buffer amplifier fails - high signal
16. Channel γ flow extractor #1 fails - high signal
17. Channel γ flow extractor #2 fails - high signal
18. Channel γ flow summer amplifier fails - high signal
19. Channel γ function generator fails - no trip signal
20. Channel γ function generator output cable fails - no trip signal
21. Channel γ power/flow comparator fails - no trip signal output



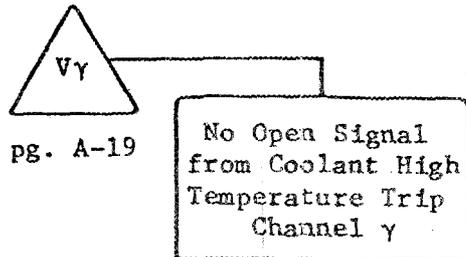


pg. A-18

No Open Signal
from Coolant Low
Pressure Trip
Channel γ

| |
|---|
| Y |
| A |
| B |
| C |
| D |

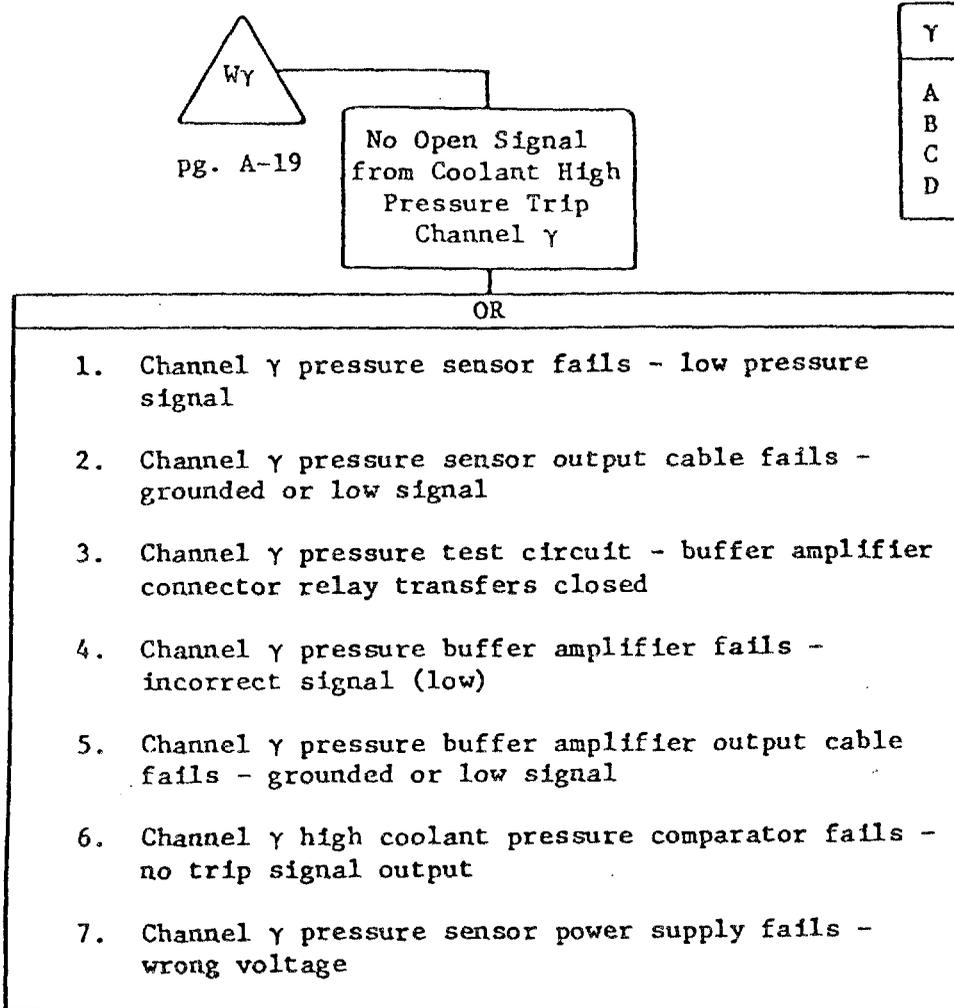
- OR
1. Channel γ pressure sensor fails - high signal
 2. Channel γ pressure test circuit - buffer amplifier connector relays transfer closed
 3. Channel γ pressure buffer amplifier fails - incorrect signal (high)
 4. Channel γ low coolant pressure comparator fails - no trip signal output
 5. Channel γ pressure sensor power supply fails - wrong voltage

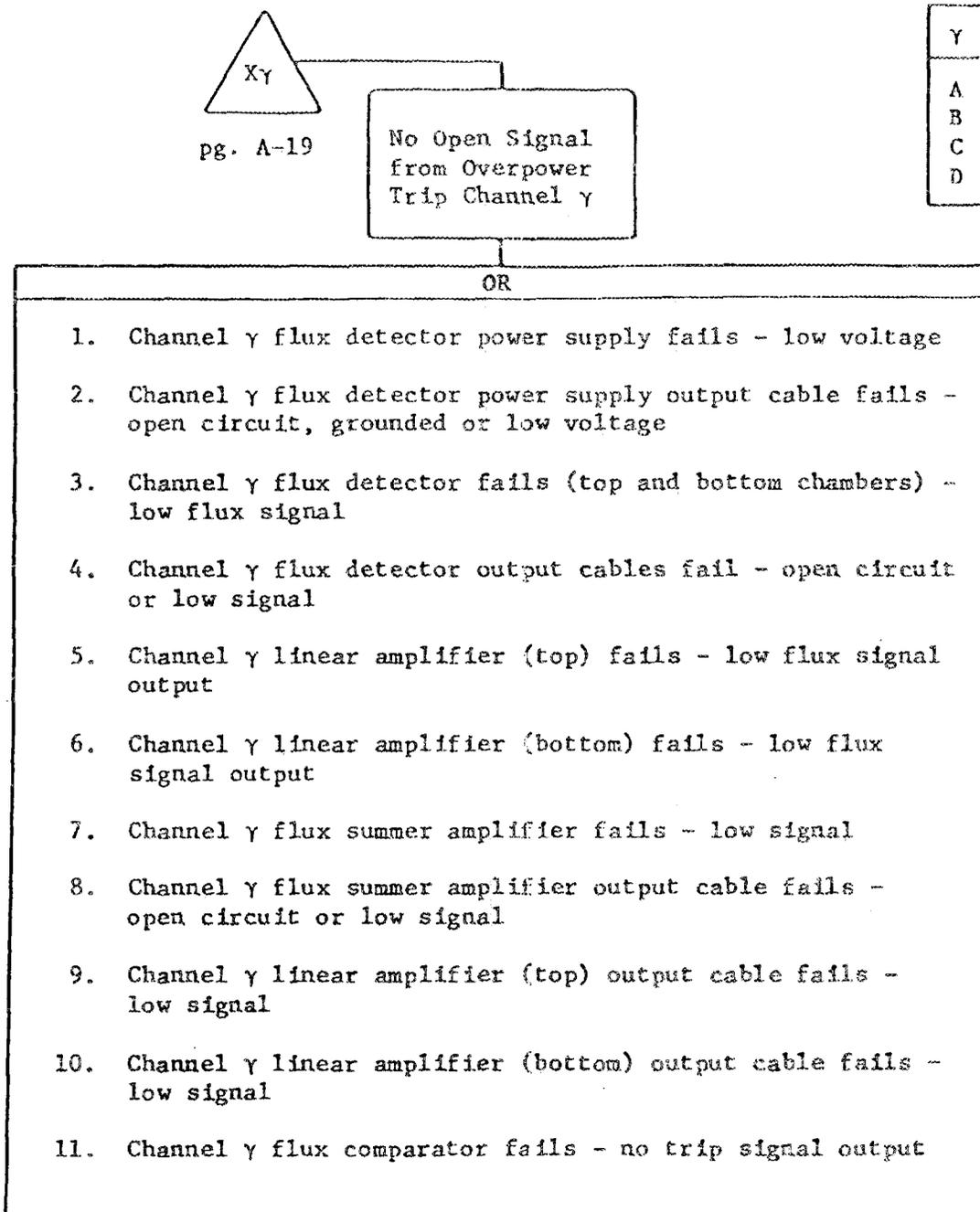


| |
|---|
| Y |
| A |
| B |
| C |
| D |

OR

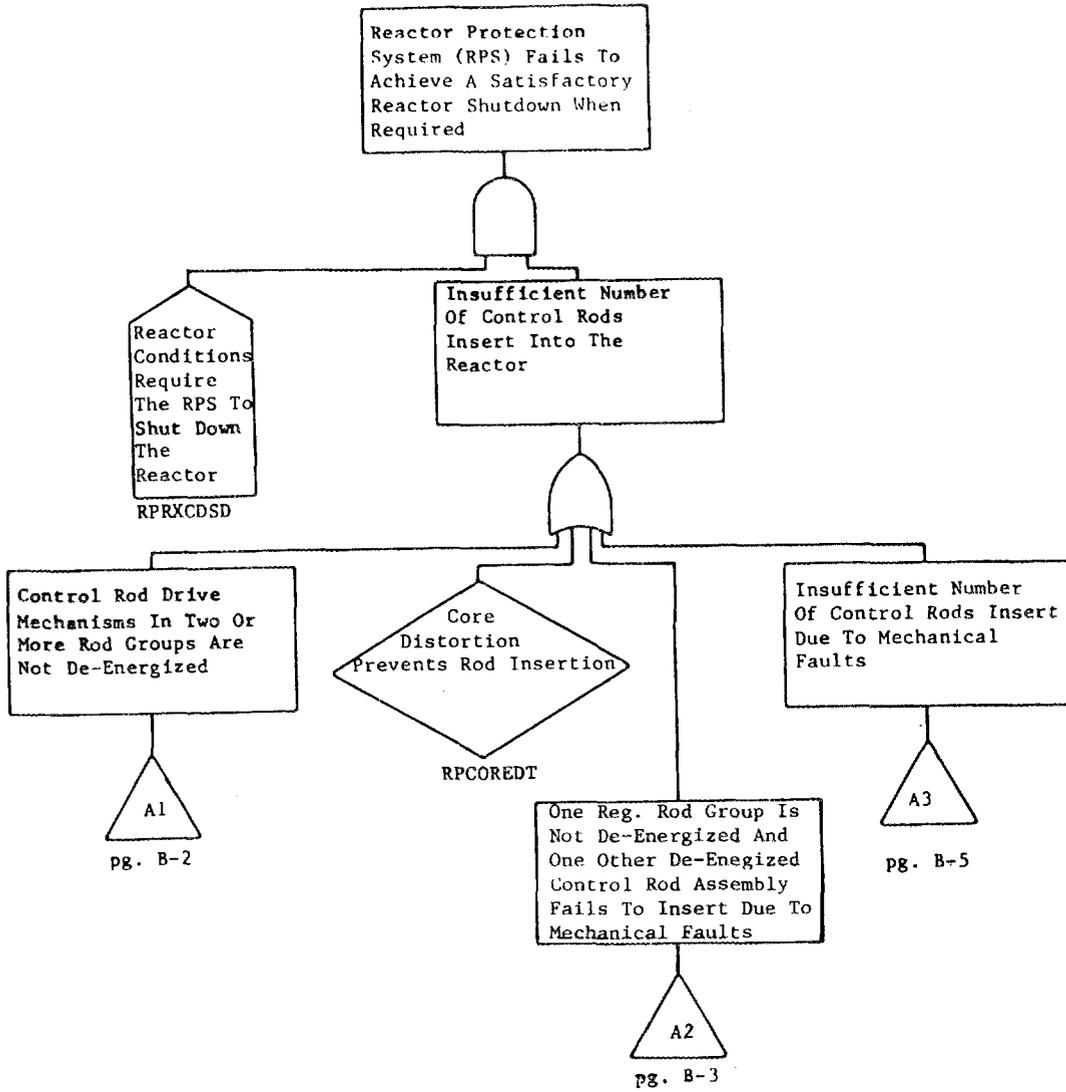
1. Channel γ RTD fails - low temperature signal output
2. Channel γ RTD output cable fails - grounded or low signal
3. Channel γ Rosemount linear bridge fails - low temperature signal output
4. Channel γ temperature test circuit - bridge connection relays transfer closed
5. Channel γ temperature test circuit - signal converter cable fails - grounded or low signal
6. Channel γ signal converter fails - low temperature signal output
7. Channel γ signal converter to temperature comparator output cables fail - grounded or low signal
8. Channel γ temperature comparator fails - no trip signal output
9. Channel γ power supply into bridge fails - low voltage

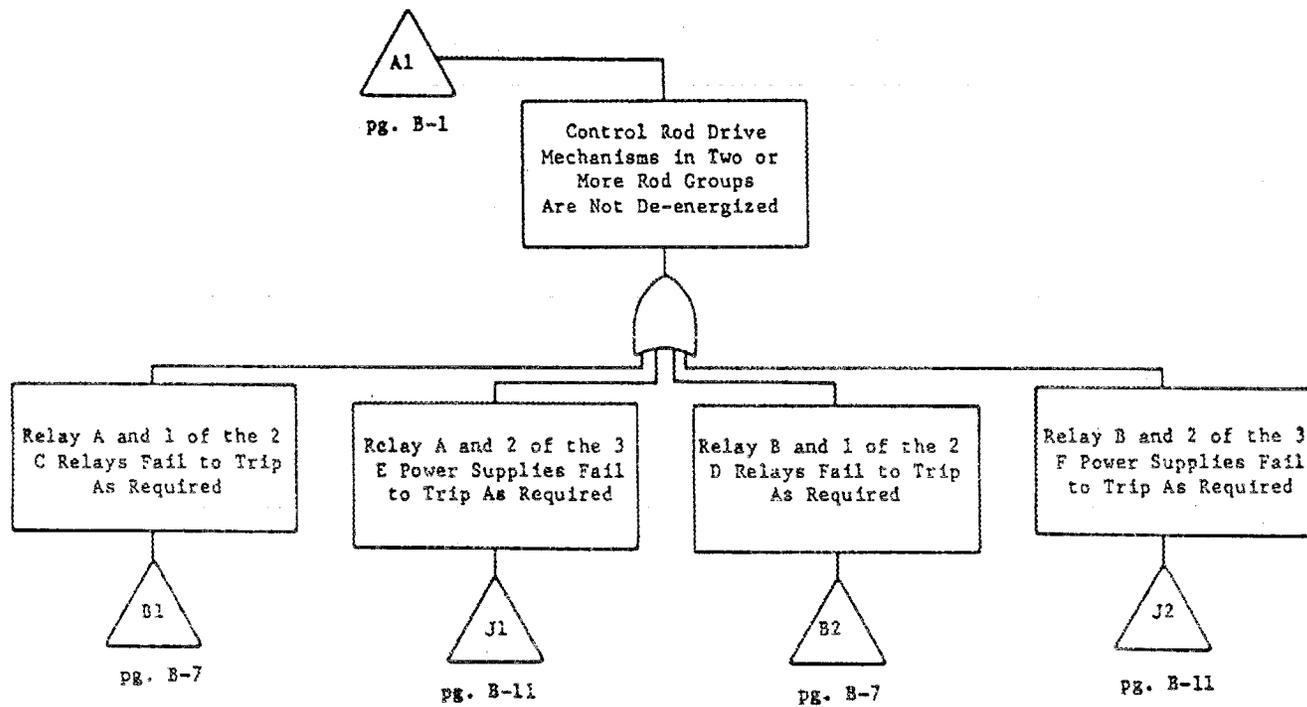


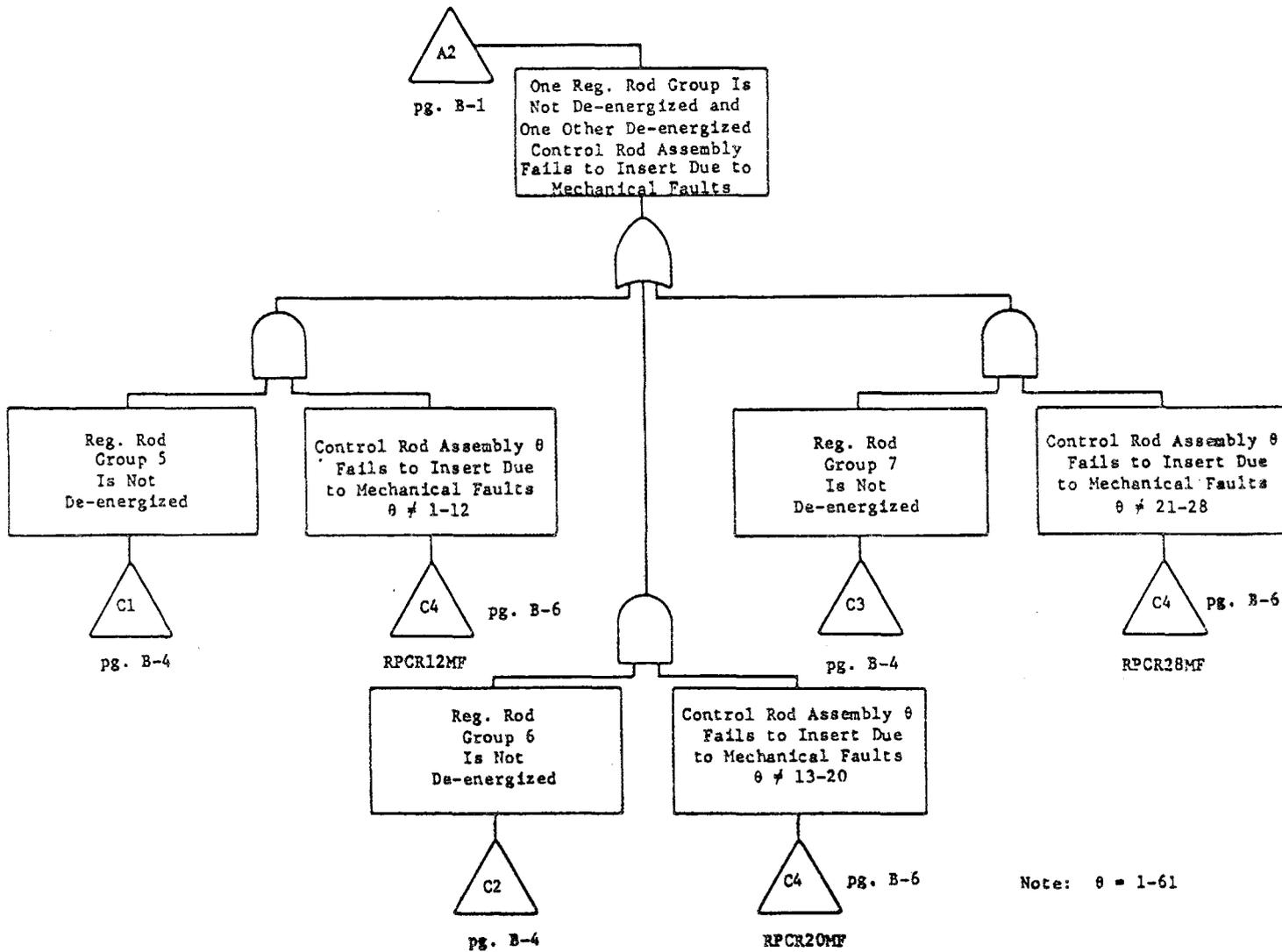


APPENDIX B

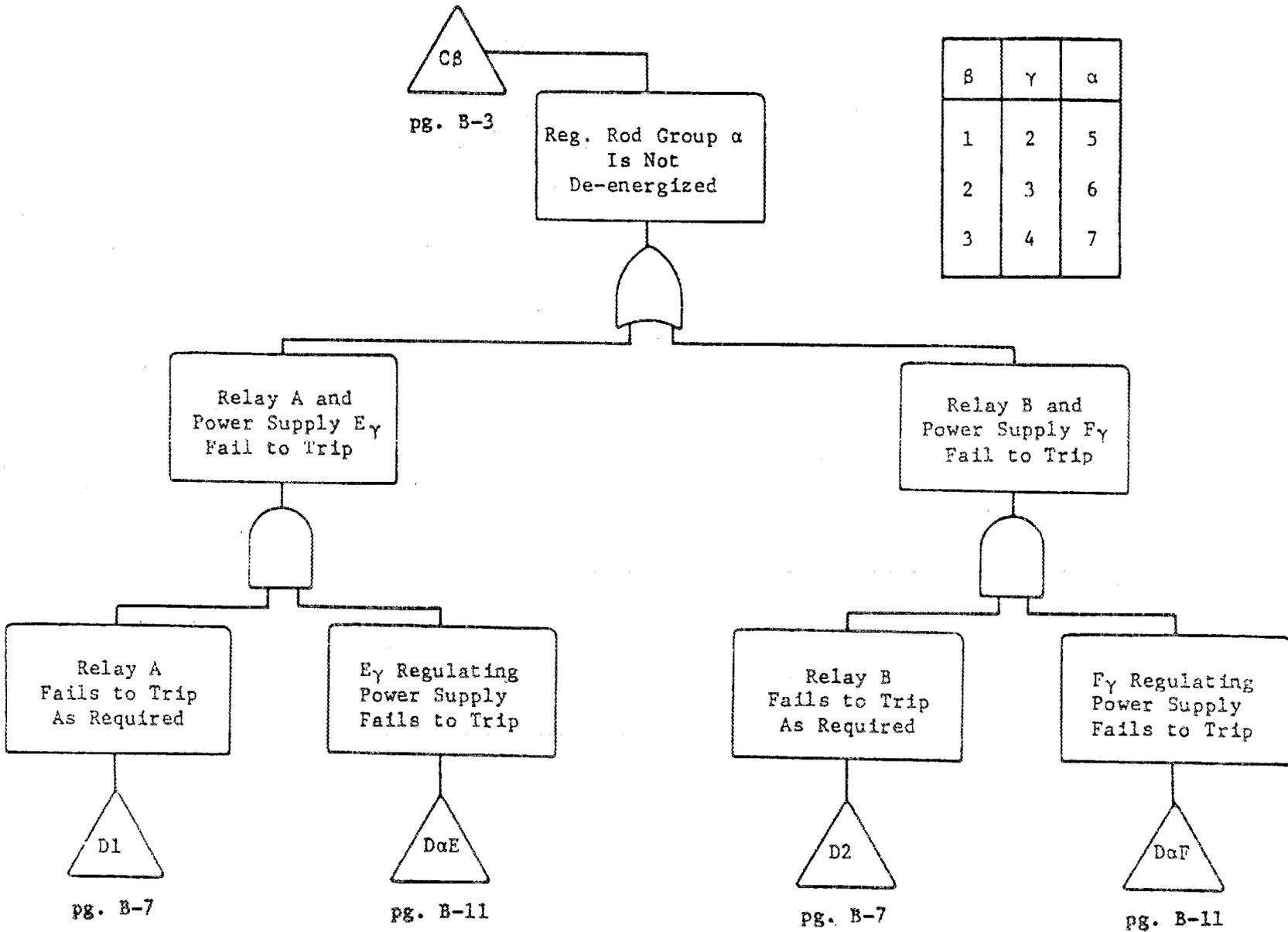
Reduced Fault Tree
of the ANG-1 Scram System

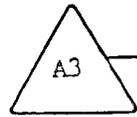






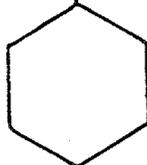
B-4





pg. B-1

Insufficient
Number of Control
Rods Insert Due
to Mechanical
Faults

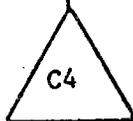


An Appropriate Set of
5 Control Rod Assemblies
Fails to Insert Given 5
Control Rod Assemblies
Are Failed

RPCR05SC



Control Rod
Assembly θ Fails
to Insert Due to
Mechanical Faults

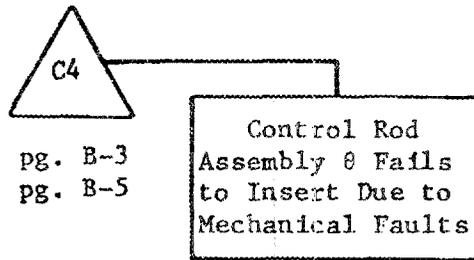


RPCR61MF

pg. B-6

Note: $\theta = 1-61$

B-6



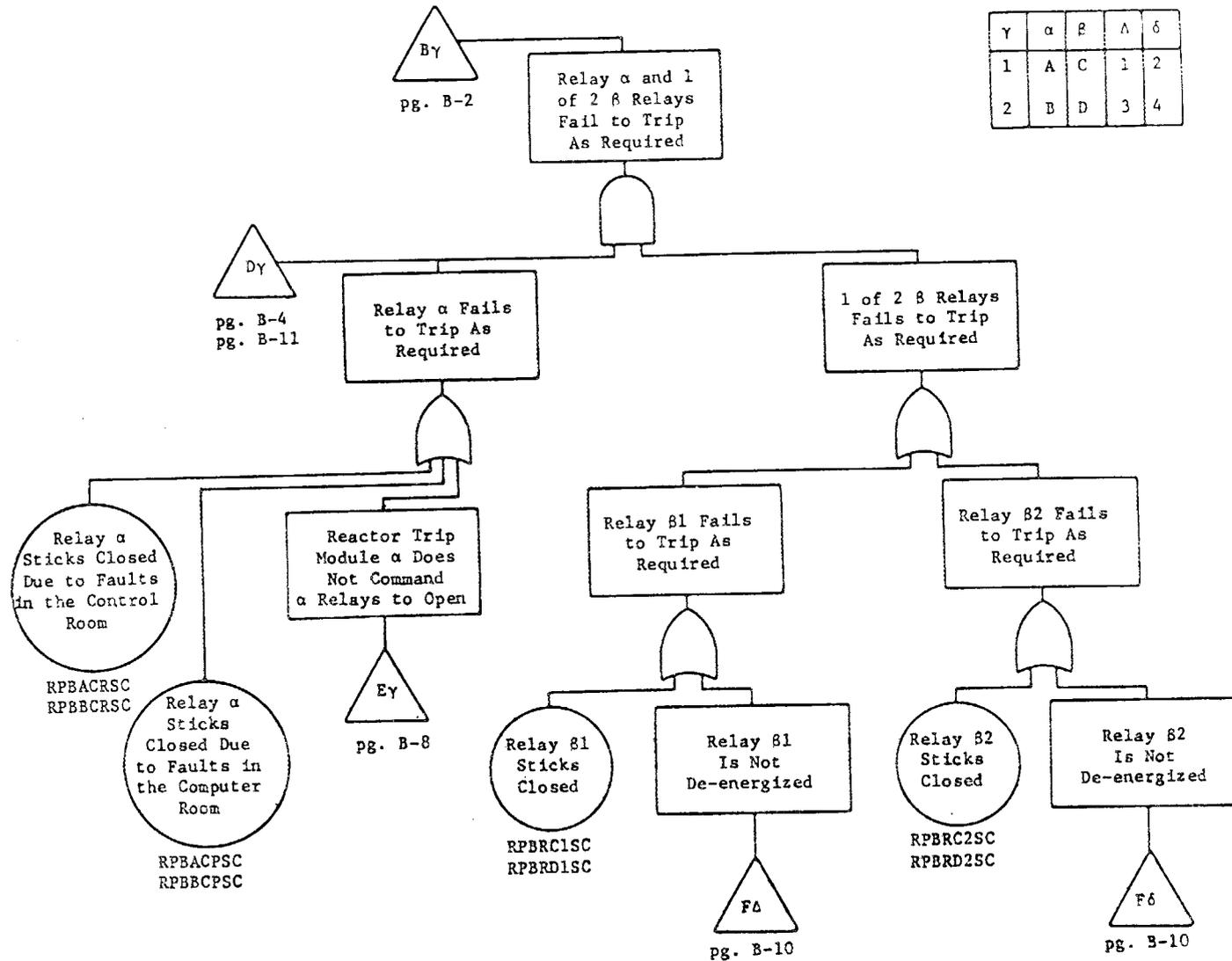
pg. B-3
pg. B-5

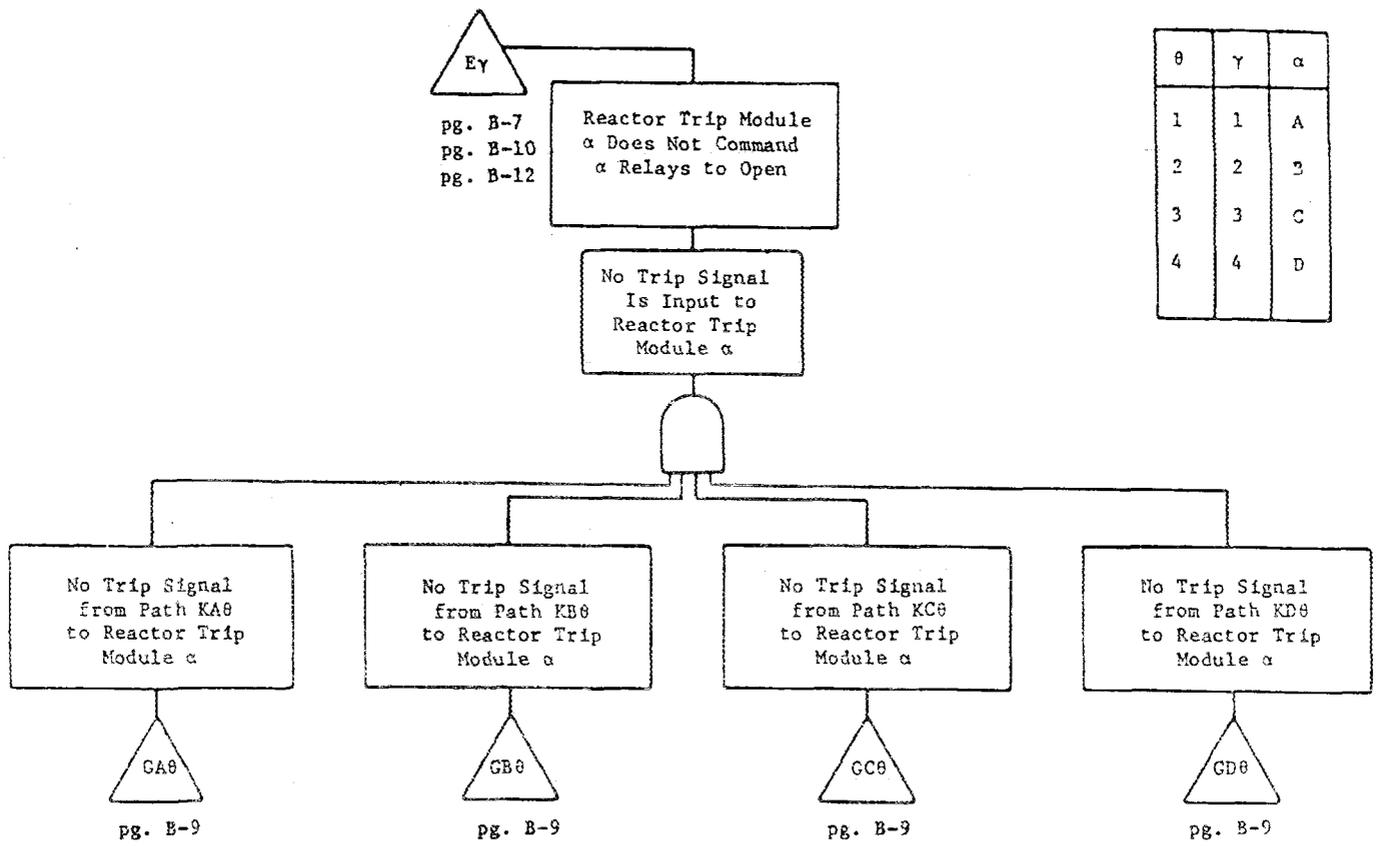
Control Rod
Assembly θ Fails
to Insert Due to
Mechanical Faults

OR

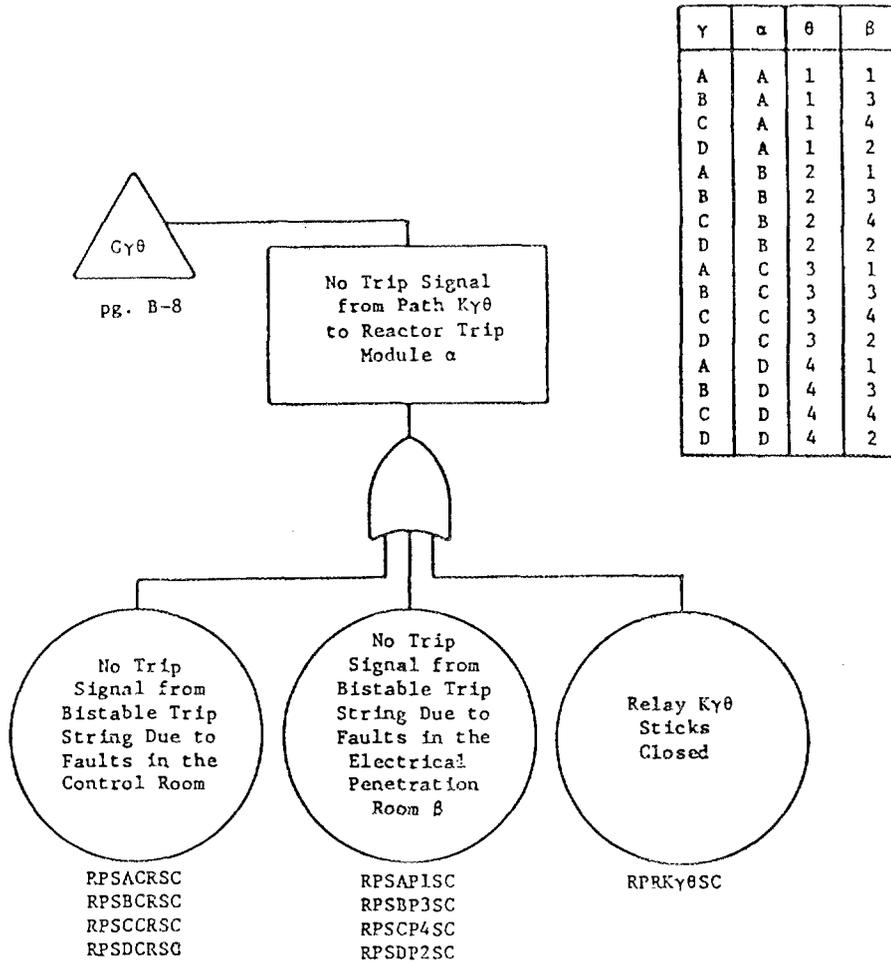
1. Segment arm springs fail - loss of compression
2. Segment arm assembly pivot pin fails - does not allow segment arms to pivot
3. Roller nuts fail - welded to lead screw
4. Lead screw fails - jammed
5. Upper guide bushing fails - jammed against lead screw
6. Lower guide bushing fails - jammed against lead screw
7. Driveline shaft fails - jammed
8. Piston and dashpot cup fail - jammed
9. Actuating shaft fails - jammed
10. Position indicator rod bushing fails - jammed against position indicator rod
11. Position indicator rod bushing fails - jammed against position indicator rod
12. Actuating shaft spring breaks
13. Loss of absorber material from the control rod assembly
14. Control rod guide tubes fail - warped or misaligned
15. Control rods fail - warped, misaligned, or swollen

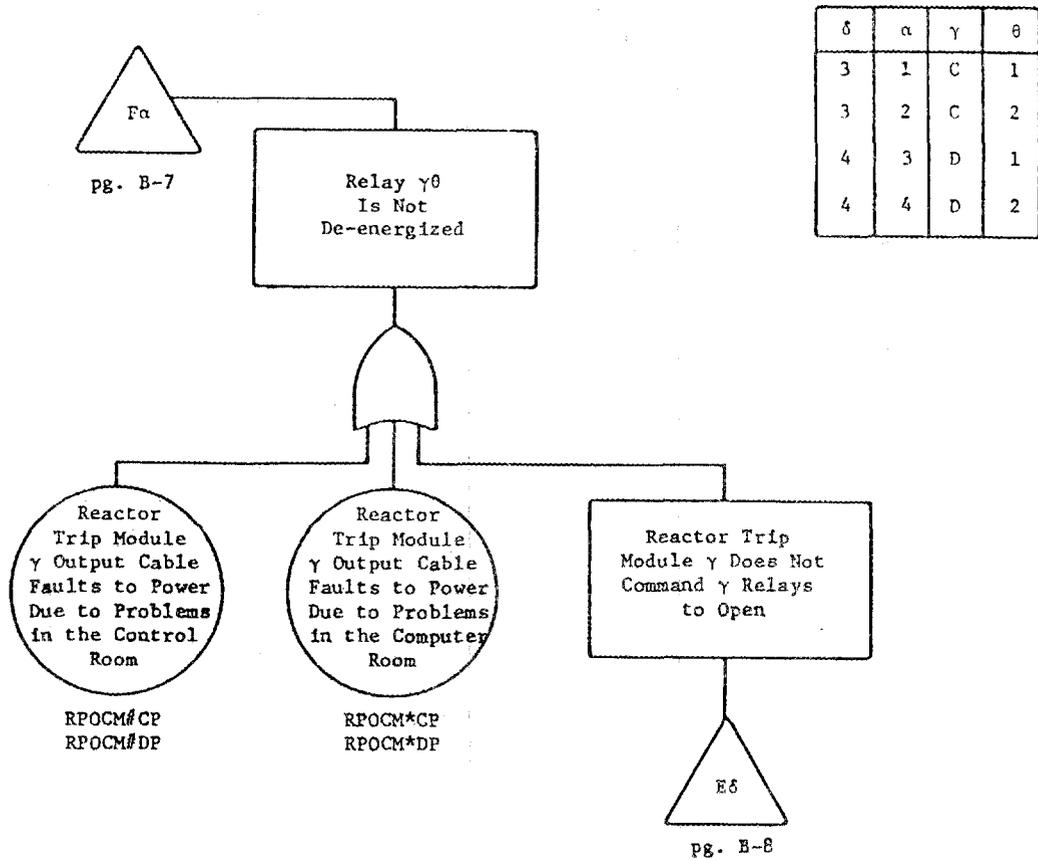
Note: θ = 1-61

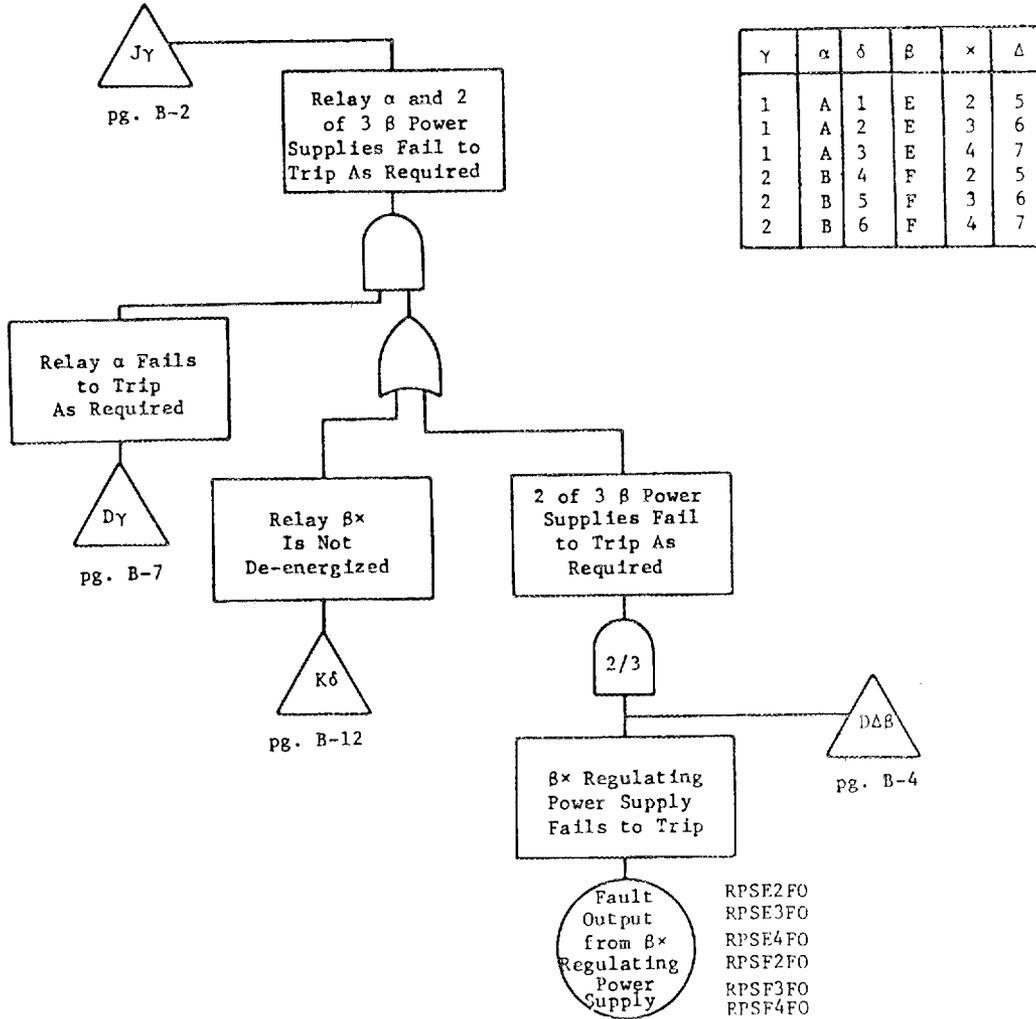


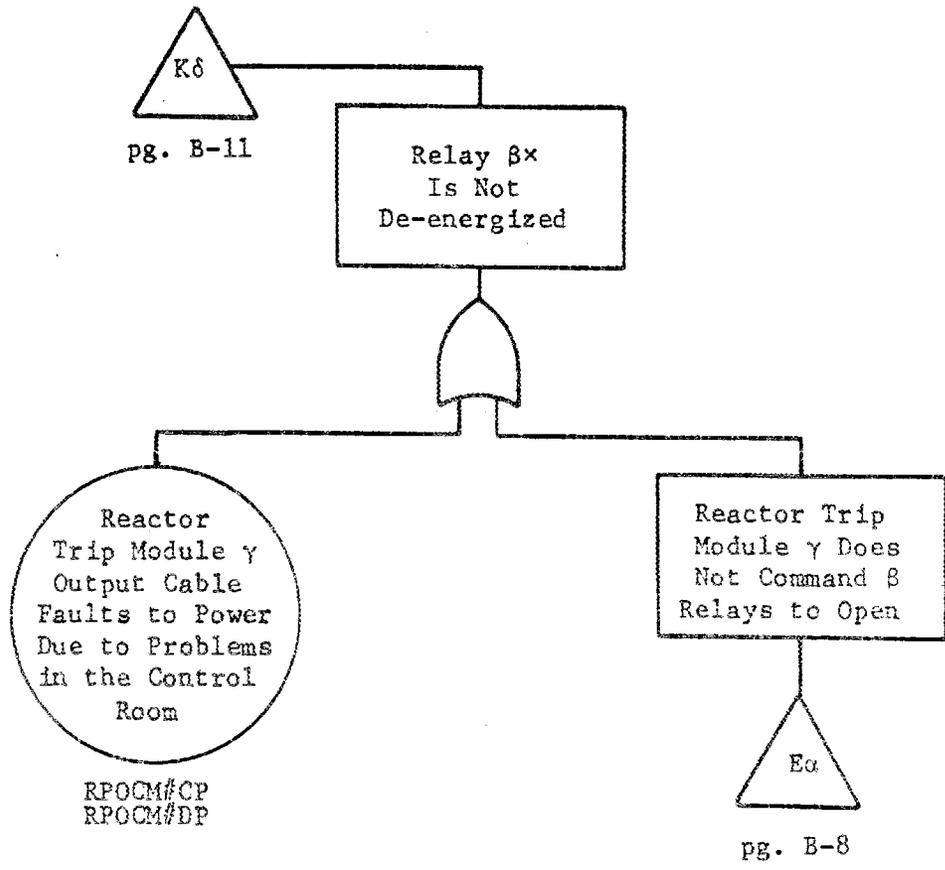


| θ | γ | α |
|---|---|---|
| 1 | 1 | A |
| 2 | 2 | B |
| 3 | 3 | C |
| 4 | 4 | D |









| δ | β | × | γ | α |
|---|---|---|---|---|
| 1 | E | 2 | C | 3 |
| 2 | E | 3 | C | 3 |
| 3 | E | 4 | C | 3 |
| 4 | F | 2 | D | 4 |
| 5 | F | 3 | D | 4 |
| 6 | F | 4 | D | 4 |

APPENDIX C

Basic Event Descriptions and Data

Table C.1 Basic Event Descriptions and Failure Data

| BASIC EVENT | FAILURE DESCRIPTION | FAILURE RATE (/hr or /demand) | MEAN DOWNTIME | UNAVAILABILITY |
|-------------|-------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------|-----------------------|
| RPCOREDT | Core distortion prevents rod insertion | ————— | ————— | ————— |
| RPCR12MF | Control rod assembly θ ($\theta = 1-12$) fails to insert - mechanical faults | $49(10^{-4}/d)$ | | 4.9×10^{-3} |
| RPCR20MF | Control rod assembly θ ($\theta = 13-20$) fails to insert - mechanical faults | $53(10^{-4}/d)$ | | 5.3×10^{-3} |
| RPCR28MF | Control rod assembly θ ($\theta = 21-28$) fails to insert - mechanical faults | $53(10^{-4}/d)$ | | 5.3×10^{-3} |
| RPCR61MF | Control rod assembly θ ($\theta = 1-61$) fails to insert - mechanical faults (any 5 assemblies) | $(61)(10^{-4}/d)^5$ 5 | | 5.9×10^{-14} |
| RPCR05SC | Sufficiency condition - appropriate set of 5 control rod assemblies fails to insert given 5 assemblies are failed | | | 9.6×10^{-6} |
| RPBACRSC | Relay A sticks closed (faults in the control room) | | | |
| | input cable faults to power (1/2 of cable) | $0.5 \times 10^{-8}/hr$ | 360 | 1.8×10^{-6} |
| RPBACPSC | Relay A sticks closed (faults in the control room) | | | |
| | breaker sticks closed | $1.0 \times 10^{-3}/d$ | | 1.0×10^{-3} |

Table C.1 (continued)

| BASIC EVENT | FAILURE DESCRIPTION | FAILURE RATE (/hr or /demand) | MEAN DOWNTIME | UNAVAILABILITY |
|-------------|--------------------------------------------------------|----------------------------------|------------------|----------------------|
| RPBBCRSC | Relay B sticks closed (faults in the control room) | | | |
| | input cable faults to power (1/2 of cable) | $0.5 \times 10^{-8}/\text{hr}$ | 360 | 1.8×10^{-6} |
| RPBBCPSC | Relay B sticks closed (faults in the computer room) | | | |
| | breaker sticks closed | $1.0 \times 10^{-3}/\text{d}$ | | 1.0×10^{-3} |
| RPBRC1SC | Relay C1 sticks closed | | | |
| | breaker sticks closed | $1.0 \times 10^{-3}/\text{d}$ | | 1.0×10^{-3} |
| RPBRD1SC | Relay D1 sticks closed | | | |
| | breaker sticks closed | $1.0 \times 10^{-3}/\text{d}$ | | 1.0×10^{-3} |
| RPBRC2SC | Relay C2 sticks closed | | | |
| | breaker sticks closed | $1.0 \times 10^{-3}/\text{d}$ | | 1.0×10^{-3} |
| RPBRD2SC | Relay D2 sticks closed | | | |
| | breaker sticks closed | $1.0 \times 10^{-3}/\text{d}$ | | 1.0×10^{-3} |

Table C.1 (continued)

| BASIC EVENT | FAILURE DESCRIPTION | FAILURE RATE (/hr or /demand) | MEAN DOWNTIME | UNAVAILABILITY |
|-------------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|------------------|-------------------------|
| RPSACRSC | Bistable Trip String A fails to output a trip signal (faults in the control room) | | | 2.24 x 10 ⁻² |
| | signal processing equipment fails - no trip | 1.7 x 10 ⁻⁷ /d | | |
| | Bistable Trip String Relay KA sticks closed Bistable Trip String A out of service for testing and maintenance | 1.0 x 10 ⁻⁸ /hr 4(1.4 x 10 ⁻³ /hr) | 360 4 | |
| RPSBCRSC | Bistable Trip String B fails to output a trip signal (faults in the control room) | | | 3.8 x 10 ⁻⁶ |
| | signal processing equipment fails - no trip | 1.7 x 10 ⁻⁷ /d | | |
| | Bistable Trip String Relay KA sticks closed | 1.0 x 10 ⁻⁸ /hr | 360 | |
| RPSCCRSC | Bistable Trip String C fails to output a trip signal (faults in the control room) | | | 3.8 x 10 ⁻⁶ |
| | signal processing equipment fails - no trip | 1.7 x 10 ⁻⁷ /d | | |
| | Bistable Trip String Relay KC sticks closed | 1.0 x 10 ⁻⁸ /hr | 360 | |

C-4

Table C.1 (continued)

| BASIC EVENT | FAILURE DESCRIPTION | FAILURE RATE (/hr or /demand) | MEAN DOWNTIME | UNAVAILABILITY |
|-------------|---------------------------------------------------------------------------------------|--------------------------------------|------------------|-----------------------|
| RPSDCRSC | Bistable Trip String D fails to output a trip signal (faults in the control room) | | | 3.8×10^{-6} |
| | signal processing equipment fails - no trip | $1.7 \times 10^{-7}/d$ | | |
| | Bistable Trip String Relay KD sticks closed | $1.0 \times 10^{-8}/hr$ | 360 | |
| RPSAP1SC | Bistable Trip String A fails to output a trip signal (faults in the penetration room) | | | |
| | sensor output signal cables fault to power (3 cables) | $1.0 \times 10^{-8}/hr$ per cable | 360 | 4.7×10^{-17} |
| RPSBP3SC | Bistable Trip String B fails to output a trip signal (faults in the penetration room) | | | |
| | sensor output signal cables fault to power (3 cables) | $1.0 \times 10^{-8}/hr$ per cable | 360 | 4.7×10^{-17} |
| RPSCP4SC | Bistable Trip String C fails to output a trip signal (faults in the penetration room) | | | |
| | sensor output signal cables fault to power (3 cables) | $1.0 \times 10^{-8}/hr$ per cable | 360 | 4.7×10^{-17} |
| RPSDP1SC | Bistable Trip String D fails to output a trip signal (faults in the control room) | | | |
| | sensor output signal cables fault to power (3 cables) | $1.0 \times 10^{-8}/hr$ per cable | 360 | 4.7×10^{-17} |

Table C.1 (continued)

| BASIC EVENT | FAILURE DESCRIPTION | FAILURE RATE (/hr or /demand) | MEAN DOWNTIME | UNAVAILABILITY |
|-------------|-----------------------------------------------|------------------------------------------------------------------|------------------|----------------------|
| RPRKA1SC | Relay KA1 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKA2SC | Relay KA2 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRK3ASC | Relay KA3 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKA4SC | Relay KA4 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKB1SC | Relay KB1 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKB2SC | Relay KB2 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |

Table C.1 (continued)

| BASIC EVENT | FAILURE DESCRIPTION | FAILURE RATE (/hr or /demand) | MEAN DOWNTIME | UNAVAILABILITY |
|-------------|-----------------------------------------------|------------------------------------------------------------------|------------------|----------------------|
| RPRKB3SC | Relay KB3 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKB4SC | Relay KB4 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKC1SC | Relay KC1 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKC2SC | Relay KC2 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKC3SC | Relay KC3 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKC4SC | Relay KC4 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |

Table C.1 (continued)

| BASIC EVENT | FAILURE DESCRIPTION | FAILURE RATE (/hr or /demand) | MEAN DOWNTIME | UNAVAILABILITY |
|-------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------|------------------|----------------------|
| RPRKD1SC | Relay KD1 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKD2SC | Relay KD2 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKD3SC | Relay KD3 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPRKD4SC | Relay KD4 sticks closed | | | 7.2×10^{-6} |
| | relay sticks closed cable faults to ground | $1.0 \times 10^{-8}/\text{hr}$ $1.0 \times 10^{-8}/\text{hr}$ | 360 360 | |
| RPOCM#CP | Reactor Trip Module C Output Cable faults to power (faults in the control room) (1/2 of cable) | $0.5 \times 10^{-8}/\text{hr}$ | 360 | 1.8×10^{-6} |
| RPOCM#DP | Reactor Trip Module D Output Cable faults to power (faults in the control room) (1/2 of cable) | $0.5 \times 10^{-8}/\text{hr}$ | 360 | 1.8×10^{-6} |

Table C.1 (continued)

| BASIC EVENT | FAILURE DESCRIPTION | FAILURE RATE (/hr or /demand) | MEAN DOWNTIME | UNAVAILABILITY |
|-------------|-------------------------------------------------------------------------------------------------|----------------------------------|------------------|-----------------------|
| RPOCM*CP | Reactor Trip Module C Output Cable faults to power (faults in the computer room) (1/2 of cable) | $0.5 \times 10^{-8}/\text{hr}$ | 360 | 1.80×10^{-6} |
| RPOCM*DP | Reactor Trip Module D Output Cable faults to power (faults in the computer room) (1/2 of cable) | $0.5 \times 10^{-8}/\text{hr}$ | 360 | 1.80×10^{-6} |
| RPPSE2FO | Fault output from E2 regulating power supply | | | 1.35×10^{-3} |
| | Relay E2 sticks closed | $1.0 \times 10^{-8}/\text{hr}$ | 360 | |
| | Gate Drive E2 fails - power on | $1.4 \times 10^{-7}/\text{hr}$ | 360 | |
| | E2 silicon-controlled rectifiers fail - power output | $36(10^{-7}/\text{hr})$ | 360 | |
| RPPSE3FO | Fault output from E3 regulating power supply | | | 1.35×10^{-3} |
| | Relay E3 sticks closed | $1.0 \times 10^{-8}/\text{hr}$ | 360 | |
| | Gate Drive E3 fails - power on | $1.4 \times 10^{-7}/\text{hr}$ | 360 | |
| | E3 silicon-controlled rectifiers fail - power output | $36(10^{-7}/\text{hr})$ | 360 | |
| RPPSE4FO | Fault output from E4 regulating power supply | | | 1.35×10^{-3} |
| | Relay E4 sticks closed | $1.0 \times 10^{-8}/\text{hr}$ | 360 | |
| | Gate Drive E4 fails - power on | $1.4 \times 10^{-7}/\text{hr}$ | 360 | |
| | E4 silicon-controlled rectifiers fail - power output | $36(10^{-7}/\text{hr})$ | 360 | |

Table C.1 (continued)

| BASIC EVENT | FAILURE DESCRIPTION | FAILURE RATE (/hr or /demand) | MEAN DOWNTIME | UNAVAILABILITY |
|-------------|---------------------------------------------------------|----------------------------------|------------------|-----------------------|
| RPPSF2FO | Fault output from F2 regulating power supply | | | 1.35×10^{-3} |
| | Relay F2 sticks closed | $1.0 \times 10^{-8}/\text{hr}$ | 360 | |
| | Gate Drive F2 fails - power on | $1.4 \times 10^{-8}/\text{hr}$ | 360 | |
| | F2 silicon-controlled rectifiers fail - power output | $36(10^{-7}/\text{hr})$ | 360 | |
| RPPSF3FO | Fault output from F3 regulating power supply | | | 1.35×10^{-3} |
| | Relay F3 sticks closed | $1.0 \times 10^{-8}/\text{hr}$ | 360 | |
| | Gate Drive F3 fails - power on | $1.4 \times 10^{-7}/\text{hr}$ | 360 | |
| | F3 silicon-controlled rectifiers fail | $36(10^{-7}/\text{hr})$ | 360 | |
| RPPSF4FO | Fault output from F4 regulating power supply | | | 1.35×10^{-3} |
| | Relay F4 sticks closed | $1.0 \times 10^{-8}/\text{hr}$ | 360 | |
| | Gate Drive F4 fails - power on | $1.4 \times 10^{-7}/\text{hr}$ | 360 | |
| | F4 silicon-controlled rectifiers fail | $36(10^{-7}/\text{hr})$ | 360 | |

Table C.2 Reduced Fault Tree Basic Event Locations

| Basic Event | Location |
|-------------|---------------------|
| PRCR12MF | Containment |
| RPCR20MF | Containment |
| RPCR28MF | Containment |
| RPCR61MF | Containment |
| RPCR05SC | a |
| RPBACRSC | Control Room |
| RPBACPSC | Computer Room |
| RPBBCRSC | Control Room |
| RPBBCPSC | Computer Room |
| RPBRC1SC | Computer Room |
| RPBRD1SC | Computer Room |
| RPBRC2SC | Computer Room |
| RPBRD2SC | Computer Room |
| RPSACRSC | Control Room |
| RPSBCRSC | Control Room |
| RPSCCRSC | Control Room |
| RPSDCRSC | Control Room |
| RPSAP1SC | Penetration Room #1 |
| RPSBP3SC | Penetration Room #3 |

^aThis is an inhibit condition, not a component failure; it has no location.

Table C.2 (continued)

| Basic Event | Location |
|-------------|---------------------|
| RPSCP4SC | Penetration Room #4 |
| RPSDP2SC | Penetration Room #2 |
| RPRKA1SC | Control Room |
| RPRKA2SC | Control Room |
| RPRK3ASC | Control Room |
| RPRKA4SC | Control Room |
| RPRKB1SC | Control Room |
| RPRKB2SC | Control Room |
| RPRKB3SC | Control Room |
| RPRKB4SC | Control Room |
| RPRKC1SC | Control Room |
| RPRKC2SC | Control Room |
| RPRKC3SC | Control Room |
| RPRKC4SC | Control Room |
| RPRKD1SC | Control Room |
| RPRKD2SC | Control Room |
| RPRKD3SC | Control Room |
| RPRKD4SC | Control Room |
| RPOCM#CP | Control Room |
| RPOCM#DP | Control Room |
| RPOCM*CP | Computer Room |

Table C.2 (continued)

| Basic Event | Location |
|-------------|---------------|
| RPOCM*DP | Computer Room |
| RPPSE2FO | Computer Room |
| RPPSE3FO | Computer Room |
| RPPSE4FO | Computer Room |
| RPPSF2FO | Computer Room |
| RPPSF3FO | Computer Room |
| RPPSF4FO | Computer Room |

APPENDIX D

Conditional Failure Probabilities
for Basic Events

Table D.1 lists the conditional probability of failure, given a generic environment or a common link, for each of the basic events considered in the analysis of the ANO-1 scram system. Blanks in the table indicate that basic events are not susceptible to the corresponding generic environments and common links.

Table D.1 Conditional Failure Probabilities for Basic Events

| Basic Event | Generic Environment | | | | | | | | Common Link | | | | | | | | | | | |
|-------------|---------------------|-----------|--------|------|----------|-------------|------|-------------------------|------------------------|------------------------|-----------|-----------|-----------------|-----------------|-----------------|-----------------|----------------|----------------|----------------|----------------|
| | Vibration | Corrosion | Impact | Grit | Moisture | Temperature | Fire | Cooling Water | dc bus #1 | dc bus #2 | dc bus #1 | dc bus #2 | vital ac bus #A | vital ac bus #B | vital ac bus #C | vital ac bus #D | 15V dc power A | 15V dc power B | 15V dc power C | 15V dc power D |
| RPCOREDT | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPCR12MF | .9 | .9 | .9 | .9 | .9 | .9 | .9 | .1 | 10 ⁻³ | 10 ⁻³ | - | - | - | - | - | - | - | - | - | - |
| RPCR20MF | .9 | .9 | .9 | .9 | .9 | .9 | .9 | .1 | 10 ⁻³ | 10 ⁻³ | - | - | - | - | - | - | - | - | - | - |
| RPCR28MF | .9 | .9 | .9 | .9 | .9 | .9 | .9 | .1 | 10 ⁻³ | 10 ⁻³ | - | - | - | - | - | - | - | - | - | - |
| RPCR61MF | .9 | .9 | .9 | .9 | .9 | .9 | .9 | .74 | 5.6 x 10 ⁻⁹ | 5.6 x 10 ⁻⁹ | - | - | - | - | - | - | - | - | - | - |
| RPCRO5SC | .999 | .999 | .999 | .999 | .999 | .999 | .999 | 1.35 x 10 ⁻⁴ | 9.6 x 10 ⁻⁶ | 9.6 x 10 ⁻⁶ | - | - | - | - | - | - | - | - | - | - |
| RPBACRSC | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPBACPSC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | .5 | - | - | .5 | - | - | - | - | - | - | - | - |
| RPBBCRSC | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPBBCPSC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | - | .5 | - | .5 | - | - | - | - | - | - | - | - |
| RPBRC1SC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | .5 | - | - | .5 | - | - | - | - | - | - | - | - |
| RPBRD1SC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | - | .5 | - | - | .5 | - | - | - | - | - | - | - |

Table D.1 (continued)

| Basic Event | Generic Environment | | | | | | | Common Link | | | | | | | | | | | | |
|-------------|---------------------|-----------|--------|-------|----------|-------------|------|---------------|-----------|-----------|-----------|-----------|-----------------|-----------------|-----------------|-----------------|----------------|----------------|----------------|----------------|
| | Vibration | Corrosion | Impact | Grift | Moisture | Temperature | Fire | Cooling Water | ac bus 11 | ac bus 12 | dc bus 11 | dc bus 12 | vital ac bus A4 | vital ac bus A9 | vital ac bus AC | vital ac bus A0 | 15V dc power A | 15V dc power B | 15V dc power C | 15V dc power D |
| RPRC2SC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | .5 | - | - | - | - | - | .5 | - | - | - | - | - |
| RPRD2SC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | - | .5 | - | - | - | - | - | .5 | - | - | - | - |
| RPSACRSC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | - |
| RPSBCRSC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | - | - | - | - | - | - | - | - | - | .5 | - | - |
| RPSCORSC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | - | - | - | - | - | - | - | - | - | .5 | - | - |
| RPSDCRSC | .1 | .5 | .1 | .9 | .1 | .1 | .1 | - | - | - | - | - | - | - | - | - | - | - | .5 | - |
| RPSAP1SC | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPSBP3SC | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPSCP4SC | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPSDP2SC | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPRKA1SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | - |
| RPRKA2SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | - |

Table D.1 (continued)

| Basic Event | Generic Environment | | | | | | | Common Link | | | | | | | | | | | | |
|-------------|---------------------|-----------|--------|-------|----------|-------------|------|---------------|-----------|-----------|-----------|-----------|-----------------|-----------------|-----------------|-----------------|----------------|----------------|----------------|----------------|
| | Vibration | Corrosion | Impact | Grift | Moisture | Temperature | Fire | Cooling Water | dc bus 11 | dc bus 22 | dc bus 11 | dc bus 22 | vital ac bus A4 | vital ac bus A9 | vital ac bus AC | vital ac bus A9 | 15y dc power A | 15y dc power B | 15y dc power C | 15y dc power D |
| RPRKA3SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | - | - | .5 | - |
| RPRKA4SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | - | - | - | .5 |
| RPRKB1SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | - |
| RPRKB2SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | - |
| RPRKB3SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | .5 |
| RPRKB4SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | .5 |
| RPRKC1SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | - |
| RPRKC2SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | - |
| RPRKC3SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | .5 |
| RPRKC4SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | .5 |
| RPRKD1SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | - |
| RPRKD2SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | .5 | - | - | - |

Table D.1 (continued)

| Basic Event | Generic Environment | | | | | | | Common Link | | | | | | | | | | | | | |
|-------------|---------------------|-----------|--------|------|----------|-------------|------|---------------|-----------|-----------|-----------|-----------|-----------------|-----------------|-----------------|-----------------|----------------|----------------|----------------|----------------|----|
| | Vibration | Corrosion | Impact | Grft | Moisture | Temperature | Fire | Cooling Water | dc bus #1 | ac bus #2 | dc bus #1 | dc bus #2 | vital ac bus #4 | vital ac bus #3 | vital ac bus #C | vital ac bus #D | 15V dc power A | 15V dc power B | 15V dc power C | 15V dc power D | |
| RPRKD3SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | - | - | - | .5 | - |
| RPRKD4SC | .1 | .5 | .1 | .9 | .9 | .1 | .1 | - | - | - | - | - | - | - | - | - | - | - | - | - | .5 |
| RPOCH/CP | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPOCH/DP | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPOCH*CP | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPOCH*DP | .003 | - | .003 | .003 | .003 | - | .003 | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| RPPSE2FO | .25 | .25 | .1 | .25 | .1 | .25 | .25 | - | .5 | - | .5 | - | - | - | - | - | - | - | - | - | - |
| RPPSE3FO | .25 | .25 | .1 | .25 | .1 | .25 | .25 | - | .5 | - | .5 | - | - | - | - | - | - | - | - | - | - |
| RPPSE4FO | .25 | .25 | .1 | .25 | .1 | .25 | .25 | - | .5 | - | .5 | - | - | - | - | - | - | - | - | - | - |
| RPPSF2FO | .25 | .25 | .1 | .25 | .1 | .25 | .25 | - | - | .5 | - | .5 | - | - | - | - | - | - | - | - | - |
| RPPSF3FO | .25 | .25 | .1 | .25 | .1 | .25 | .25 | - | - | .5 | - | .5 | - | - | - | - | - | - | - | - | - |
| RPPSF4FO | .25 | .25 | .1 | .25 | .1 | .25 | .25 | - | - | .5 | - | .5 | - | - | - | - | - | - | - | - | - |

APPENDIX E

Example Calculation of the Conditional
Failure Probability for a Basic Event

The following example illustrates the method used in this study to estimate the conditional failure probability for a basic event, given a root cause event type.

Step 1

Determine the failure probability (or failure rate) for the basic event by first calculating the failure rate for the type of component defined by the basic event, taking into consideration all possible failure modes. (We used WASH-1400 failure data to determine this total failure rate):

Component type: relay

| | | |
|----------------|----------------|-------------------------------|
| Failure modes: | sticks closed | $\lambda = 10^{-8}/\text{hr}$ |
| | transfers open | $\lambda = 10^{-7}/\text{hr}$ |

total failure rate $\lambda_T = 1.1 \times 10^{-7}/\text{hr}$

Step 2

Calculate an initial estimate of the probability the component will fail in one specific unsafe mode (e.g., sticks closed) given the component does fail.

$$P(\text{sticks closed} \mid \text{failure}) = \frac{10^{-8}}{1.1 \times 10^{-7}} = 0.1$$

Step 3

Using engineering judgment, adjust this initial estimate of the conditional failure probability for each generic environment type that

affects the component type. In this study, the following conditional failure probabilities were used:

| | | | |
|----------------------------------|---|-----|------------------|
| P(sticks closed vibration) | = | 0.1 | |
| P(sticks closed corrosion) | = | 0.5 | (adjusted value) |
| P(sticks closed impact) | = | 0.1 | |
| P(sticks closed contamination) | = | 0.9 | (adjusted value) |
| P(sticks closed moisture) | = | 0.9 | (adjusted value) |
| P(sticks closed temperature) | = | 0.1 | |
| P(sticks closed fire) | = | 0.1 | |

INTERNAL DISTRIBUTION

- | | | | |
|------|-------------------|--------|-----------------------------|
| 1. | R. J. Borkowski | 13. | A. Zucker |
| 2. | T. E. Cole | 14. | P. W. Dickson (Consultant) |
| 3-5. | G. F. Flanagan | 15. | G. H. Golub (Consultant) |
| 6. | P. M. Haas | 16. | R. M. Haralick (Consultant) |
| 7. | H. E. Knee | 17. | D. Steiner (Consultant) |
| 8. | T. S. Kress | 18-19. | Central Research Library |
| 9. | F. C. Maienschein | 20. | Y-12 Document Ref. Section |
| 10. | A. P. Malinauskas | 21-22. | Laboratory Records Dept. |
| 11. | F. R. Mynatt | 23. | Laboratory Records ORNL, RC |
| 12. | D. L. Selby | 24. | ORNL Patent Office |
| | | 25. | EPMD Reports Office |

EXTERNAL DISTRIBUTION

26. Office of the Assistant Manager for Energy Research and Development, DOE/ORO, P. O. Box E, Oak Ridge, TN. 37831.
- JBF Associates, Inc., 1000 Technology Park Center, Knoxville, TN. 37922.
27. J. B. Fussell
- 28-32. D. J. Campbell
- 33-37. D. F. Montague
- U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC 20555.
38. P. W. Baranowsky
39. B. Buchbinder
40. G. R. Burdick
41. M. L. Ernst
42. J. C. Glynn
43. C. E. Johnson
44. J. W. Johnson
45. L. E. Lancaster
46. J. A. Murphy
47. D. M. Rasmuson

U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor
Regulation, Washington, DC 20555.

- 48. R. M. Bernero
- 49. A. El Bassioni
- 50. J. W. Pittman
- 51. F. H. Rowsome
- 52. A. C. Thadani

- 53. K. G. Murphy, Jr., NRC Region I, 631 Park Avenue, King of
Prussia, PA. 19406.

- 54. J. B. Martin, NRC Region IV, 611 Ryan Plaza Drive, Suite
1000, Arlington, TX. 76011.

- 55-81. Technical Information Center, Oak Ridge, TN. 37831.

When you no longer need this report,
please return it to G. F. Flanagan,
Engineering Physics and Mathematics
Division, Building 6025, Room 8W,
Oak Ridge National Laboratory, P.O.
Box X, Oak Ridge, TN. 37831.