NUREG/CR-3593, Vol. 1
UCRL-53467

Systems Interaction Results from the Digraph Matrix Analysis of a Nuclear Power Plant's High Pressure Safety Injection Systems
Volume 1

I. J. Sacks, B. C. Ashmore, and H. P. Alesso

Prepared for
U.S. Nuclear Regulatory Commission

Lawrence
Livermore
National
Laboratory

NOTICE

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

NOTICE

Availability of Reference Materials Cited in NRC Publications

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

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555

2. The NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission,
   Washington, DC 20555

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

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the NRC/GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG/CR-3593, Vol. 1
UCRL-53467
RD, RM

Systems Interaction Results from the Digraph Matrix Analysis of a Nuclear Power Plant's High Pressure Safety Injection Systems
Volume 1

Manuscript Completed: January 1984
Date Published: July 1984

Prepared by
I. J. Sacks, B. C. Ashmore (Analytic Information Processing, Inc.), and H. P. Alesso (Lawrence Livermore National Laboratory)

Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550

Prepared for
Division of Safety Technology
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN No. A0403

ABSTRACT

Spatial and functional coupling (including human actions) of nuclear power plant systems that lead to interdependencies are called Systems Interactions. At present, the U.S. Nuclear Regulatory Commission (NRC) is investigating ways of identifying and evaluating systems interactions. One approach is based on graph-theoretic methods utilizing matrix representations of logic diagrams called Digraph Matrix Analysis (DMA).

Our objective in this report is to demonstrate the capabilities of Digraph Matrix Analysis to model an accident sequence (including front-line systems, support systems and human actions) as a continuous, well-integrated logic model in order to identify and evaluate functional systems interactions.

The selected accident sequence, loss of high pressure safety injection during a LOCA, was modeled and qualitative and quantitative comparisons were made to the Reactor Safety Study (WASH 1400) and other studies. The results demonstrate that: (1) DMA is highly capable of modeling and evaluating an accident sequence (including front-line systems, support systems, and human actions) as a continuous and well-integrated logic model in order to identify and evaluate systems interactions; (2) numerous, non-intuitive systems interactions were found between front-line and support systems that collectively contributed significantly to the overall failure probability, and (3) the reactor operators can provide a significant improvement in safety if they correctly respond to the failure of an automatic system.

NRC SUMMARY

The NRC staff has been evaluating methods that analyze for intersystems dependencies. The evaluations were both (a) for the resolution of Unresolved Safety Issue A-17 (Systems Interaction in Nuclear Power Plants) and (b) for the treatment of dependencies in Probabilistic Risk Assessments. One method, Digraph-Matrix Analysis, appeared effective although previously not applied to nuclear systems. The NRC endeavored to describe and demonstrate Digraph-Matrix Analysis for application to commerical nuclear power systems. Digraph-Matrix Analysis was described in NUREG/CR-2915 (Initial Guidance on Digraph-Matrix Analysis for Systems Interaction Studies). This present report describes the demonstration of the Digraph-Matrix Analysis on a Nuclear Power Plant's High Pressure Injection System.

The plant was selected to facilitate a comparison of results with the results from prior work using Fault Tree analysis (NUREG/CR-1321, Final Report-Phase I, Systems Interaction Methodology Applications Program). Both the results reported here and the prior results came from work beyond the scope of the criteria used by the NRC to license nuclear power plants.

The objective of the systems interaction analysis was to provide assurance that the independent functioning of the High Pressure Injection System was not jeopardized by components that cause faults to be dependent. The analysis discovered seven components whose failure could jeopardize the High Pressure Injection System given the postulated accident. All seven of these components were considered both in the safety analysis and in the licensing review (Section 7.6.6 of the Final Safety Analysis Report). Special means had been established to preclude the spurious alignment of the active components (Section 8.3.1.7, NUREG-0847). The Digraph-Matrix Analysis confirmed that the licensing review provided assurance against adverse intersystems dependencies.

The large number of doubletons discovered relative to the number of singletons was not the best parameter to assess the significance of the doubletons. The relative contributions of the singletons and the doubletons to the unavailability of the High Pressure Injection System was estimated to gather better evidence concerning the significance of the doubletons. The component failure rates were selected from available reports as input to the estimates. There is limited consensus of component failure rates among various reports. The ranges in the data can be quite large possibly due to implicit considerations (e.g., the classification of failure modes, the placement of position indicators, the role of maintenance, and component design differences). Consequently, the estimated unavailabilities could have large uncertainties that are not necessarily bounded by the two Cases herein. In either case, the doubletons appear to be at least as important as the singletons.

The results reported herein demonstrate the capability of Digraph-Matrix Analysis to discover components that could jeopardize the independent functioning of safety-related systems in commercial nuclear power plants. Also, the method is scrutable and can be used on a complex system which contains both a large number of components and dependent loops. The method is being applied at another plant with a fuller scope including human dependencies and spatial susceptibilities.

Digraph-Matrix Analysis appears to have the potential to be a tool for accident management. The method could readily identify feasible causes of accident symptoms and list optional responses for the operator. The feature could be useful before an accident to explore postulated scenarios like a loss of offsite power. The method could be used in safeguards analysis also.

The NRC staff acknowledges that progress is being made on systems interaction methods by other organizations. We encourage comments on the use of Digraph-Matrix Analysis that are based upon experience with the method or other methods.

TABLE OF CONTENTS

Page

Volume I

Abstract iii

NRC Summary v

List of Figures xi

Glossary xvii

Explanation of DMA Symbol Format xxi

Executive Summary 1

1. Introduction 5

1.1 Background 5

1.2 Objective 10

1.3 Summary of Results 11

1.4 Organization of this Report 12

2. Digraph Matrix Analysis Demonstration 13

2.1 Scope of Study 13

2.2 Description of Front-line Systems 16

2.2.1 The High Pressure Injection System Description 16

2.3 Overview of Digraph Matrix Analysis Procedure 21

2.4 Construction of Global Digraph 23

2.4.1 Review Final Safety Analysis Report and Collect Piping and Instrumentation Diagrams 23

2.4.2 Identify and Model the Success Criteria 25

2.4.3 Model Front-line Systems 27

2.4.4 Identify and Model Support Systems 40

2.4.5 Identify and Create Component Unit Models 41

2.4.5.1 Flow Control Valve Unit Model 42

Page

2.4.5.2 Solenoid Valve Unit Model 49

2.4.5.3 Pump Unit Model 53

2.4.6 Addition of Support System and Unit Models 55

2.4.7 Modeling Human Intervention 56

2.4.8 Partitioning 56

3. Results of the DMA of the High Pressure Safety Injection System 59

3.1 Results for Fully Automatic Operation (No Human Mitigation): Case I 64

3.1.1 Analysis of Failure Mode 1 73

3.1.2 Analysis of Failure Mode 2 75

3.1.3 Analysis of Failure Mode 3 78

3.1.4 Analysis of Failure Mode 4 78

3.1.5 Analysis of Failure Mode 5 81

3.1.6 Analysis of Failure Mode 6 81

3.1.7 Analysis of Failure Mode 7 81

3.1.8 Analysis of Failure Mode 8 85

3.1.9 Analysis of Failure Mode 9 87

3.1.10 Analysis of Failure Mode 10 89

3.1.11 Analysis of Failure Mode 11 89

3.1.12 Analysis of Failure Mode 12 92

3.2 Results with Human Mitigation 94

3.3 Error Checking Using Failure Modes 98

4. Quantitative Analysis 99

4.1 Quantitative Results 102

4.2 Discussion of Failure Probability Calculation 104

4.3 Data Base 107

5. Conclusions 115

References 117

Addendum 121

Page

Appendix A: Digraph Matrix Analysis 123
A.1 Overview of DMA 125
A.2 Expansion of Unit Models 129
A.3 Break Modeling 133
A.4 Modeling Complex Networks with Bidirectional Flows 139
A.5 Adjacency & Reachability 143
A.6 Efficient DMA Codes 149
A.6.1 ADJ 149
A.6.2 CONDENSE 149
A.6.3 REACHABILITY 151
A.6.4 Output Codes 155
A.7 Partitioning 158
A.8 Tripleton Code 160

References for Appendix A 161

Volume 2

Abstract iii
Table of Contents v
List of Figures vii
Preface ix

Appendix B: Complete Set of Failure-Oriented Digraphs for SIPIS B-1

Appendix C: Complete Adjacency Input for Safety Injection Pump System C-1

Appendix D: Probability Data Base D-1

LIST OF FIGURES

Page

1-1 Systems Interaction Performed via Enhanced Fault Tree versus DMA 8

2-1 Flow Diagram - Safety Injection System 17
2-2 Approximate Relationship of Major Subsystems of High Pressure Safety Injection System 20
2-3 Global Digraph Construction Procedure 24
2-4 Safety Injection Success Criteria 26
2-5 Overview of Front-Line Systems 28
2-6 RWST.DAT Network Connecting RWST to SIPIS and CCPIS 29
2-7 Safety Injection Pump Path to the Core, SIPIS 31
2-8 Charging Pump Path to the Core, CCPIS 34
2-9 SBREAK.DAT Break Model for SIPIS 36
2-10 CBREAK.DAT Break Model for CCPIS 38
2-11 Redundancy to Valve Link 43
2-12 Control of Motive Power to Valve Motor 43
2-13 Control Power Switching 43
2-14 Safety Injection Logic Activation 45
2-15 Switch SWA1 45
2-16 Indicator Light Actuation 45
2-17 Power for the Valve Heater 47
2-18 Backup Remote Operations, SWC1 47
2-19 Local Operator Valve Actuation 47
2-20 FCV.DAT Flow Control Valve Unit Model 48
2-21 Solenoid Flow Control Valve Unit 52
2-22 Pump Unit Model 54
2-23 Addition of Support System and Unit Models 55

3-1 Doubleton Format 63
3-2 RWST.DAT Network Connecting RWST to SIPIS and CCPIS 65

Page

3-3 Doubletons for Case I: No Human Mitigation 67

3-4 Doubletons for Case I: No Human Mitigation. Doubletons Resulting from Failures of Both Trains of a Doubly Redundant System Appear as Blanks. 70

3-5 Failure Mode 1 74

3-6 Doubletons for Case I: No Human Mitigation. Doubletons Resulting from Failures in Component Cooling System Are Circled. 76

3-7 Failure Mode 2 77

3-8 Failure Mode 3 79

3-9 Failure Mode 4 80

3-10 Failure Mode 5 82

3-11 Failure Mode 6 83

3-12 Failure Mode 7 84

3-13 Failure Mode 8 86

3-14 Failure Mode 9 88

3-15 Failure Mode 10 90

3-16 Failure Mode 11 91

3-17 Failure Mode 12 93

3-18 Doubletons for Case II: Human Mitigation Enabled 95

3-19 Triple Redundancy of Automatic Systems and Local and Remote Operators 97

4-1 Simplified Example of Common Mode Failures 100

Addendum

AD-1 Addition of FCV6348 to RWST 122

Appendix A

A-1 Overview of Digraph Matrix Analysis 125

Page

A-2 Conventions for the Use of AND and OR Gates in the Digraph 126

A-3 (a) Simplified Corewater Injection System 127

(b) Digraph of Corewater Injection System 127

A-4 Pump Unit Model 129

A-5 Pump with Redundant Power and Control 130

A-6 Partial First Stage Unit Model Expansion of the Digraph of the Corewater Injection System 131

A-7 Effect of Pipe Break 134

A-8 Break and Block Digraphs 135

A-9 Use of a Strong Component 136

A-10 Modeling of Break Mitigation 137

A-11 Crosstie Network 140

A-12 Digraph of Crosstie Network 140

A-13 Graph and Corresponding Adjacency Matrix 143

A-14 Weighted Graph and Equivalent Logic 145

A-15 Representation of an AND Operation 146

A-16 Representation of an OR Operation 146

A-17 Example of Multiple Gate Logic Network 147

A-18 Component Matrices 147

A-19 Adjacency Matrix for Logic Network of Figure A-17 147

A-20 Reachability Matrix for the Network of Figure A-17 148

A-21 DMA Data Processing Flow 150

A-22 Input/Output for Code ADJ 149

A-23 Condensation Program Operation 151

A-24 Reachability Code Flow 152

A-25 The Deconditioned Graph 153

A-26 Output from Code SHORT 156

A-27 Output from Code MATRIX 156

A-28 Output from Code NEW2 157

LIST OF TABLES

Page

2-1 Scope of Study 15

2-2 Overview of Digraph Matrix Analysis 21

2-3 Adjacency Input Data for FCV.DAT 50

3-1 Summary of Results 63

3-2 Characterization of the 12 Doubleton Failure Modes Appearing in Case I 72

4-1 HP Safety Injection Failure Probabilities 102

4-2 Effect of Maintenance Outage 103

4-3 Components not in Probability Data Base 105

4-4 Singleton/Doubleton Contribution 106

4-5 Effect of Locked Off Valves and Maintenance Outage 107

4-6 Generic Failure Data Base 110

GLOSSARY

Adjacency Matrix - The Boolean matrix which describes connectivity between a node in a graph and its "nearest neighbors".

Component - A component is a physical element, human action, location, or any other "thing" which can impact system operation.

Compression - The step in the DMA processing sequence in which redundant (repeated) connections in the adjacency data are deleted.

Condensation - The step in the DMA processing sequence in which nodes which are in series are combined under certain conditions into a single node.

Crosstie - A cross-connected header or cross-connected electical bus which allows bi-directional flow of fluid or electricity. DMA has an algorithm for digraphing these complex connections.

Cut Set - The term "cut set" is used in this report to mean a component or group of components whose failure would cause system(s) failure.

DMA - Digraph Matrix Analysis is the procedure through which a conditioned directed graph of a system is constructed, processed, and displayed to yield failure sets of the system.

Digraph - A graph consisting of a group of nodes that are connected by edges and logical connectives which indicate the direction of flow of effects.

Doubleton - A pair of components whose joint failure will cause failure of a component or system(s).

Edge - The connection between two nodes.

Functional Dependency - Dependency due to either process coupling of support systems or human actions.

Header - The junction of 2 or more pipes.

LOCA - Loss of Cooling Water Accident.

LWR - Light Water Reactor.

NRC - U.S. Nuclear Regulatory Commision.

Node - The symbol in the digraph which represents physical component, physical location, plant operating mode, human interaction, etc. Thus a node represents anything which could affect system interaction.

PASNY - Power Authority of the State of New York.

PWR - Pressurized Water Reactor.

Reachability Matrix- The Boolean matrix which describes all possible pairs of connections between pairs of nodes in the digraph. This matrix represents the transitive closure of the digraph.

S1 LOCA - The rupture of primary coolant piping equivalent to the break of a single pipe whose diameter is greater than 1.5" (approximately), but less than or equal to 3" [Ref 17].

SI - Systems Interactions.

Singleton - A single component whose failure will cause failure of a component or system(s).

Spatial Dependency - Dependence due to shared location or shared environmental conditions.

Strong Component - A strong component consists of a group of nodes which are bidirectionally and unconditionally connected.

Systems Interactions - Spatial and functional coupling (including human actions) of nuclear power plant systems that lead to interdependencies.

Unit Model - A detailed directed graph model of a component of the system. The unit model represents the decomposition of a large component, such as a valve, into its parts.

EXPLANATION OF DMA SYMBOL FORMAT

The symbols used to represent components in this DMA of a High Pressure Safety Injection System follow a consistent format. In general, the symbols contain the component identification used in the piping and instrumentation diagrams, and electrical line drawings. In some cases, a prefix has been added to indicate the type of component being modeled. For example, the prefix FCV has been used to identify flow control valves. The following list explains the prefix symbols used throughout this report.

125VVB	- 125 volt dc Vital Battery Board
480MOV	- 480 volt ac Motor Operated Valve Electrical Power Bus
480VS	- 480 volt ac Shutdown Board
6900VS	- 6900 volt ac Shutdown Board
BIT	- Boron Injection Tank
CCHXR	- Component Cooling Heat Exchanger
CCP	- Centrifugal Charging Pump
CCPISCORE	- Charging Pump Portion of Safety Injection System
CCS	- Component Cooling System
CCWP	- Component Cooling Water Pump
COIL	- Breaker Actuating Coil
EINRLK	- Electrical Interlock Transfer Device
EPS	- Electrical Power System (500 kvac to 480 vac)
FCV	- Flow Control Valve
FE	- In-line Flow Meter Orifice
FUSE	- Electrical Fuse
HDR	- Pipe Header (junction)
LCV	- Level Control Valve
MINRLK	- Mechanical Interlock Transfer Device
MOT	- Motor
OILCOOL	- Component Oil Cooler Interface with Component Cooling System
OFFSITE	- Master Node connected to all Offsite Power Sources
ONSITE	- Master Node connected to all Onsite Power Sources

OPR	- Operator Action to Override failed Component (Operator Right)
OPRMASTER	- Master Node connected to all OPR's
OPW	- Operator taking incorrect action (Operator Wrong)
PS	- Protection Set System (Vital Instrumentation and Control Power)
R	- Relay or Circuit Breaker
RCS	- Reactor Cooling System (the Terminal Node)
RHR	- Residual Heat Removal System
RWST	- Refueling Water Storage Tank
SILOGIC	- Safety Injection Logic Actuation System
SIP	- Safety Injection Pump
SIPISCORE	- Safety Injection Pump Portion of Safety Injection System
SISIG	- Safety Injection Signal
STRAINR	- Strainer
SW	- Control Power Switch
TR	- Electrical Transformer
TW	- In-line Temperature Sensor
VB	- Butterfly Valve
VC	- Check Valve
VGA	- Gate Valve
VGL	- Globe Valve
X	- Component whose type could not be determined from the available documentation

EXECUTIVE SUMMARY

Complex events such as those at Three Mile Island-2, Brown's Ferry-3, and Crystal River-3 have demonstrated that previously unidentified system interdependencies can be important to safety. A major aspect of these events was dependent faults (common cause/mode failures). The term Systems Interactions (SI) was introduced by the Nuclear Regulatory Commission (NRC) to identify the concepts of spatial and functional coupling of systems which led to these system interdependencies. Spatial coupling refers to dependencies coupled by a shared environmental condition; functional systems interaction refers to dependencies coupled by a component shared between safety or support systems and includes interdependencies due to human actions. The NRC is currently developing guidelines to search for and evaluate potential systems interactions at light water reactors. The identification of system interactions is being addressed from several approaches, the most conventional being the enhancement of existing fault tree methodology. This is generally accomplished by expanding the scope and boundary conditions of the fault tree analysis, giving added emphasis to dependency analysis such as minimum cut-set common cause analysis. An alternative approach utilizes graph-theoretic methods and is called Digraph Matrix Analysis (DMA). This methodology is specifically tuned to the SI problem.

A preliminary description of DMA was presented in NUREG/CR-2915 [1] with preliminary results of the SI analysis given in Reference 2. Our objective in this report is to present the final results from the DMA application and to contrast these with the results from the more traditional fault tree approaches. This will demonstrate the capabilities of DMA to model an entire accident sequence as a single well-integrated logic model in order to identify and evaluate systems interactions.

DMA differs from traditional fault tree techniques in four major ways:

1. Construction of the logic model is performed directly from plant schematics (piping and instrumentation diagrams, electrical schematics safety logic diagrams). The resulting model could be overlaid on the plant schematics. Thus, the model can be readily understood, reviewed and corrected.

2. The resulting digraph (directed graph with logic connectives) can represent physical situations which are cyclic. In fault tree methodology the analyst must "break" each loop or cycle and construct a logical equivalent.

3. The digraph is processed through DMA computer codes based on a conditioned reachability calculation. These codes determine all single component failures (singletons) and all pairs of component failures (doubletons) which would cause failure of the group of systems collectively and any single component individually.

4. DMA computer codes can process very large models. Presently, an entire accident sequence, consisting of several front-line systems and their support systems, is modeled as a single digraph. The ability of the DMA codes to process such large models is based on its graph-theoretic approach as opposed to Boolean equation substitution codes (e.g., SETS [3] or FTAP [4]) currently used to find fault tree cut-sets.

The models generated in a DMA are quite large (thousands of components) and include physical components (such as pumps, valves, motors, etc.), plant operational modes, and human operators. These models can represent systems or combinations of systems. The problems are solved for all singletons* and doubletons** without any "culling" (probabilistic truncation). Hence,

----

* Singletons correspond to cut sets of order one.
** Doubletons correspond to cut sets of order two.

as opposed to other techniques, common events cannot be inadvertently suppressed during truncation. DMA codes have been designed to run on minicomputers for these large problems.

The DMA model of the high pressure safety injection system was analyzed for all singletons and doubletons in both the fully automatic mode (Case I) and the operator assisted mode (Case II). In the first case, seven components were found whose failure would cause safety injection failure. These failures were previously identified in NUREG 0847 [5]. In addition, approximately 4300 doubletons were found by DMA for the fully automatic case. Some of these doubletons involve two components in front-line systems, however, many involve components in support systems. An example of the second type is the doubleton composed of a flow control valve in the component cooling system and a fuse in the control system for one of the charging pumps. Several of the doubletons involve power from a second unit. These arise since one of the Unit I component cooling pumps draws its normal power from Unit II.

The high pressure safety injection system was designed with the human as the ultimate backup. The operator assisted case (Case II) illustrated this situation. The results of this case show only two singletons and 708 doubletons. Most of these doubletons were concentrated in or near front-line systems.

A quantitative analysis of the results of the two cases showed a significant contribution from the doubletons. A significant improvement in reliability is indicated when constructive operator overrides are considered. The effect of incorrect operator actions was modeled and analyzed only for actions that might have been taken prior to safety injection. No attempt was made in this study to determine what detrimental effects would occur due to systematic operator incorrect action during the LOCA. Also, no attempt was made to determine the effect of coordinated operator action prior to the LOCA.

Our findings include: (1) DMA is highly capable of modeling and evaluating an accident sequence (including front-line systems, support systems, and human actions) as a continuous well-integrated logic model in order to identify and evaluate systems interactions, (2) numerous, non-intuitive systems interactions were found between front-line and support systems that collectively were significant, and; (3) the operators can contribute a significant improvement in safety if they correctly respond to the loss of an automatic system.

1. INTRODUCTION

1.1 Background

The term Systems Interaction (SI) has been introduced by the U.S. Nuclear Regulatory Commission (NRC) to identify the concept of spatial and functional coupling of nuclear power plant systems which lead to system interdependencies. Spatial coupling refers to dependencies resulting from shared environmental conditions within the plant; functional systems interactions include coupling due to shared support systems (process coupling) and interdependencies due to dynamic human error.

The Office of Nuclear Reactor Regulation of the NRC is developing a program to further define and subsequently implement SI regulatory requirements for light water reactors (LWR's). Battelle Columbus/Pacific Northwest Laboratories [6], Brookhaven National Laboratory [7], and Lawrence Livermore National Laboratory [8] assisting the NRC, recommended that reliability assessment techniques, such as event tree/fault tree methods supplemented by minimum cut set common cause/mode analysis, combined with walk-through inspections could be used for identifying SI's. The Power Authority of the State of New York (PASNY) has independently developed a systems interaction methodology for application to the interconnected systems at Indian Point-3 [9,10]. The method was based on "shutdown logic diagrams" which were success-paths of operational sequences.

At present, the NRC is considering three concepts for the integration of a systems interaction study with existing Probabilistic Risk Assessment (PRA) techniques.

One concept is that systems interactions can be adequately analyzed by expanding the scope and boundary conditions of the fault tree analysis portion of a PRA and by putting additional emphasis on dependency analysis techniques such as generic analysis [11] and minimum cut-set common cause/mode analysis [11]. The NRC's initial guidance for this point of view has already begun [12].

A second, and closely related concept is that systems interactions can be incorporated into a PRA at the event tree stage of analysis. This approach attempts to capture systems interactions at an earlier stage of analysis. By treating dependencies in the event tree analysis portion of a PRA, the requirement of fault tree modeling at additional levels of detail is reduced [12].

The third concept is based on graph-theoretic methods utilizing a conditioned matrix representation of logic diagrams and is called Digraph Matrix Analysis (DMA) [1, 13]. The concept of analyzing nuclear power plant systems for systmes interaction was first suggested by Battelle Northwest [6]. This assessment technique* would be applied after an event tree analysis has identified the accident sequences; it treats an accident sequence consisting of several systems along with their support systems and human interactions as a single logic model. Thus, instead of constructing a reliability block diagram (or equivalent) in preparation of fault tree construction for each individual system in an accident sequence, as in the Reactor Safety Study [15], the entire accident sequence is modeled as a schematic-based operational logic diagram (which includes AND and OR gates). The advantages of such a model are: (1) the ease of schematic-oriented modeling directly including loops and cycles in the physical system; and (2) highly efficient graph based computer processing for singletons and doubleton cut sets.**

DMA differs from an analysis based on traditional fault tree techniques in four major ways:

1. Construction of the logic model is performed directly from plant schematics (piping and instrumentation diagrams, electrical schematics, safety logic). The resulting model could be overlaid on the plant schematics. Thus, the model can be readily understood, reviewed, and corrected.

* A full risk assessment using DMA would, as in a PRA, consider the consequence of each accident sequence.

** Technically, the singletons and doubletons found in a DMA are not cut sets of the digraph. They are single nodes or pairs of nodes which can reach a terminal node. The term cut set is used only because of its use in traditional PRA's.

2. The resulting digraph (directed graph with logic connectives) is not limited to a "tree" structure and hence can represent physical situations which are cyclic. Cycles arise from the effect of the failure in a component propagating to a second component and then back to the original component. Cyclic situations are quite common in piping networks and electrical power and control schematics. Fault tree analysts must individually "break" every cycle and construct a logical equivalent.

3. The digraph is processed through DMA computer codes based on a conditioned reachability calculation. These codes determine all single component failures (Singletons) and all pairs of component failures (Doubletons) which would cause system failure and the failure of any other component.

4. DMA computer codes can process very large models. Presently, an entire accident sequence, consisting of front-line systems, their support systems and human actions, is modeled as a single digraph. The ability of the DMA codes to process such large models is based on its graph-theoretic approach as opposed to Boolean equation substitution codes (e.g., SETS [3] or FTAP [4]) currently used to find cut-sets of fault trees.

A review of the fundamental mathematical aspects of fault-oriented and success-oriented reliability analyses (including Digraph-Matrix Analysis) was presented in Reference 13, which offered insight into the trade-off advantages and disadvantages of each. Initial guidance for DMA was presented in Reference 1. A report on the preliminary results of the DMA of the safety injection pump portion of the high pressure safety injection system was presented in Reference 2.

Figure 1-1 illustrates how an enhanced fault tree systems interaction study as suggested above would compare to a DMA approach. The enhanced fault tree approach would consist of several medium-size models (fault trees) of front-line systems. These fault trees would have basic events (e.g., A, B, C) and would be processed for minimum cut sets (MCS). The listing of

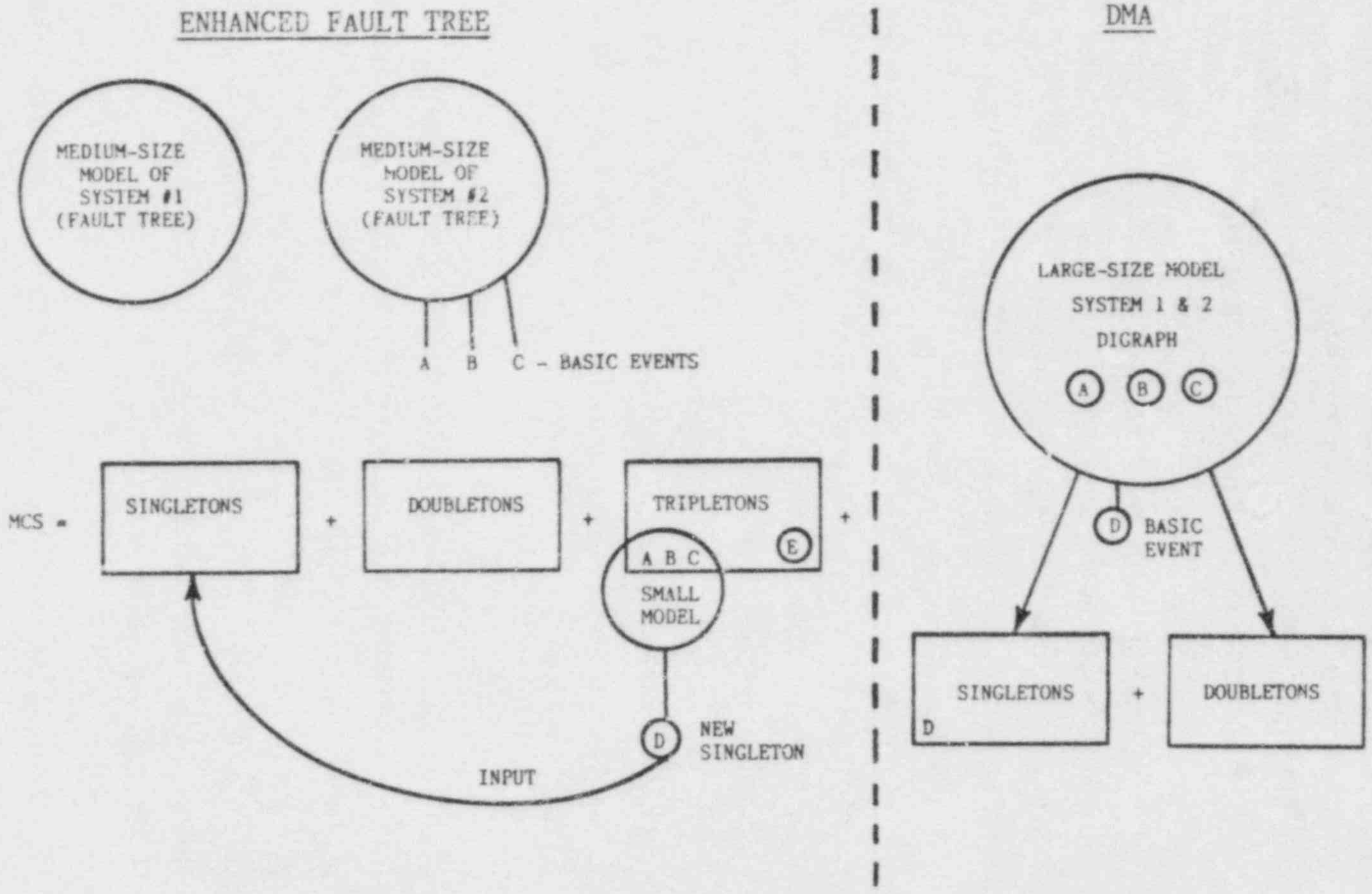


Figure 1-1. Systems Interaction Performed via Enhanced Fault Tree versus DMA

minimum cut sets would include the singleton, doubleton, tripleton, etc., cut sets. Then, perhaps, a minimum cut set common cause/mode analysis based on Failure Modes and Effects Analysis (FMEA) would be conducted in order to find high order cut sets from each fault tree that could be reduced for the systems (e.g., ABC becomes D). In comparison, DMA constructs a single continuous well-integrated logic model for the entire accident sequence in which the intention is to model to sufficient detail such that the singleton D would result naturally as a "basic event".

1.2 Objective

The NRC is examining candidate systems interaction methodologies that can be recommended for future regulatory requirements.

The objective of this report is to demonstrate the capabilities of Digraph Matrix Analysis (DMA) to model an accident sequence (including safety systems, support systems and human actions) as a continuous well-integrated logic model in order to identify and evaluate functional systems interactions. The selected accident sequence, loss of high pressure safety injection during the early stages of a LOCA, is modeled and qualitative and quantitative comparisons are made to BNL [14], WASH 1400 [15], Sandia [16], and Zion [17] studies. The scope of the analysis includes both front-line systems (safety injection pump and centrifugal charging pump injection systems) and their support systems (electrical, instrumentation, safety injection logic, and component cooling) as well as operator actions (random human error and constructive operator actions that can mitigate an accident).

1.3 Summary of Results

Our findings from this study include:

1. DMA is highly capable of modeling and evaluating an accident sequence (including front-line systems, support systems, and operator actions) as a continuous well-integrated logic model in order to identify and evaluate systems interactions.

2. Numerous, non-intuitive systems interactions exist between front-line and support systems that contribute significantly to the overall system unreliability. This is demonstrated by comparing our Case I (fully automatic, no operator mitigating action) with the recent BNL study [14] and with the well-known WASH 1400 study [15]:

Loss of High Pressure Injection[a]

DMA (Case I)[b]	BNL[c]	WASH 1400[d]
4×10^{-2}	3.1×10^{-3} ($\beta = 0$)	8.6×10^{-3}
(3.2×10^{-3})[e]	1.8×10^{-2} ($\beta = 0.3$)	

3. Support systems clearly depend on operator action in order to provide redundant safety. The operators can provide significant improvement in safety when they correctly respond to the loss of an automatic system. This is illustrated by comparing our Case II results (constructive operator intervention allowed) (4.9×10^{-3}) with Case I. The ratio of the failure probability of Case I to the failure probability of Case II was 8.2.

----

a. Since a PRA on the plant has not been completed, comparisons were made to the results of studies which were only roughly comparable.

b. This somewhat overstates the unavailability of the High Pressure Injection Systems due to scope limitations in modeling maintenance (see Section 4.1).

c. The success criteria used in the BNL [14] report was 1/2 SIP and 1/2 CCP. A DMA analysis based on this success criteria was made and yielded a failure probability of approximately the same value. A DMA run using a 2/4 success criteria again yielded approximately the same result.

d. The comparison is to the WASH 1400 small (S2) LOCA (0.5" - 2") which had a success criteria of 1/3 HPIP.

e. Restricted Maintenance Outage case.

1.4 Organization of this Report

This report is organized into two volumes. Volume I includes the main report and Appendix A. The details of the modeling of the front-line and support systems are given in Section 2.0 of this volume. Section 3.0 presents a discussion of the qualitative results including the impact of various types of operator failures. In Section 4.0, a comparison of the failure probabilities for the cases analyzed is presented along with a comparison to the results of an equivalent analysis from BNL and WASH 1400. Volume I concludes with Appendix A which provides an overview of DMA and its computer codes. Volume II consists of: Appendix B, the complete set of digraphs for the HPSIS; Appendix C, the corresponding adjacency listings; and Appendix D, the data base used for the quantitative analysis. A glossary of the terms used in this report is given following the list of illustrations.

2. DIGRAPH MATRIX ANALYSIS DEMONSTRATION

2.1 Scope of Study

The objective of this effort is to demonstrate the utility of Digraph Matrix Analysis, DMA, in the determination of functional systems interactions. Unfortunately for the purposes of comparison, a Probabilistic Risk Assessment of the plant has not been completed to date. Therefore, selection of the demonstration accident sequence was made by comparison to existing PRA's of other plants. Since this study was not intended as a safety analysis some latitude was exercised in choosing loss of high pressure injection during an S1 LOCA as the accident sequence to be studied. We specified the LOCA to be at the lower range of an S1 LOCA during its initial phase, therefore, requiring initiation of SI pumps in order to avoid core melt. This accident sequence leads to core melt for the Indian Point-3 Plant [9] and can be directly compared to loss of high pressure injection for an S1 LOCA, as described in WASH 1400. The latter comparison will illustrate the impact of a detailed analysis of support systems upon risk.

The scope has been restricted to the two safety injection systems which would be called upon to respond to an S1 LOCA and does not consider low pressure injection pumps. These systems are the Safety Injection Pump Injection System, SIPIS, and the Centrifugal Charging Pump Injection System, CCPIS. This systems interaction study covers the necessary support systems which include:

1. Electrical Power (down to 480v)
    - 1.1 Off-Site
    - 1.2 On-Site
        Nuclear Unit Source Generators
        4 Auxiliary Diesel Generators

2. Vital Instrumentation and Control Power (to 125vdc and 120vac)
    - 2.1 Transformers
    - 2.2 Vital Batteries and Chargers
    - 2.3 Distribution to all four protection sets
3. Safety Injection Logic
    - 3.1 Automatic
    - 3.2 Manually Initiated
4. Component Cooling Water System

The search for spatial systems interactions (common component location) has been excluded from this study by sponsor directive.* System interactions due to human errors have been studied, including the effects of:

1. operator non-action in overriding a failed automatic system or component; and

2. incorrect operator action.

An example of the first situation is the failure of an operator to manually switch from a dead power bus to a live bus. An example of the second type would be the accidental or deliberate switching of a pump from "Automatic" to "Manual". Plant operating procedures have not been modeled in detail, however the dependence of certain procedures on specific instrumentation has. No attempt was made to analyze effects from coordinated incorrect human operator actions. Table 2-1 summarizes the scope of the study.

* DMA can be used to analyze the effects of common component location, however this analysis would have required the determination of the physical location of each component, which was beyond the scope of this effort.

Front-line Systems	Safety Injection Charging Injection Residual Heat Removal	Included Included Partially Included
Support Systems	Electrical Power Vital Instrumentation and Control Power Safety Injection Logic Component Cooling Water	Included Included Included Included
Operator Dependency	Random Human Error Mitigation by Operator Systematic Diagnosis Errors Coordinated Incorrect Actions	Included Included Excluded Excluded
Other	Common Maintenance Common Location Common Environmental Condition Common Manufacturer	Partially Excluded Excluded Excluded Excluded

Table 2-1. Scope of Study

2.2 Description of Front-Line Systems

The plant was one of two identical units employing a Pressurized Water Reactor (PWR) Nuclear Steam Supply System (NSSS) with four coolant loops furnished by Westinghouse Electric Corporation. Both units are similar to those of other plants recently licensed or currently under review by the U.S. Nuclear Regulatory Commission. Each of the two reactor cores is rated at 3,411 MWt.

2.2.1 High Pressure Safety Injection System Description

Two high pressure safety injection systems are used to inject coolant into the reactor coolant system (RCS) at high pressure (greater than 1600 psi) in the event of an S1 (1.5" to 3.0") LOCA. These systems are:

-Safety Injection Pump Injection System (SIPIS), and
-Centrifugal Charging Pump Injection System (CCPIS).

Each system uses two high head centrifugal pumps and is triggered by a safety injection signal generated either manually or by the safety injection logic. The flow diagram for the Safety Injection System is shown in Figure 2-1, with a safety injection coolant flow path traced in heavy dashed black lines.

Both injection systems draw borated water from the refueling water storage tank (RWST) and electrical power from the electrical power system (EPS). Injection into the RCS through the charging pump injection system requires the changing of the state of several flow control valves whereas injection through the safety injection pump systems requires no valve position changes. Flow from the charging pump injection system will generally pass through the boron injection tank (BIT), with alternate paths possible if manually actuated. Injection flow from both injection systems is generally into the cold leg of each of the four coolant loops with alternate

Figure 2-1

Flow Diagram Safety Injection System

(NOTE: See full-size map in back pocket).

injection paths provided into the hot legs.

An alternate path around the primary path from the RWST has been provided through the residual heat removal pumps to the suction side of both the safety injection and charging pumps. This flow path is not opened automatically by the safety injection logic and requires operator actuation.

Power for both sets of injection pumps is provided by the Electrical Power System (EPS). This system provides all electrical power down to 480 vac. Motor operated flow control valves are operated from this electrical power source. Electrical power for vital instrumentation and control is provided by the Protection Set (PS) system which converts the 480 vac to 120 vac and 125 vdc.

Centrifugal pump lubrication is achieved by self contained lubrication pumps and reservoirs. Pump heat removal is accomplished by the Component Cooling System (CCS), which rejects pump heat via the essential raw cooling water system to the atmosphere. The component cooling system requires motive power from EPS and control power from PS. Three of the five component cooling water pumps are normally off and must be turned on to function during safety injection. During normal operation, the A train charging pump and safety injection pump are not in service, however, they do receive cooling water (Table 9.2-3 FSAR [18]).

High pressure safety injection is actuated automatically by the safety injection logic (SILOGIC). Inputs to SILOGIC are derived from the vital instrumentation. Manual backups and overrides have been incorporated into the safety injection system to ensure reliability. The relationship of the major subsystems is shown schematically in Figure 2-2. More detail on the operation of each subsystem is given in the section which describes the construction of its digraph.

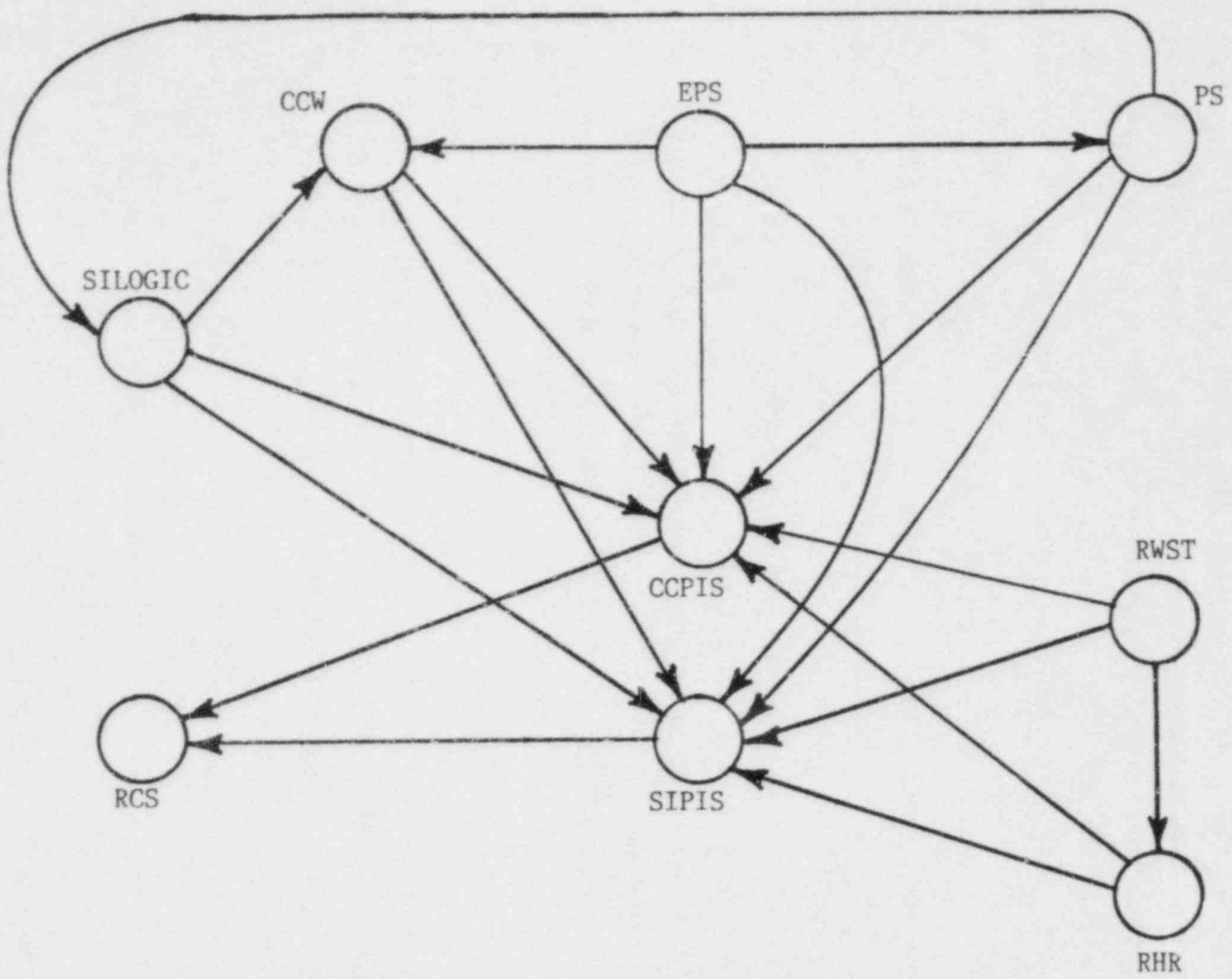


Figure 2-2. Approximate Relationship of Major Subsystems of High Pressure Safety Injection System

2.3 Overview of the Digraph Matrix Analysis Procedure*

Digraph Matrix Analysis can be broken down into the 4-step effort as shown below in Table 2-2. (A detailed description of the graph-theoretic basis of DMA and its computer codes is given in Appendix A.)

Step 1:	Select combinations of systems for detailed evaluation. (This is equivalent to the PRA event tree analysis designed to find accident sequences.)
Step 2:	Construct a global digraph model for each accident sequence.
Step 3:	Find singleton and doubleton and specific tripleton minimum cut-sets of accident sequences using the DMA codes.
Step 4:	Evaluate singletons, doubletons, and specific tripletons and display results.

Table 2-2. Overview of Digraph Matrix Analysis

Step one starts with the review of the plant design and continues with the development of complete accident sequences composed of combinations of safety subsystems which are required to respond to the accident.

The construction of the global digraph (step 2) follows an iterative procedure using a series of expansion steps. These expansions, which are centered on each of the components identified in the digraph, follow a specified algorithm. The expansion of each of these components identifies new components that must then be expanded. This expansion procedure is

* Digraph Matrix Analysis is described in NUREG/CR-2915, "Initial Guidance on Digraph-Matrix Analysis for Systems Interaction Studies at Selected LWR's".

repeated until all components of the subsystems have been included. As noted, each successive expansion identifies new components such as indicator lights, batteries, motors, etc. The expansion process also identifies subsystems, such as electrical power, which are required for component operation.

The expansion process is complete when no new components are identified or when all new components are outside of the physical or functional boundaries chosen for the system interaction analysis. This set of components may, at some later time, become a new set for expansion. The expansion of each component is performed using a specified algorithm called a "unit model", which specifies a description of the direct relationships of each component to the other components in the system. The following section contains a detailed description of the construction of the global digraph which represents the complete high pressure safety injection system and its support systems.

After the global digraph is constructed, it is processed through the DMA reachability code to determine all singletons and doubletons which can "reach" both the success criteria (RCS in this case) and every component in the global digraph. The reachability calculation is an analytic solution to the digraph model and does not perform a path finding operation or an exhaustive search on the input data. The reachability calculation solves for all connectivity between nodes in the network. These single and pairs of components would be called minimal cut sets in a traditional fault tree analysis. This processing is described in detail in Appendix A. The following section describes the construction of the global digraph.

2.4 Construction of Global Digraph

The High Pressure Safety Injection System (HPSIS) was analyzed to determine the components which could cause the failure of high pressure injection in response to an S1 LOCA (1.5" to 3.0") during its early stages. This analysis required the construction of a global digraph which included the safety injection system and its support systems. Included in this approximately 3700 node model were electrical power, component cooling, safety injection logic, and operator interactions with the plant subsystems.

The construction of the global digraph follows the procedure shown in Figure 2-3 and will now be discussed.

2.4.1 Review Final Safety Analysis Report and Collect Piping and Instrumentation Diagrams

The first step in the construction of the global digraphs was the review of the Final Safety Analysis Report (FSAR) [18]. A preliminary identification of the systems which would be called on to respond to an S1 LOCA in its early stages (at the low end of the LOCA size range) was made from this report. It was determined that the initial response to the LOCA would be emergency coolant injection (ECI) from the high pressure safety injection system. As discussed earlier, injection would occur due to the action of the safety injection pumps and charging pumps. These two sets of pumps and their associated emergency coolant flow paths are the front-line systems. Review of the piping and instrumentation diagrams from the FSAR allowed the identification of specific detailed plant diagrams which were obtained from the Watts Bar reactor operators during a plant visit. These schematics were then converted into a set of digraphs which represented the front-line systems and support systems using the procedure described below.

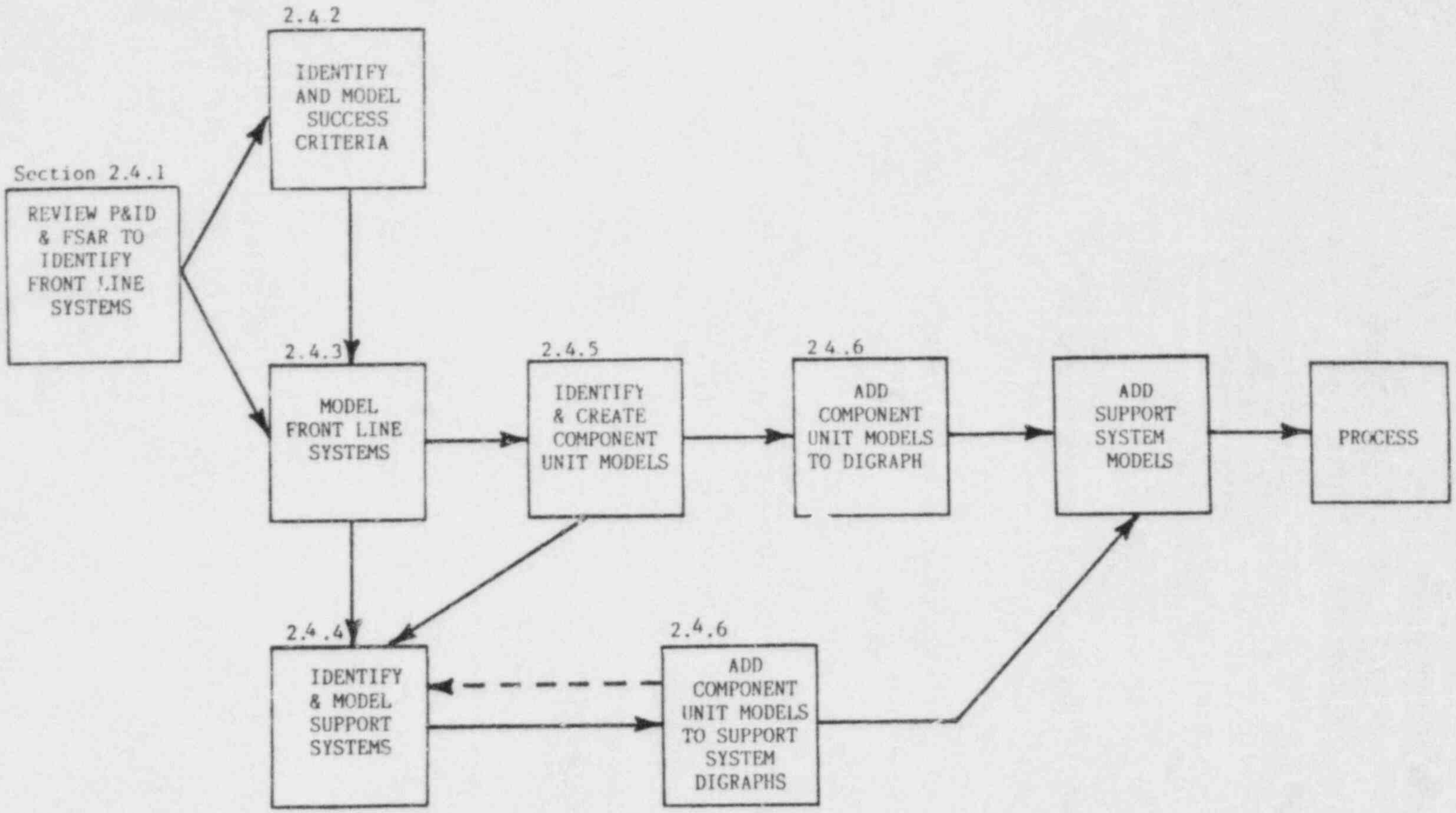

Section 2.4.1
REVIEW P&ID & FSAR TO IDENTIFY FRONT LINE SYSTEMS
2.4.2
IDENTIFY AND MODEL SUCCESS CRITERIA
2.4.3
MODEL FRONT LINE SYSTEMS
2.4.5
IDENTIFY & CREATE COMPONENT UNIT MODELS
2 4 .6
ADD COMPONENT UNIT MODELS TO DIGRAPH
ADD SUPPORT SYSTEM MODELS
PROCESS
2.4.4
IDENTIFY & MODEL SUPPORT SYSTEMS
2.4.6
ADD COMPONENT UNIT MODELS TO SUPPORT SYSTEM DIGRAPHS

Figure 2-3. Global Digraph Construction Procedure

2.4.2 Identify and Model the Success Criteria

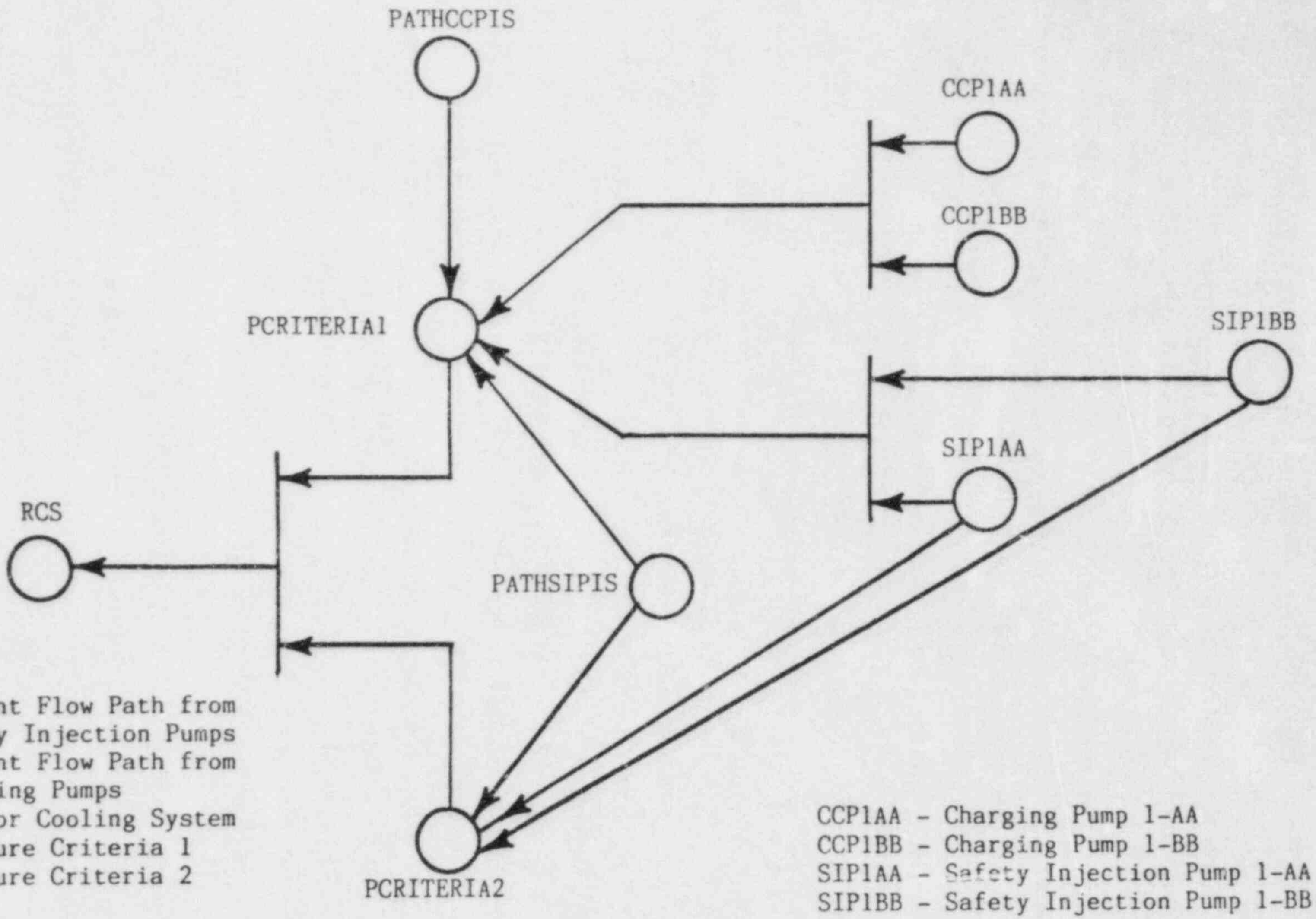
The accident sequence which was modeled is the failure of the high pressure safety injection system used for the emergency coolant injection (ECI) in response to a loss of coolant accident (LOCA) (1.5" to 3.0"). It has been assumed for the purpose of this study that both safety injection (SI) pumps *or* at least one SI pump and one centrifugal charging pump are required to supply adequate flow at *early* times in this scenario.* Following page 15.3-3 of the FSAR, we have not considered use of injection from the residual heat removal (RHR) pumps for this early time portion of the scenario (and for LOCA sizes at the low end of the range) although we have allowed the use of the flow paths through RHR from the RWST to the suction sides of the safety injection and charging pumps.

Success for high pressure safety injection is composed of two parts; a flow path to RCS and sufficient pressure to force coolant into the RCS. The digraph model for this success criterion is shown in the digraph of Figure 2-4 where PCRITERIA1 represents sufficient pressure from one safety injection pump and one charging pump and PCRITERIA2 represents sufficient pressure from both safety injection pumps. A violation of both of these criteria is required for a high pressure safety injection system failure. PCRITERIA1 will be violated if the path from the charging pump portion of the safety injection system, PATHCCPIS, *or* the path from the safety injection system, PATHSIPIS, *or* if both charging pumps fail, *or* if both safety injection pumps fail. PCRITERIA2 is violated if the path from the safety injection pumps fail *or* if either safety injection pump fails.

The nodes CCP1AA, CCP1BB, SIP1AA, SIP1BB, PATHSIPIS, and PATHCCPIS in the digraph become the nodes for which system digraphs will be constructed. That is, a complete system digraph will be constructed with these nodes as terminal nodes. Notice that a different success criteria (such as only one pump needed) would not require any changes in the global digraph except for the success criteria connections.

----

* This LOCA is called a "small LOCA" in Reference 17. The success criteria used for early times in this study is consistent with the criteria of this reference. An alternate success criteria allowing any two of the four pumps (SIP or CCP) was also examined with the quantitative results essentially the same.



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 2-4. Safety Injection Success Criteria

2.4.3 Model Front-Line Systems

The key diagram which was used in modeling the high pressure safety injection system is the diagram which was shown in Figure 2-1. The modeling was accomplished by tracing all the piping from the refueling water storage tank, the source of borated safety injection water, through the injection pumps to the RCS. A simplified flow diagram for the two safety injection systems is given in Figure 2-5.

As discussed above, there are two main portions of the high pressure safety injection system: SIPIS and CCPIS. Flow for SIPIS from the refueling water storage tank (RWST) will generally pass through the Safety Injection Pumps (SIP's) to the crosstie (DMA algorithm digraphing bi-directional flow) and then into the cold legs of the reactor cooling system (RCS). The digraph for the safety injection pump front-line system is called SIPISCORE. Flow from the charging pumps system will generally flow from the RWST through the charging pumps (CCP's) and the boron injection tank (BIT) to the coolant loops. An alternate path around flow control valve FCV635 and check valve VC63510, which must be manually actuated, is available from the RWST through the residual heat removal (RHR) pumps to both the safety injection and charging pumps. Another alternate injection path confirmed by the operators is the normal charging path from the CCP's and through the regenerative heat exchanger. This path must be manualy enabled.

The construction of the digraphs for the front-line system of the SIPIS and CCPIS is accomplished by tracing all paths from the source of the borated safety injection water to the core using the piping and instrumentation diagram of Figure 2-1. Figure 2-6 shows the digraph for the piping from the RWST to the pumps.

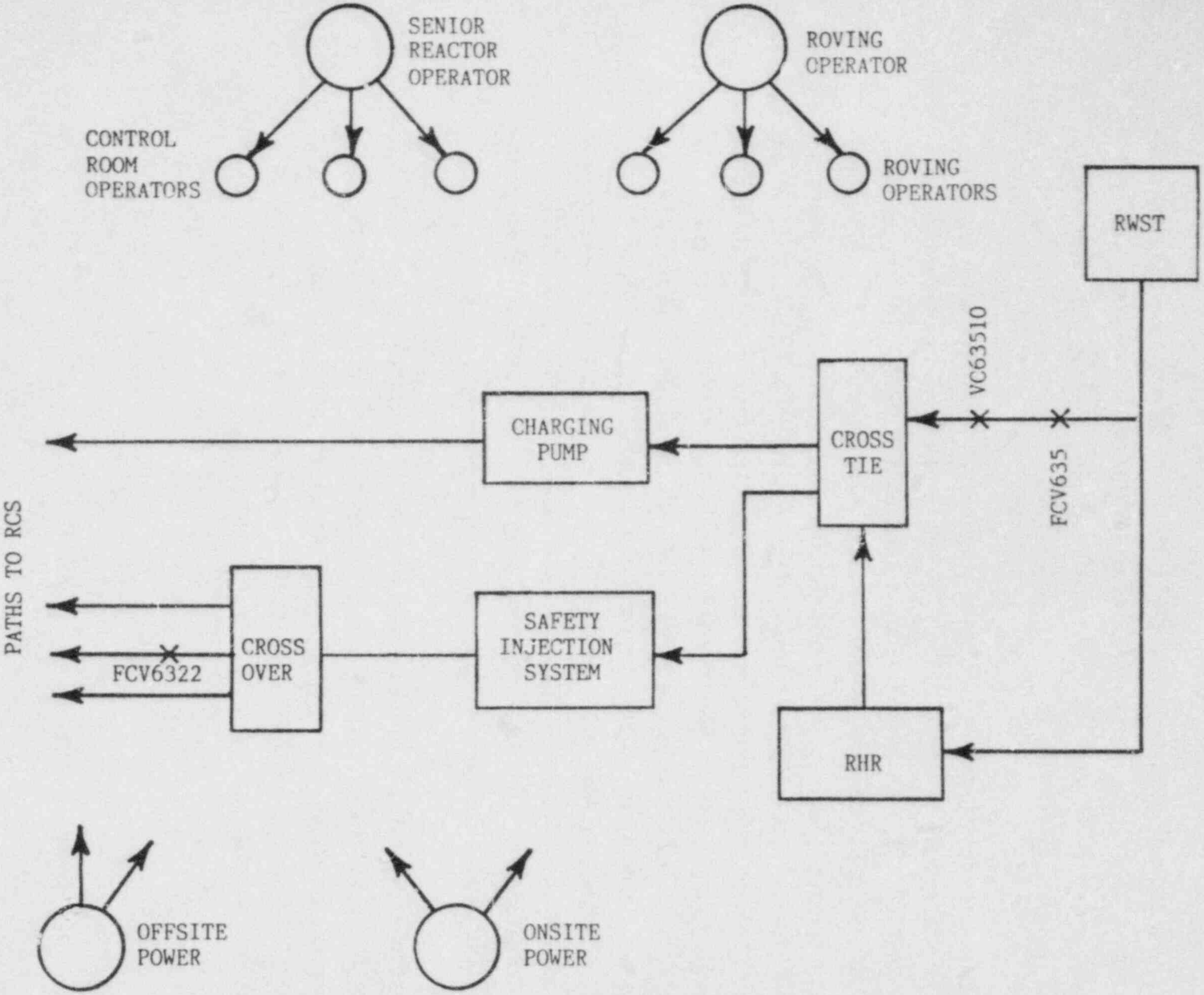
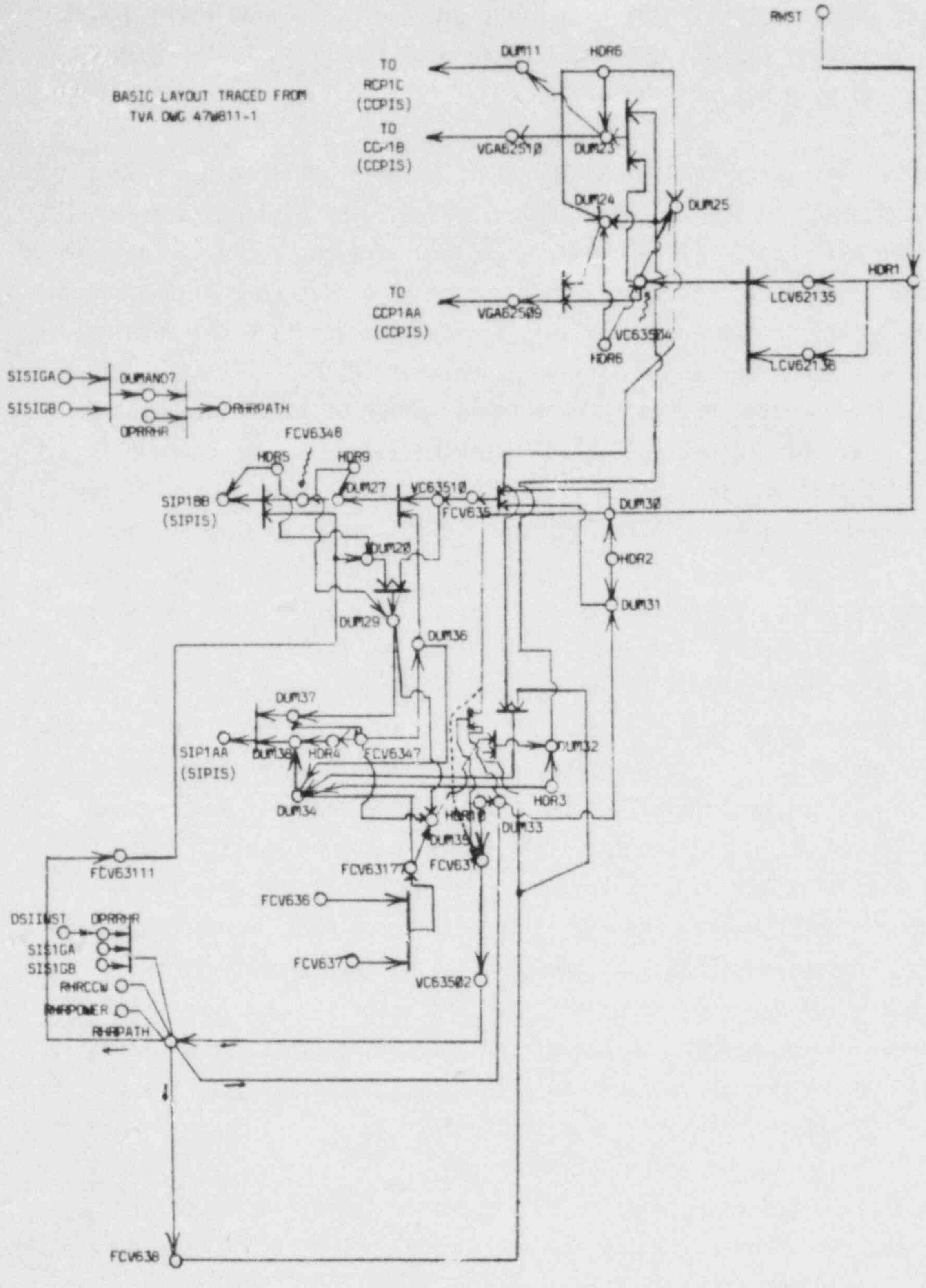


Figure 2-5. Overview of Front Line Systems



BASIC LAYOUT TRACED FROM
TVA DWG 47W811-1

Figure 2-6. RWST.DAT Network Connecting RWST to SIPIS & CCPIS

This digraph has been drawn so as to overlay on the P&ID of Figure 2-1. Notation consistent with the P&ID has been used throughout the digraphs to assist the reader. Each component on each of the paths in the P&ID is represented by a node in the digraph.

Figure 2-7 shows the portion of the SIPISCORE digraph from the safety injection pumps to the reactor cooling system. The digraph is drawn to represent that continuity of flow in any one of eight paths to the core is adequate for safety injection. In the digraph of Figure 2-7, the eight input AND gate to the node PATHSIPIS indicates that all eight paths would have to fail in order for a failure to reach PATHSIPIS. Flow to subgroups of these eight paths passes through at least one of three flow control valves, FCV63157, FCV6322, or FCV63156. The safety injection pump flow paths are "trained" to these valves with the upper train on the digraph corresponding to pump 1B-B and the lower train corresponding to pump 1A-A.

The designers have provided a cross-over from the train corresponding to safety injection pump 1B-B to valves FCV6322 and FCV63156.
A cross-over from TRAIN A is provided to corresponding valves in TRAIN B. It can be seen from this digraph that a failure in RWST would propagate forward through both safety injection pump trains to the cross-over network. In the absence of the path through the residual heat removal system (RHRPATH), a failure in either RWST, FCV635 or VC63510 would stop the flow in both trains. At this level of modeling, the only singletons for the SIPISCORE portion of safety injection are RWST, HDR1, HDR2, HDR9, FCV6322, FCV635 and VC63510 (without residual heat removal paths). Flow through the residual heat removal pumps and associated hardware would remove two of the header and two of the valve singletons. Doubletons for SIPISPATH occur due to failures in both safety injection pump trains. For example, SIP1BB and SIP1AA form a doubleton.

The centrifugal charging pump injection system (CCPIS) draws borated water (concentration of boron is approximately 2000 ppm) from the refueling water storage tank (RWST) for injection into the core. Like the safety injection pump injection system, this injection system employs two high head pumps to

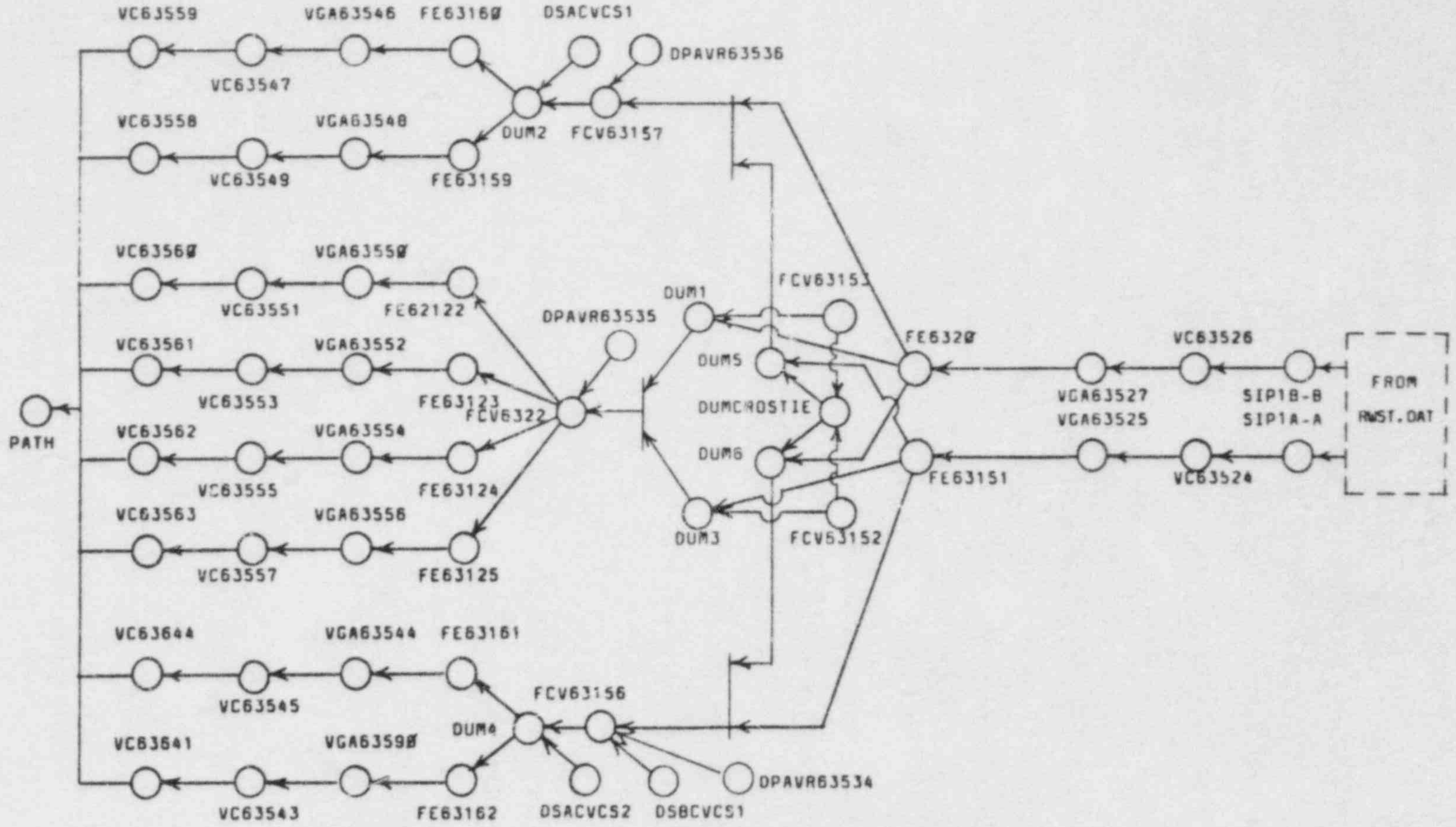


Figure ?-7. Safety Injection Pump Path to the Core. SIPIS pressurize the flow. In this injection system, though, the path to the core is not normally open and several valves must be actuated to enable the injection paths. A principal feature of this system is the boron injection tank (BIT), a 900 gallon vessel filled with highly concentrated borated water (concentration of boron is 21000 ppm) maintained at 135°F or above to maintain solubility. During normal plant conditions, flow is routed through a path between the Boron Recycle System (BRS) and the BIT to maintain the boron concentrations in the tank and to keep the coolant from stratifying.

At receipt of the safety injection signal, several components in the charging system actuate. The two charging pumps turn on and 13 valves reorient to isolate the BIT from the BRS and align the pumps with the BIT for injection to the core. Figure 2-8 shows the digraph for the portion of the charging pump system downstream of the charging pumps. In the modeling of the front-line systems several components that must actuate have been identified. These components must be expanded via unit models.

The digraph construction procedure described to this point models only the effects of the blockage of a path. In order to model the integrity of the path from the RWST to the core, effects of flow diversion due to leakage must be considered. The digraph model of break propagation is similar to the model of flow blockage since the physical paths along which both effects propagate are identical.* The digraphs are not identical, however. A blockage is a failure which propagates downstream only, in effect causing failures in downstream path because of the inability of coolant from the RWST to reach those points. But when a component ruptures, leaks, or breaks, a "sink" is created into which coolant from any direction may be drawn. Thus, a break anywhere in the system may prevent flow from reaching the core even in a parallel redundant path.**

----

* A more detailed description of break modeling is given in Appendix A.

** Valves have been placed in the piping to isolate these breaks and thus mitigate the effects of pipe breaks.

The effects on the injection system hydrodynamics of any specific break is a complex function of the configuration of the piping network, the break size, and location as well as the initial system pressure and other system parameters. It was not within the scope of this project to generate this function; however, a very conservative model was developed based upon the following assumptions: 1) The effects of all breaks in the primary injection path propagate identically, 2) pumps introduce no mitigating effects.

The models for break propagation in the high pressure injection systems appear in Figures 2-9 and 2-10. The main difference between these breakage models and their blockage counterparts (Figures 2-7 and 2-8) is that all AND-gates have been replaced by OR-gates and that nearly every edge between break nodes is unconditionally bidirectional. These breakage models are valid only for the case of no human intervention to change the piping network to mitigate break effects. The model could have been generalized to include this capability with the addition of "mitigation" unit models, however, this was outside the project scope. Also, no paths through the residual heat removal system through which breaks can propagate or originate have been included.

In the break model digraphs, nodes in the break propagation model are either unprimed, single primed, or double primed. An unprimed node is one which also appears in the blockage model. There are a few connections between the two models which will be explained later. Singly primed nodes represent breakage of a component or the pipe connecting it to the next component downstream. There is a one-to-one correspondence between these nodes and unprimed nodes. Doubly primed nodes represent special cases in which break effects are kept from propagating due to automatic mitigators such as check valves or normally closed valves. These mitigating nodes are AND-ed with the normal propagation path and their failure represents the enabling of a break propagation path through them. Failure of a check valve which is double primed implies its ability to block flow in one direction has failed. Failure of a normally closed valve which is double primed implies that it is open. Of course, each of these components has a

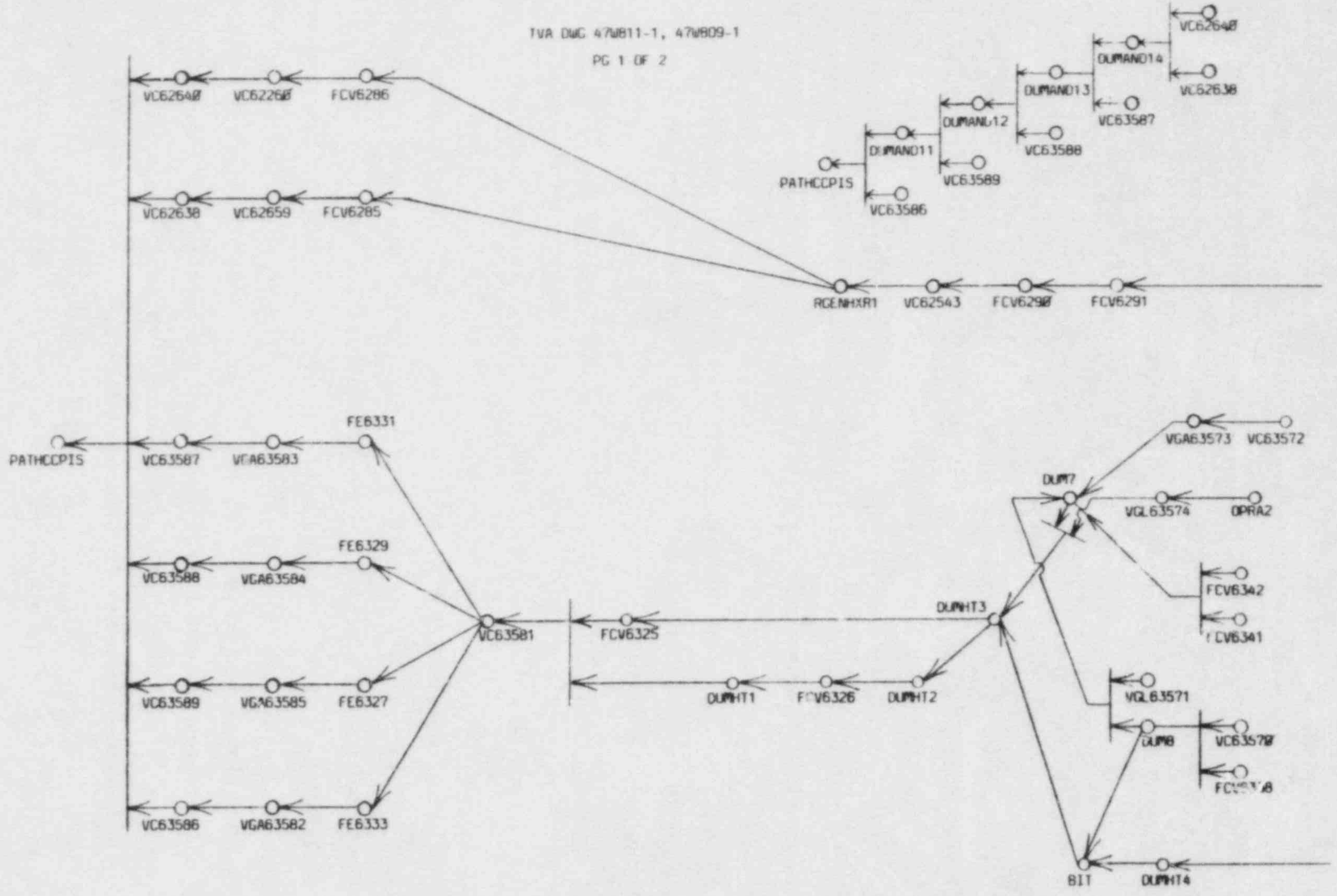
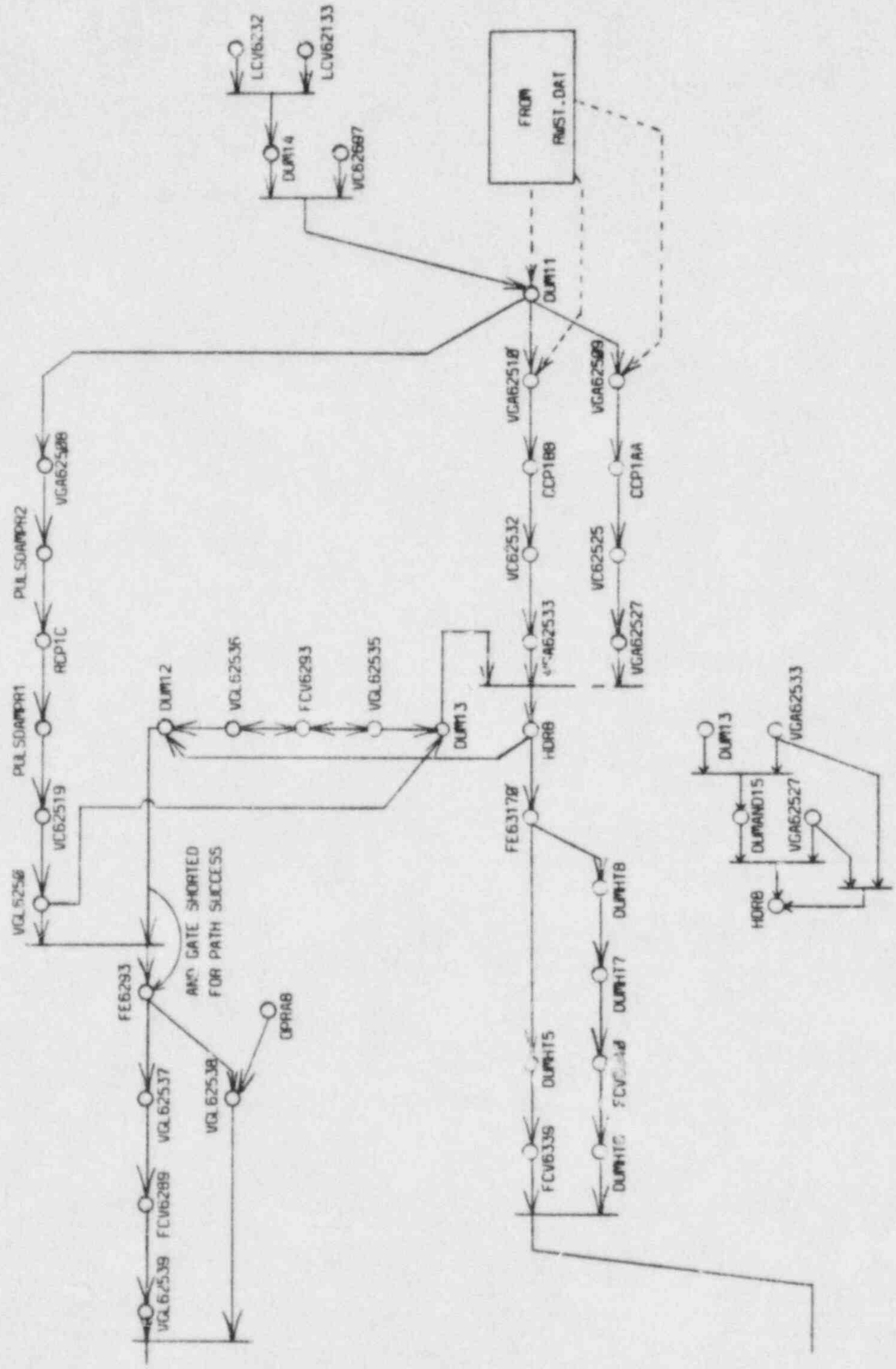


Figure 2-8. Charging Pump Path to the Core, CCPIS

PG 2 OF 2


LCV6232
LCV62133
DUM14
VC62687
FROM
RWST.DAT
DUM11
VGA62508
PULSDAMPR2
RCP1C
PULSDAMPR1
VC62519
VGL6256
VGA62510
CCP1BB
VC62532
VGA62533
VGA62509
CCP1AA
VC62525
VGA62527
DUM12
VGL62536
FCV6293
VGL62535
DUM13
HDR8
FE63170
DUMHT8
DUMHT7
FCV6
DUMHT5
FCV6339
DUMHT6
AND GATE SHORTED
FOR PATH SUCCESS
FE6293
OPRA8
VGL62537
VGL62538
FCV62089
VGL62539
DUM13
VGA62533
DUMAND15
VGA62527
HDR8

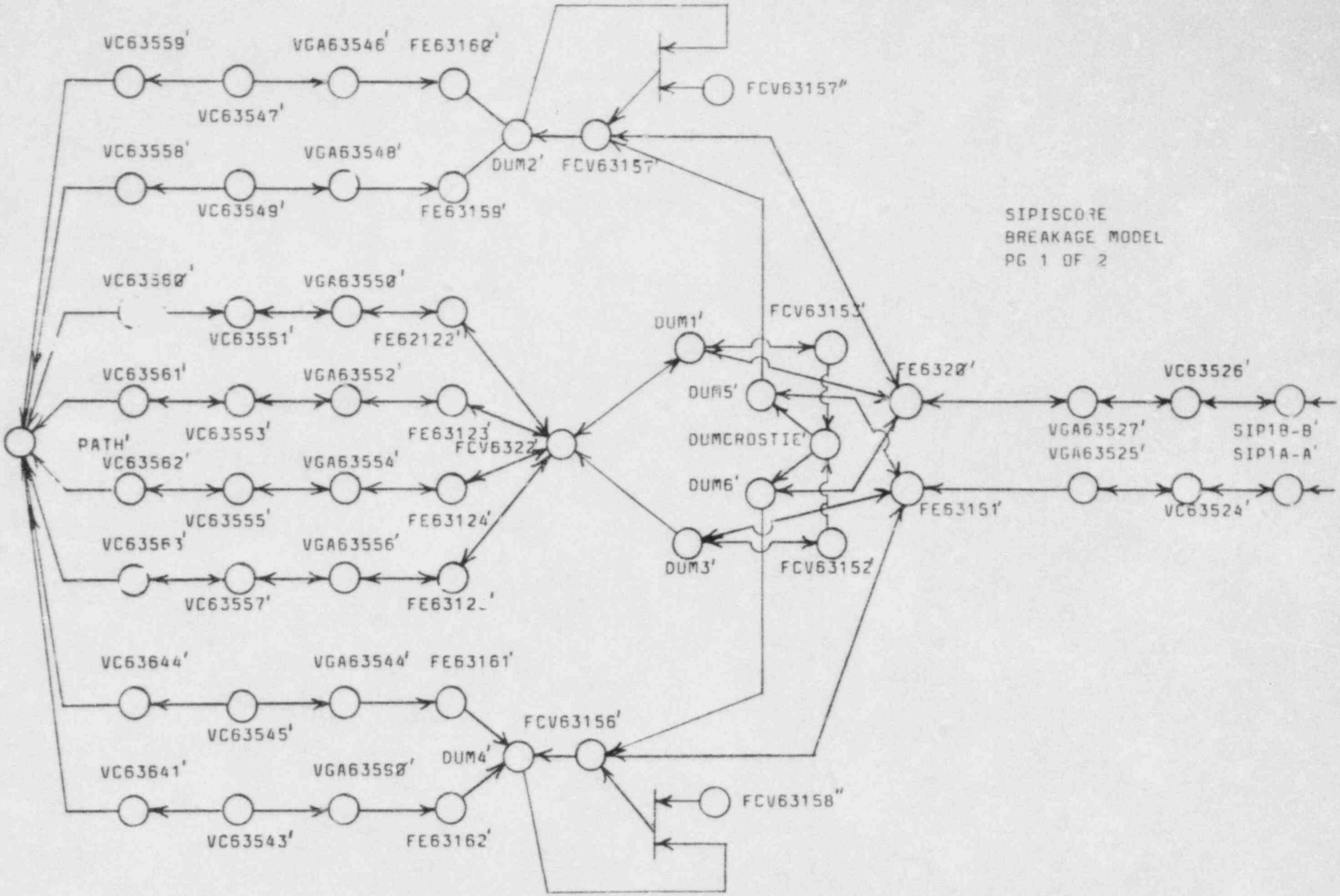
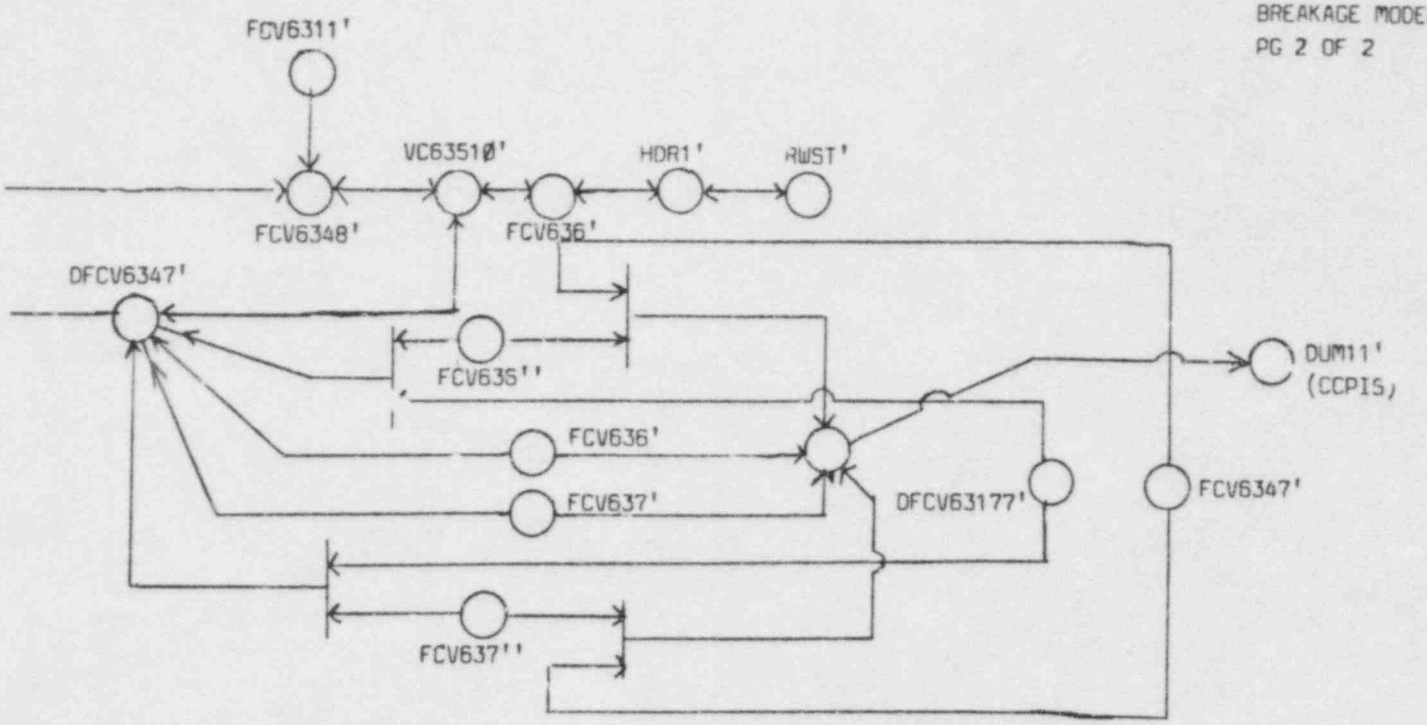


Figure 2-9. SBREAK.DAT Break Model for SIPIS

SIPISCORE
BREAKAGE MODEL
PG 2 OF 2



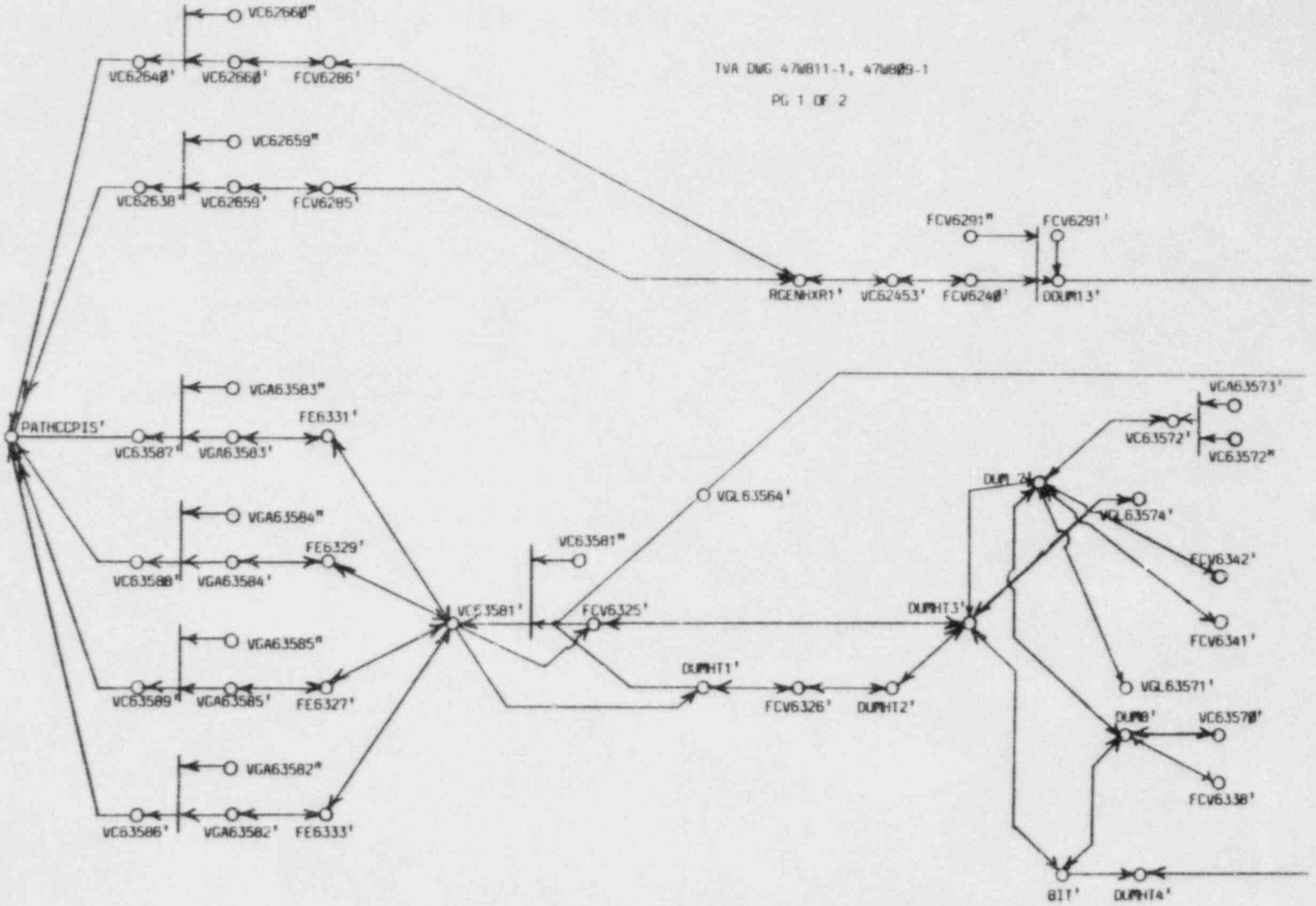
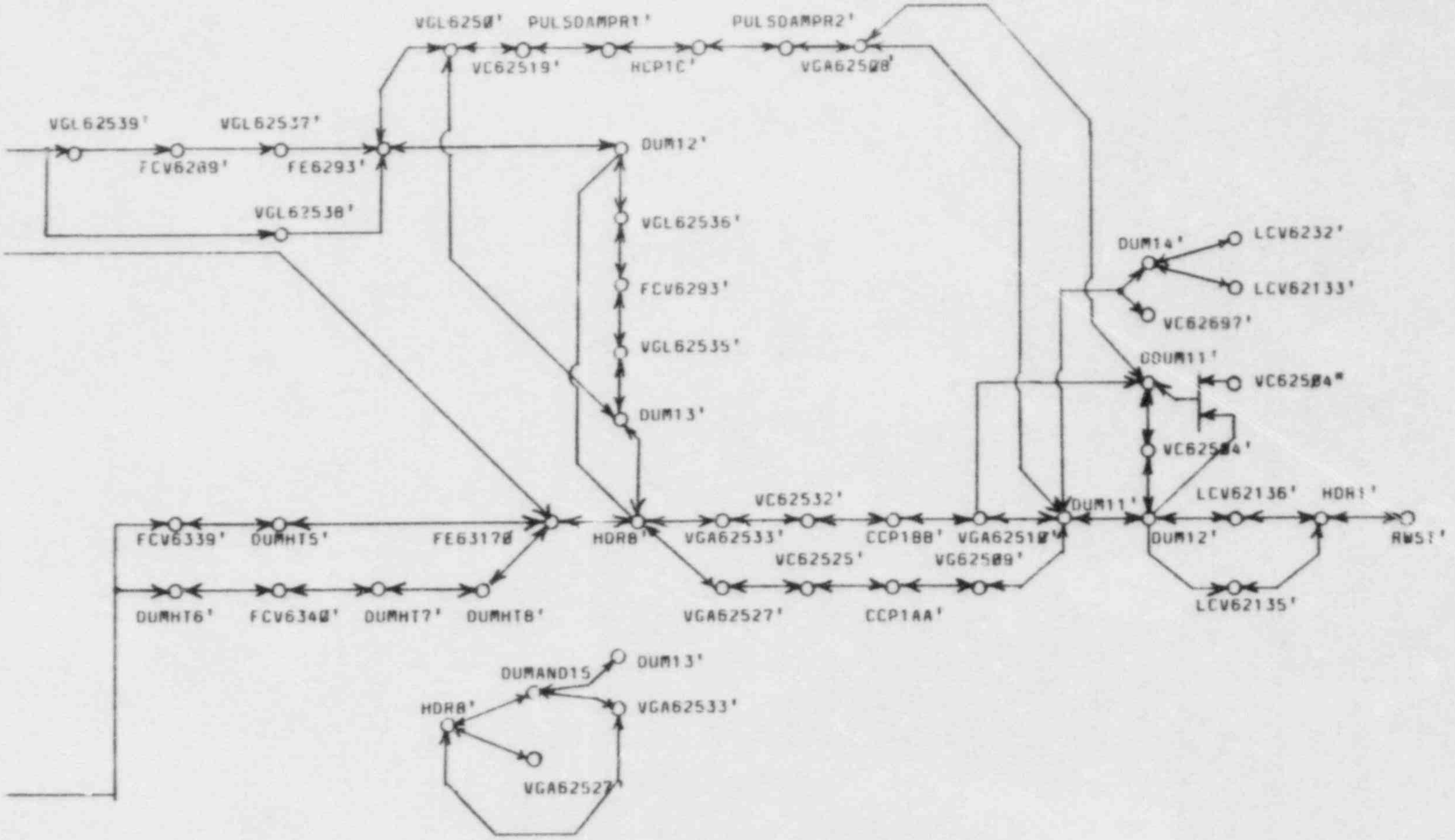


Figure 2-10. CBREAK.DAT Break Model for CCPIS

TVA DWG 47W811-1, 47W809-1

PG 2 OF 2



primed counterpart since they can break as well.

The terminal nodes for these two models are the primed versions of the terminal nodes which appear in the blockage model. Both primed terminal nodes connect to their unprimed versions which are connected to the system success criteria. This represents the fact that the inability to inject through a path can be the result of breakage <u>or</u> blockage. Also, each primed pump connects to its unprimed counterpart since a ruptured pump cannot generate pressure and therefore cannot contribute to satisfaction of the success criteria. These are the only connections between the primed and unprimed systems.

2.4.4 Identify and Model Support Systems

Components of front-line systems which change state (such as the opening and closing of motor-operated valves) require support systems for operation. These support systems were identified by expansion of the components into unit models and are listed below.

PS	- Protection Set
EPS	- Electrical Power Supply
SILOGIC	- Safety Injection Logic
CCS	- Component Cooling System

Large portions of the support systems can be considered as super unit models. For example, there are four nearly identical portions of the Protection Set. One of these was modeled in detail, then reused (with the appropriate labeling and component modifications) as the three other portions.

2.4.5 Identify and Create Component Unit Models

Many of the components identified in the digraphs of the front-line and support systems can now be expanded using the appropriate unit model. This expansion procedure, in addition to providing detail about the operation and construction of specific components, identifies additional support systems necessary for safety injection. For example, unit model expansion for a Flow Control Valve (FCV) identifies Electrical Power Support (EPS), Protection Set (PS), and Safety Injection Logic (SILOGIC) as support systems for safety injection as well as the operator inputs which function as backup to the automatic system, and operator inputs which can defeat the correct operation of the component.

Unit models are constructed using detailed information about the mechanical configuration, operation, control, and connectivity of a component in the system. Unit models for the specific use of a component are generally created from a generic unit model for the component type. Thus a unit model may be used many times in a system digraph with appropriate modification and notation. In modeling the front-line portion of the safety injection system, the following unit models were used:

FCV	- Flow Control Valve
PUMP	- Pump
SOLFCV	- Solenoid Valve
PS	- Protection Set
BREAKER	- Breaker Transfer Hardware
250VBAT	- 250 Volt Battery System

A detailed generic unit model was created for each of these components and then tailored to the specific application within the system digraph. Each of these unit models was independently tested, debugged and revised before being integrated into the global digraph. The digraph and commented adjacency element data for each of these models is presented in Appendices B and C, respectively. The construction of the unit model for the flow control valve will be described in detail below along with a brief summary of the construction of two other unit models.

2.4.5.1 Flow Control Valve Unit Model

The flow control valve* can be actuated in three ways, two by the motor (remote and local), and one by manual cranking of the link (LINK1) to the valve plug. The valve is normally driven from an electric motor, MOT1, which draws power from a 480 vac Reactor Motor Operated Valve Board (POWER1) in the Electrical Power Support (EPS) system. If the motor drive were to fail, the operator (OPRA1) could override. Thus both the motor and the operator would have to fail for the link not to be turned. This redundancy is shown in Figure 2-11 as an AND gate to the valve plug.

Control of Motive Power to Valve Motor (See Figure 2-12)

The valve motor, MOT1, needs both a control signal and electrical power to operate. The control signal energizes the relay coil, COIL1, which closes Switch, SW51. Motive power from the variable magnetic overcurrent trip, VMOT1, then flows through switch, SW51, to contact 1, CON1, and then to the motor. The current to the over current trip, VMOT1, passes through relay, R1, and comes from a 480 vac Reactor Motor Operated Valve Board, POWER1.

Control Power Switching (See Figure 2-13)

Limit switch SW56 enables current to flow to COIL1 if the valve isn't being commanded to open when it is already open and vice-versa. Two other switches, SW54 and SW59, act similarly. Power to SW56 and COIL1 is supplied through actuation of one of four switches. These are:

SWA1	- The normal remote operator actuated switch
SWB1	- A local operator switch (at the valve)
SWC1	- Alternate remote operator actuated switch
SWSI2	- The automatic actuation switch.

-----

* Details about the valve operation and construction were obtained from Drawings: 45W760-63-8 and 45W751-8.

Legend

FCV	=	Flow Control Valve
LINK2	=	Mechanical shaft which moves valve plug
MOT	=	Valve Motor
OPRA	=	Operator who overrides valve motor

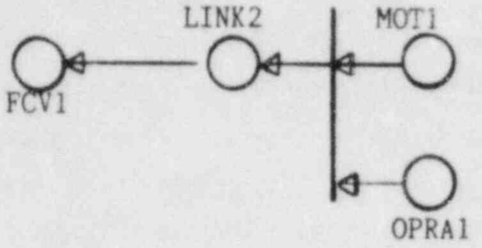


Figure 2-11. Redundancy to Valve Link

Legend

VMOT	=	Variable magnetic overcurrent trip
CON	=	Contact
COIL	=	Relay coil
SW	=	Switch
R	=	Relay
POWER	=	Reactor power board

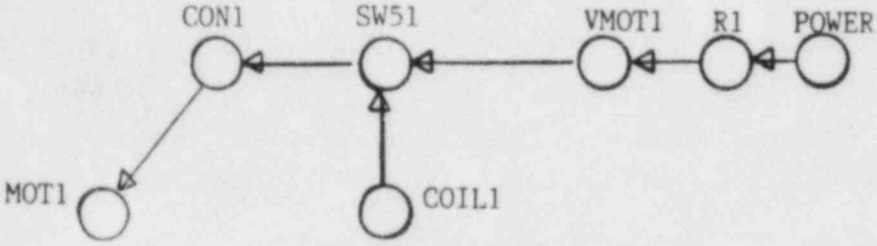


Figure 2-12. Control of Motive Power to Valve Motor

Legend

COIL	=	Relay coil
SWA	=	Normal remote operator actuated switch
SWSI	=	Automatic actuation swtich
SWC	=	Alternate remote operator actuated switch
SWB	=	Local operator operator switch (at the valve)

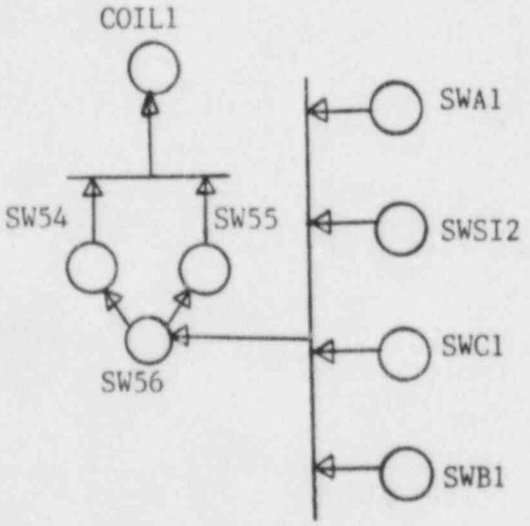


Figure 2-13. Control Power Switching

Safety Injection Logic Activator (See Figure 2-14)

The flow control valve automatic actuation occurs when SWSI2 closes. This switch closes on receipt of the safety injection logic signal, SILOGIC1, unless the switch, SWA4, has been switched from the "auto" position by the operator, OPWF1. The node OPWF1 represents the failure of the operator to leave this switch in the "auto" position. Control power which will pass through this switch comes through the fuse, FUSE2, from the transformer, XFMR1. The circuit is completed to the positive pole if FUSE4 is intact.

Remote Operator Switch (See Figure 2-15)

Switch SWA1, the normal remote operator actuated switch, receives its power from FUSE2. The switch is actuated by a remote operator, OPRF1, in the main control room who receives information on the need for safety injection from the safety injection instrumentation, DSIINST, and from the knowledge that the valve is in the wrong position, DUM11. The operator can get this information in one of five ways, all of which must fail in order for no information to be available. These are:

1. The local operator at the valve, OPRC1;

2. An indicator light, LT2 (Red or Green);

3. An indicator light, LT1 (Green or Red);

4. Flow data, FDATA; and

5. A local operator at the valve who manually operates the valve, OPRA1.

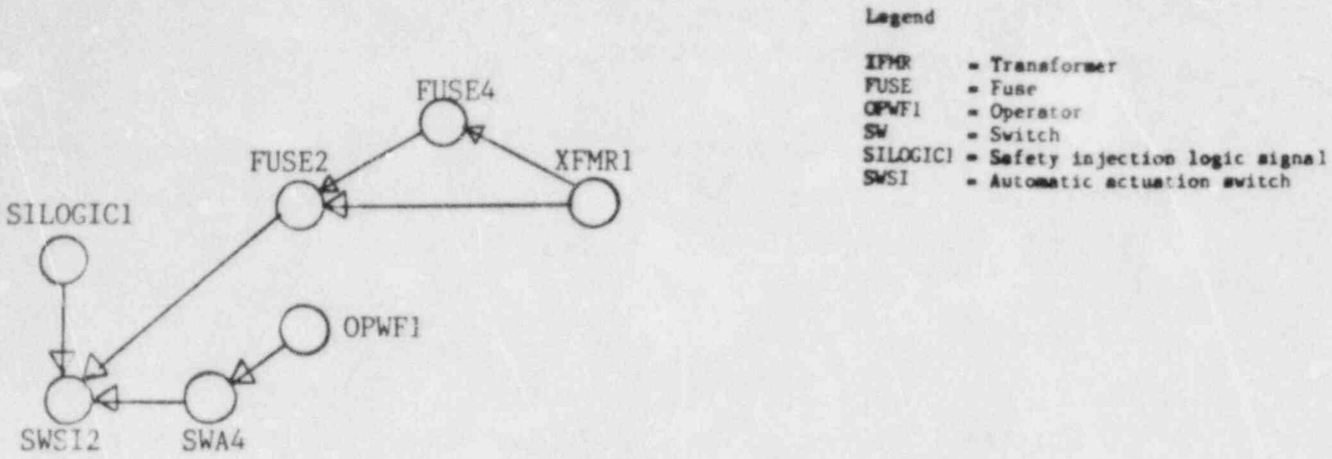


Figure 2-14. Safety Injection Logic Activation

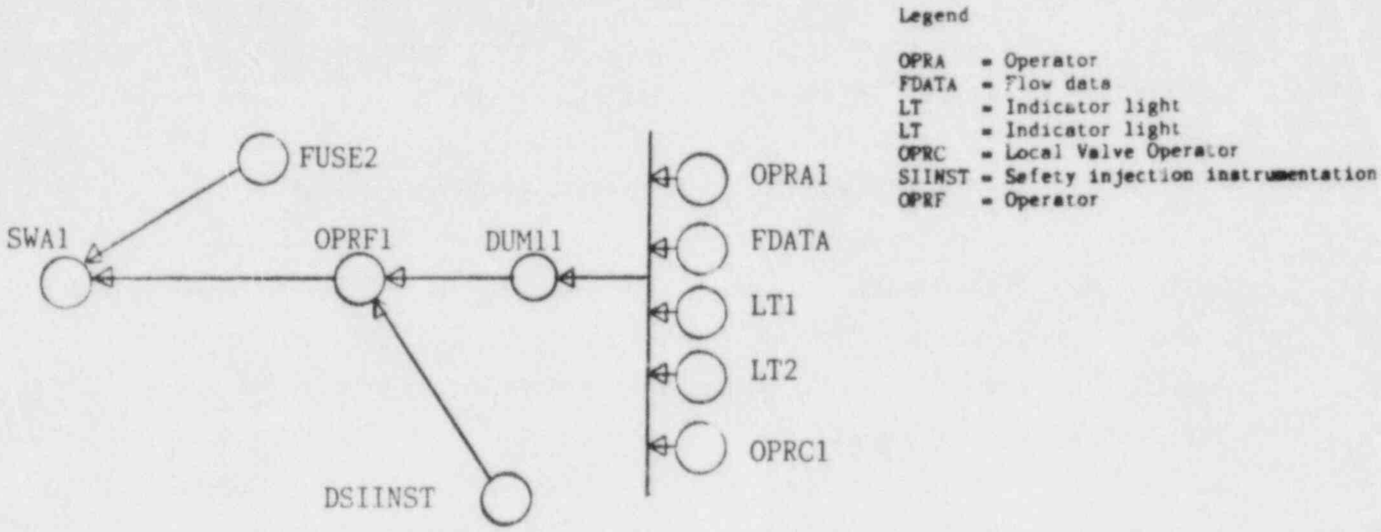


Figure 2-15. Switch SWA1

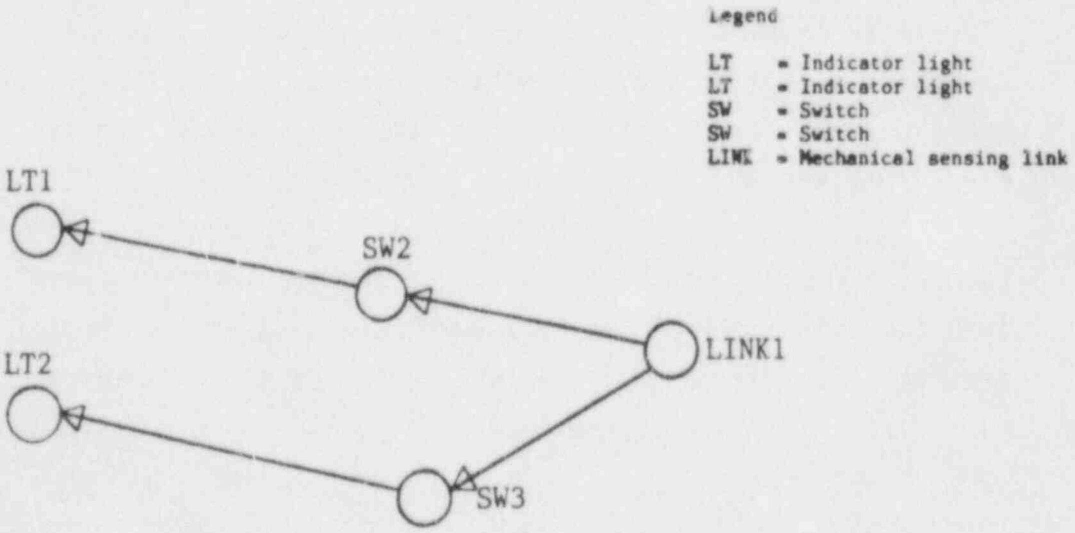


Figure 2-16. Indicator Light Actuation

Indicator Light Actuation (See Figure 2-16)

The indications of valve position, LT1 and LT2, are derived from two separate switches, SW3 and SW2 which are driven by the mechanical sensing link, LINK1, attached to the valve plug.

Power for the Valve Heater (See Figure 2-17)

Power for the valve heater, VHTR1, comes through either FUSE1 or FUSE2 from transformer, XFMR1. The power is routed generally through FUSE2, unless the remote operator, OPRF3, switches the transfer switch SWX1. The operator would switch over on the basis of an indicator light, LT5 or on indication of valve position data, DUM11.

Backup Remote Operations (See Figure 2-18)

Switch SWC1, the remote backup actuation switch receives its power from FUSE1 and must be actuated by a remote operator, OPRF2, who needs information from the safety injection instrumentation and the valve position indication, DUM11.

Local Operator Valve Actuation (See Figure 2-19)

Switch SWB1, the local operator actuated switch that enables control power from either fuse, DUM12, is actuated by the local operator OPRC1. This operator responds to valve position indication, DUM13. Indicators LT4 and LT3 are separate local indicators, hence separate from LT1 and LT2. This operator is also allowed all of the information available to the remote operators, DUM11. LINK1 represents the direction of the resistance to manually cranking the valve stem.

Each of the parts of the operation of the Flow Control Valve are combined into the unit model of Figure 2-20. Depending on the specific implementation of the FCV, various nodes, such as lights or operators, may be fed from a single master node. It is easy to see how common location,

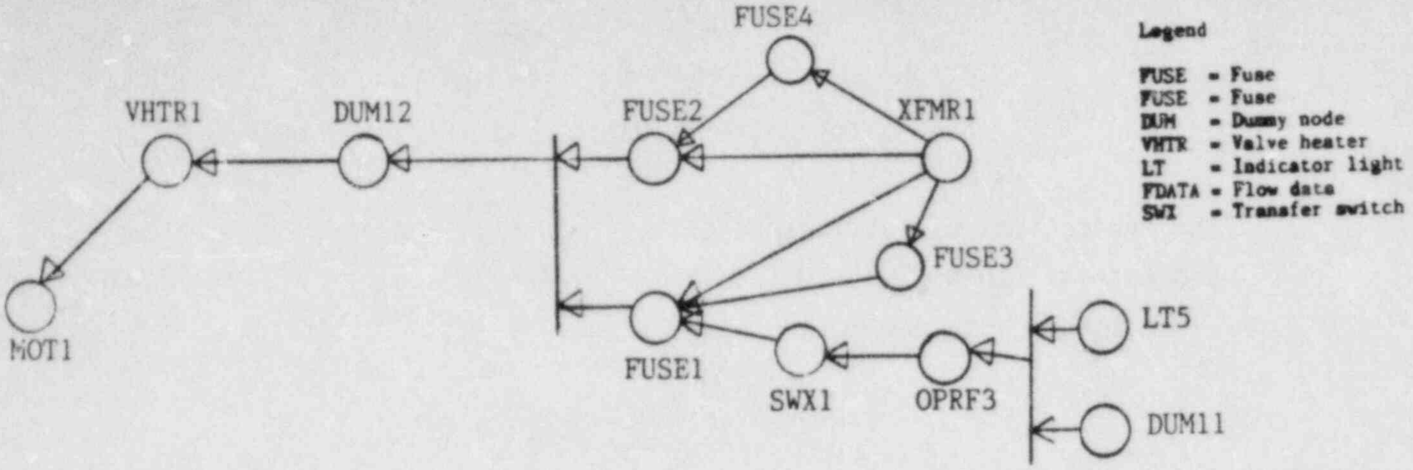


Figure 2-17. Power for the Valve Heater

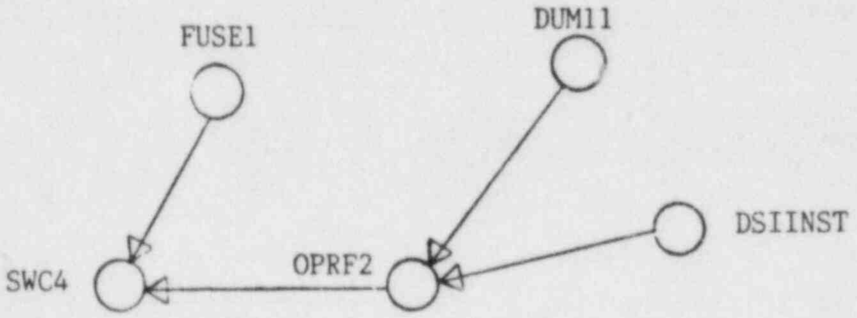


Figure 2-18. Backup Remote Operations, SWC1

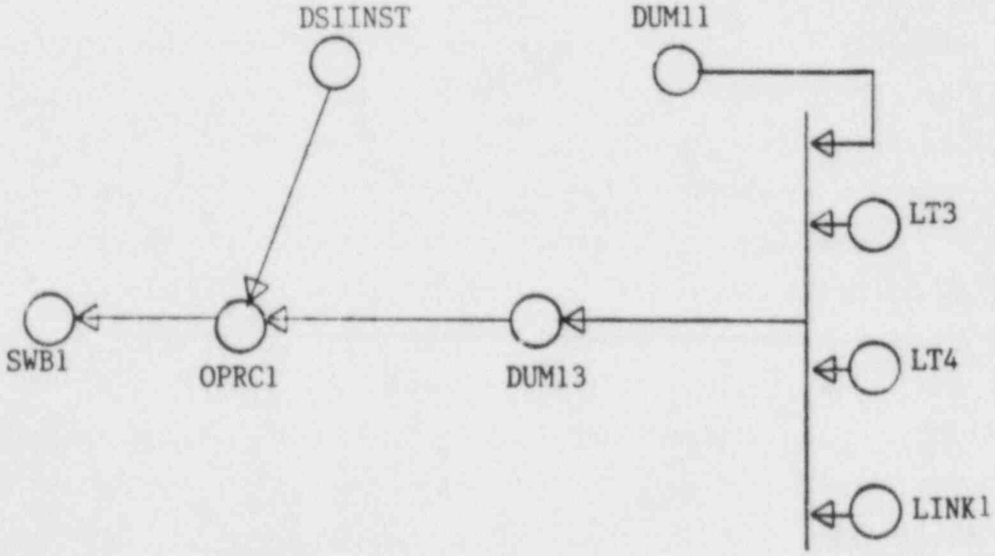
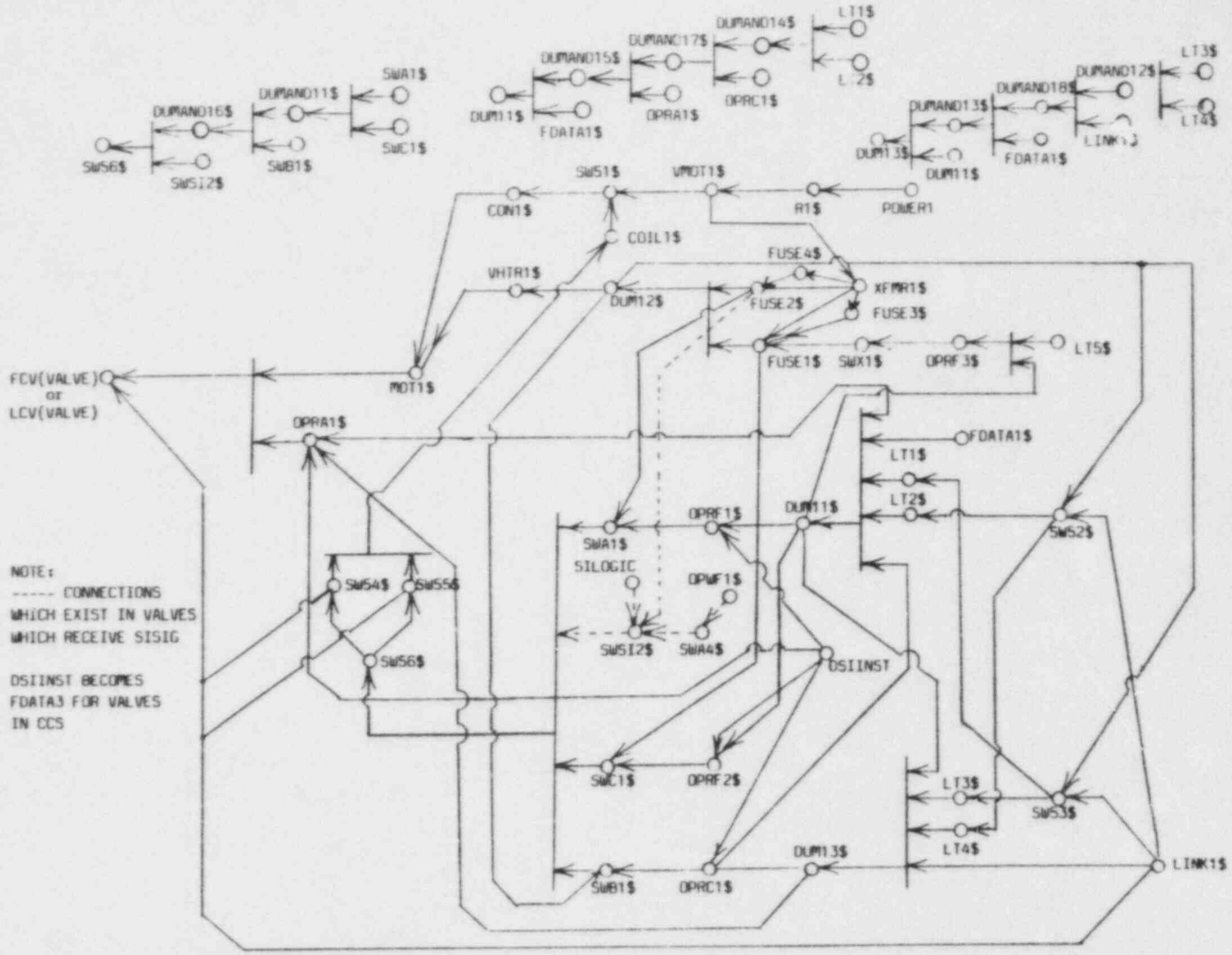


Figure 2-19. Local Operator Valve Actuation



NOTE:
----- CONNECTIONS
WHICH EXIST IN VALVES
WHICH RECEIVE SISIG

DSIINST BECOMES
FDATA3 FOR VALVES
IN CCS

Figure 2-20. FCV.DAT Flow Control Valve Unit Model

manufacturer, and maintenance could be added to the unit model.

Table 2-3 is the adjacency element data for the FCV unit model. The decomposition of multiple input AND gates into a series of two input AND gates is done to fit within the constraints of the present codes.

2.4.5.2 Solenoid Valve Unit Model (Figure 2-21)

Three solenoid valves are used in the CCPIS portion of HPSIS. These valves are open under normal plant conditions, enabling flow between the boron recycle system and the boron injection tank. When the valve solenoid coil is energized, the valve plug is lifted out of the flow path. The valves are therefore designed to fail safe, closing upon loss of power. During an accident, each valve succeeds if power to the coil is switched off and this can be accomplished manually or automatically.

Any one of the three switches, SWA2$, SWC1$, SWSI1$, can cut the power to the coil. The first two switches are manually actuated and remote, i.e., away from the locality of the valve. Since the valve is supposed to close during an accident, the operators actuating these switches are performing a function which is "right", i.e., beneficial to the system, so the nodes are labeled OPR. Like the operator nodes in the other unit models, they have two inputs and one output. The operator knows an accident is occurring from the safety injection instrumentation (DSIINST), and that the valve must change position from the position indicating lights LT1$ - LT4$. All four lights monitor the position of the valve plug via two sense switches, SW1$ and SW2$. The output from each operator node is the signal to actuate that operator's switch to cut power to the coil.

Switch SWSI1$ connects to the automatic safety injection signal logic and opens upon receipt of safety injection. This automatic mode must be enabled beforehand by an operator and therefore can be disabled by an OPW, an operator who does the "wrong" thing and degrades the system. In this case, OPWF1$ can use switch SWA1$ to disable the automatic closure of the valve.

```
      ADJACENCY INPUT FOR MOTOR OPERATED FLOW CONTROL VALVE UNIT MODEL

                         DATA FROM TVA DWG 45W760-63-8

   ¶     To create a unique valve, change (VALVE) to valve number, POWER1
   ¶     to motive power source, SILOGIC1 to logic train, and $ to component
   ¶     index. If valve connects to SILOGIC, remove tabs in '*Connections...'.
   ¶     This model is for a valve which must be opened.  If specific valve
   ¶     is of same type, search for all 'closed#' and 'open#' and delete '#'.
   ¶     If specific valve is of the opposite type, search out the words,
   ¶     delete '#', and replace the words with their complements.
   ¶
   ¶     D E L E T E   A L L   L I N E S   B E G I N N I N G   W I T H   " ¶ "

         ** FCV(VALVE) **
LINK1$,FCV(VALVE),1         LINK1$ is connection from MOT1$ to FCV(VALVE).  MOT1$
MOT1$,FCV(VALVE),OPRA1$ is the motor that moves valve plug FCV(VALVE).  OPRA1$
OPRA1$,FCV(VALVE),MOT1$ determines whether FCV(VALVE) is open or closed from
DUM13$,OPRA1$,1         flow data, valve position indicating lights, and
                        direction of resistance to cranking of LINK1$.
                        LINK1$ is the connection from the operator's hand
                        to the valve plug.  These valve status parameters
                        for local OP's are AND-ed inputs to DUM13$.
CON1$,MOT1$,1           CON1$ is wire connection.
SW51$,CON1$,1           SW51$, when closed, allows power to flow to MOT1$.
VMOT1$,SW51$,1          VMOT1$ is Variable Magnetic Overcurrent Trip.
R1$,VMOT1$,1            R1$ is a relay.
POWER1,R1$,1     POWER1 is process electrical power.
VHTR1$,MOT1$,1          VHTR1$ is valve heater.
DUM12$,VHTR1$,1
FUSE2$,DUM12$,FUSE1$    FUSE2$ is normal control power positive voltage fuse.
XFMR1$,FUSE2$,1         XFMR1$ is potential transformer.
XFMR1$,FUSE3$,1
FUSE4$,FUSE2$,1         FUSE4$ is normal control power negative voltage fuse.
XFMR1$,FUSE4$,1
FUSE3$,FUSE1$,1         FUSE3$ is auxillary control power neg. voltage fuse.
VMOT1$,XFMR1$,1
FUSE1$,DUM12$,FUSE2$    FUSE1$ is auxillary control power pos. voltage fuse.
XFMR1$,FUSE1$,1
SWX1$,FUSE1$,1          OPRF3$ monitors with LT5$ the power out of the control
OPRF3$,SWX1$,1          power fuse and can use SWX1$ to switch to the
LT5$,OPRF3$,DUM11$      auxillary fuse.  OPRF3$ also uses remote valve position
DUM11$,OPRF3$,LT5$      data DUM11$ to ascertain if valve can be actuated.
COIL1$,SW51$,1          COIL1$, when energized, closes SW51$.

SW54$,COIL1$,SW55$      COIL1$ can be energized iff valve is not fully open#
SW55$,COIL1$,SW54$      as determined by sense switch SW56$.
LINK1$,SW54$,1
LINK1$,SW55$,1
SW56$,SW55$,1           SW55$ is pos'n sense switch (closed iff valve closed#).
SW56$,SW54$,1           SW54$ is torque limit switch (open iff valve open#).
LINK1$,SW56$,1
SWB1$,SW55$,DUMAND51$   SWB1$ is local switch which electrically energizes
DUMAND51$,SW56$,SWB1$   COIL1$.
```

Table 2-3. Adjacency Input Data for FCV.DAT

```
          *Connections for hardware connected to SILOGIC*
     Indented 1 tab since not used in SIPIS.  If used, remove tabs and
     indent the 2 lines of code above this insert.
          SWSI2$,SW56$,DUMAND56$  SWSI2$ closes upon receipt of SILOGIC signal.
          DUMAND56$,SW56$,SWSI2$  When SWSI2$ is closed, normal control power
          FUSE2$,SWSI2$,1         flows to SW56$ which closes SW51$.
          OPWF1$,SWA4$,1          OPWF1$ switches SWA4$ so that SWSI2$ is enabled
          SWA4$,SWSI2$,1          to close upon receipt of SILOGIC.
          SILOGIC1,SWSI2$,1
          SWB1$,DUMAND56$,DUMAND51$
          DUMAND51$,DUMAND56$,SWB1$

SWC1$,DUMAND51$,SWA1$   SWC1$ is auxillary remote control switch.
SWA1$,DUMAND51$,SWC1$   SWA1$ is normal remote control switch.
DSIINST,OPRF1$,1        DSIINST is safety injection indication instrumentation.
DSIINST,OPRA1$,1        All valve actuating operators need this input to
DSIINST,OPRF2$,1        know that injection is necessary.
DSIINST,OPRC1$,1

OPRC1$,SWB1$,1          OPRC1$ is local operator who ascertains valve position
DUM13$,OPRC1$,1         by inputs to DUM13$ (see comment in 3rd line).
DUM12$,SWB1$,1          SWB1$ is actuator for both normal and emerg. power.

        Inputs to DUM13$
LINK1$,DUMAND58$,DUMAND52$
DUMAND52$,DUMAND58$,LINK1$
DUMAND53$,DUM13$,DUM11$
DUM11$,DUM13$,DUMAND53$
FDATA1$,DUMAND53$,DUMAND58$
DUMAND58$,DUMAND53$,FDATA1$
LT4$,DUMAND52$,LT3$      LT3$ and LT4$ are valve position sensing lights located.
LT3$,DUMAND52$,LT4$      next to the valve.

DUM12$,SW53$,1          SW53$ uses normal or auxillary control power.
SW53$,LT3$,1            SW53$ is valve pos'n sense switch (open iff valve not closed#).
LINK1$,SW53$,1          LINK1$ is connection of valve plug to SW52$ - SW56$
DUM12$,SW52$,1          SW52$ uses normal or auxillary control power.
SW52$,LT4$,1            SW52$ is valve pos'n sense switch (closed iff valve closed#).
LINK1$,SW52$,1

OPRF2$,SWC1$,1
FUSE1$,SWC1$,1           SWC1$ is actuator for emergency control power.
DUM11$,OPRF2$,1
OPRF1$,SWA1$,1
FUSE2$,SWA1$,1           SWA1$ is actuator for normal control power.
DUM11$,OPRF1$ 1

        Inputs to DUM11$
LT1$,DUMAND54$,LT2$      LT1$, LT2$ are red and green valve plug position
SW53$,LT1$,1             indicator lights located in unit main control room.
LT2$,DUMAND54$,LT1$
SW52$,LT2$,1
DUMAND54$,DUMAND57$,OPRC1$
OPRC1$,DUMAND57$,DUMAND54$
DUMAND57$,DUMAND55$,OPRA1$
OPRA1$,DUMAND55$,DUMAND57$
DUMAND55$,DUM11$,FDATA1$
FDATA1$,DUM11$,DUMAND55$
0,0,0
```

Table 2-3. (continued)

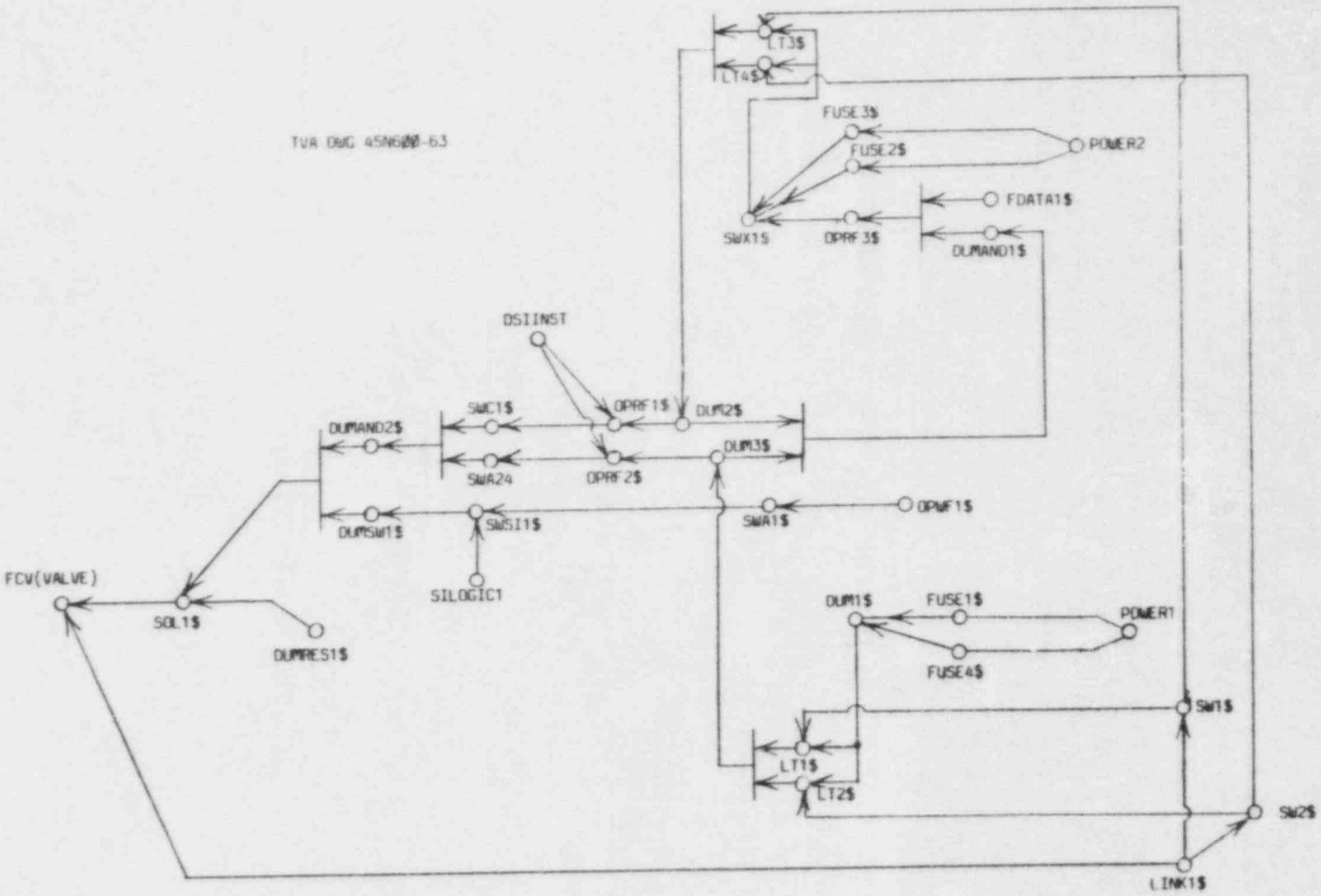


Figure 2-21. Solenoid Flow Control Valve Unit

2.4.5.3 Pump Unit Model (Figure 2-22)

All of the pumps use essentially the same control logic. Control power and motive power are supplied by separate power sources. When relay R2 is closed, motive power (POWER1) flows to the motor which drives the pump. The relay is closed by a switching mechanism driven by a coil which is energized by control power when the pump is actuated. There is only one source of motive power but there are two sources of control power, one which is normally enabled and an emergency source which can be manually enabled if necessary.

Any one of four switches can enable current to flow to the coil provided that the control power source aligned with the switch is enabled. The four switches, SWB2, SWC2, SWA2 and SWSI1 therefore form the inputs to a four input AND gate. The first three switches are manually actuated and the fourth one is connected to the automatic safety injection actuation logic. One of the four switches, SWB2, is a manual switch next to the pump and it alone can enable current to the coil from either the normal or emergency control sources. SWC2 is in a remote control room. It is the remote backup manual actuation switch and requires emergency control power. The normal remote actuation switch is SWA2 and it enables normal control power to the coil. Operator inputs to these three switches are OPR-'s, that is, the operators do the "right" thing by actuating their switches. Inputs to the operators are DSIINST, the safety injection instrumentation that indicates an accident is occurring, flow data (FDATA2), and lights that indicate whether the pump is on and working.

The switch SWSI1, which automatically actuates the pump on receipt of the safety injection signal, is aligned with the normal control power supply. This switch must be enabled beforehand and can be disabled if an OPW-, an operator whose action degrades the system, switches SWA3 from "automatic" to "manual". Of course, this doesn't affect the ability of operators to manually actuate the pump but manual activation is based on reliable input to the operators and operator decision making as per the modeling described above.

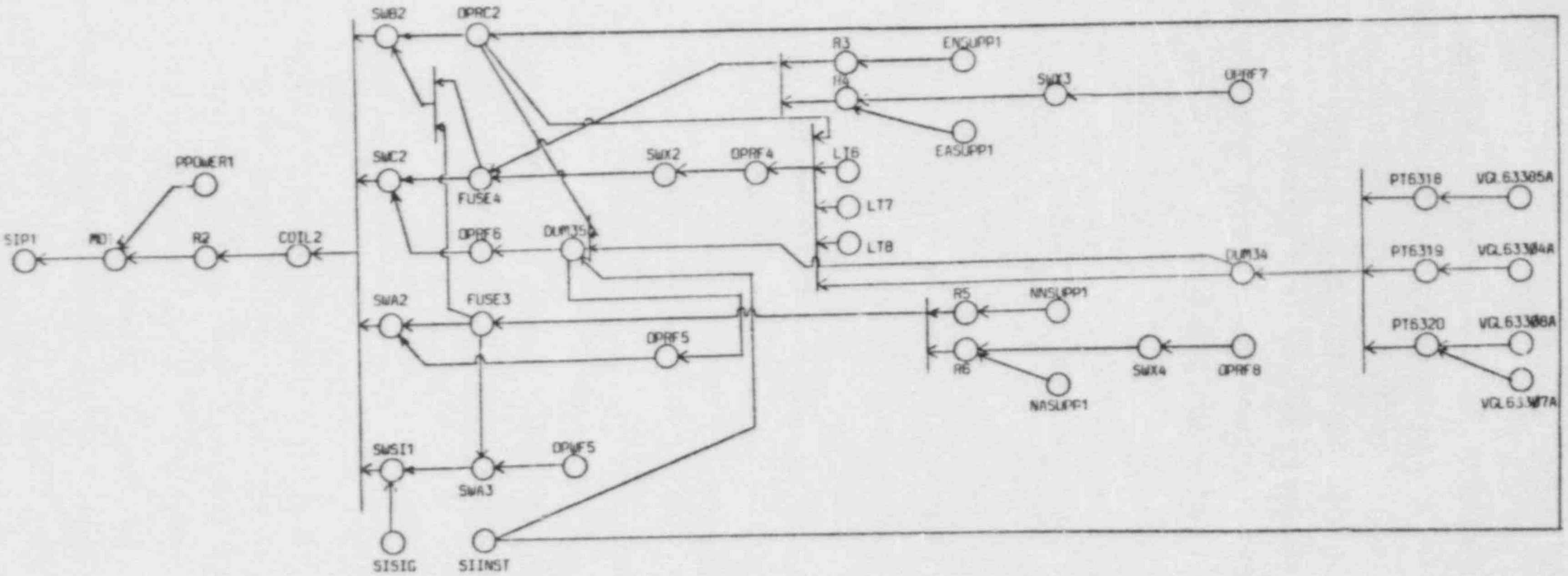
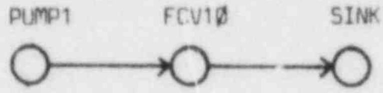


Figure 2-22. Pump Unit Model

2.4.6 Addition of Support System and Unit Models

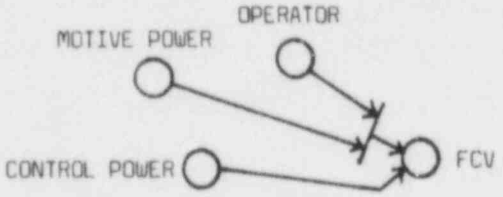
The connection of the support system models and unit models into the global digraph is performed by using the same notation for the unit model terminal node as the component notation in the core digraph. Each of the unit models is tailored to the specific component by using the component identification in each subcomponent name in the event model. The actual connection of the unit models to the core digraph is done via the adjacency input. Figure 2-23 illustrates this procedure.



(a) Typical Core System Digraph

```
PUMP1, FCV1Ø,1
FCV1Ø,SINK,1
```

(b) Adjacency Input



(c) Simplified Unit Model for FCV

```
OPR,FCV,MP
MP,FCV,OPR
CP,FCV,1
```

(c) Generic Adjacency Input

```
OPR1Ø,FCV1Ø,MP1Ø
MP1Ø,FCV1Ø,OPR1Ø
CP1Ø,FCV1Ø,1
```

(e) Specific FCV10 Adjacency Input

```
PUMP1,FCV1Ø,1
FCV1Ø,SINK,1
OPR1Ø,FCV1Ø,MP1Ø
MP1Ø,FCV1Ø,OPR1Ø
CP1Ø,FCV1Ø,1
```

(f) Total Adjacency

Figure 2-23. Addition of Support System and Unit Models

2.4.7 Modeling Human Intervention

The Safety Injection System depends on the human operator as backup to the automatic functioning of the front-line and support systems. Consequently, the unit models used in the global digraph have inputs which correspond to operator actions. Two types of operator actions have been identified: those which result in a beneficial result (OPR) and those which result in a detrimental result (OPW). Operators may also be local (at the component) or remote (generally in the main control room). Operators also are sometimes used to override power or control. By grouping these operator nodes by location, impact, power or control, etc., it is possible to assess their aggregate effect on system operation. One limitation imposed on the modeling of OPW's is that their impact had to be restricted to times before the LOCA. This condition was due to lack of information of hardware design which would have provided a basis for modeling the case of OPW inputs simultaneous to OPR inputs.

In the flow control valve unit model six operator nodes were identified. In the complete model for HPSIS, about 370 of these operator nodes were used. During normal plant operations, there are only two remote operators, so grouping of these nodes is necessary. This grouping is performed by creating a "master node" which is adjacent to a set of operator nodes. For example, we could study the operation of the system if all remote operators failed to perform a manual override operation.

2.4.8 Partitioning

The digraph produced by the series of expansion steps described grew to be quite large for the High Pressure Safety Injection System. This digraph contained about 3700 nodes. At some size, no matter what computer is used, the digraph will outgrow the computer memory capacity and require excessive processing time. To overcome this limitation, a procedure known as "partitioning" has been developed. This procedure identifies subgraphs which can be independently solved for their singletons and doubletons and then replaced by an input/output equivalent "circuit". This equivalent circuit contains all singletons and doubletons of the original subgraph in terms of only the subgraph boundary nodes. These boundary nodes are nodes in the subgraph which have connections to any nodes which lie outside of the subgraph. The unit models used in the expansion of the digraph are chosen as the modules which are used for replacement by equivalent circuits.

The singletons and doubletons of the global digraph with these modules replaced by their equivalent circuits are then found using the processing described above. The full solution in terms of the original nodes is then obtained by replacement of the singletons and doubletons which represent the terminal node of each module by the singletons and doubletons of that module. By using this procedure along with condensation, the 3700 node HPSIS problem was reduced to approximately 900 nodes. The partitioning procedure is more fully explained in Appendix A.

3. RESULTS OF THE DMA OF THE HIGH PRESSURE SAFETY INJECTION SYSTEM

The results of the analysis of the DMA model of the high pressure safety injection system will now be presented. The accident sequence selected for this demonstration was loss of emergency core cooling injection during the early phase of the response to an S1 LOCA (at the lower end of the size range). This accident sequence corresponds roughly to the S1DKCE (#13 small LOCA) accident sequence in the SSMRP study [17] and to configuration 1 in the BNL study. Originally, it was intended to compare the findings from this DMA with the results from the Sandia Systems Interaction study [16]. The Sandia study, however, was not based on the evaluation of accident sequences for systems interactions. Instead, fault trees for the plant based on four safety functions were constructed. As a result, no direct cut-set comparison between our effort and the Sandia effort was possible.

We were able to: (a) qualitatively compare the accident sequence singletons and doubletons cut-sets we found by DMA to both Zion [17] PRA results and to NUREG-0847 [5], and (b) quantitatively compare the probability of loss of high pressure injection of our study with roughly comparable analyses from WASH 1400 [15] and BNL [14]. Two scenarios were studied; Case I in which the high pressure safety injection system was analyzed for failures in the fully automatic mode with no operator mitigating intervention allowed; and Case II in which the system was analyzed in the more realistic mode with operator mitigating intervention allowed. The results from the analysis of Case I were compared to those from the earlier studies. The results from Case II were not compared since it does not appear that the earlier studies considered the effects of positive operator intervention in any systematic way.

The results from this DMA clearly indicate that:

1. DMA is highly capable of modeling and evaluating an accident sequence (including front-line systems, support systems, and operator actions) as a continuous well-integrated logic model in order to identify and evaluate systems interactions.

2. Numerous, non-intuitive systems interactions exist between front-line and support systems and are collectively significant. This is demonstrated by comparing Case I (fully automatic) with a recent BNL study [14] and with WASH 1400 [15].

<u>Loss of High Pressure Injection+</u>

DMA (Case I)*	BNL**	WASH 1400***
4×10^{-2}	3.1×10^{-3} ($\beta = 0$) 1.8×10^{-2} ($\beta = 0.3$)	8.6×10^{-3}

The BNL study [14] evaluated the impact of typical variations in configuration of design of the high pressure injection system (HPIS) on system unavailability. The HPIS's in 17 nuclear power plants were reviewed for variations in designs, systems operation, testing, maintenance policies, and possible sources for common-cause failures. The factor dependency , β , method was used to parametrically quantify the dependent failures. $\beta = 0$ indicated an absence of dependence and $\beta = 0.3$ indicated very strong dependencies. Their configuration #1 (one of two safety injection pumps and one of two charging pump criteria) is a more stringent criteria than our current DMA study.

+ Since a PRA on the plant has not been completed to date only gross comparisons can be made to other available studies.

* This overestimates the unavailability of the High Pressure Injection Systems due to scope limitations in modeling maintenance (see Section 4.1).

** The success criteria used by BNL [14] was 1/2 SIP and 1/2 SCP which differs from our criteria.

*** Our comparison is made to the S2 small LOCA (1/2" to 2") in WASH 1400 which has a success criterial of (1/3 HPIP).

3. Support systems clearly depend on positive operator intervention to provide redundant safety. The operators provide significant enhancements in safety injection system reliability and robustness when they correctly respond to the loss of an automatic system.

A significant difference between the scope of the DMA and the two earlier studies (Zion and WASH 1400) is DMA's more extensive investigation of the accident sequence's support systems, such as component cooling, the various electrical power systems, and the plant operators. One of the biggest areas of concern in the analysis of systems interactions is the effect of human operators on the reliability of the front-line systems. The modeling done in this DMA of human actions, both to provide successful redundant backup to automatic systems and to provide a source of dynamic human error is not directly comparable to available traditional PRA studies. The effects of coordinated operator actions were not included in this study due to lack of specific plant operating procedures. The effect of pipe breaks, which was extensively investigated in the Zion study, was modeled only in a cursory manner in this DMA. The primary reason for the lack of a detailed analysis of the effects of breaks was the lack of knowledge of the actions the operators could or would take to mitigate these breaks.

It was found that a significant number of doubleton failure sets arise from incorrect operator action prior to safety injection. There were 237 doubletons sets found involving incorrect operator actions with three of these failure sets involving two operator errors.

To point up the positive contribution of operator actions, Case II, the fully redundant case, was analyzed with both remote (control room) and local (at the equipment) operators wherever needed to override failed automatic systems. In this second scenario, only blockage was considered as a failure in the pipes and valves of the high pressure safety injection and component cooling systems with breaks not included. It was found that the high pressure safety injection system was significantly more robust in this case than in the fully automatic case. It will be shown in Section 4 that these operators can significantly reduce the probability of failure of

HPSIS. A summary of the results of the qualitative analyses of Cases I and II is given in Table 3-1. As can be seen from this table, the effect of positive operator override is dramatic. There are seven singletons and 4314 doubletons in the automatic case with only two singletons and 708 doubletons in the manual override case. It will be shown in Section 4 that the addition of the manual override improves the high pressure safety injection system reliability by about a factor of 8.

The detailed results discussed below will be presented in the matrix format shown in Figure 3-1. In this figure an asterisk indicates that a doubleton is composed of the components indicated by the row and the column entry. Each of the elements shown in the doubleton matrix may in turn represent several components. Thus if a row element represents n components and the column element represents m components, the total number of doubletons represented by the asterisk is n X m. This reduction of several components into "super" components occurs because of the condensation step described in Appendix A. The cut set numbers given above represent the fully expanded cut sets.

	Singletons	Doubletons
Case I: Automatic Systems Only	7	4314
Case II: Positive Human Intervention Enabled	2	708

Table 3-1. Summary of Results

	A	B	C	D	E
A	-	*	-	*	-
B	*	-	-	-	-
C	-	-	-	-	-
D	*	-	-	-	-
E	-	-	-	-	-

(a) Doubleton Matrix

A*B

A*D

(b) Cut Sets

Figure 3-1. Doubleton Format

3.1 Results for Fully Automatic Operation (No Human Mitigation): Case I

The first case analyzed was that of fully automatic operation with no positive human intervention allowed. In this case the high pressure safety injection system relies only on its automatic systems for success. The analysis of this case should expose the largest number of singletons and doubletons since the plant seems to have been designed to rely on operators to enable many important backups. It is also expected that the reliability of the HPSIS would be the lowest for this case. The model for this case and Case II included explicit nodes for the effects of incorrect operator actions.

Seven singletons were found which can keep high pressure safety injection from succeeding. The singletons are:

RWST	the refueling water storage tank
HDR1, HDR2, HDR9	pipe headers
FCV635, FCV6322	flow control valves
VC63510	a check valve
(OPWF20*)	a control room operator who turns off safety injection during the injection phase

The pipe headers (pipe branch points) are in the network connecting the RWST to the front-line systems.** These headers are shown in Figure 3-2. HDR1 is immediately downstream of the RWST. Should flow fail through this header, both front-line injection systems would fail. Check valve VC63510 and motor operated flow control valve FCV635,*** are in the normal path

----

* This operator has not been included in the singleton count or the quantitative analysis since his incorrect action occurs during the LOCA.

** Inclusion of headers in the HPSIS DMA model was limited to this network.

*** The importance of this valve was recognized by the operators and consequently it is planned to check the state of this valve every eight hours.

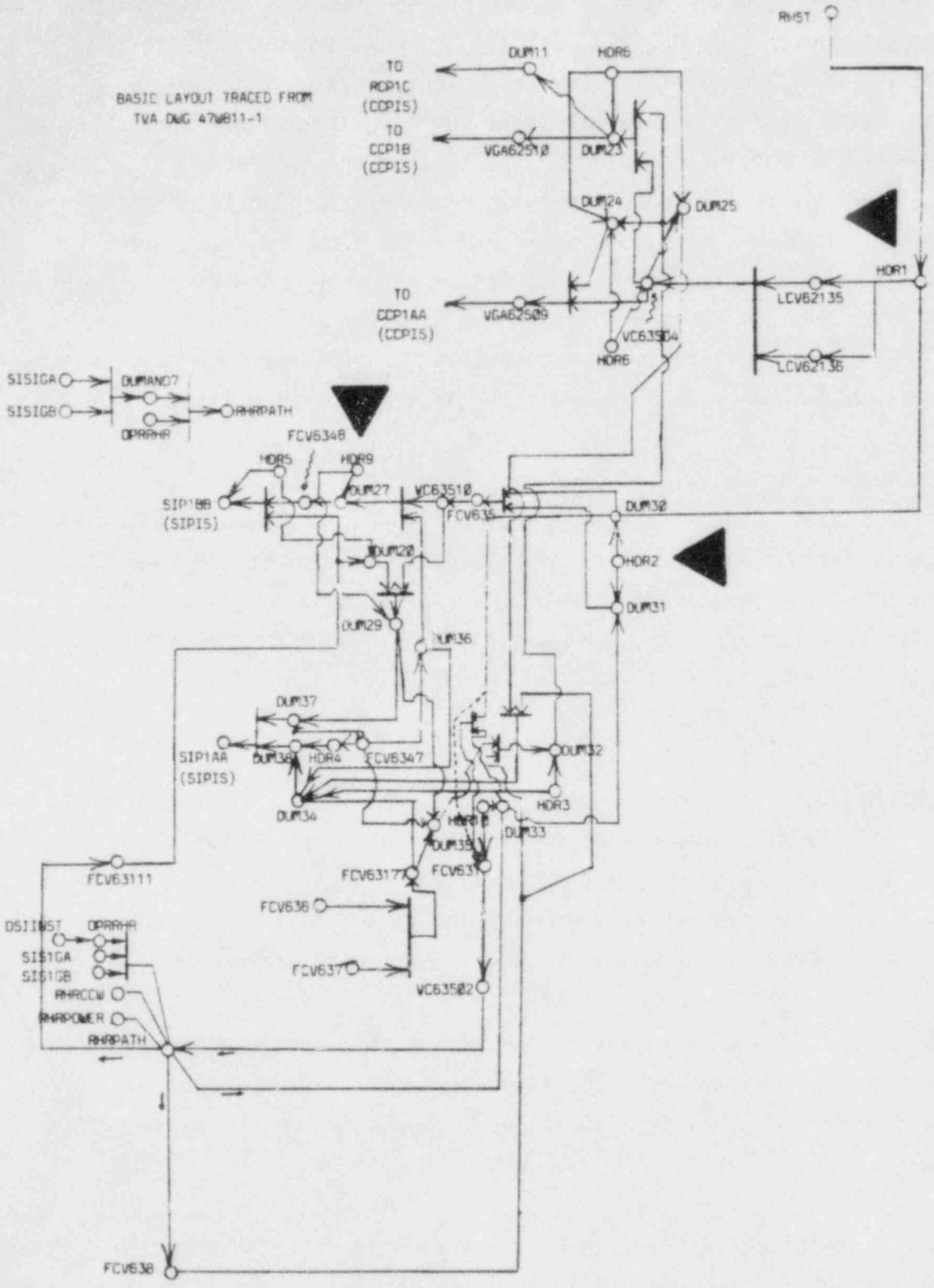


Figure 3-2. RWST.DAT Network Connecting RWST to SIPIS & CCPIS

from the RWST to SIPIS. Should they fail closed or should the flow control valve be closed by mistake, no flow would reach the safety injection pumps. Headers 2 and 9 are immediately upstream and downstream, respectively, of VC63510 and FCV635 so their failure effects the system the same as the valves. Downstream of the safety injection pumps is another flow control valve, FCV6322, which can shut off flow through the (sole) normal injection path into containment. There are two alternate injection paths into containment, however, these can only be enabled manually. There are two operator induced singletons which do not appear explicitly in the singleton list. These two are the OPW's (incorrect actions) which could cause the valves FCV635 and FCV6322 to be closed. The probability data base used for the quantitative analysis includes data for these possibilities.

The doubletons for Case I are shown in Figure 3-3. The asterisks in this figure represent 4314 failure sets. Of these, 237 are due to an operator incorrect action. All but three of these 237 failure sets include the failure of a component along with an operator incorrect action. The remaining three are due to a combination of two operator errors and are:

OPWF5S * OPWF5YS
OPWF5U * OPWF5V
OPWF5U * OPWF5YS

where:

OPWF5S is an operator taking CCP1AA out of automatic mode
OPWF5YS is an operator taking CCWPCS out of automatic mode
OPWF5U is an operator taking SIP1AA out of automatic mode
OPWF5V is an operator taking SIP1BB out of automatic mode

No attempt has been made to assess the effect of coordinated operator incorrect actions or to determine if one operator could perform multiple incorrect actions. This type of analysis should be pursued further in a subsequent study.

Distinct patterns can be seen in the doubleton matrix of Figure 3-3. These patterns arise from the fact that the front-line systems and many of the support systems were designed as trains to ensure redundancy. The results

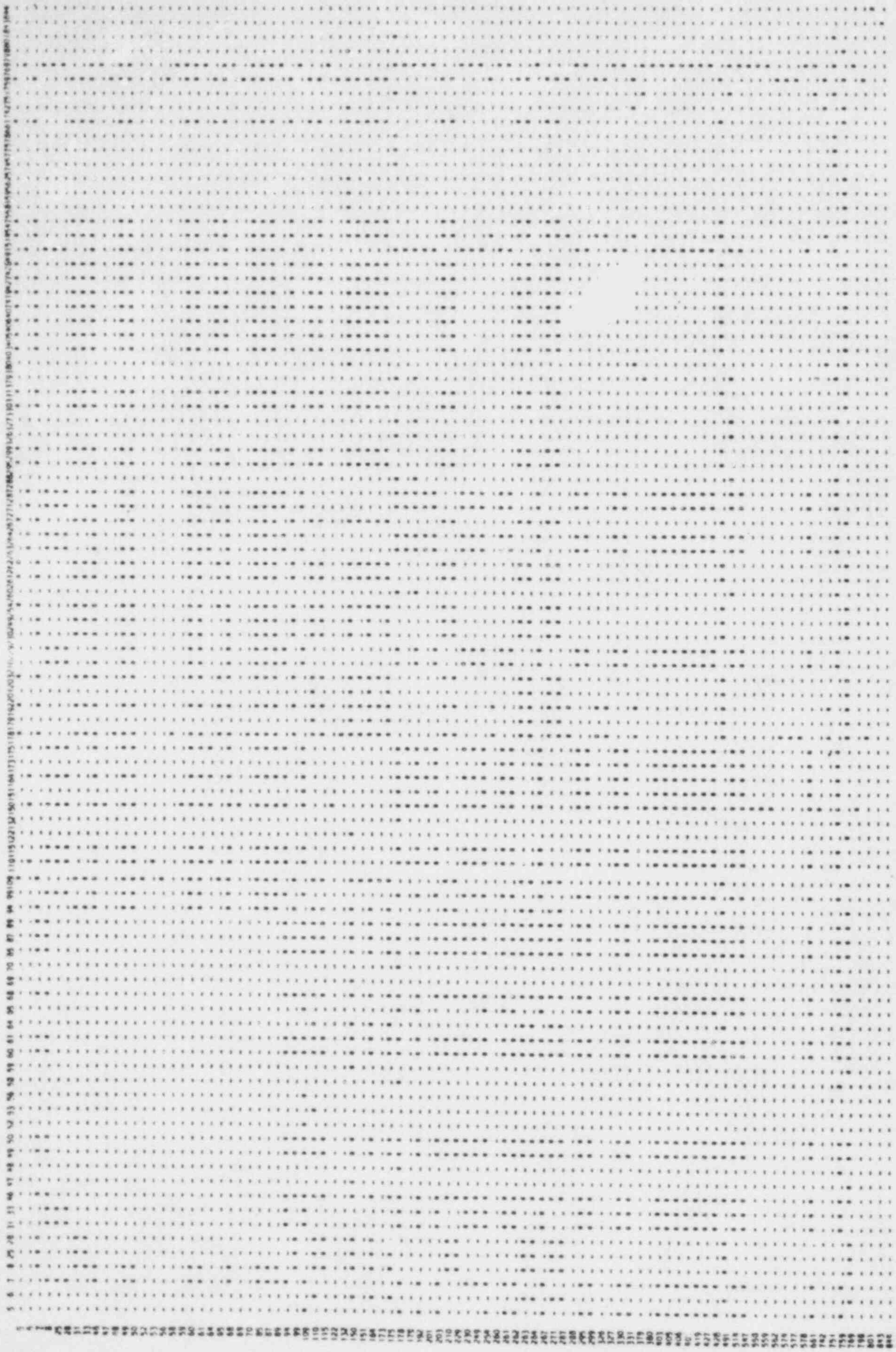


Figure 3-3. Doubletons for Case I: No Human Mitigation.

5	CCP1AA
5	VGA62509
5	MOT2S
5	R2S
5	COIL2S
5	OILCOOLS
5	VGL553A
5	TW170146B
5	VGL552A
5	VGL554A
5	TW170146A
5	FE170146
5	VGL557A
6	CCP1BB
6	VGA62510
6	MOT2T
6	R2T
6	COIL2T
6	OILCOOLT
6	VGL553B
6	TW170145B
6	VGL552B
6	VGL554B
6	TW170145A
6	FE170145
6	VGL557B
7	SIP1AA
7	MOT2U
7	R2U
7	COIL2U
7	OILCOOLU
7	TW170147B
7	VGL558A
7	TW170147A
7	FE170147
7	VGL562A
7	VGA170725A
8	SIP1BB
8	MOT2V
8	R2V
8	COIL2V
8	OILCOOLV
8	TW170148B
8	VGL558B
8	TW170148A
8	FE170148
8	VGL562B
8	VGA170725B
25	FE6320
25	VGA63527
25	VC63526
29	FCV6322
28	FCV63153
31	FE63151
31	VGA63525
31	VC63524
33	FCV63152
46	VC63581
47	FCV6325
48	FCV6326
49	BIT
50	FE6343
50	VGA63573
50	VC63572
52	FCV6342
53	FCV6341
56	VC63570
58	FCV6339
59	FCV6340
60	FE63170
61	HDR8
64	VGA62533
64	VC62532
65	VGA62527
65	VC62525
68	VC62504
69	LCV62136
70	LCV62135
85	HDR6
87	VC63504
89	HDR7
94	HDR5
95	HDR9
96	VC63510
96	FCV635
99	FCV6347
109	SISIGB
110	SISIGA
115	HDR4
122	480MOV1B1B
132	480MOV1A1A
150	6900VS1AA
151	SWSI1S
151	SWA3S
151	OPWF5S
164	FUSE10I
173	FUSE3S
175	R5S
178	6900VS1BB
179	SWSI1T
179	SWA3T
179	OPWF5T
192	FUSE10II
201	FUSE3T
203	R5T
210	SWSI1U
210	SWA3U
210	OPWF5U
229	FUSE3U
230	SWSI1V
230	SWA3V
230	OPWF5V
249	FUSE3V
254	CCWPCS
254	MOT2Y
260	CCWP1AA
260	MOT2YQ
260	R2YQ
261	FE170165
261	FCV1703
262	TW17072
262	FCV17075
263	FE170159
263	FCV1702
264	TW17070
267	FCV7012
267	TW70162
267	CCHXRC
267	VB070510
267	TW70201
267	FE70201
271	FCV708
271	TW170161
271	CCHXRA
271	VB170510
271	TW170199
271	FE170199
287	FCV7025
288	VB170505A
295	VB070505
299	FCV7022
326	VC170504A
327	STRAINR1AA
327	VB170503A
330	VC070504
331	STRAINRCS
331	VB070503
379	480VS1A1A
379	R50
379	TR1A1A
379	R49
380	480VS1B1B
380	R31
380	TR1B1B
380	R30
403	R2YS
403	R2YSWG1
403	COIL2YS
405	MINRLKSWG1
406	480VS2B2B
406	R19B
406	TR2B2B
406	R18B
407	SWSI1YS
407	SWA3YS
407	OPWF5YS
419	FUSE20IV
427	FUSE3YS
428	R5YS
491	125VVBI
514	125VVBII
547	125VVBIV
558	R32
559	X2
562	R33
574	R51
577	R53
578	X4
651	6900VS2BB
742	EINRLK31
751	EINRLK50
759	EINRLK1726
769	EINRLK1718
798	MINRLK33
801	MINRLK53
843	ONSITE
844	OFFSITE
847	OPRMASTER

Variable Name Key for Case I and Case II of a reachability calculation on the global model with human backups disabled reveals many doubletons which are the result of a failure of both trains of doubly redundant front-line or support systems. The doubleton matrix also contains many more doubletons which represent pairs of failures between components in dissimilar systems, including components from the other nuclear unit.

In Figure 3-4, the doubletons which occur due to failure of both trains of a doubly redundant front-line or support system appear as blanks. Each asterisk represents a failure of the row node with the column node. As described earlier, each node number may represent the failure of several pieces of equipment and/or operator inputs. For example, consider the doubleton at the intersection of node numbers 151 and 406. Node 151 represents the failure of switches, SWI1S or SWA3S, and incorrect operator action OPWF5S. In the automatic mode, these are all singletons to one of the centrifugal charging pumps, CCP1AA. Switch SWSI1S is the switch in the pump control logic that closes upon receipt of an automatically generated safety injection signal. Switch SWA3S is a switch in the reactor control room that can normally set to "Auto" and enables flow from the control power source to the process power breaker should SWSI1S close and should OPWF5S not have set SWA3S to "Manual". Node 406 represents the failure of 480VS2B2B, R19B, TR2B2B, or R18B. Any of these failures would cause the component cooling system to fail to cool the two front-line system pumps CCP1BB and SIP1BB. All node 406 components are located in the electrical power system of the other nuclear power plant, Unit II. The first is a 480 vac shutdown bus, the two R-'s are breakers, and TR2B2B is a transformer. The doubleton at 151 and 406 means, therefore, that any of the following doubletons will cause the HPSIS to fail:

SWSI1S * 480VS2B2B
SWSI1S * R19B
SWSI1S * TR2B2B
SWSI1S * R18B
SWA3S * 480VS2B2B
SWA3S * R19B
SWA3S * TR2B2B
SWA3S * R18B
OPWF5S * 480VS2B2B
OPWF5S * R19B
OPWF5S * TR2B2B
OPWF5S * R18B

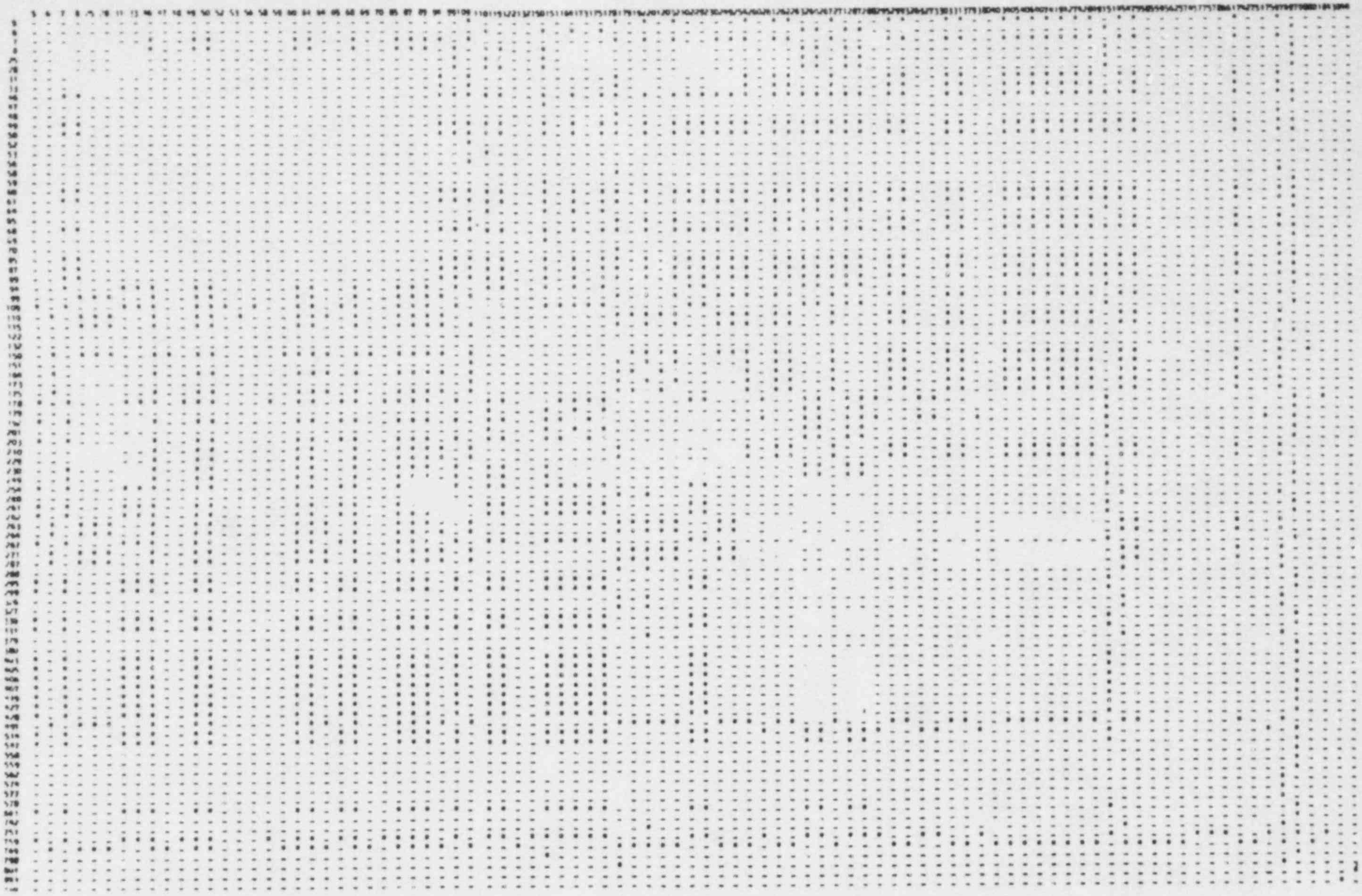


Figure 3-4. Doubletons for Case I: No Human Mitigation. Doubletons Resulting from Failures of Both Trains of a Doubly Redundant System Appear as Blanks.

Patterns in the doubleton array (Figure 3-4) can be further categorized. The effect of the individual components which contribute to the doubletons fall into the nine categories below which result in the doubleton failure modes shown in Table 3-2.

1. CCPIS-A Failure of CCPIS train A (path or pressurization)
2. CCPIS-B Failure of CCPIS train B (path or pressurization)
3. SIPIS-A Failure of SIPIS train A (path or pressurization)
4. SIPIS-B Failure of SIPIS train B (path or pressurization)
5. PATHCCPIS Failure in CCPIS causes all paths from RWST to core through that system to fail
6. AA Failure in support system causes A trains of safety injection and charging systems to fail
7. BB Failure in support system causes B trains of safety injection and charging systems to fail
8. AA' Failure in support system A train
9. BB' Failure in support system B train

Failures in categories AA and BB originate in the safety injection logic (SILOGIC), the electrical power system (EPS), the protection set (PS), and the component cooling system (CCS). Failures in AA' and BB' originate in EPS, with CCS failures occurring only in the AA' category. Table 3-2 summarizes all of the doubleton failure modes which appear in this case. The pattern in the table is largely the manifestation of the SILOCA success criteria (Figure 2-4) which requires the integrity of the A and B trains of SIPIS or the integrity of at least one train from each front-line system. Each of the failure categories has singletons from several systems, making for a great deal of systems interaction which results in doubleton failures. Each of the failure modes will now be discussed by use of the success criteria diagram. In the figures that follow, the failure category will be underlined and the propagation path of this failure will be traced in heavy lines with the affected systems shaded.

	CCPIS-A	CCPIS-B	SIPIS-A	SIPIS-B	PATHCCPIS	AA	BB	AA'	BB'
CCPIS-A							FM1		
CCPIS-B						FM2			
SIPIS-A				FM3	FM4		FM5		
SIFIS-B			FM3		FM6	FM7			
PATHCCPIS			FM4	FM6		FM8	FM9		
AA		FM2		FM7	FM8		FM10		
BB	FM1		FM5		FM9	FM10		FM11	
AA'							FM11		FM12
BB'								FM12	

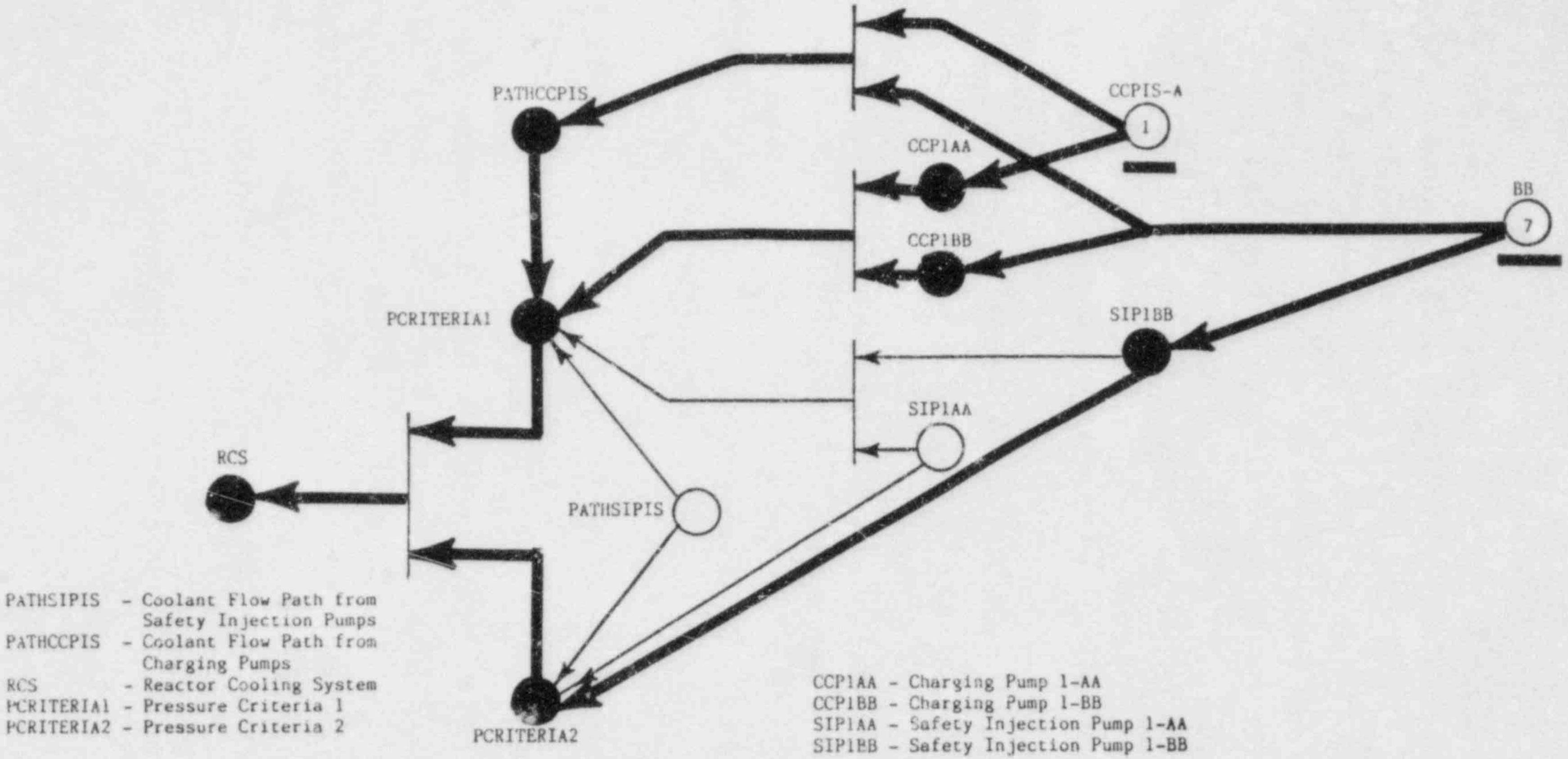
Table 3-2 Characterization of the 12 Doubleton Failure Modes Appearing in CASE I

3.1.1 Analysis of Failure Mode 1

Failure mode 1 is a failure of a CCPIS-A singleton* with a BB singleton and is shown in Figure 3-5. Singletons to CCPIS-A include charging pump CCP1AA and valves in the component cooling system which would block injection pump heat removal. Without heat removal, a pump could fail in 5 to 30 minutes.** BB singletons exist in the safeguards actuation logic system (SILOGIC), the electrical power system in both units (EPS), the protection set vital instrumentation and control power system (PS), and in the component cooling system (CCS). An example of a BB singleton is the failure of the train B safety injection signal. Failure of this signal to be generated or transmitted will keep the B-trains in both front-line systems from actuating. The HPSIS doubleton results from both B-train pumps not pumping coupled with the failure of the CCPIS-A train since the pressure from the remaining SIPIS-A train is insufficient for S1LOCA injection requirements. Other BB singletons include FUSE20IV in PS. Should this fuse fail open, component cooling water pump CCWPCS, the swing pump, would not receive control power. This can be seen from Figure B-10, the digraph for the component cooling system. This pump is not normally running so receipt of the 125 vdc control power is necessary for its actuation. It is a BB singleton because, per FSAR Figure 9.2-19, only pump CCWPCS is normally aligned with both front line train B pumps. This pump alone normally circulates cooling water through the pumps' lubrication heat exchangers and therefore, the failure of CCWPCS to pump would result in the overheating of those front-line pumps. The failure of fuse FUSE20IV which disables CCWPCS is an example of a failure of part of one support system causing the failure of part of another support system to fail which in turn causes a failure in part of a front-line system. FUSE20IV is fuse #304 in the vital battery board IV and is the normal conduit for control power to the hardware driven by the 480 vac shutdown board in Unit 2 mentioned above. That shutdown board is the normal motive power supply to CCWPCS so the board is also a BB singleton. The components in CCS, besides the

* A "****" singleton is a single component which causes a failure in the "****" category of the previous page. Thus, a CCPIS-A singleton is a component which causes the CCPIS train A to fail.

** As confirmed by operators.



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-5. Failure Mode 1

CCWPCS that are also BB singletons, are all valves or other hardware in the recirculation path from the CCWPCS to the front-line pump heat exchangers and back to the CCWPCS. There are 26 BB singletons in CCS. The doubletons resulting from interactions with the component cooling system are circled in Figure 3-6.

3.1.2 Analysis of Failure Mode 2

Failure mode 2 listed in Table 3-2 is a CCPIS-B singleton failing with an AA singleton and is shown in Figure 3-7. The CCPIS-B singletons are, like the CCPIS-A singletons, components which cause only one CCPIS train to fail. Many valves in both trains have to actuate in the CCPIS to enable injection, because during normal plant operations the CCPIS is in a recirculation mode with the boron recycle system (BRS). The recirculation is used to control boron concentration in the coolant and to keep the coolant in the boron injection tank (BIT) from stratifying. Therefore, failure of a CCPIS train may not only mean failure of a pump, but perhaps failure of the automatic isolation of that system from the BRS or failure of the system to align for injection. The modeling assumption was made that the failure of this isolation would cause a failure in high pressure safety injection from the charging pumps. Failure of this isolation would cause a one-inch diameter opening to essentially atmospheric pressure in a high pressure four-inch pipe. It was assumed for this analysis that such a failure would lead to failure of High Pressure Safety Injection. A complete hydrodynamic analysis would be needed to determine the effects of this "break". In the absence of this analysis, a sensitivity of the total system failure probability to this break was performed. It was found that removal of the doubletons which arise from this isolation failure will cause the system failure probability to decrease less than 10%.

The doubleton of node 122 with 150 is a failure mode 2 doubleton. Node 122 represents only one component, 480MOV1B1B, a 480 vac motor operated valve board. It supplies power to 5 of the 7 B-train valves in CCPIS that must reorient to enable injection. Node 150 is 6900VS1AA, a 6900 vac shutdown board, which supplies power not only directly to charging pump CCP1AA and to safety injection pump SIP1AA, but also to a motor operated valve board

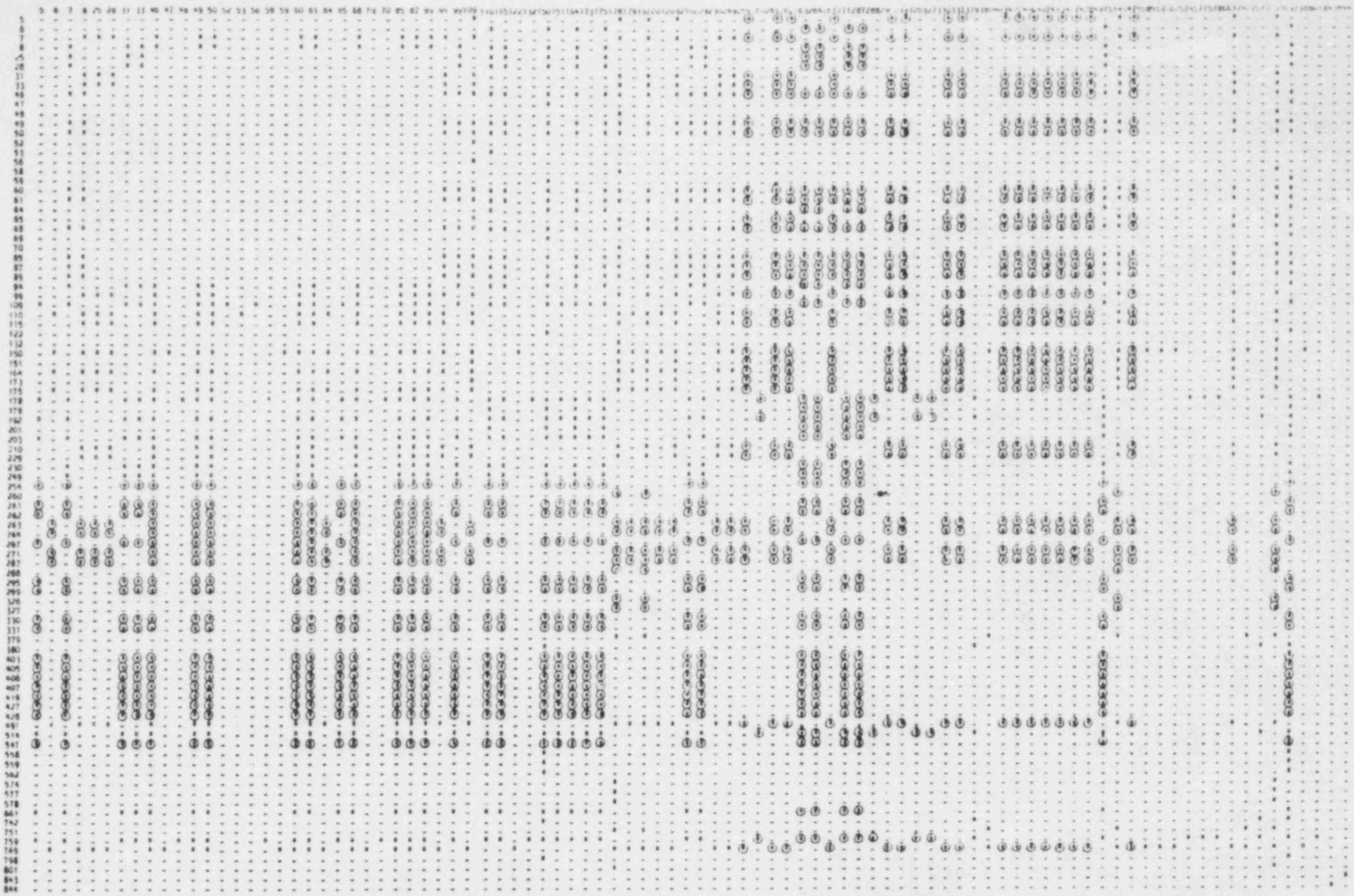
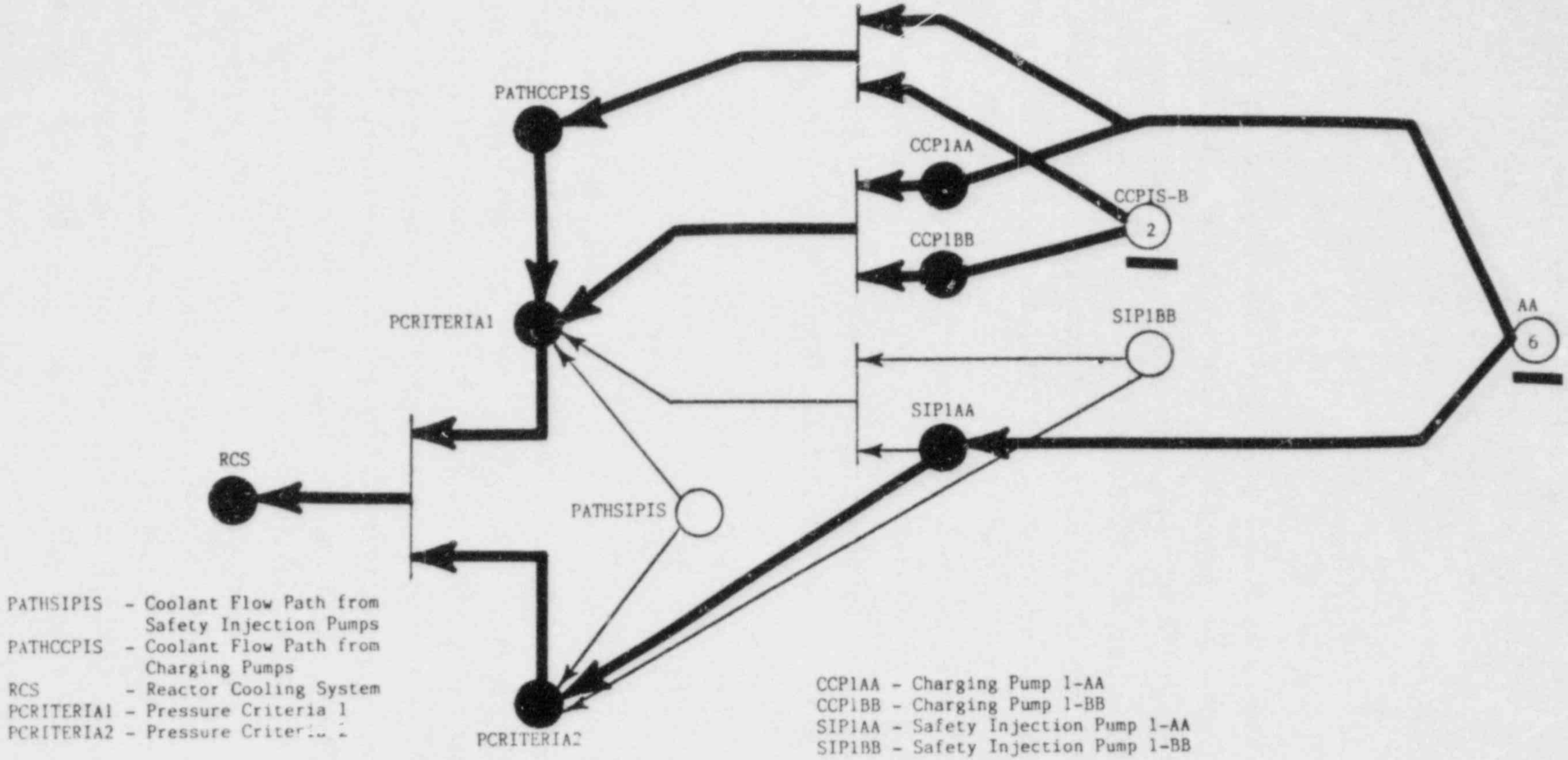


Figure 3-6. Doubletons from Case I: No Human Mitigation. Doubletons Involving the Component Cooling System are Circled.



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-7. Failure Mode 2

that drives 5 of the 6 A-train valves in CCPIS that must reorient. The result of the doubleton is that a path to the core through CCPIS is not available and one of the two safety injection pumps, SIP1AA, is not pumping. Flow from the single safety injection pump, SIP1BB alone is insufficient so HPSIS fails.

3.1.3 Analysis of Failure Mode 3

Failure mode 3, shown in Figure 3-8, is failure of a SIPIS-A singleton with a SIPIS-B singleton. These doubletons are front-line (safety injection system) doubletons. For instance, the doubleton of node 8 with node 31 is a failure of singletons to SIP1BB with some main line components downstream of SIP1AA. There are 12 components which compose node 8 including: 1) hardware within SIP1AA which it needs to start and to keep running; and 2) valves in CCS near SIP1AA which, if closed, would prevent heat removal from the pump. There are three components in node 31 including a gate valve and a check valve downstream of SIP1BB which, if they were to block flow, would disable the ability of that pump to inject. The doubleton of 8 with 31 therefore represents 36 individual doubletons which could cause HPSIS to fail.

3.1.4 Analysis of Failure Mode 4

Failure mode 4, shown in Figure 3-9, involves the kinds of singletons just described for SIPIS-A along with singletons to the path through the charging pump flow path, CCPIS, to the core. The node name representing "openness" of this path is called PATHCCPIS. An example of components included in this failure mode is the doubleton of node 229 with node 61. This doubleton is a combination of fuse and a header (junction of 3 or more pipes). Node 229 is FUSE3U, a singleton to the automatic actuation hardware in SIP1AA. Its failure prevents SIP1AA from turning on upon receipt of the safety injection signal. Node 61 is HDR8, a piping header through which the discharge of both centrifugal charging pumps flows. Its blockage or rupture would cause the only discharge path to the core to fail, thus causing PATHCCPIS to fail. Therefore, the HPSIS success criteria would not be met since only one pump, SIP1BB, would inject into the core.

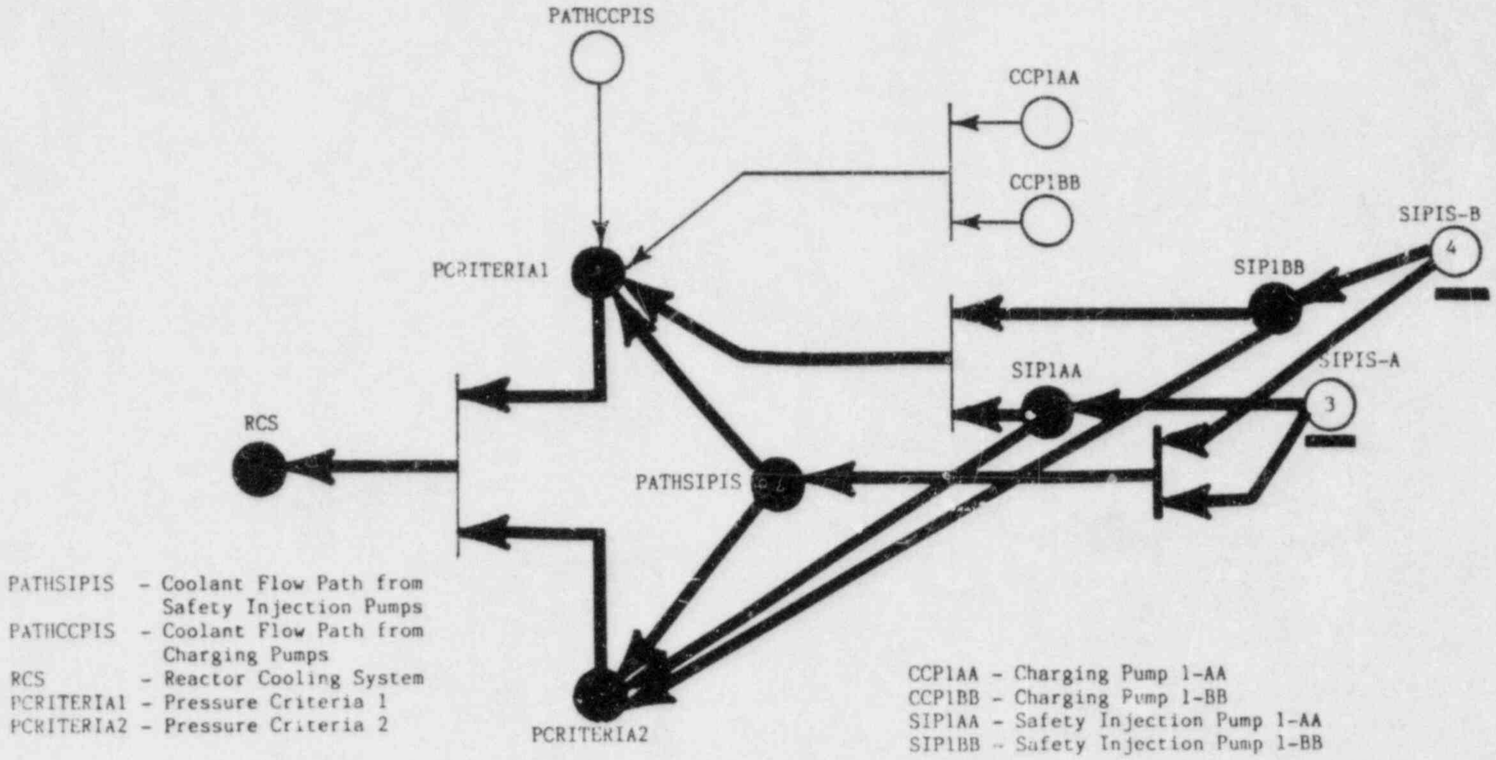
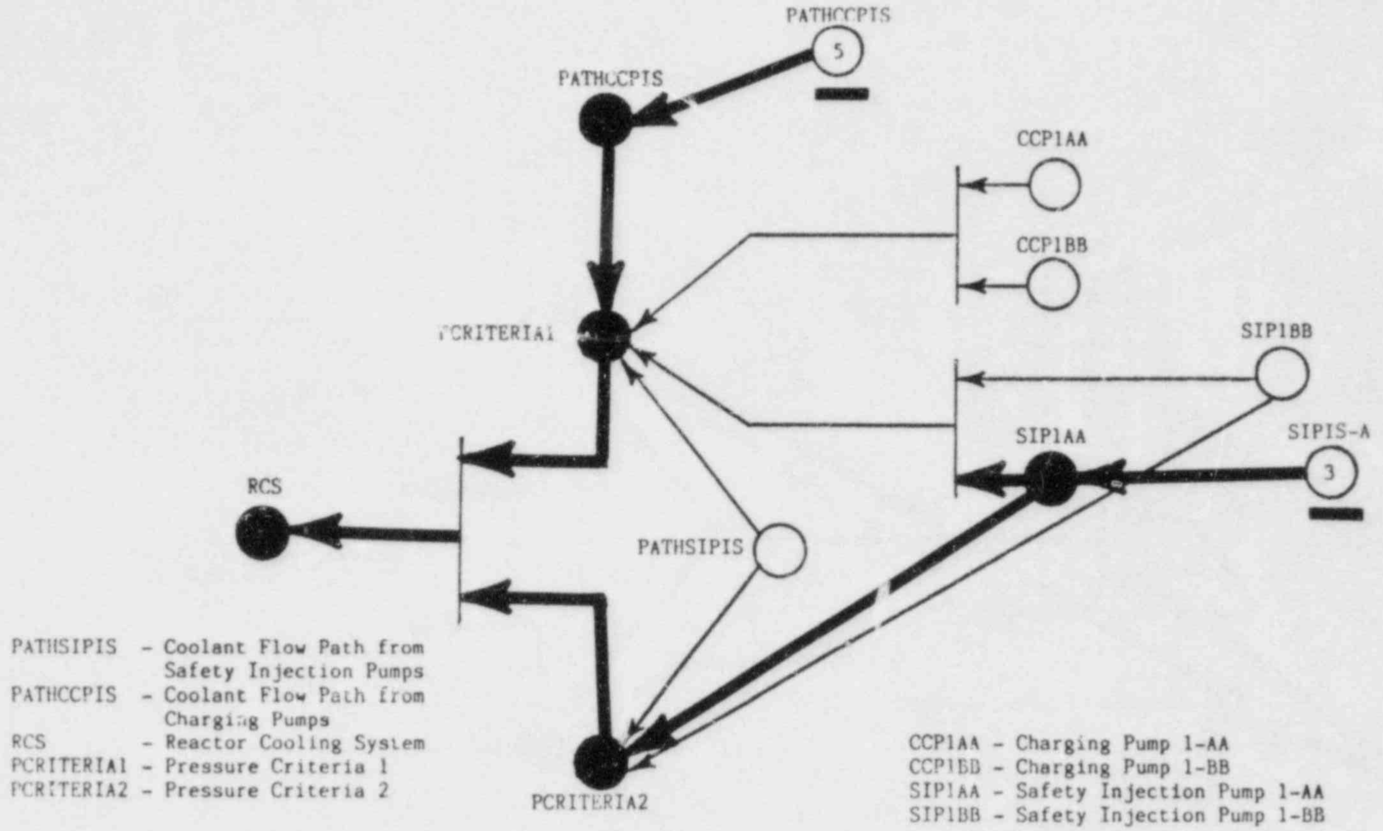

PATHCCPIS
CCP1AA
CCP1BB
SIPIS-B
4
PCRITERIA1
SIP1BB
SIP1AA
SIPIS-A
3
RCS
PATHSIPIS
PCRITERIA2
PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2
CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-8. Failure Mode 3



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-9. Failure Mode 4

3.1.5 Analysis of Failure Mode 5

Failure mode 5, shown in Figure 3-10, again involves singleton failures to SIPIS-A, but this time with BB singletons, that is, single components which cause both front-line B-trains to fail. Most of these BB singletons arise from the normal configuration of the component cooling water system as described in the discussion of failure mode 1 above. Another cause of a BB singleton is represented by node 203, R5T. This is a switch through which control power flows to components driven by 6900VS1BB, a 6900 volt shutdown board. This switch, which appears in the pump unit model shown (Figure B-9) is part of the vital instrumentation and control system, and is a necessary conduit for control power to both front-line B-train pumps CCP1BB and SIP1BB. Failure of this switch to successfully enable control power to these pumps would keep them from starting. Again, only one pump would be functioning, CCP1AA, which does not satisfy the S1LOCA injection requirements.

3.1.6 Analysis of Failure Mode 6

Failure mode 6, shown in Figure 3-11, involves singleton failures to SIPIS-B (the train B in the safety injection system) and a singleton to PATHCCPIS, the availability of a path to the core from the refueling water storage tank, RWST, through CCPIS. Examples of such singletons have been discussed above in failure modes 3 and 4. This failure mode cancels the contribution of the 2 pumps in the charging system and also the contribution of train-B in SIPIS. The flow from the remaining pump in SIPIS is insufficient by itself for high pressure safety injection for the S1 LOCA.

3.1.7 Analysis of Failure Mode 7

Failure mode 7, shown in Figure 3-12, is a doubleton between a singleton to SIPIS-B and one to both A-trains. Like the BB singletons, there are single components in the component cooling system which can disable both A trains. Instead of 26 such components which are BB singletons, only 10 components

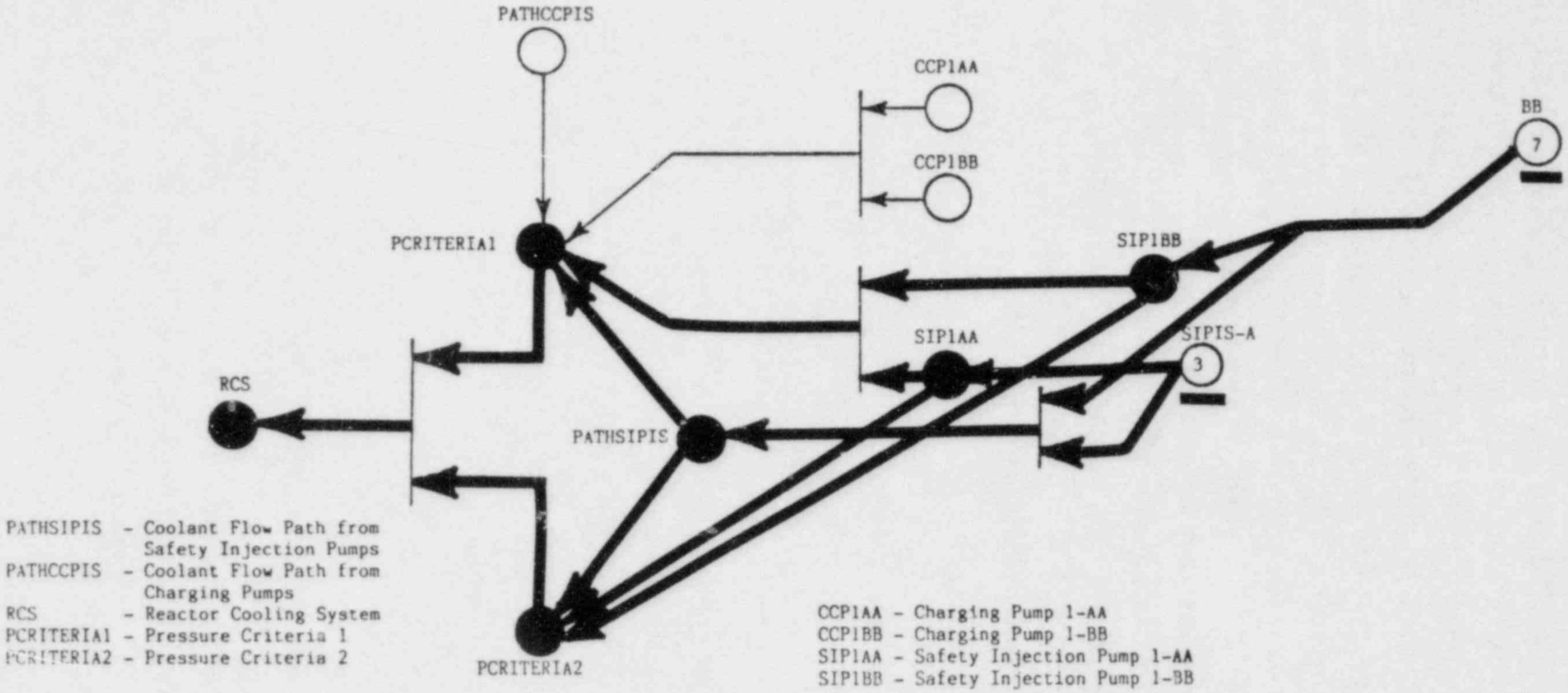
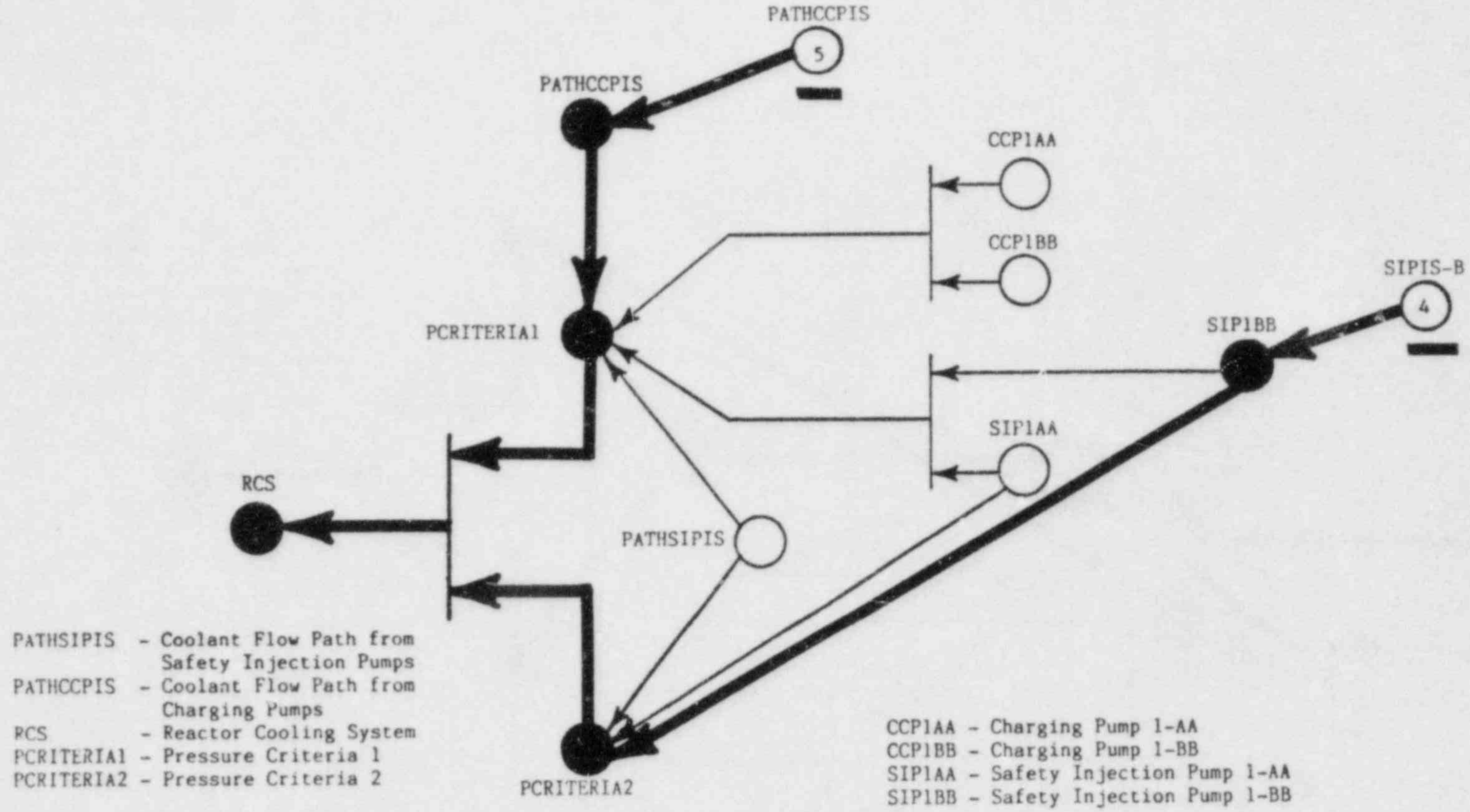

PATHCCPIS
CCP1AA
CCP1BB
BB
7
PCRITERIA1
SIP1BB
SIP1AA
SIPIS-A
3
RCS
PATHSIPIS
PCRITERIA2
PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2
CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

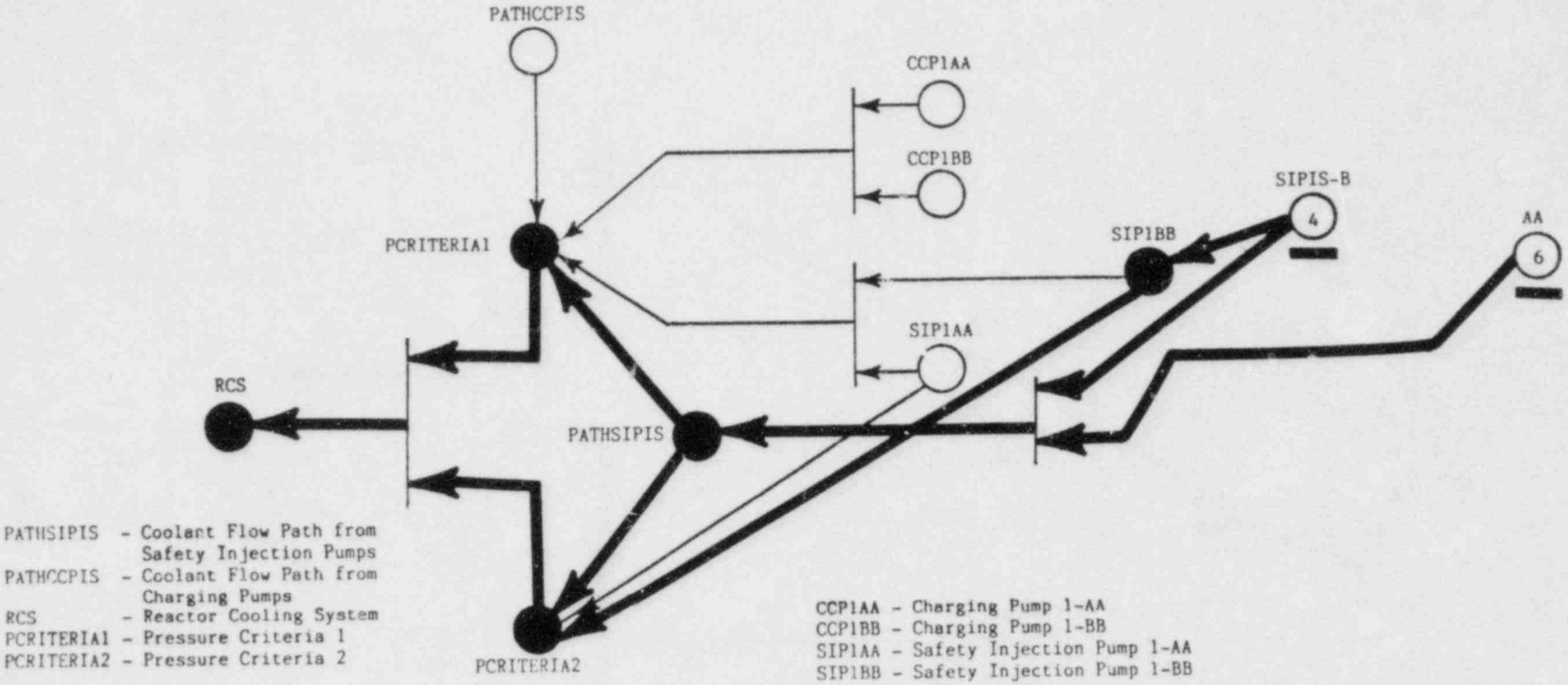
Figure 3-10. Failure Mode 5



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-11. Failure Mode 6



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

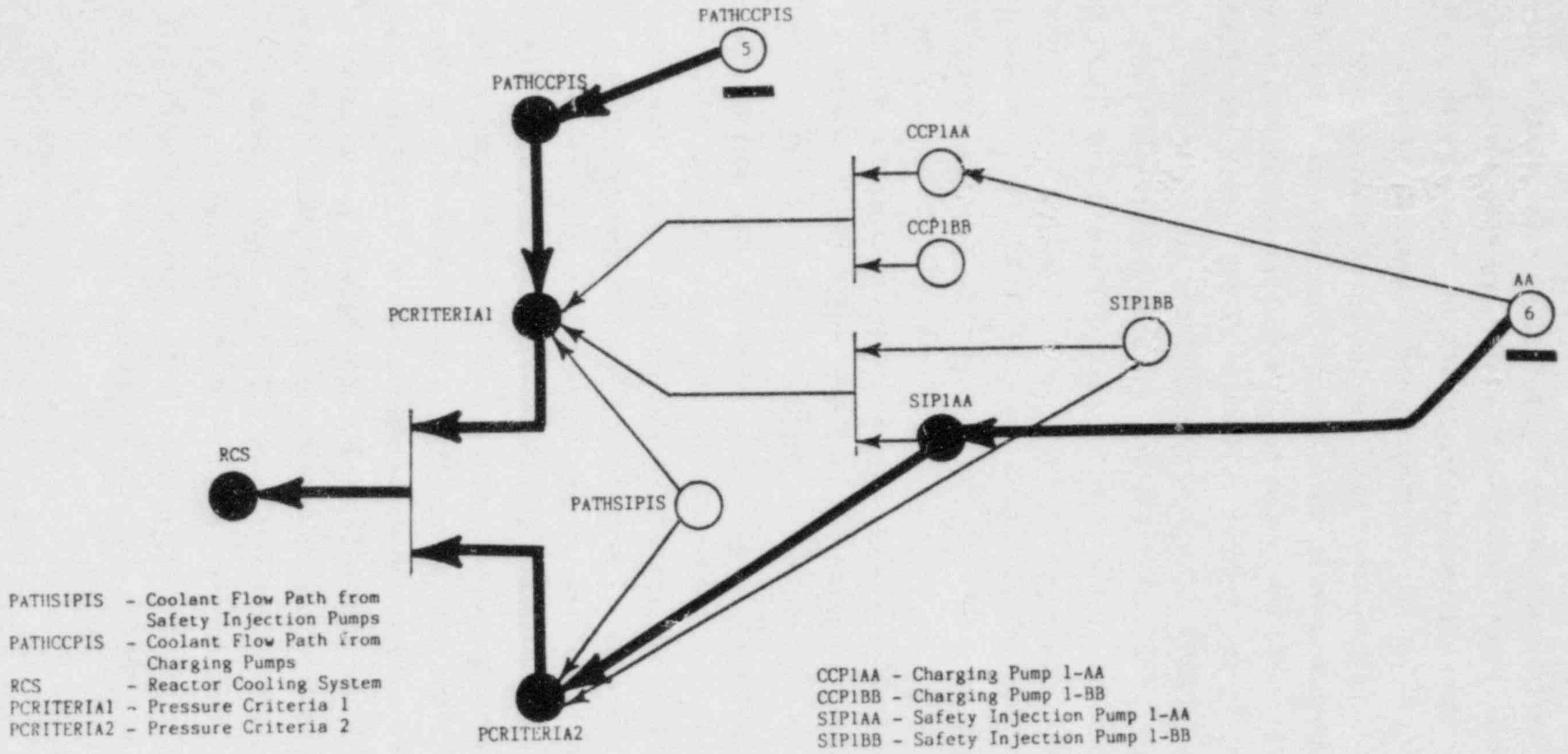
CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-12. Failure Mode 7

in the component cooling water system, CCS, are AA singletons. This is because there are normally 2 component cooling pumps, CCWP1AA and CCWP1BB, dedicated to drawing heat away from the front-line A-trains (FSAR Figure 9.2-19) and one of these pumps, CCWP1AA, is already running during normal plant operation. For the heat removal from the front-line B-trains, only 1 pump, CCWPCS, is dedicated and it must be turned on. Both CCWP1AA and CCWP1BB share the same recirculation path and the 10 AA singleton components include such hardware as the component coolant heat exchanger A (CCHXRA), butterfly valve VB170510, and flow control valve FCV1702. There is no single component in the systems studied which can defeat both CCWP1AA and CCWP1BB. Failure of heat removal from both front line A trains disables those trains' pumps. That failure, coupled with the loss of SIPIS-B, disables three out of the four injection pumps and hence does not meet the S1LOCA requirements.

3.1.8 Analysis of Failure Mode 8

Failure mode 8, shown in Figure 3-13, is a singleton failure to PATHCCPIS with a singleton failure to both front-line A-trains. An example of a singleton to PATHCCPIS is a blockage in the boron injection tank (BIT), node 49. All flow to the core through CCPIS normally flows through the BIT and alternate paths must be manually enabled. Thus, in the fully automatic mode, should a blockage occur anywhere in the BIT, from the sparger type inlet assembly used to mix the flow to the tank's interior or outlet, PATHCCPIS would fail. No constraints are imposed as to the origin or nature of the blockage. All that matters is that flow through the BIT is either blocked or reduced to an unacceptably low level. An example of the AA singleton is EINRLK1713, node number 769. This component (or collection of components) is used in the transfer of power from the normal 6900VS1AA shutdown board feeder to an alternate feeder upon loss of normal power. Its presence was deduced from the representation of electrical interlocks between the feeders to the bus (FSAR Figure 8.3-16). Such an automatic transfer device is an "auctioneering circuit" or hardware which, in this case, would monitor voltages and/or currents. The auctioneering circuit can open and close any of the breakers to enable power to the bus. A



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

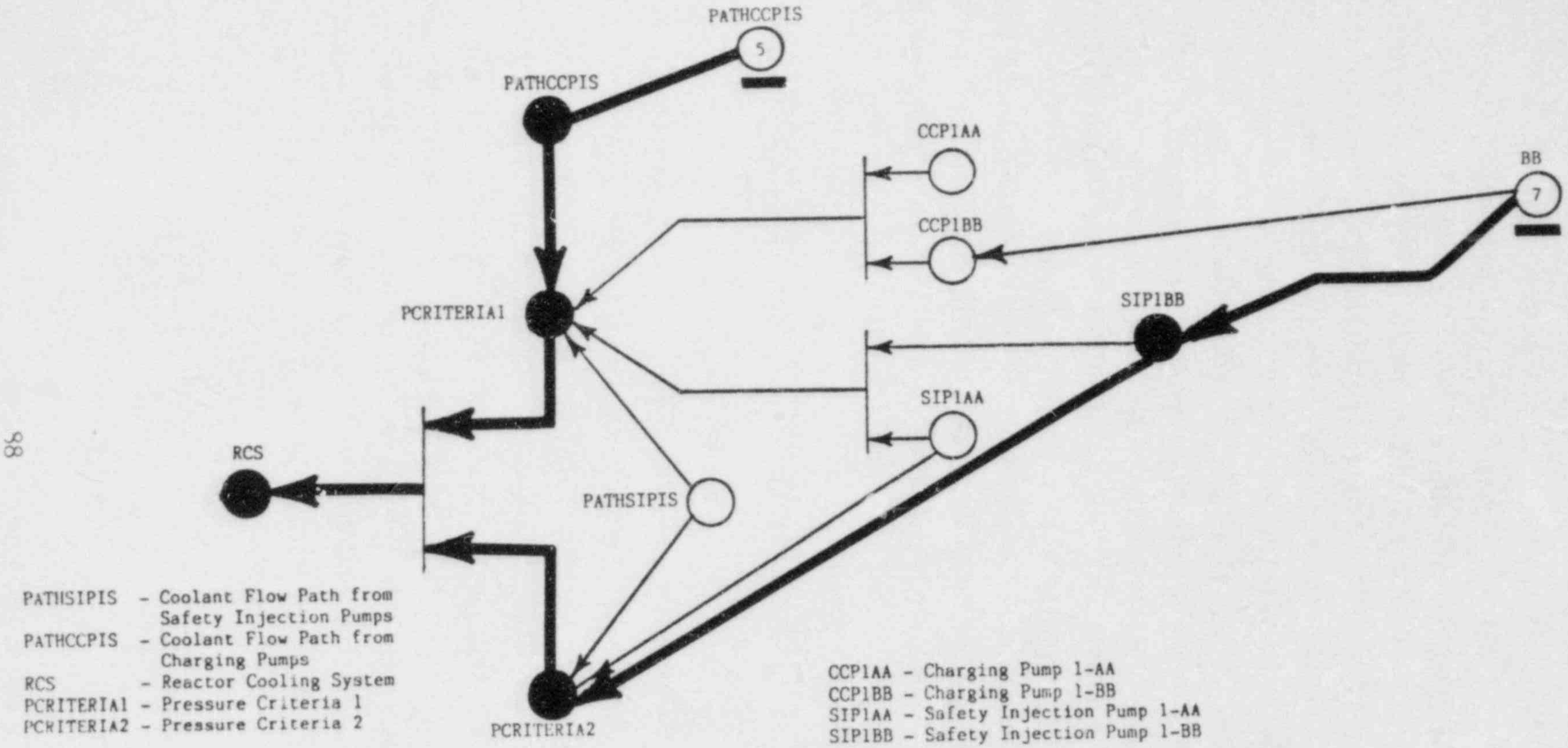
CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-13. Failure Mode 8

failure of this component which would result in all of the breakers being opened will cause the entire bus to fail. Analogies to this kind of possible failure can be found in systems ranging from a push button car radio to the space shuttle. A typical push button car radio has a mechanical interlock which allows only one button to be engaged at any time. The failure of mechanical linkages in the interlock, i.e., auctioneer, could enable more than one button or no button to be pushed in. In the space shuttle, three onboard computers monitor vehicle status and input to an electronic auctioneer which decides if all three computers are in agreement. The result is that the auctioneer is the single component or network of components which is the singleton that defeats a perceived triple redundancy. In the HPSIS, without more detailed hardware descriptions it is impossible to determine the smallest section of the bus auctioneer which is the singleton. The auctioneer has four feeder inputs and a single output, the normally closed breaker. Should EINRLK1718 fail by opening normally closed feeder breaker 1718 without closing any of the redundant feeder breakers, the bus would fail. Failure of that bus would keep the A train of the charging and injection pump systems from operating. This, coupled with blockage in the BIT, would keep the HPSIS from meeting the success criteria for the S1 LOCA.

3.1.9 Analysis of Failure Mode 9

Failure mode 9, shown in Figure 3-14, is a failure of PATHCCPIS with a BB singleton failure. An example of this is the doubleton composed of node 46 with any of the BB singletons mentioned above. Node 46 is check valve VC63581 which is inside containment. All flow through the normal injection path through CCPIS passes through this valve so if it were to fail shut, CCPIS would fail. This, again, is only in the case where no positive human intervention is allowed since alternate paths can be manually enabled. Loss of CCPIS, coupled with the loss of safety injection pump SIP1BB due to the BB singleton, leaves only one pump running which is inadequate.



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

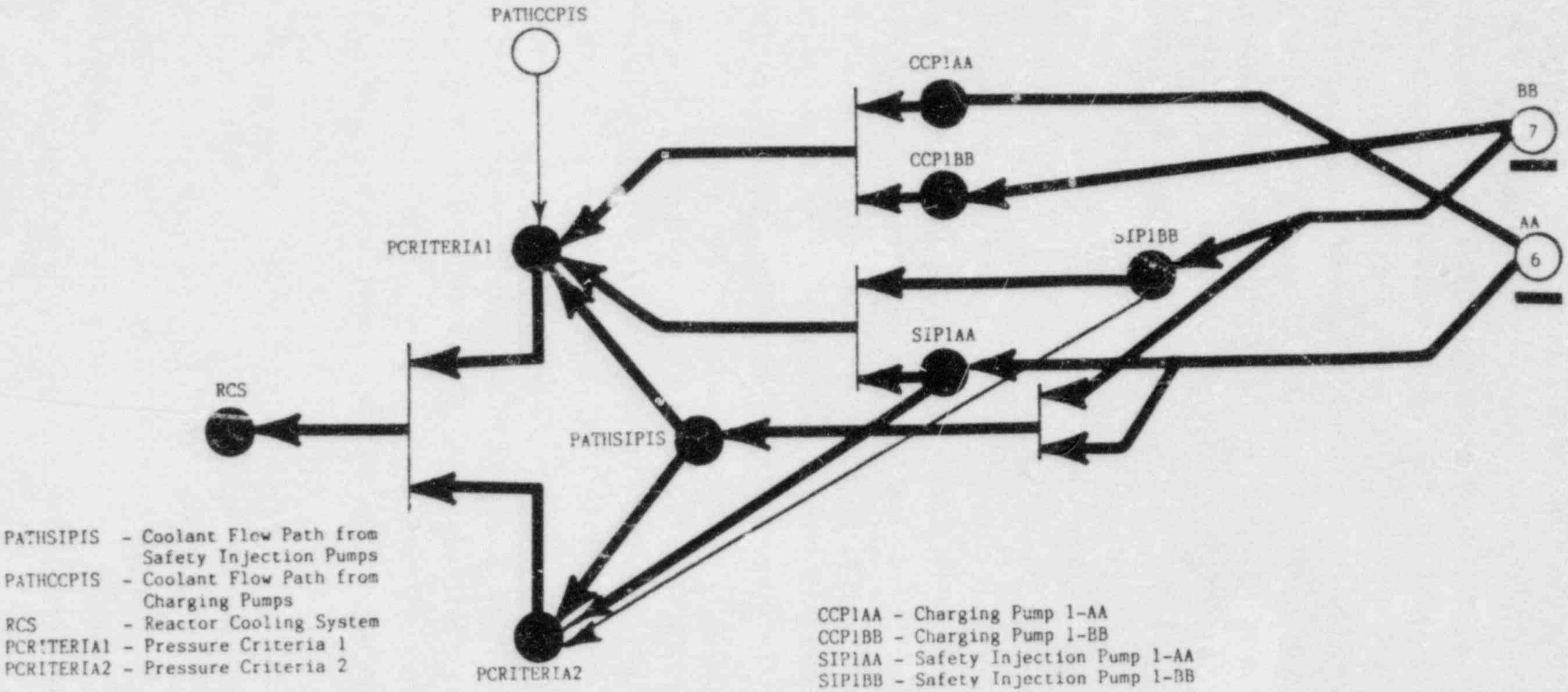
Figure 3-14. Failure Mode 9

3.1.10 Analysis of Failure Mode 10

Failure mode 10, shown in Figure 3-15, is an AA singleton failure coupled with a BB singleton failure. Neither of these types of singletons exist in front-line systems. An example of each is given by the doubleton pair, nodes 164 and 192. These are two fuses in the vital instrumentation and control system, respectively. Node 164 is FUSE10I which is fuse #201 in vital battery board I. It is the normal control power to components driven by 6900VS1AA, such as CCP1AA and SIP1AA. Failure of that fuse prevents those pumps from starting. Failure of FUSE10II has the analagous effect on the two train B pumps CCP1BB and SIP1BB. FUSE10II is fuse #201 in vital battery board II.

3.1.11 Analysis of Failure Mode 11

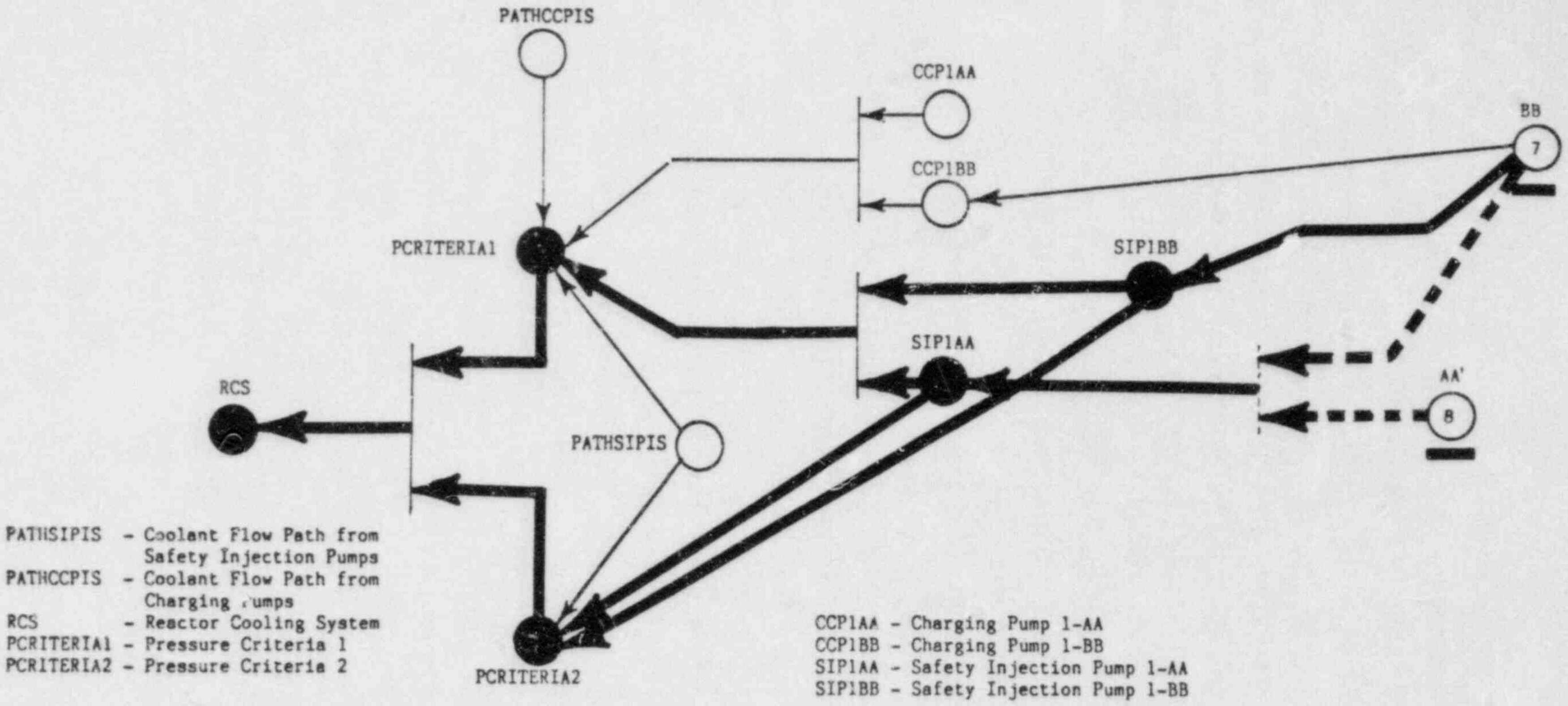
Failure mode 11, shown in Figure 3-16, is a doubleton composed of any of the BB type singletons mentioned thus far with AA' type singletons. Primed singletons by themselves do not fail a front-line train, but do fail a part of a support system so that in combination with another single component failure (both support and front-line) can cause the system to fail. All AA' singletons act to disable part of the component cooling system, CCS. For instance, node 321 is a 480 volt shutdown board 480VS1A1A. It is the normal power supply to CCWP1AA, one of the two component cooling pumps which supports both front-line A trains. Failure of that pump alone does not cause a front-line train to fail since the other pump, CCWP1BB, is sufficient. However, should node 192, FUSE10II (fuse #201 in vital battery board II), fail then not only doesn't CCWP1BB receive the control power it needs for actuation, but neither do CCP1BB and SIP1BB. The result is that both front-line train A's lose heat removal and both front-line train B's lose pump control power so that all four injection pumps fail.



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCR:TERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-15. Failure Mode 10



PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2

CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-16. Failure Mode 11. Dotted lines represent connections through support systems which, together, cause SIP1AA to fail.

3.1.12 Analysis of Failure Mode 12

Failure mode 12 is a doubleton composed of a failure of a BB' singleton with an AA' singleton and is shown in Figure 3-17. An example of this doubleton is that of node 742 with node 379, both in EPS. Node 742 is EINRLK31, a manually actuated electrical interlock between the normal and alternate feeders to 480 vac shutdown bus 1B1B (480VS1B1B). Should this interlock fail in such a way that disconnects the norma, power supply to the bus, there is no automatic means of restoring that power or of transferring to the alternate power supply. Hence, everything supported by that bus would fail. As it pertains to this doubleton, those failed components would be found in 2 different systems, CCPIS and CCS. In CCPIS, they would be all of the B-train motor operated valves that must re-orient to isolate the system from the boron recycling system for injection. In CCS, the affected component would be CCWP1B1B, the unit 1 B-train component cooling pump. 480VS1B1B is the power supply to the pump so the pump would fail to perform its task of circulating coolant to the two front-line A-train pumps. That CCWP is redundant to another, however, namely CCWP1AA. Like CCWP1BB, this pump derives its power from a 480 vac shutdown board, 480VS1A1A, node 379. Also in node 379 is the breaker in the path of the normal feeder. The breaker is labeled R50 on the digraph of EPS shown in Figure B-20 (no identifier was found on the P&ID). Should this breaker have been opened, either due to a mechanical failure or operator error, then normal power to the bus would be lost and, as with the other shutdown bus, there is no automatic way to restore power. Components affected by loss of power to that bus are: 1) The A-train motor operated valves in CCPIS which must re-orient to enable an injection path and, 2) The component cooling pump CCWP1AA. The high pressure injection system fails because, with both A and B-train valves in CCPIS unable to re-orient, that system cannot be used for injection. In addition, loss of both redundant component cooling water pumps CCWP1AA and CCWP1BB used to cool the front-line A-train pumps keeps SIP1AA from functioning due to overheating. The remaining pump, SIP1BB, is inadequate for injection.

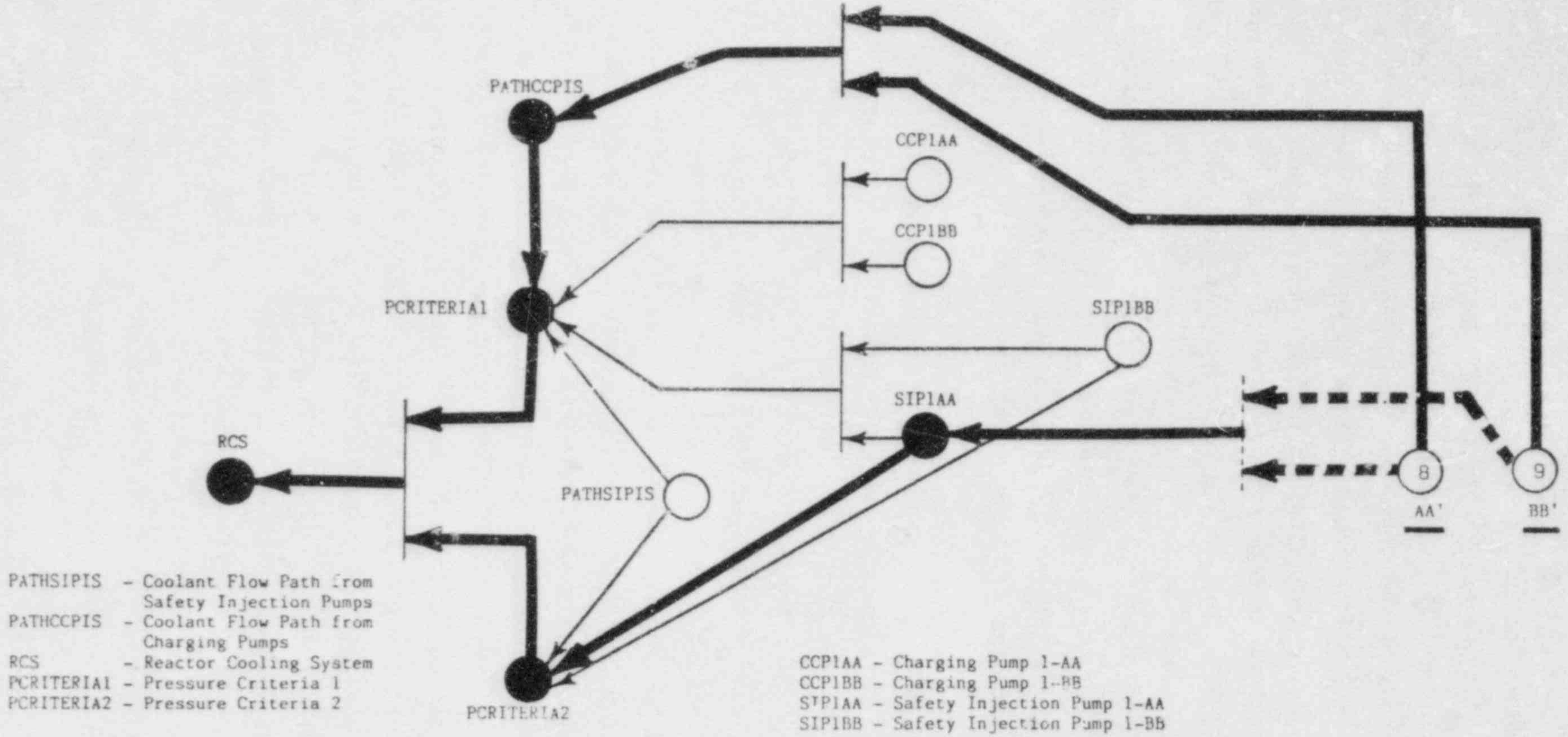

PATHCCPIS
CCP1AA
CCP1BB
PCRITERIA1
SIP1BB
SIP1AA
RCS
PATHSIPIS
8
9
AA'
BB'
PCRITERIA2
PATHSIPIS - Coolant Flow Path from Safety Injection Pumps
PATHCCPIS - Coolant Flow Path from Charging Pumps
RCS - Reactor Cooling System
PCRITERIA1 - Pressure Criteria 1
PCRITERIA2 - Pressure Criteria 2
CCP1AA - Charging Pump 1-AA
CCP1BB - Charging Pump 1-BB
SIP1AA - Safety Injection Pump 1-AA
SIP1BB - Safety Injection Pump 1-BB

Figure 3-17. Failure Mode 12. Dotted lines represent connections through support systems which, together, cause SIP1AA to fail.

3.2 Results with Human Mitigation

When operators are allowed to act as backups to failed systems the robustness of the plant improves dramatically. The doubleton array for Case II is given in Figure 3-18. Seventy percent of the singletons and 80 percent of the doubletons of the fully automatic case disappear when positive human intervention is allowed. The only remaining singletons are RWST and HDR1. The 5 other singletons, HDR2, HDR9, FCV635, VC63510, and FCV6322, found in Case I can all be bypassed manually. The first two can be bypassed by routing flow through the residual heat removal system. This alternate route was validated by the operators. The third valve can be easily bypassed by opening either FCV63156 or FCV63157. These valves require manual actuation and route flow into the hot legs of the RCS rather than the cold legs. Although injection into the cold legs is preferred, injection into the hot legs is satisfactory.

The number of doubletons is 708, down significantly from the 4314 for the case of total reliance on automatic systems. Ninety-four percent of the 2741 doubletons arising from the normal configuration of the component cooling water system, CCS, disappear since that system's piping is a veritable switchyard, making it possible for the operator to work around nearly any singleton failure. The many doubletons due to blown fuses in the vital instrumentation and control system are easily manually circumvented with backup normal power, normal emergency power or backup emergency power. Failures of 480 volt shutdown and motor operated valve boards can be overcome by transferring manually from normal to alternate feeders. Singleton failures to PATHCCPIS which occur downstream of HDR8 (see failure mode 4) can be bypassed by opening up the flow control valves FCV6290 and FCV6291 for injection through the regenerative heat exchanger. There is a lot of commonality between the failure modes which exist in Case I and Case II. In both cases, doubletons due to failure modes 1-10 arise. This is due to the presence of failure categories 1-7 in both cases. Failure modes 11 and 12 do not arise in Case II since there are no AA' or BB' singletons in Case II. These singletons arose due to the normal dependence of the front-line systems on the component cooling system, CCS, and are not consequential if alternate paths are enabled manually.

```
      5  6  7  8 25 29 31 61 64 65 68 85 87 89 94 95 96102115117120150178261262263264759769843844847
   5  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  *  *  -  -  *  -  -  -  -
   6  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  -  -  -  *  *  -  *  -  -  -
   7  -  -  -  *  *  -  -  *  -  -  *  *  -  -  *  -  -  -  -  -  -  -  *  *  *  -  -  *  -  -  -  -
   8  -  -  *  -  -  -  *  *  -  -  *  *  -  -  -  -  -  -  *  -  -  *  -  -  -  *  *  -  *  -  -  -
  25  -  -  *  -  -  -  *  -  -  -  -  -  -  -  -  -  -  -  *  -  -  *  -  -  -  *  *  -  *  -  -  -
  29  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *
  31  -  -  -  *  *  -  -  -  -  -  -  -  -  -  *  -  -  -  -  -  -  -  *  *  *  -  -  *  -  -  -  -
  61  -  -  *  *  -  -  -  -  -  -  -  -  -  -  *  -  -  -  *  -  -  *  *  *  *  *  *  *  *  -  -  -
  64  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  -  -  -  *  *  -  *  -  -  -
  65  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  *  *  -  -  *  -  -  -  -
  68  -  -  *  *  -  -  -  -  -  -  -  -  -  -  *  -  -  -  *  -  -  *  *  *  *  *  *  *  *  -  -  -
  85  -  -  *  *  -  -  -  -  -  -  -  -  -  -  *  -  -  *  *  -  -  *  *  *  *  *  *  *  *  -  -  -
  87  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  89  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  -  -  -  -  *  *  *  -  -  *  -  -  -  -
  94  -  -  *  -  -  -  *  *  -  -  *  *  -  -  -  -  -  -  *  -  -  *  -  -  -  *  *  -  *  -  -  -
  95  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *
  96  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *
 102  -  -  -  -  -  -  -  -  -  -  -  *  *  *  -  -  -  -  *  *  *  -  -  -  -  -  -  -  -  -  -  *
 115  -  -  -  *  *  -  -  *  -  -  *  *  -  -  *  -  -  *  -  -  -  -  *  *  *  -  -  *  -  -  -  -
 117  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 120  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 150  -  *  -  *  *  -  -  *  *  -  *  *  -  -  *  -  -  -  -  -  -  -  *  *  *  -  -  *  -  -  -  -
 178  *  -  *  -  -  -  *  *  -  *  *  *  -  *  -  -  -  -  *  -  -  *  -  -  -  *  *  -  *  -  -  -
 261  *  -  *  -  -  -  *  *  -  *  *  *  -  *  -  -  -  -  *  -  -  *  -  -  -  *  *  -  *  -  -  -
 262  *  -  *  -  -  -  *  *  -  *  *  *  -  *  -  -  -  -  *  -  -  *  -  -  -  *  *  -  *  -  -  -
 263  -  *  -  *  *  -  -  *  *  -  *  *  -  -  *  -  -  -  -  -  -  -  *  *  *  -  -  *  -  -  -  -
 264  -  *  -  *  *  -  -  *  *  -  *  *  -  -  *  -  -  -  -  -  -  -  *  *  *  -  -  *  -  -  -  -
 759  *  -  *  -  -  -  *  *  -  *  *  *  -  *  -  -  -  -  *  -  -  *  -  -  -  *  *  -  *  -  -  -
 769  -  *  -  *  *  -  -  *  *  -  *  *  -  -  *  -  -  -  -  -  -  -  *  *  *  -  -  *  -  -  -  -
 843  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  -
 844  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  *  -  -
 847  -  -  -  -  -  *  -  -  -  -  -  -  -  -  -  *  *  *  -  -  -  -  -  -  -  -  -  -  -  -  -  -
```

Figure 3-18. Doubletons for Case II: Human Mitigation Enabled

Positive operator intervention introduces new kinds of doubleton failures. These arise from the enabling of alternate paths around what in Case I were singletons to the entire HPSIS. The alternate paths are in the manually enabled network between the RWST and the front-line pumps (RWST.DAT). For instance, in Case I, HDR2 was a singleton to HPSIS. In Case II, however, it appears in 7 doubletons. In fact, all of the 5 nodes which are singletons in Case I but not in Case II appear in the doubleton array for Case II. They contribute a total of 85 new doubletons. Given their small failure probabilities, the new doubletons contribute much less to the overall probability of system failure than the singletons they replace.

There is a failure mode in Case II which doesn't occur in Case I which results from enabling alternate paths from the RWST to the front-line pumps. Failure of HDR2 with either HDR4, FCV63177, or HDR3 keeps flow from reaching both safety injection pumps. These are not failures of a trained system, but rather the failures of the normal SIPIS injection path combined with a failure to use the crosstie connection between CCPIS and SIPIS.

Finally, in an effort to assess the aggregate impact of two groups of operator inputs, two master nodes were created. OPRREMOTE connects to all OPR operator inputs actuating components by remote control. These actuations occur in the main and auxiliary control rooms. OPRLOCAL connects to all OPR operator inputs actuating components locally (at the component). When these two master nodes are connected to the two operator node groups, each group represents either a single operator or a group of operators acting as one. The analysis of this case showed neither of the master nodes appearing either in the singleton list or the doubleton array. This implies the triple redundancy depicted in Figure 3-19 between remote operators, local operators, and the automatic system. It means that none of the redundancy (as measured by singletons and doubletons) acquired by allowing humans to mitigate positively is lost if the operator(s) are only in the control rooms or only roving through the plant. There are two caveats here. First, the roving operator(s) would be assumed to be aware of the state of the plant by being dependent upon the same instrumentation as the control room operator(s). Second, there may be coupling between the two groups of operators which would arise if plant operational procedures were included and modeled.

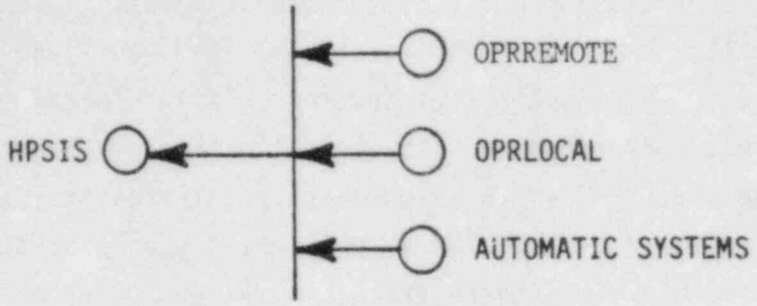


Figure 3-19. Triple Redundancy of Automatic Systems and Local and Remote Operators

3.3 Error Checking Using Failure Modes

Grouping the doubleton failures into failure catagories and failure modes provides an opportunity for error checking. Based upon the logic of the success criteria logic, certain kinds of doubleton failure modes can be expected to occur and, conversely, others are not expected. Some failure modes which would be expected can be determined by calculating reachability on the RCS success criteria alone. The results are a subset of the entire set of doubletons possible since there are many "master" nodes not in the success criteria digraph which can cause more than one node in the success criteria to fail. An example of such a master node is 6900VS1AA, a common power supply to CCP1AA and SIP1AA. This is an AA singleton since its failure causes both front-line A trains to fail. Without modeling the dependence of the nodes in the success criteria on other systems, this doubleton can't be anticipated. On the other hand, if a doubleton occurs between an AA singleton and possibly a CCPIS-A singleton, it would be expected to be erroneous. Referring to the success criteria, it can be seen that the failure of both front-line A trains with a CCPIS-A singleton (e.g., CCP1AA) will not propagate through to RCS. Each of the failure modes found in Case I and Case II were checked against the RCS success criteria logic for validation.

To summarize, error checking using failure modes consisted of the following steps:

1. Categorize the nodes in the doubleton array by the part of the global system they can defeat. This defines a set of failure categories.

2. Generate a list of all combinations of pairs of failure categories that arise in the doubleton array. These pairs are the failure modes.

3. Compare failure modes to RCS success criteria logic for validation.

4. QUANTITATIVE ANALYSIS

As discussed above, two cases were analyzed. In the first, the fully automatic case, 7 singletons and 4314 doubletons were found. In the second, the constructive operator case, 2 singletons and 708 doubletons were found. In order to determine the significance of these singletons and doubletons a quantitative analysis was performed. This analysis was conducted by assigning a failure probability to each component which was a member of the failure sets. The data used for component failure probabilities was taken from: WASH 1400 [15], IEEE Standard 500 [19], the Zion Seismic Safety Study [17], the Indian Point-3 Probabilistic Safety Study [20] and others [21, 22, 23, 24]. All component failures which appeared in singletons or doubletons were treated as independent. This independence assumption is accurate to the level of modeling detail of this DMA. Any physical dependency which could be identified was included in the DMA model except for the following:

Common Location
Common Maintenance
Common Manufacturer
Common Environmental Conditions.

Shared support systems which would make apparently independent components dependent were explicitly modeled. For example, the failure of two centrifugal charging pumps because of the loss of a common component in the component cooling system would appear in a failure set with the component cooling component as a singleton or as part of a doubleton. The pump which fails due to the cooling failure would not appear in the failure set. Figure 4-1 illustrates this situation for a simplified case.

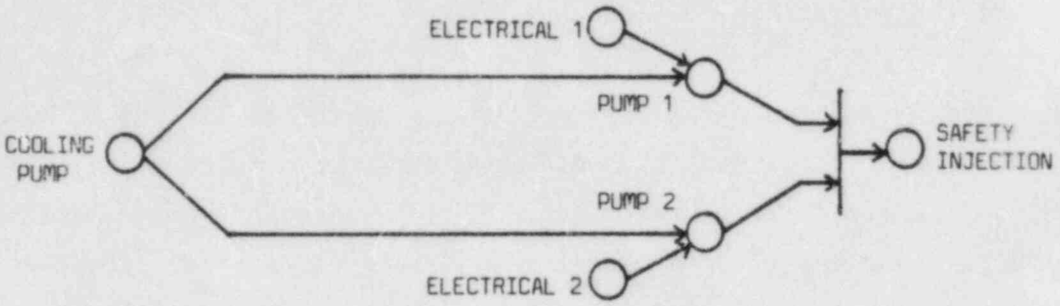


Figure 4-1. Simplified Example of Common Mode Failures

The failure sets for this case are:

Cooling Pump
Electrical 1 * Electrical 2
Pump 1 * Pump 2
Electrical 1 * Pump 1
Electrical 2 * Pump 2

Notice that the pumps do not appear in a cut set with the cooling pump. The appearance of a pump in the cut set means that the pump itself fails due to internal reasons not due to the failure of an external component.

The data bases used indicate that most components have several failure causes. Each of these failure causes was taken as independent and combined into a single failure probability for the component by the following equation:

$$P = 1 - \prod_{i=1}^{n} (1-P_i)$$

where n is the number of failure causes of the component and P_i is the probability of failure due to the i^th cause.

The total probability of failure due to all singletons (and doubletons) was computed using the SIGPI code developed at LLNL [25, 26]. In this code the cut sets are not assumed to be independent. The SIGPI program uses two fast complementary methods of computing the probabilistic performance of complex systems: the PI method and the SIGMA method. The former exploits the fact that, when system variables are carefully defined, these variables are often statisticaly independent conditional to the environment in which they are embedded, a very convenient fact from a computational point of view. The latter is used to compute the probability of combinations of events produced by the PI method by disjointing such events, thereby allowing the exact computation of performance. The computational complexity of the overall process is a polynomial function of the number of components. For very large problems, where costs of precise answers may be prohibitive, a desired accuracy can be specified, and the SIGPI algorithms will halt when that accuracy has been reached.

4.1 Quantitative Results

The quantitative results from the analysis of the two cases studied is given below in Table 4-1. It can be seen from this table that the contribution from the doubletons is slightly larger than the contribution from the singletons in the fully automatic case.

	Fully Automatic (Case I)	Fully Redundant (Case II)
DMA Singletons	$1.8 \times 10^{-2*}$	1.0×10^{-12}
DMA Total (1.5 - 3.0) LOCA	$4.0 \times 10^{-2*}$	4.9×10^{-3}
WASH 1400 (1.5 - 2.0) LOCA	8.6×10^{-3}	
BNL [14] (1/2 SIP & 1/2 SCP)	3.1×10^{-3} ($\beta = 0$) 1.8×10^{-2} ($\beta = 0.3$)	

Table 4-1. HP Safety Injection System Failure Probabilities

As stated in an earlier section, the designers rely on the human operators as the ultimate backup. The ratio of the failure probability of the fully automatic case to the failure probability of the constructive operator case = 8.2 dramatically illustrates this.

The probability data base used includes a "failure probability" for the component outage due to maintenance (0.80×10^{-2}). This failure probability is actually an unavailability which appears to be the result of the normal availability calculation given by

* NRC Licensing Conditions lower the singleton probability to 1×10^{-4} and the DMA total to 2×10^{-2} (see Section 4.2).

$$A = \frac{MTBF}{MTBF + MTTR}$$

where MTBF is the mean time between failure and MTTR is the mean time to repair. Using these unavailability numbers in the calculation of the high pressure safety injection system failure probability most likely leads to a significant upward bias. It is likely that the maintenance procedures require that bypass paths be enabled when a component is down for maintenance. In the absence of the maintenance procedures for the plant, it was assumed that this was not the case. Thus, the failure probability has most likely been overestimated.* To quantify this effect a failure analysis was performed with the maintenance outage unavailability for components set to zero for all components except the two charging and two safety injection pumps.** Table 4-2 compares the results of this analysis for the fully automatic case.

	Outage	Restricted Outage
Fully Automatic	4.0×10^{-2}	3.2×10^{-3}

Table 4-2. Effect of Maintenance Outage

There is a complicating factor in this analysis. There is a small, but possibly significant, probability that the bypass paths will not be enabled during maintenance due to operator error. This could be modeled in DMA, but given the constraint of no procedural information, was not.

A third quantitative analysis was performed wherein components in the component cooling system were eliminated from the singleton and doubleton failure sets. Elimination of these failure sets reduced the number of doubletons from 4314 to 1573. The corresponding system failure probability changed from 4.0×10^{-2} in the complete case to 2.3×10^{-2} for the case without the cooling system.

----

* Scope limitations on maintenance considerations have lead to overestimation of this case.

** Included in the failure sets is a set which includes both safety injection pumps. Removal of the maintenance unavailability for this set has a very slight (<1%) effect on the system unavailability.

4.2 Discussion of Failure Probability Calculation

As discussed above, the failure probability calculation was performed using a new code, SIGMA PI [26], developed by Lawrence Livermore National Laboratory. The inputs to this code are:

1) the failure sets generated by the DMA codes; and
2) a list of component names with associated failure probabilities.

These failure probabilities were taken from a variety of references as discussed in Section 4.3. The probability data base is given in Appendix D.

All components which were not listed in the failure data base were assumed to have a failure probability of zero. Thus, the failure probability of any failure set which included an "unknown" component was zero. The data base included data for 177 components. Approximately 2965 failure sets out of 4314 doubleton sets were not evaluated due to missing data. In these missing sets there was a total of 76 components which were not in the probability data base. These components are listed below in Table 4-3, where it can be seen that most of the components were parts internal to motors and valves.

The quantitative result from the DMA of the fully automatic HPSIS case was:

4×10^{-2} for failure sets including singletons and doubletons.

A recent study by BNL [14] reported that an apparently equivalent case was studied using "conventional" fault tree techniques. The results of this study indicated an unavailability of SI from 3.1×10^{-3} to 1.8×10^{-2} depending on the dependency factor, β. The smaller number corresponded to no dependency ($\beta = 0$) and the larger to strong dependency ($\beta = 0.3$). If the assumption is made that the failure probability data bases used are

MOT2S
R2S
COIL2S
TW170146B
TW170146A
FE170146
R5T
MOT2Y
FE170165
TW17072
TW70162
TW70201
FE70201
R2YS
COIL2YS
MINRLKSWG1
SWSI1YS
SWA3YS
FUSE3YS
R5YS
125VVBII
125VVBIV
MOT2T
R2T
COIL2T
TW170145B
TW170145A
FE170145
R5S
FE170159
TW17070
TW170161
TW170199
FE170199
125VVBI
MOT2U
R2U

COIL2U
TW170147B
TW170147A
FE170147
MOT2V
R2V
COIL2V
TW170148B
TW170148A
FE170148
FE6320
BIT
FE6343
VC63572
FE63170
VC62504
SWSI1V
SWA3V
FUSE3V
FE63151
SWSI1U
SWA3U
FUSE3U
SWSI1S
SWA3S
FUSE3S
SWSI1T
SWA3T
FUSE3T
X2
MINRLK33
MOT2YQ
R2YQ
VC170504A
X4
MINRLK53
ONSITE
OFFSITE

Table 4-3. Components not in Probability Data Base

consistent, it appears that the quantitative results from the DMA of the HPSIS are comparable to those of BNL and indicate a high dependency. It must be noted that the explicit modeling of all components in the DMA removes the need for including any unknowable dependency factors.

The contributions from the singletons and doubletons to the failure probability are given in Table 4-4. From this table, it can be seen that only about 50% of the failure probability is due to the singletons. All of the singletons identified by the DMA were identified by NRC in the Evaluation Report [27] and special "means have been provided to preclude such spurious misalignment". The effect of these "means" would be to effectively remove the failure contribution from the singletons and thus reduce the failure probability of HPSIS from 4 x 10^{-2} to about 2.2 x 10^{-2}.

	Fully Automatic
DMA Singletons	1.8 x 10^{-2}
DMA Doubletons	2.2 x 10^{-2}
DMA Total	4.0 x 10^{-2}
DMA with License Conditions	2.2 x 10^{-2}

Table 4-4. Singleton/Doubleton Contribution

A sensitivity study was run with the failure probability (and unavailability) of the following "locked off valves" set to 0 for the full maintenance outage and no maintenance outage case. The valves which had their failure probabilities set to zero were:

VGA 62509
VGA 62510
VGA 63527
VGA 63525

FCV 6322
FCV 635

The results from these sensitivity runs are summarized in Table 4-5.

	FULL MAINTENANCE	RESTRICTED	NO MAINTENANCE
	UNAVAILABILITY	MAINTENANCE	UNAVAILABILITY
	INCLUDED	(PUMPS ONLY)	
BASELINE	4×10^{-2}	3.2×10^{-3}	2.7×10^{-3}
LOCKED OFF VALVES (P_f=0)	2.7×10^{-2}		1.5×10^{-3}

Table 4-5. Effect of Locked Off Valves and Maintenance Unavailability

It should also be noted that we did not include any failures due to seismic, fire, or flood events, hence the failure probability calculated is for a benign environment only.

4.3 Data Base

The complete probability data base used for this analysis is shown in Appendix D. This data was extracted from WASH 1400 [15], IEEE Standard 500 [19], the LLNL Zion Seismic Safety Report [17] and others [20, 21, 22, 23, 24]. Care was taken not to include external causes in the failure probabilities used for each component. Table 4-6 contains the generic data base which was extracted from these sources and used to the full data base listed in Appendix D. Negative signs were used in this table to indicate a failure rate to the computer and were multiplied by 0.5 hours to obtain a failure probability on the assumption that the safety injection phase would last about one-half hour.

The first two components on the list are check valves that need to open and to close respectively, The Indian Point data base indicated a failure rate of 1×10^{-4} per demand for a check valve to fail to open on demand and a failure rate of 0.5×10^{-7}/hour for excessive leakage. The first active component in the generic data base was a motor operated valve which had to open (VMOAO) for safety injection. The generic data base contained six failure modes for this type of valve. These were:

Failure Mode	Source	Probability
(1) Failure to Operate on Demand	IP	4×10^{-3}
(2) Failure due to Closure (or Plugging)	IP	1.4×10^{-8}
(3) Inadvertently Closed	Zion	1×10^{-3}
(4) Maintenance Error leads to Blockage	Zion	1×10^{-4}
(5) Out of Service for Test	Zion	7×10^{-4}
(6) Out of Service for Maintenance	Zion	8×10^{-3}

As can be seen, the first two failure modes are due to mechanical failures, whereas the last four are due to incorrect human interactions with the valve. These last terms were taken from the Zion SEISIM data base [28]. If the six terms are taken as independent, the resulting failure probability for the VMOAO is

$$P_H = 1- \prod_{i=1}^{N} (1 - P_i) = 0.0137$$

where P_i is the ith term in the probability data base.

If all four human interaction terms are dropped, the failure probability is reduced to:

$$P_{NH} = .004$$

The bulk of the reduction in failure probability occurs due to the removal of the "out of service for maintenance" term. The failure probability can be recalculated including only the first five terms and yields:

$$P_{HNA} = 0.0058$$

Thus, about one-half of the probability of valve failure is due to the unavailability due to valve maintenance and about one-half of the remaining failure probability is due to other human interactions.

The fourth component in the generic data base (Table 4-6) was a motor operated valve (VMOAC) which had to close for safety injection. As can be seen from the table, the first two failure terms were taken from the Indian Point data base and are hardware related failures. The remaining four terms were taken from the Zion data base and are human failure related. Except for the second term, the failure probabilities are identical to the VMOAO, and the impact of removing maintenance, and human related terms is about the same as for the motor operated valve that needs to open.

There were two generic classes of pumps identified in this study, the pump which was off and turns on at the receipt of the SI signal and the pump that was already running at the time of safety injection. The safety injection pumps fit into the first category (PUMPNO). The first two terms in Table 4-6 for the PUMPA are terms due strictly to mechanical failure, whereas the last two terms are caused by human error. The failure data for the normally running pump does not contain a term due to failure to turn on since it is already operating. The pump failure data is again dominated by the "unavailability due to maintenance" term with the second largest effect contributed by a human operator inadvertently turning the pump off.

Thus, the failure data used in the quantitative analysis of the HPSIS appears to be dominated by failures due to incorrect human interactions with the components of the system.

Negative probabilities represent probabilities per hour. References in parentheses are the entry number in Table 1-5, 1-4 in IP2PRA, "IP2 Specialized Component Hardware Failure Data". References to Zion are from Table D of SSMRP naming scheme and the SSMRP data base of random failures.

GENERIC FAILURE	COMPONENT (FUNCTION)	PROBABILITY OF FAILURE	DESCRIPTION OF FAILURE	REFERENCE
VCAO	CHECK VALVE (ACTUATE TO OPEN)	1.E-04	FAILURE TO OPEN ON DEMAND	(3)
VCNC	CHECK VALVE (NORMALLY CLOSED)	-5.E-07	FAILURE TO SEAT/EXCESSIVE REVERSE LEAKAGE	(4)
VMOAO	MOTOR OP VALVE (ACTUATE TO OPEN)	4.E-03	FAILURE TO OPERATE ON DEMAND	(6)
		-2.8E-08	TRANSFER CLOSED	(1)
		1.E-03	INDAVERTENTLY CLOSED (OD)	ZION
		1.E-04	MAINTENANCE ERROR LEADS TO BLOCKAGE (OK)	ZION
		7.E-04	OUT OF SERVICE - TEST (ON)	ZION
		8.E-03	OUT OF SERVICE - MAINTENANCE (OO)	ZION
VMOAC	MOTOR OP VALVE (ACTUATE TO CLOSE)	4.E-03	FAILURE TO OPERATE ON DEMAND	(6)
		-1.E-07	TRANSFER OPEN/EXCESSIVE LEAKAGE	(7)
		1.E-03	INADVERTENTLY OPENED (OC)	ZION
		1.E-04	MAINTENANCE ERROR LEADS TO LEAK (OJ)	ZION
		7.E-04	OUT OF SERVICE - TEST (ON)	ZION
		8.E-03	OUT OF SERVICE - MAINTENANCE (OO)	ZION

Table 4-6 Generic Failure Data Base

GENERIC FAILURE DATA BASE (PAGE 2)

GENERIC FAILURE	COMPONENT (FUNCTION)	PROBABILITY OF FAILURE	DESCRIPTION OF FAILURE	REFERENCE
VNO	MOTOR OP VALVE OR	-2.8E-8	TRANSFER CLOSED	(1)
	MANUAL VALVE	1.E-3	INADVERTENTLY CLOSED (OD)	ZION
	(NORMALLY OPEN)	8.E-3	OUT OF SERVICE - MAINTENANCE (OO)	ZION
VNO1	MOTOR OP VALVE OR	-2.8E-8	TRANSFER CLOSED	(1)
	MANUAL VALVE	1.E-3	INADVERTENTLY CLOSED (OD)	ZION
	(NORMALLY OPEN)			
VMONC	MOTOR OP VALVE	-1.E-7	TRANSFER OPEN/EXCESSIVE LEAKAGE	(7)
	(NORMALLY CLOSED)	1.E-3	INADVERTENTLY OPENED (OC)	ZION
		1.E-4	MAINTENANCE ERROR LEADS TO LEAK (OJ)	ZION
		7.E-4	OUT OF SERVICE - TEST (ON)	ZION
		8.E-3	OUT OF SERVICE - MAINTENANCE (OO)	ZION
VNC	MANUAL VALVE	-2.E-8	TRANSFER OPEN/EXCESSIVE LEAKAGE	(2)
	(NORMALLY CLOSED)	1.E-3	INADVERTENTLY OPENED (OC)	ZION
		1.E-4	MAINTENANCE ERROR LEADS TO LEAK (OJ)	ZION
		7.E-4	OUT OF SERVICE - TEST (ON)	ZION
		8.E-3	OUT OF SERVICE - MAINTENANCE (OO)	ZION
PUMPA	ANY PUMP	5.E-4	FAILURE TO START ON DEMAND	(11)
	(MUST ACTUATE)	-2.E-5	FAILURE DURING OPERATION	(13)-(21)
		1.E-3	OPERATOR FAILS TO LEAVE RUNNING (OG)	ZION
		8.E-3	OUT OF SERVICE - MAINTENANCE (OO)	ZION
PUMPNO	ANY PUMP	-2.E-5	FAILURE DURING OPERATION	(13)-(21)
	(NORMALLY ON)	1.E-3	OPERATOR FAILS TO LEAVE RUNNING (OG)	ZION
		8.E-3	OUT OF SERVICE - MAINTENANCE (OO)	ZION
HXR	HEAT EXCHANGER	-4.56E-6	RUPTURE/EXCESSIVE LEAKAGE	(24)
	PROBABILITY OF EITHER THE SHELL SIDE OR TUBE SIDE OF A HEAT EXCHANGER BEING PLUGGED IS NEGLIGIBLY SMALL (25), (26), ZION			
OILCL	OIL COOLER	1.E-4	FOR PUMPS ONLY: FAILURE OF PUMP (SIP OR CCP) DUE TO INSUFFICIENT COOLING	ZION

GENERIC FAILURE DATA BASE (PAGE 3)

GENERIC FAILURE	COMPONENT (FUNCTION)	PROBABILITY OF FAILURE	DESCRIPTION OF FAILURE	REFERENCE
GNDSLA	DIESEL GENERATOR	3.E-2	FAILURE TO START ON DEMAND	(27)
	(MUST ACTUATE)	2.E-2	FAIL DURING OPERATION	(28)
		1.E-3	OPERATOR FAILS TO LEAVE RUNNING	ZION*
		8.E-3	OUT OF SERVICE - MAINTENANCE	ZION*
BKRAC	BUS FEED BREAKERS	1.E-7	FAILURE TO CLOSE ON DEMAND	(29)
	(ACTUATE TO CLOSE)	-3.Ø8E-9	TRANSFER OPEN	(31)
		1.E-3	INADVERTENTLY OPENED BY OPERATOR (OC)	ZION*
BKRAO	BUS FEED BREAKERS	2.27E-5	FAILURE TO OPEN ON DEMAND	(30)
	(ACTUATE TO OPEN)		NO DATA ON PROBABILITY OF TRANSFER CLOSED	
		1.E-3	INADVERTENTLY CLOSED BY OPERATOR (OD)	ZION*
BKRNC	BUS FEED BREAKERS	-3.Ø8E-9	TRANSFER OPEN	(31)
	(NORMALLY CLOSED)	1.E-3	INADVERTENTLY OPENED BY OPERATOR (OC)	ZION*
AXPRA	AUTO TRANSFER DEVICE (MUST ACTUATE)	5.E-7	FAILURE TO TRANSFER ON DEMAND	(36)
BUS	METAL ENCLOSED BUS	-6.44E-1Ø	OPEN CIRCUIT	(37)
MINRLKA, MXFRA	MANUAL TRANSFER DEVICE	ϵ	TRANSFER OPEN FAILURE PROBABILITY NEGLIGIBLY SMALL	(38)
FUSE	125VDC POWER FUSE	-2.15E-9	OPENS PREMATURELY	(46)
SIMRLY	SAFEGUARDS ACTUATION	4.92E-7	FAILS TO ENERGIZE ON DEMAND	(47)
	MOTOR RELAY (ACTUATE TO CLOSE)	1.E-3	INADVERTENTLY OPENED BY OPERATOR (OC)	ZION
SIGRLY	SAFEGUARDS ACTUATION GENERAL RELAY (NORMALLY CLOSED)	-3.E-8	CONTACTS OPEN	(48)

* FAILURES OF THIS COMPONENT NOT LISTED IN THE STUDY. FAILURE MODES AND ASSOCIATED PROBABILTIES ASSUMED DUE TO SIMILARITY OF COMPONENT ACTUATION TO OTHERS.

GENERIC FAILURE DATA BASE (PAGE 4)

GENERIC FAILURE	COMPONENT (FUNCTION)	PROBABILITY OF FAILURE	DESCRIPTION OF FAILURE	REFERENCE
PIPE	PIPE	-3.E-12	PLUGS	(43)
STRANR	STRAINER (SHOULD BE REMOVED)	8.E-3	OUT OF SERVICE - MAINTENANCE	ZION
XFRMR	TRANSFORMER (NORMALLY ON)	-1.44E-7	FAILURE DURING OPERATION	(32)
OPW	OPERATOR (DOES WRONG ACTION)	1.E-3		ZION

5. CONCLUSIONS

The objective of this report has been to demonstrate the capabilities of Digraph Matrix Analysis to model and evaluate an accident sequence (which included its front-line and support systems as well as human actions) as a single well-integrated logic model in order to identify and evaluate functional systems interactions. We modeled the accident sequence for loss of high pressure injection during the early stages of a LOCA. This roughly corresponded to the loss of high pressure injection accident for PWR's in the WASH 1400 [15] study and to a recent BNL study [14]. We utilized this correspondence to make qualitative and quantitative comparisons.

Our conclusions include:

1. DMA is highly capable of modeling and evaluating an accident sequence (including front-line systems, support systems, and human actions) as a continuous well-integrated logic model in order to identify and evaluate systems interactions.

2. Numerous, non-intuitive systems interactions were found between front-line and support systems that were collectively significant.

3. The operators can contribute a significant improvement in safety when they correctly respond to a loss of a safety system or component.

REFERENCES

1. H. P. Alesso, I. J. Sacks, and C. F. Smith, "Initial Guidance on Digraph Matrix Analysis for Systems Interaction Studies at Selected LWR's," U.S. Nuclear Regulatory Commission, NUREG/CR-2915, March 1983

2. I. J. Sacks, B. C. Ashmore, and H. P. Alesso, "Preliminary Systems Interaction Results from the Digraph Matrix Analysis of the Watts Bar Nuclear Power Plant Safety Injection Systems," Lawrence Livermore National Laboratory, UCID-19707, June 1983

3. R. B. Worrell, "Using the Set Equation Transformation System in Fault Tree Analysis," Reliability and Fault Tree Analysis, R. E. Barlow, J. B. Fussel and N. D. Singpurwalla (editors), SIAM, 1975.

4. R. R. Willie, "Computer-Aided Fault Tree Analysis," Operations Research Center, University of California, Berkeley, ORC 78-14, August 1978.

5. Tennessee Valley Authority, "Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Units 1 and 2," U.S. Nuclear Regulatory Commission, NUREG-0847, June 1982.

6. P. Cybulskis, et al., Battelle Memorial Institute, "Review of Systems Interaction Methodologies," U.S. Nuclear Regulatory Commission, NUREG/CR-1896, January 1981.

7. A. Buslik, I. Papazoglou, and R. Bari, Brookhaven National Laboratory, "Review and Evaluation of Systems Interactions Methods," U.S. Nuclear Regulatory Commission, NUREG/CR-1901, January 1981.

8. J. J. Lim, R. K. McCord, T. R. Rice, and J. E. Kelly, Lawrence Livermore National Laboratory, "Systems Interaction: State-of-the-Art Review and Methods Evaluation," U.S. Nuclear Regulatory Commission Report NUREG/CR-1859, January 1981.

9. Power Authority of the State of New York, "Systems Interaction Study," December 1981, Vol. I and II (Draft).

10. H. P. Alesso, "Review of PASNY Systems Interaction Study," Lawrence Livermore National Laboratory, UCID-19130, April 1982.

11. D. M. Rasmuson, G. R. Burdick, and J. R. Wilson, "Common Cause Failure Analysis Techniques: A Review and Comparative Evaluation," EG&G Idaho, Inc., TREE 1349, September 1979.

12. F. D. Coffman, "Initial Guidance for the Performance of Systems Interaction Reviews of Selected LWR's," U.S. Nuclear Regulatory Commission, October 1, 1981 (Draft).

13. H. P. Alesso, "Some Fundamental Aspects of Fault Tree and Digraph-Matrix Relationships for a Systems Interaction Evaluation Procedure," Lawrence Livermore National Laboratory, UCID-19131, May 1982.

14. Y. H. Sun, A. Fresco, and I. A. Papazoglou (BNL), "Availability of High Pressure Safety Injection System in PWR's," ANS Transactions, ANS winter meeting, November 1-4, 1983.

15. U. S. Nuclear Regulatory Commission, "Reactor Safety Study," WASH-1400 (NUREG-75/014), October 1975.

16. G. J. Boyd, et al., "Final Report - Phase 1 Systems Interaction Methodology Applications Program," NUREG/CR-1321, SAND 80-0384, April 1980.

17. J. E. Wells, et al., "Seismic Safety Margins Program, Phase I Final Report- Systems Analysis (Project VII)," U. S. Nuclear Regulatory Commission, NUREG/CR-2015, Vol. 8, November 1981.

18. "Watts Bar Nuclear Plant, Final Safety Analysis Report," Tennessee Valley Authority.

19. "Reliability Data for Nuclear Power Generating Stations," IEEE Standard 500 - 1977

20. "Indian Point Probabilistic Safety Study," Power Authority of the State of New York, Consolidated Edison Company of New York, Inc., 1982.

21. U. S. Nuclear Regulatory Commission, "Data Summaries of LER's of Valves at U. S. Commerical Nuclear Power Plants," 1976 - 1978, NUREG/CR-1363, Vols. 1, 2, 3.

22. U. S. Nuclear Regulatory Commission, "Data Summaries of LER's of Pumps at U. S. Commerical Nuclear Plants," January 1, 1972 - September 30, 1980, NUREG/CR-1205.

23. U. S. Nuclear Regulatory Commission, "Data Summaries of Diesel Generators at U. S. Nuclear Power Plants," January 1976 - December 1978, NUREG/CR-1362.

24. "Nuclear Plant Reliability Data Systems," 1976, Available from: INPO, Atlanta, Georiga.

25. C. J. Patenaude, "STOP: A Fast Method of Disjointing Binary Product Sets," Lawrence Livermore National Laboratory, UCID-30192, January 14, 1983.

26. G. C. Corynen, "STOP: A Fast Procedure for the Exact Computation of the Performance of Complex Probabilistic Systems," Lawrence Livermore National Laboratory, UCRL-53230, 1982.

27. "Safety Evaluation Report Related to the Operation of the Watts Bar Nuclear Plant, Units 1 and 2," Docket Nos. 50-390 and 50-391, Tennessee Valley Authority, U.S. Nuclear Regulatory Commission, June 1982.

28. A. D. Swain, H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Sandia Laboratories, NUREG/CR-1278.

ADDENDUM

Modeling Error Found During Review of Report (11/30/83)

A flow control valve located upstream of SIP1BB was omitted from the adjacency input for the model. This valve, FCV6348, is shown in Figure 2-6 between SIP1BB and DUM27 (see Figure AD-1). The impact on the system performance can be assessed exactly since, had the node been included, it would have been condensed with DUM27 (for a discussion of condensation, see Appendix A.6.2). Therefore, its reachability would be the same as for DUM27, node number 92. Using the existing reachability output of both Case I and Case II, reachability of node 92 to the RCS was found, resulting in the following 28 doubleton additions to the failure sets of Case I (there was no change to Case II results):

FCV6348 * FE63170
FCV6348 * HDR8
FCV6348 * VC62504
FCV6348 * HDR6
FCV6348 * VC63504
FCV6348 * HDR7
FCV6348 * FCV6347
FCV6348 * SISIGA
FCV6348 * HDR4
FCV6348 * 6900VS1AA
FCV6348 * FUSE10I
FCV6348 * R5S
FCV6348 * SWSI1U
FCV6348 * SWA3U
FCV6348 * OPWF5U
FCV6348 * FUSE3U
FCV6348 * FE170159
FCV6348 * FCV1702
FCV6348 * TW17070
FCV6348 * FCV708
FCV6348 * TW170161
FCV6348 * CCHXRA
FCV6348 * VB170510
FCV6348 * TW170199
FCV6348 * FE170199
FCV6348 * FCV7025
FCV6348 * 125VVBI
FCV6348 * EINRLK1718

The addition of these failure sets to the Case I results will result in an insignificant increase in the overall failure probability.

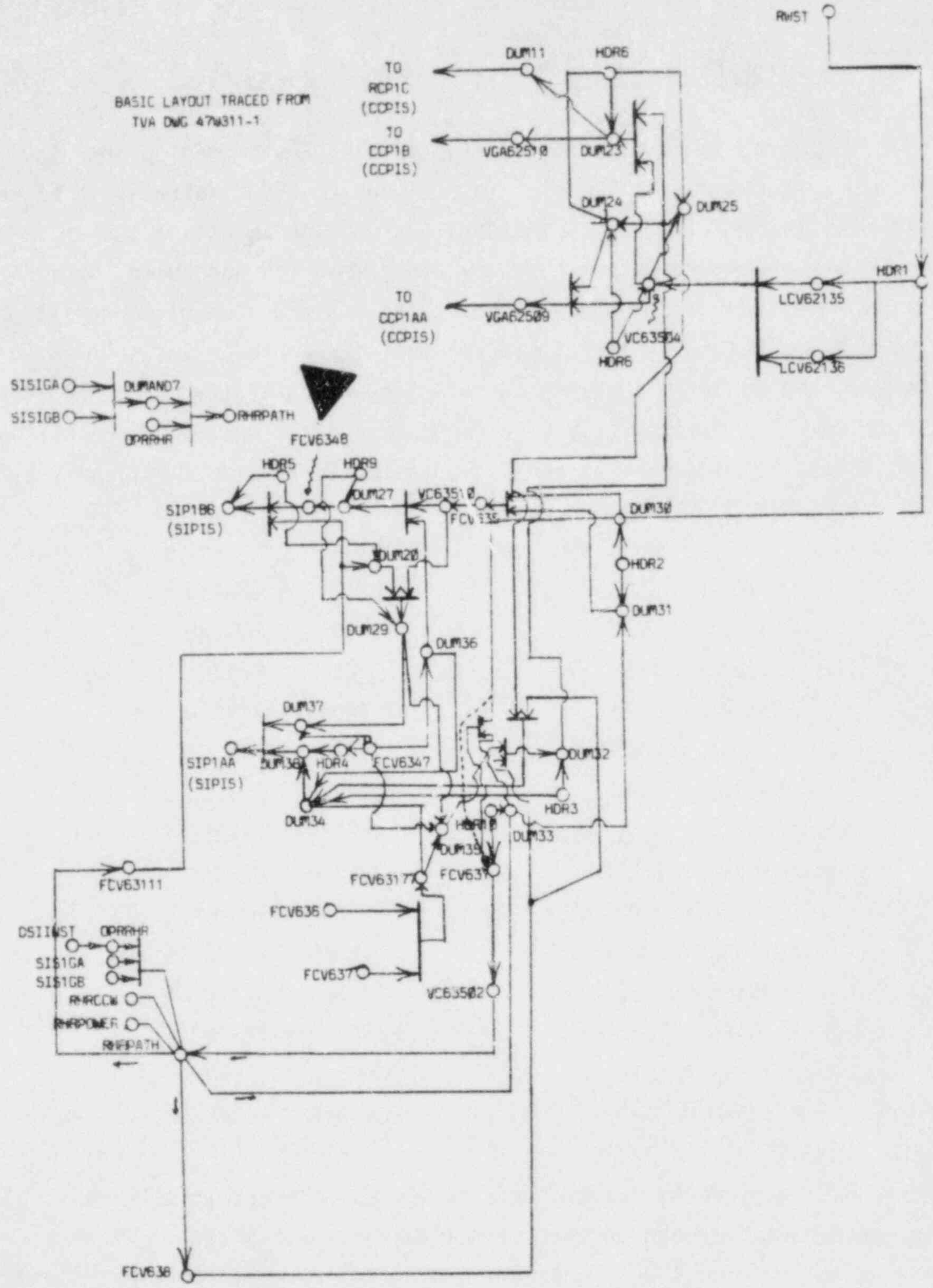


Figure AD-1. Addition of FCV6348 to RWST

APPENDIX A

DIGRAPH MATRIX ANALYSIS

A.1 Overview of DMA

Digraph Matrix Analysis (DMA) is based on the use of directed graphs to represent a physical network and a special purpose reachability code to identify any component or pair of components that could cause network failure. The DMA failure analysis of a system is composed of the iteration of three major steps, as shown in Figure A-1. These are:

1. Construct the system digraph using plant schematics, piping and instrumentation diagrams, operational procedures, etc.;

2. Process this digraph using the special reachability code; and

3. Expand the system digraph using unit models for each of the components, thus creating a new system digraph.

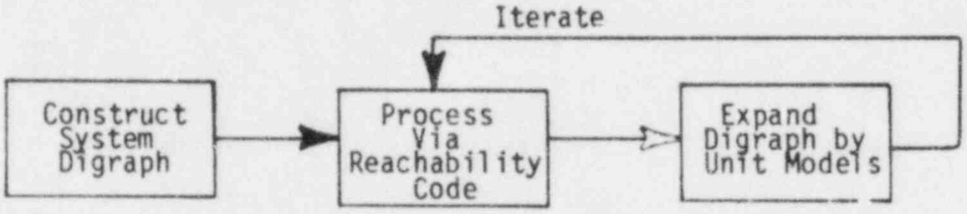


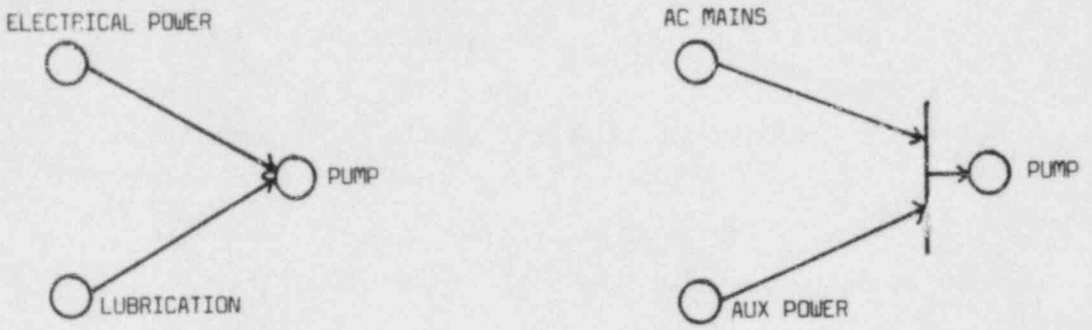
Figure A-1. Overview of Digraph Matrix Analysis

The first of these steps involves the identification of all of the components directly necessary for system operation. These components are then represented by nodes in a graph. This digraph is constructed by using AND and OR gates to explicitly model the logic relationships between components required for successful system functioning. The following rules are used for choosing the appropriate gate for the schematic-oriented graph.

> If a component requires the successful operation of two or more components that supply it, these supply components are connected to it by an OR gate. For example, a pump may require both electrical power and lubrication. The convention for the use of the OR gate is shown in Figure A-2a. (It should be noted that no special symbol is used to

represent the OR gate.)

If a component requires the successful operation of only one of a group of components that supply it, these components are connected to it by an AND gate. For example, a pump might be supplied with electrical power from the mains or from an auxiliary generator. The use of the AND gate is shown in Figure A-2b. (The notation used is that of the Petri Net [A-1].



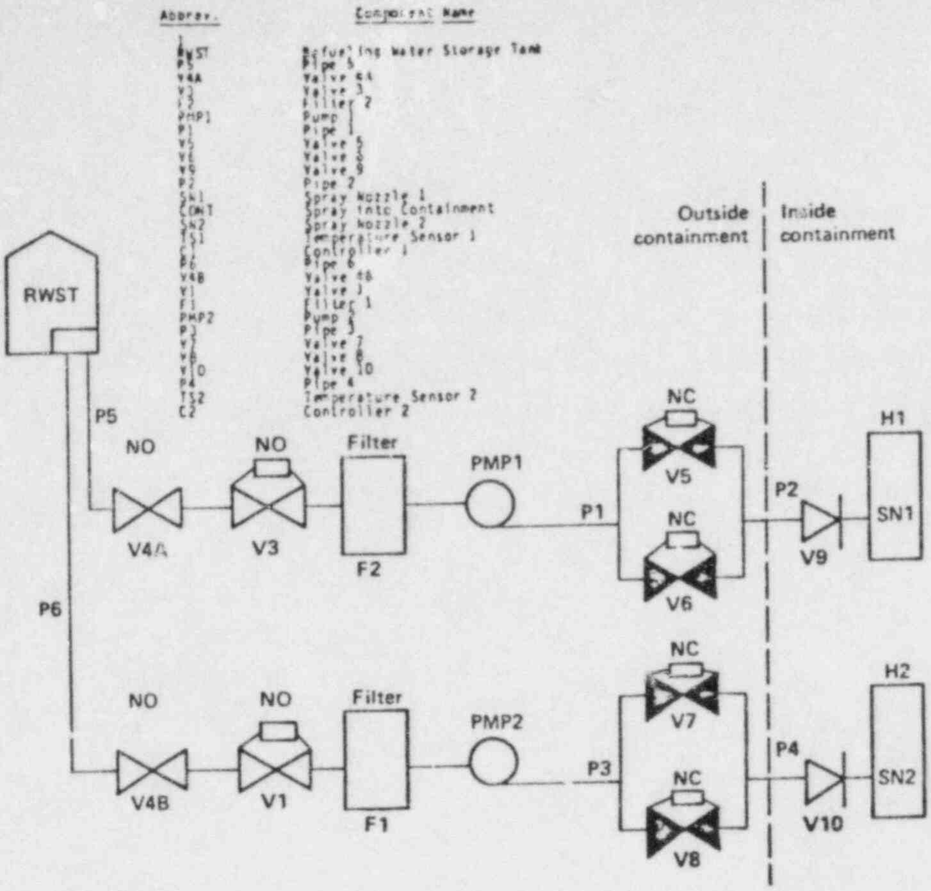
a) Use of the OR Gate

b) Use of the AND Gate

Figure A-2. Conventions for the Use of AND and OR Gates in the Digraph

The arrows on the edges between the nodes which represent the components in the system indicate the direction of flow or propagation of the effect of information, physical movement, power, etc. The digraph thus contains all the components directly responsible for the functioning of the system along with the logical relationships required for this functioning. A simplified system and its corresponding digraph is shown in Figures A-3a and A-3b. In this example, water from RWST flows through two parallel paths to the spray into CONT. The pumps (PMP1 and PMP2) will fail if either the supply of water OR a control signal fails, thus there is an OR gate that joins the filter (F*) and controller (C*) to the pump (PMP*). The spray into containment will fail only if a spray from both paths fail; thus the spray nozzles are joined to CONT by an AND gate.

The sets of single component failures (singletons) and sets of double component failures (doubletons) for the example can be determined by inspection of Figure A-3b. For example, RWST is a singleton since it supplies both parallel flow paths. Any pair of components from each of the



Abbrev.	Component Name
RWST	Refueling Water Storage Tank
P5	Pipe 5
V4A	Valve 4A
V3	Valve 3
F2	Filter 2
PMP1	Pump 1
P1	Pipe 1
V5	Valve 5
V6	Valve 6
V9	Valve 9
P2	Pipe 2
SN1	Spray Nozzle 1
CONT	Spray into Containment
SN2	Spray Nozzle 2
TS1	Temperature Sensor 1
C1	Controller 1
P6	Pipe 6
V4B	Valve 4B
V1	Valve 1
F1	Filter 1
PMP2	Pump 2
P3	Pipe 3
V7	Valve 7
V8	Valve 8
V10	Valve 10
P4	Pipe 4
TS2	Temperature Sensor 2
C2	Controller 2

Figure A-3a. Simplified Corewater Injection System

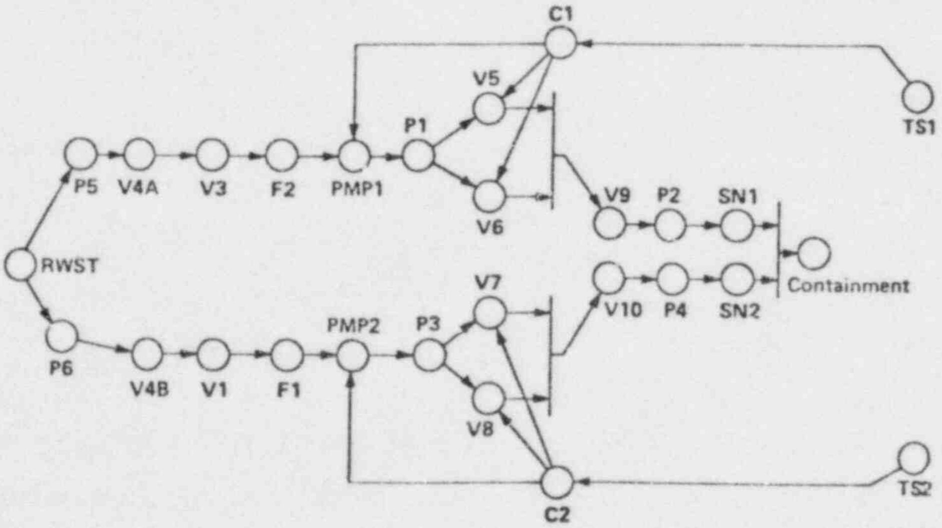


Figure A-3b. Digraph of Corewater Injection System flow paths forms a doubleton pair except for the set of V5, V6, V7, and V8.

Each of the components of the system digraph is now expanded by the use of a unit model. This expansion procedure identifies auxiliary components whose operation may affect system operation.

A.2 Expansion Via Unit Models

The basic digraph is expanded by replacing each component with a unit model for that component. These unit models describe the direct dependence of a component on other components and thus their inclusion in the system digraph will allow the analyst to uncover additional failures which are introduced by support components. The expansion of the components in the digraph into their unit models will lead to the discovery of common mode failures between components due to shared support components. A typical unit model for an active component includes the power, control, lubrication and maintenance inputs. In addition, location of the component is represented as an input to the component. The philosophy behind the construction of the unit model is the identification of all nodes on which the component depends for operation, that is, the identification of direct failures which would result in component failure. A simplified unit model for a pump is shown in Figure A-4.

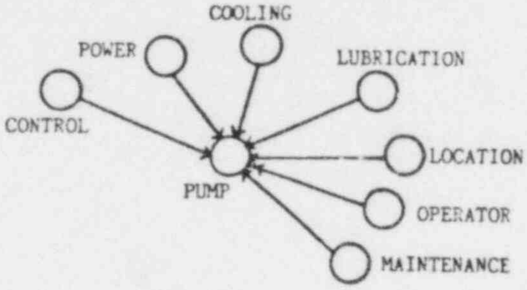


Figure A-4. Pump Unit Model

In this model, failure of control, power, cooling or lubrication will cause the pump to fail. Failure of the pump could also be caused by the propagation of an effect from its location, by an operator turning it off, or by incorrect maintenance practices. The failure due to location could be an external event such as a fire or an internal event such as the explosive failure of a component which shares the location. The discovery of singletons and doubletons involving location is as significant as the discovery of any other component failure sets. There are other possible inputs to the unit model. For example, component manufacturer could be included with a resulting expansion of the failure sets to include common manufacturer.

Most vital components such as pumps, valves, etc. are supplied from redundant power systems. Redundancy in the unit model is represented by connecting the redundant supplies to the component via an AND gate, as shown in Figure A-5, where two power supplies and a manual control backup have been provided. Note that there are two operator inputs (nodes) in this model, the operator who could mistakenly turn off the pump (OPW) and the operator who could override a control failure (OPR).

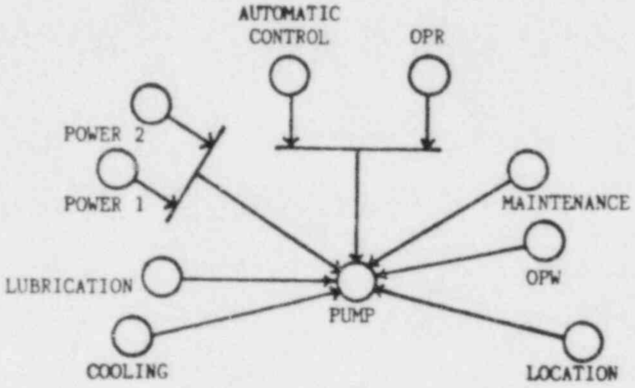


Figure A-5. Pump with Redundant Power and Control

Each of the components identified in the system digraph is expanded by the use of additional unit models. As this expansion proceeds, the generic unit model which describes each component type can be reused (with appropriate labeling changes). A partial first level unit model expansion of the digraph of Figure A-3b is shown in Figure A-6. In general, complete system digraphs, such as Figure A-6, will not be drawn by the analyst. The complete system digraph is created by adding the data for each unit model to the adjacency element list which describes the system digraph of the previous expansion.

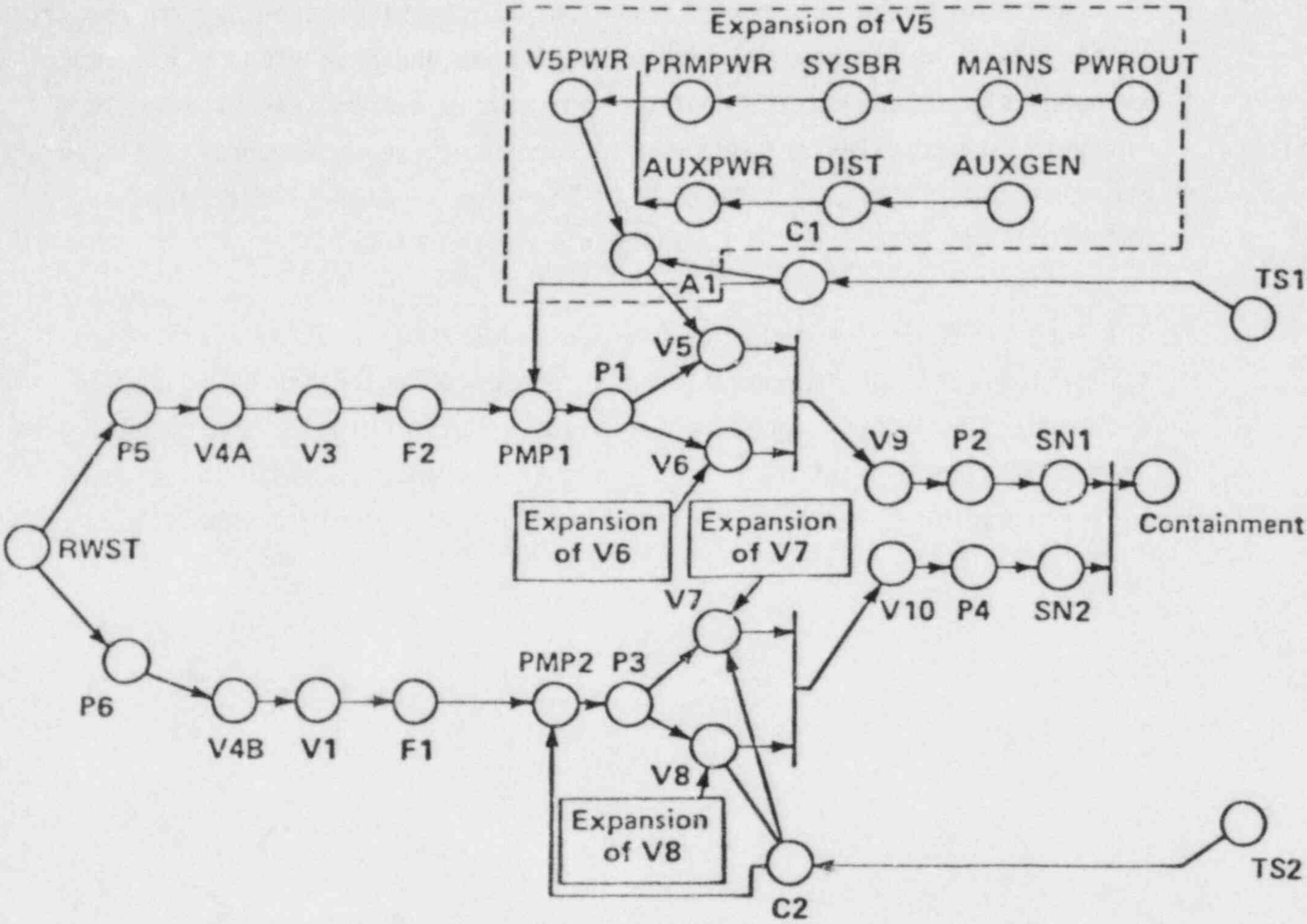


Figure A-6. Partial First Stage Unit Model Expansion of the Digraph of the Core Water Injection System

New components which are identified by the unit model expansion procedure now become the center for continued unit model expansion. For example, power should be expanded to include each transmission line, switch, relay, transformer, etc. As this expansion proceeds, components, locations, operators and maintenance shared by systems will be discovered. As the expansion steps proceed, the digraph grows to a very large size (on the order of 3700 nodes for the high pressure safety injection system analyzed in the main body of this report). Singletons and doubletons which arise through this expansion will not be apparent to the analyst or team of analysts constructing the model. To uncover these dependencies, a special computer code is used. This code is based on a reachability calculation which will be explained in a following section (A.5).

The large size of the complete digraph model also requires a procedure to divide this digraph into smaller units, each of which can be processed independently. This procedure is called "partitioning"; the results from the processing of each partition are then combined to yield the global digraph results. The partitioning procedure is described in Section A.7.

A.3 Modeling the Effects of Breaks in the System

The digraph modeling procedure described to this point is valid only for the propagation of the effects of component blockage or break downstream. That is, in the model as described, a pipe break will affect the flow through components which are downstream, but not upstream of the break. Since a pipe break acts as a sink for fluid flow, it should also affect the operation of upstream components. For example, the pipe break shown in Figure A-7 between valve 1 and pump 1 would provide a drain for the water in the RWST and would ultimately affect the flow through the alternate path composed of pump 2 and valve 2.

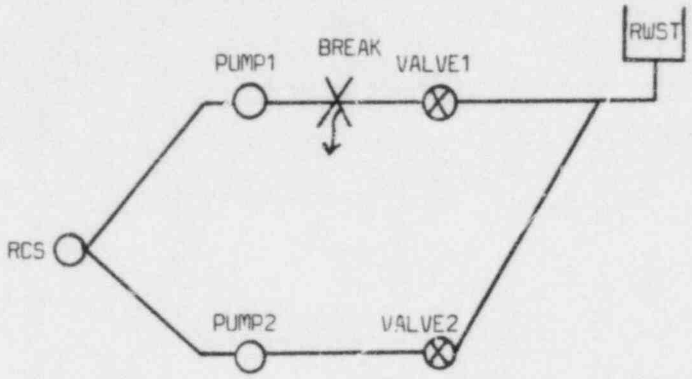
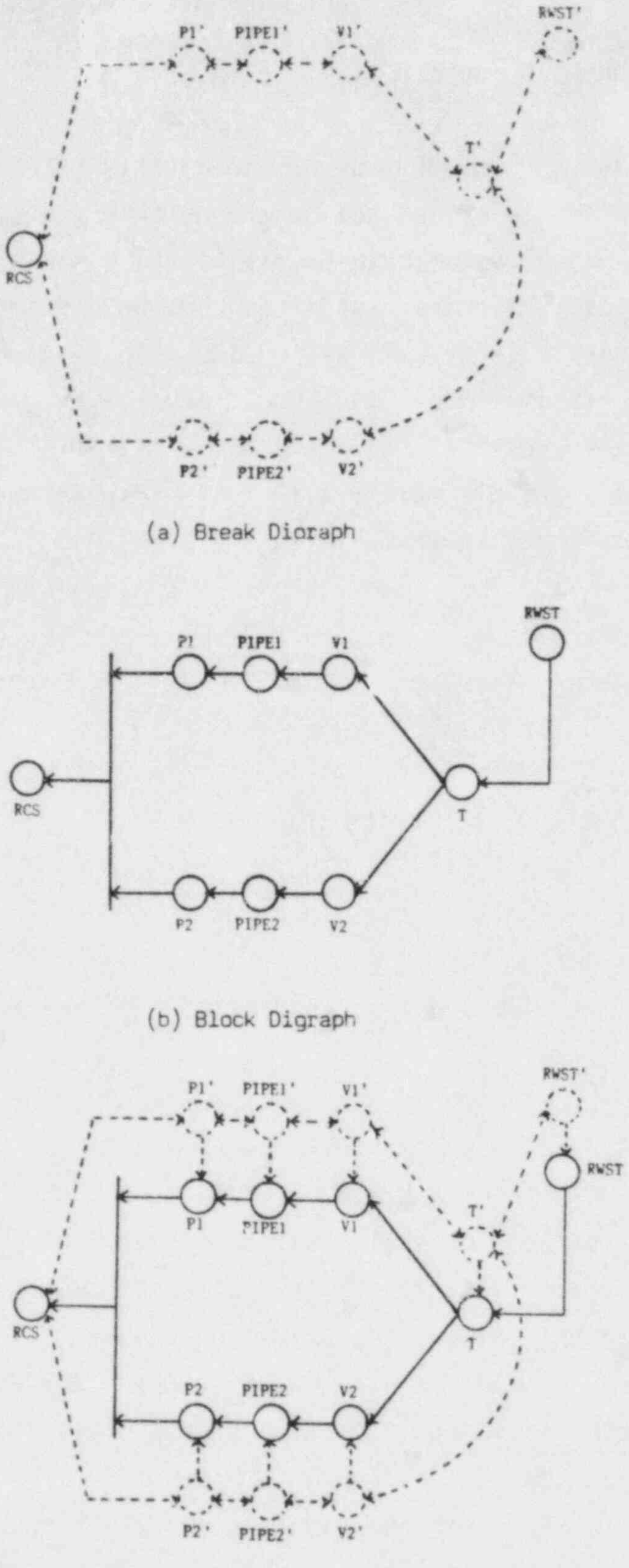


Figure A-7. Effect of Pipe Break

A procedure which extends the digraph model to include the effects of the propagation of breaks upstream will now be described. This extension propagates the effects of a break both downstream and upstream while propagating the effects of a blockage downstream only. The digraph which propagates the effect of breaks both upsteam and downstream is shown in Figure A-8a. In this figure the primed components (e.g., PIPE1') represent the failure of a component in the break mode and the arrows on both ends of the edges between the nodes indicate bidirectional flow. It can be seen from this digraph that the effect of a break failure anywhere in the system will propagate to all other components. The block model digraph is shown in Figure A-8b with the combined block/break digraph given in Figure A-8c. It should be noted that the nodes which represent component failure as a break are connected to the nodes which represent component block failure,



(a) Break Digraph

(b) Block Digraph

(c) Combination Block and Break Digraph

Figure A-8. Break and Block Digraphs

but the reverse is not true.

The addition of a break node for each component will approximately double the size of the system digraph. Fortunately, a group of bidirectionally connected nodes can be combined into a single equivalent node reducing the network size.* The effect of this reduction is shown in Figure A-9.

Any good system design will have components which are used as break mitigators. In fluid flow networks, automatically or manually operated valves and check valves are used for this purpose. In electrical networks, the break (short-circuit) mitigation function is performed by circuit breakers or fuses. In DMA, these break mitigators are modeled by an AND gate on the bidirectional edge between adjacent nodes which represent the component break modes. The modeling of a typical break mitigating component is shown in Figure A-10. In this figure, the valve, V1, can be used to limit the effect of a pipe break, PIPE1', from affecting upstream components. The use of the valve as a break mitigator is indicated by the double prime in the symbol for the valve, V1". It should be noted that a break in both PUMP1' and V1' will still propagate downstream. The nodes which represent components used for break mitigation are now candidates for unit model expansion following the procedure described in the preceeding section.

* In graph theory terminology, a grouping of bidirectionally coupled nodes is called a "strong component".

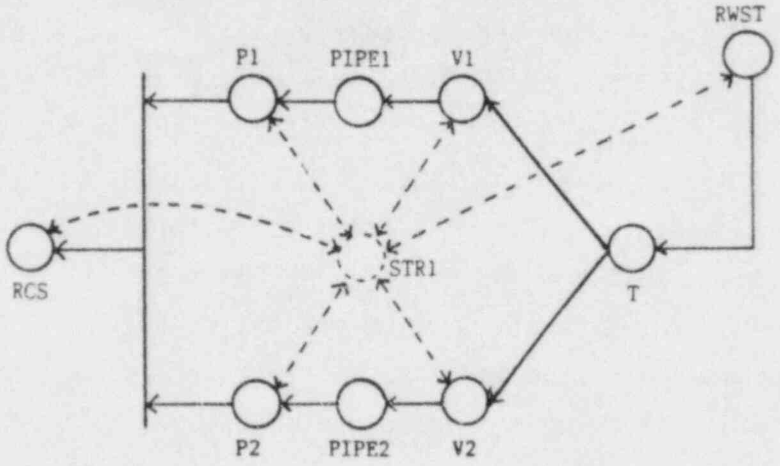


Figure A-9. Use of a Strong Component

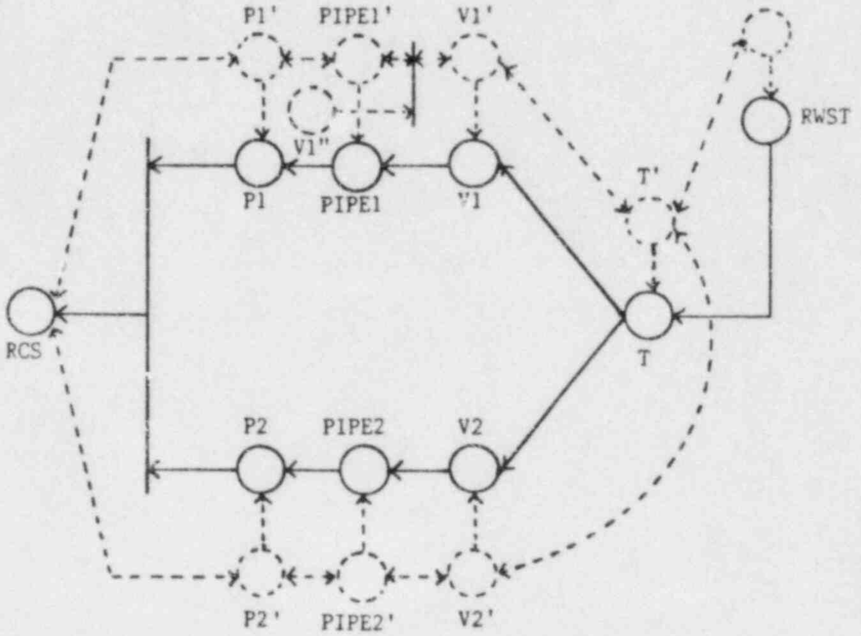


Figure A-10. Modeling of Break Mitigation

A.4 Modeling Complex Networks with Bidirectional Flows

Front-line safety injection systems and component cooling system contain piping networks which enable operators to configure alternate flow paths should normal paths fail. This design feature incorporates positive human intervention to increase, somewhat dramatically, the robustness of these systems.

The number of possible flow paths is strongly dependent upon the number of switching junctions in the network and can quickly become astronomical. In the case of piping networks, these switches are the pipe headers (pipe junctions) where the flow direction is controlled by external pressure conditions. Two approaches can be used to model the potential use of all of the possible paths. The first is a global method whereby an exhaustive list of all possible paths through the network from source(s) to sink(s) would be generated. Such a global approach would require substantial effort due to the large number of paths. The second approach is a local method whereby the network is modeled length by length and header by header using a simple digraph algorithm to capture the switching behavior of the headers. This was the procedure used in the analysis of the high pressure safety injection system and which will now be explained.

Consider the network shown in Figure A-11. Flow must pass from the RWST to pumps P1, P2, and P3. Crosstie valve V3 is normally closed so, under normal conditions, should valve V1 fail closed, P1 and P2 would not have an open path from RWST and so those injection paths would fail. However, allowing the operator to open V3 changes the outcome since flow through V2 could supply all three pumps (provided that the piping has been sized to allow for this contingency). The digraph for this network is shown in Figure A-12. The network was considered as consisting of headers and connections between them. The digraph was constructed a header at a time without the need to consider global path searches. The algorithm which was used is as follows:

At each header, flow can exit through each of the pipes which form the junction (unless a check valve or pump constrains fluid from flowing

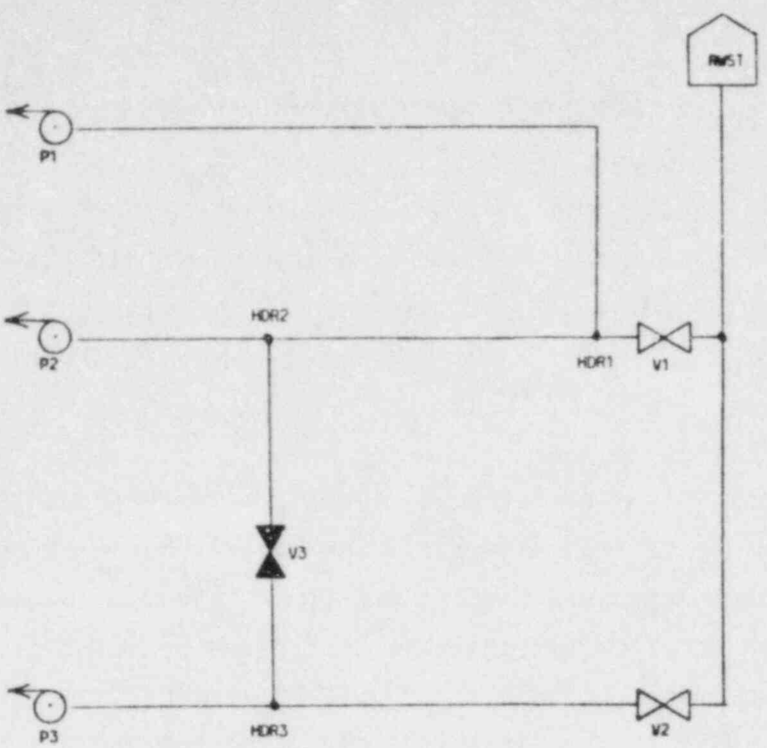


Figure A-11. Crosstie Network

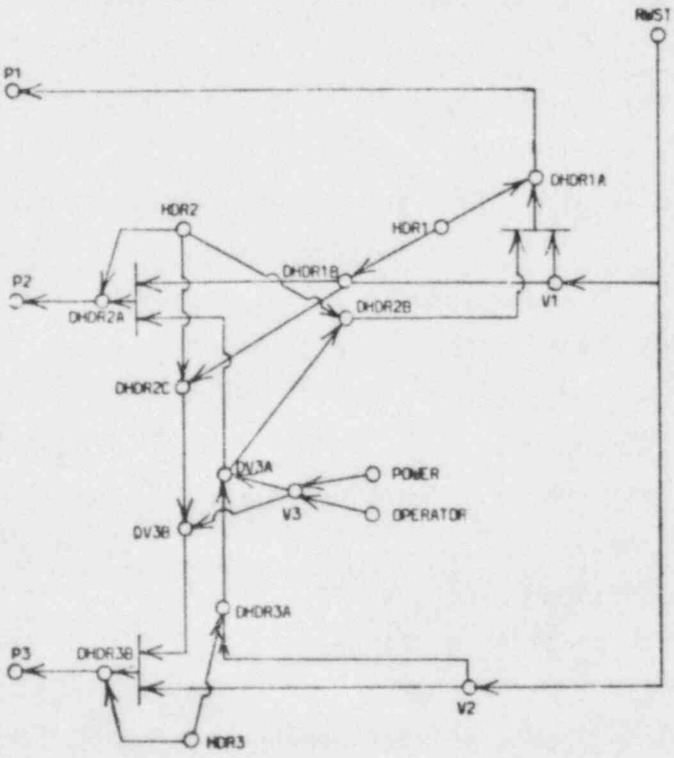


Figure A-12. Digraph of Crosstie Network away from the header in a given pipe). Considering each exit independently, the possible sources of flow to it are AND-ed together and input to a dummy node. The sources are nodes adjacent to the header. The node representing the header OR's into this dummy node and represents the necessity of an open path through the header to enable flow through the exit path being considered. This process is repeated for each output from the header and the entire scheme is repeated at each header throughout the network.

An example of this modeling is shown by the model for flow through header HDR2. This header is the junction of three pipes and fluid can flow away from the header through any of the three paths. These paths are considered one at a time, in any order, and the status (success or failure) of each path is embodied by a dummy node. Dummy nodes in this example all begin with D. Node DHDR2A is the status node for flow away from HDR2 and toward P2. Flow to it can come from either of the two other entrances to the header, so these two flow paths are AND-ed together and input to the status node. One of these flow paths originates at DHDR1B and the other at DV3A. The first is the flow away from HDR1 in the pipe connecting it to HDR2. Inputs to DHDR1B will not be developed until modeling has progressed to HDR1. Node DV3A is flow away from valve V3 in the direction toward HDR2. As before, inputs to that node will be developed when modeling has progressed to V3. Node HDR2 inputs to DHDR2A since integrity of a path through the header is needed with either of the two flow paths for the flow to reach out of the header toward P2. Once this simple analysis has been applied to the other branches out of HDR2 and to the other components through which flow can pass in more than one direction, the digraph is complete.

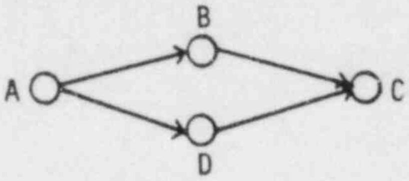
The support needed by V3 is OR'ed in and the effect of the failure of that valve can be ascertained visually by propagating it's "true-ness" through the digraph or analytically by processing through the tripleton reachability code. Reachability is an analytic operation on the adjacency input which computes single and double dependency from anywhere to anywhere in the network. The avoidance of path searching to determine dependence allows the modeling and analysis of very large and complex networks.

Examples of this modeling in HPSIS can be found in the CCS networks and in the network RWST.DAT which connects the refueling water storage tank RWST to the two front-line injection systems. RWST.DAT was initially traced from TVA P&ID 47W811-1 and then modeled. Adherence of the digraph to the original P&ID greatly facilitates generation, debugging, and auditing of these network models.

A.5 Adjacency & Reachability [A-2]

The connectivity of a network can be represented as a graph (partially or completely directed), G, or equivalently as an adjacency matrix, A. Figure A-13 shows a typical graph and its adjacency matrix. The rules that define an adjacency matrix are as follows:

a_{ij} = 1 if node i and node j are directly connected
0 otherwise.



$$\begin{array}{c|c|cccc} & & \multicolumn{4}{c}{\text{To}} \\ & & A & B & C & D \\ \hline \text{From} & A & 0 & 1 & 0 & 1 \\ & B & 0 & 0 & 1 & 0 \\ & C & 0 & 0 & 0 & 0 \\ & D & 0 & 0 & 1 & 0 \end{array}$$

Figure A-13. Graph and Corresponding Adjacency Matrix

The adjacency matrix can be viewed as describing the possibility of flow from node i to node j. One-way flow in a network from node to node is representeu by following the above definition, that is, for a pair of nodes (i,j) for which flow is allowed from i to j but not from j to i:

$$a_{ij} = 1$$
$$a_{ji} = 0.$$

The connectivity between all pairs of nodes in a network is contained in the reachability matrix. The determination of whether any arbitrary node is reachable from any other node can be made by Boolean manipulation of the adjacency matrix. This reachability matrix can be derived from the following property (transitive property):

Connection from element k to element n = a_{kn}
Connection from element n to element l = a_{nl}.

Hence, element a_{kl} is composed of two terms, a_{kn} and a_{nl}, both of which must be nonzero, that is; $a_{kl} = a_{kn}{*}a_{nl}$. Using the Boolean product operation (Boolean AND function),

$$a_{kl} = a_{kn} * a_{nl} \text{ where } \begin{array}{l} 1*1 = 1 \\ 1*0 = 0 \\ 0*1 = 0 \\ 0*0 = 0 \end{array}$$

In matrix notation, for a network containing n nodes

$$R_2 = [A] * [A] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

where R_2 represents the reachability matrix for all paths that require exactly two steps between all pairs of nodes.

For connectivity in exactly m steps, the reachability matrix becomes

$$R_m = [A]^m.$$

Thus, the reachability matrix for connections of all lengths between node pairs of any number of steps is given by

$$R = \sum_{m=1}^{\infty} A^m$$

where the summation represents the Boolean sum (logical OR) operation, i.e.,

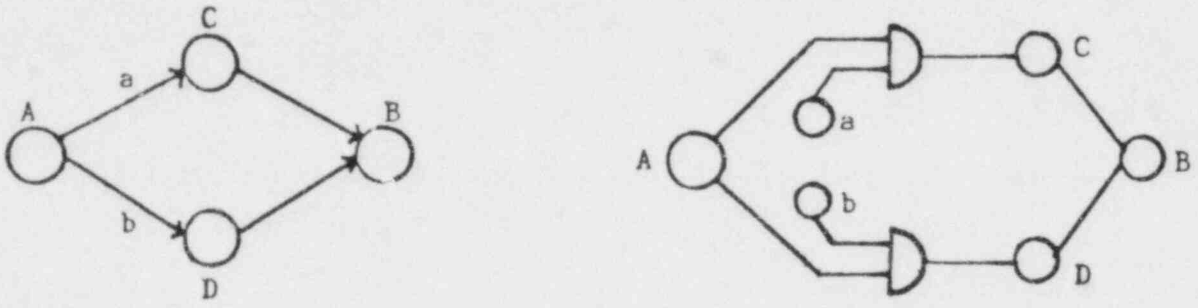
$$\begin{array}{l} 1 + 0 = 1 \\ 0 + 1 = 1 \\ 1 + 1 = 1 \\ 0 + 0 = 0 \end{array}$$

It can be shown that the R matrix converges to a steady-state value, that is,

$$R_{ss} = \lim_{m \to \infty} \sum_{n=1}^{m} A^n$$

This procedure is computationally inefficient and many algorithms have been developed to efficiently perform the reachability calculation, two of the more efficient being algorithms developed by Warren [A-3] and Warshall [A-4]. The present version of the DMA reachability code is based on the Warren Algorithm.

One of the authors, I.J. Sacks [A-2] has extended the concept of reachability to conditioned graphs* where a conditioned graph is to be used as a representation of logical network. This extension forms the basis of DMA. The weighted graph of Figure A-14a is equivalent to the logic network of Figure A-14b where the weights a and b are taken as binary variables.



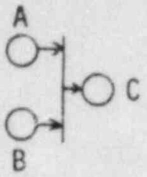
(a) Weighted Graph

(b) Logic Network

Figure A-14. Weighted Graph and Equivalent Logic

The weighting in the graph represents a control on the connectivity of the graphs. The conditioned graph can be represented by an equivalent matrix representation. Figure A-15 shows the logical AND symbol, along with the Boolean equation that it represents and an equivalent conditioned adjacency matrix. (The notation used is that of the Petri Net [A-1] where the bar represents a controlled transition.)

* This technique is somewhat similar to that proposed by Chamow [A-5].



$C = A*B$

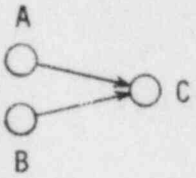
$$\begin{array}{c|ccc} & A & B & C \\ \hline A & 0 & 0 & B \\ B & 0 & 0 & A \\ C & 0 & 0 & 0 \end{array}$$

(a) AND Gate (b) Boolean Equation (c) Matrix Representation

Figure A-15. Representation of an AND Operation

The matrix of Figure A-15 is read in the same from-to manner as before, that is, to get to C from A requires B. Node C can be reached from either node A with B or from node B with A. These two adjacencies are equivalent.

Figure A-16 shows the logical OR symbol, along with the Boolean equation that it represents, and an equivalent adjacency matrix.



$C = A + B$

$$\begin{array}{c|ccc} & A & B & C \\ \hline A & 0 & 0 & 1 \\ B & 0 & 0 & 1 \\ C & 0 & 0 & 0 \end{array}$$

(a) OR Gate (b) Boolean Equation (c) Matrix Representation

Figure A-16. Representation of an OR Operation

The matrix is read in the same from-to manner as above, that is node C can be reached from either node A or node B.

Combinations of AND and OR gates are easily represented in the conditional adjacency matrix format. Figure A-17 is a logic network composed of two CR gates and one AND gate.

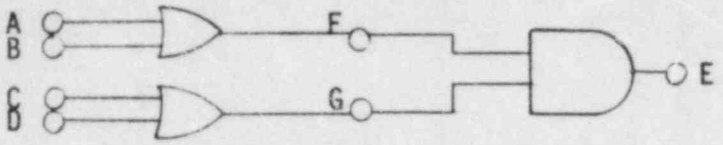


Figure A-17. Example of Multiple Gate Logic Network

The individual component logic adjacency matrices for this network are given in Figure A-18.

$$
\begin{array}{c|ccc}
 & A & B & F \\
\hline
A & 0 & 0 & 1 \\
B & 0 & 0 & 1 \\
F & 0 & 0 & 0
\end{array}
\qquad
\begin{array}{c|ccc}
 & F & G & E \\
\hline
F & 0 & 0 & G \\
G & 0 & 0 & F \\
E & 0 & 0 & 0
\end{array}
\qquad
\begin{array}{c|ccc}
 & C & D & G \\
\hline
C & 0 & 0 & 1 \\
D & 0 & 0 & 1 \\
G & 0 & 0 & 0
\end{array}
$$

Figure A-18. Component Matrices

These matrices can be combined into the single adjacency matrix shown in Figure A-19, which represents the entire network of Figure A-17.

$$
\begin{array}{c|ccccccc}
 & A & B & C & D & E & F & G \\
\hline
A & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
B & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
C & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
D & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
E & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
F & 0 & 0 & 0 & 0 & G & 0 & 0 \\
G & 0 & 0 & 0 & 0 & F & 0 & 0
\end{array}
$$

Figure A-19. Adjacency Matrix for Logic Network of Figure A-17

The reachability calculation procedure described above can be applied to this adjacency matrix to yield all singletons and doubletons for the network of Figure A-17. The question we are attempting to answer is: Can we reach node E from any single node alone or any combination of two nodes alone?

If the adjacency matrix of Figure A-19 is Boolean AND'ed with itself and the result then OR'ed with the original adjacency matrix, the conditioned reachability matrix of Figure A-20 results. This matrix is read in the same manner as the adjacency matrix, for example node E can be reached from node A with node G. Substitution for G by all nodes which reach node G then yields network connectivity to E.

$$\begin{array}{c|ccccccc}
 & A & B & C & D & E & F & G \\
\hline
A & 1 & 0 & 0 & 0 & G & 1 & 0 \\
B & 0 & 1 & 0 & 0 & G & 1 & 0 \\
C & 0 & 0 & 1 & 0 & F & 0 & 1 \\
D & 0 & 0 & 0 & 1 & F & 0 & 1 \\
E & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
F & 0 & 0 & 0 & 0 & F & 1 & 0 \\
G & 0 & 0 & 0 & 0 & G & 0 & 1
\end{array}$$

Figure A-20. Reachability Matrix for the Example Logic Network

When this substitution process is done, it is seen that the pairs

A, G
A, C
A, D
F, G
F, C
D, B, etc.

are doubletons to node E.

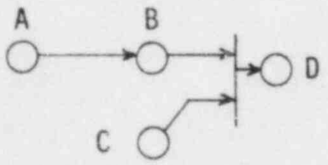
The process described above was implemented in two computer codes, CLAMOR and SQUEAK, at Lawrence Livermore National Laboratory [A-6,A-7]. Both codes are capable of finding reachability sets of any order which reach any node. These codes require a large computer (CDC7600 or equivalent) to process problems of about 200 nodes. Processing times are on the order of 30 minutes. By restricting the analysis to singletons, doubletons, and special case tripletons, a faster set of codes which run on a minicomputer and are capable of processing problems containing thousands of nodes was developed. These codes are described in the next section.

A.6 Efficient DMA Codes

The present version of DMA utilitizes a family of computer programs which work together to find singleton, doubleton, and specified tripleton cut-sets of a digraph. Figure A-21 shows the data processing flow used for the present implementation of DMA. A brief description of the operation of each program will now be given:

A.6.1 ADJ

Program ADJ converts alphanumeric adjacency element data into a numeric input and provides a list of the number of variables used in the alphanumeric input data. Example input to and output from ADJ is shown in Figure A-22.



a) Digraph

b) Adjacency List (input)	c) Variable List	d) Adjacency List (output)
A,B,1	1-1	2,3,1
B,D,C	2-A	3,4,5
C,D,B	3-B	5,4,3
0,0,0	4-D	0,0,0
	5-C	

Figure A-22. Input/Output for Code ADJ

The 0,0,0 at the end of the alphanumeric data is used to indicate the end of data.

A.6.2 CONDENSE

Program CONDENSE removes redundant node numbers from the numeric adjacency element list by a process of forward condensation. The rule for forward condensation is:

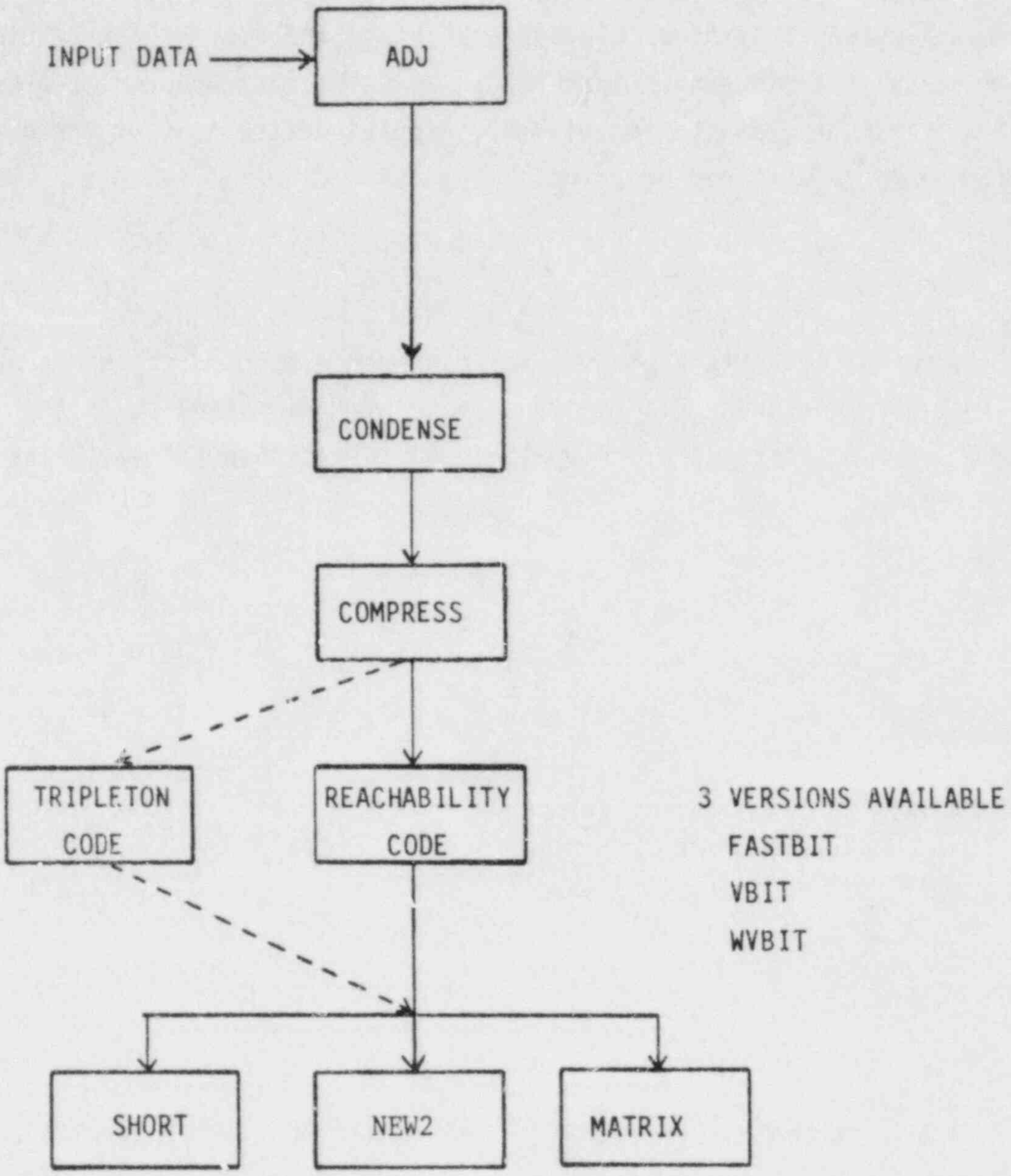
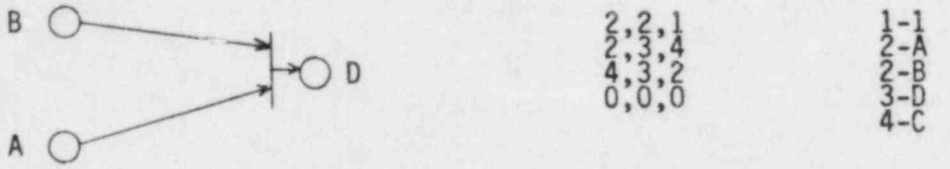


Figure A-21. DMA Data Processing Flow

If a node is adjacent tc only one other node, its number can be replaced by the adjacent node.

This step is equivalent to Boolean absorption. The digraph of Figure A-22a condenses into the digraph of Figure A-23a. The condenser program also renumbers the nodes, eliminating any repeated numbers in the numeric adjacency input. Typical output is shown in Figures A-23b and A-23c.



```
2,2,1
2,3,4
4,3,2
0,0,0
```

```
1-1
2-A
2-B
3-D
4-C
```

a) Condensed Digraph   b) Adjacency List Output   c) Variable List

Figure A-23. Condensation Progra⁻ Operation

Condensation has a high payoff in the use of a matrix reachability code since processing time is approximately proportional to the third power of the order of the adjacency matrix and the computer memory requirement is proportional to the square of the order. Condensation typically reduces problem size by about 1/3. For example, an early version of the safety injection pump injection system (SIPIS) condensed from 1004 nodes to 625 nodes.

A.6.3 REACHABILITY

The reachability code finds all of the singletons and doubletons of the system digraph. This operation is performed using the logic shown in Figure A-24.

All unconditional adjacency data (e.g., A,B,1) is processed by a f t binary reachability algorithm. To conserve storage and enhance speed, each element in the reachability (or adjacency) matrix is represented by one

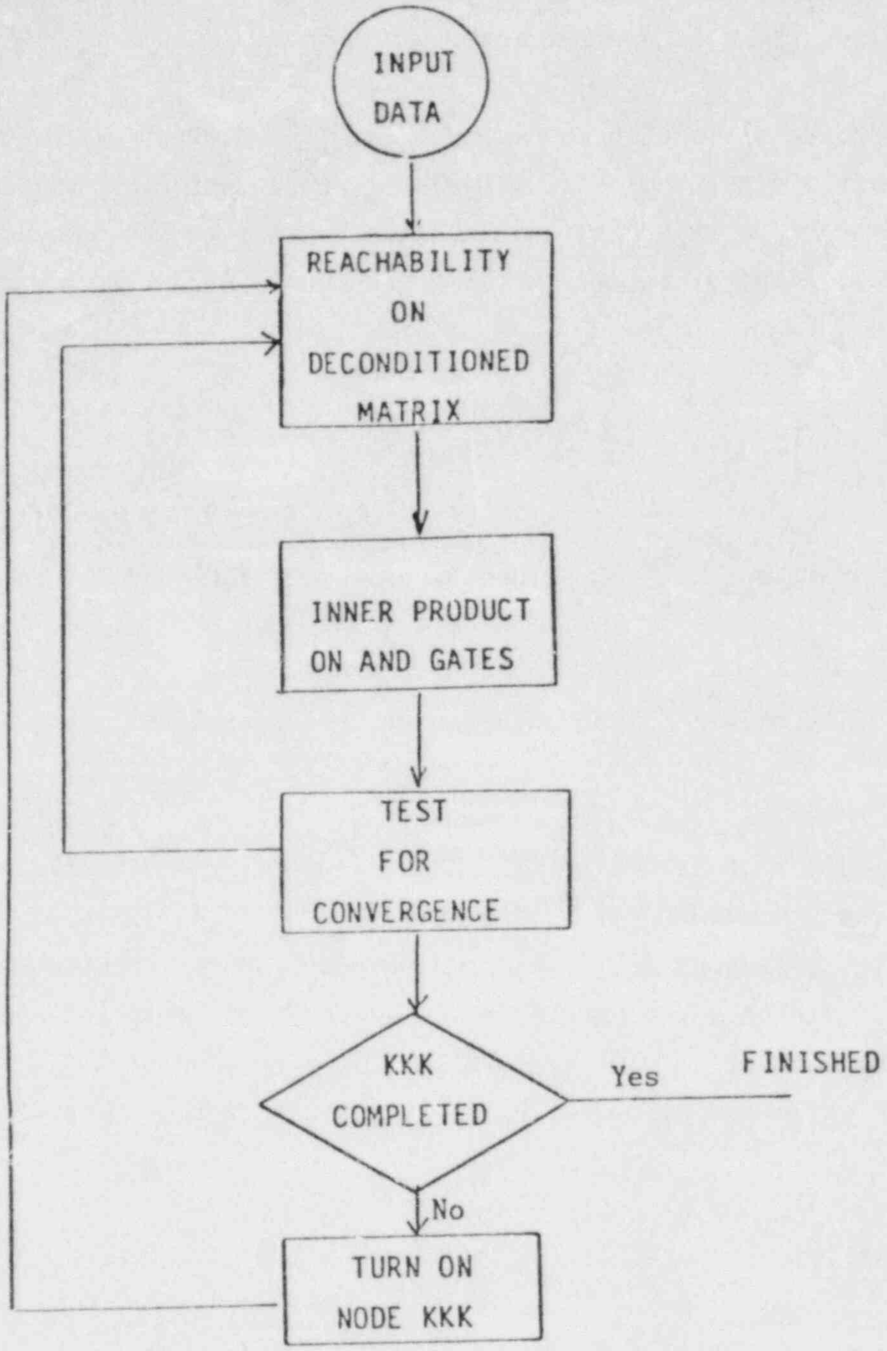
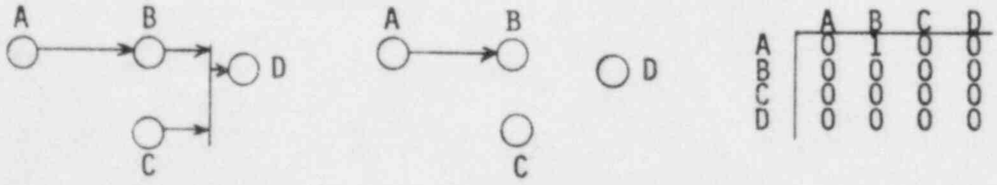


Figure A-24. Reachability Code Flow

bit, and computer hardware Boolean logic operations are used on words containing N bits. Thus, a reachability matrix of 16 elements would take 1 x 16 words of storage in a computer with a 16 bit word size. The Warren Algorithm [A-3] is now being used for the reachability calculation. This algorithm appears to be more efficient for sparse matrices than the Warshall Algorithm and is given below.

```
Warren Algorithm (Taken from [A-8])
S1  (initialization) A is the adjacency matrix of G.
S2  Do S3 for i =  2,..., n.
S3  Do S4 for j = 1, 2,..., n.
S4  If A(i,j) = 1, then Do S5 for k = 1, 2,..., n.
S5  A(i,k) = A(i,k) + A(j,k).
S6  Do S7 for i = 1, 2,..., n-1.
S7  Do S8 for j = i+1, i+2,..., n.
S8  If A(i,j) = 1, then Do S9 for k = 1, 2,..., n.
S9  A(i,k) = A(i,k) + A(j,k).
S10 HALT.
    Note:  + represents the Boolean OR operation.
```

The result of this binary reachability calculation is the set of singletons for the digraph with all AND gates removed. Figure A-25 shows this case.



$$\begin{array}{c|cccc} & A & B & C & D \\ \hline A & 0 & 1 & 0 & 0 \\ B & 0 & 0 & 0 & 0 \\ C & 0 & 0 & 0 & 0 \\ D & 0 & 0 & 0 & 0 \end{array}$$

a) Digraph   b) Deconditioned Digraph   c) Reachability Matrix

Figure A-25. The Deconditioned Graph

The reachability code then performs an inner product operation on each conditional adjacency entry. This inner product AND's the columns given by the two input entries (B and C in the example) and places the result in the column indicated by the output entry (D). Each conditioned entry is processed through this inner product.

The reachability matrix which results from this inner product process is then processed through the Warren algorithm to "connect up" all of the new partial paths found by the inner product operation. This inner product/reachability loop is repeated until the reachability matrix converges. The resulting matrix is the Single Dependency Reachability Matrix which contains all singletons of the system digraph.

Double dependency is found in a similar manner with one difference. One of the nodes in the problem is "turned on" and the single dependency calculation is repeated. The resulting "single dependency matrix" is conditional on the "turned on" node. Thus, the process identifies double dependencies (doubletons). Each of the nodes is "turned on" and the corresponding single dependency matrix generated. Thus, the output will ultimately contain all singletons and all doubletons.

A.6.4 OUTPUT CODES

There are three types of output codes presently used. These codes generate:

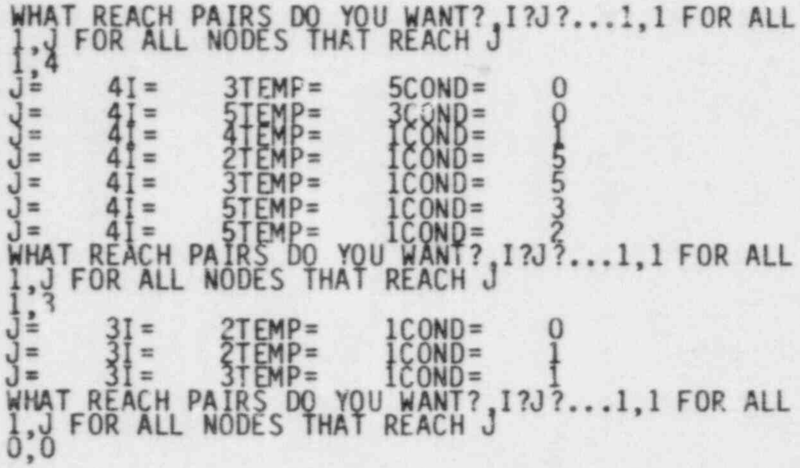
1. A list of the singletons and doubletons (SHORT);

2. A set of conditional Reachability Matrices (MATRIX); and

3. A Single/Doubleton Matrix (NEW2)

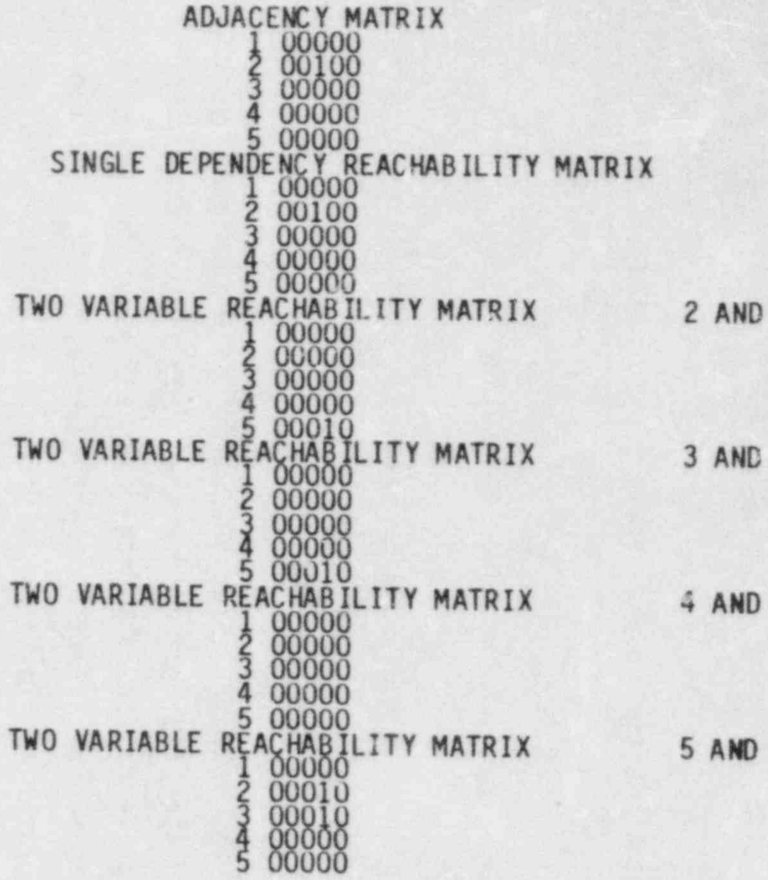
Program SHORT allows the user to search the output file generated by the reachability code for specific "reaches" either from or to a node. Using this code, it is possible to find all singletons and doubletons to a specific terminal node and to determine why they have occurred. A typical output from SHORT is shown in Figure A-26. Program MATRIX presents the reachability output file in conventional adjacency matrix format. The output from this program is composed of N+2 matrices. The first two of these are the deconditioned adjacency and single dependency reachability matrices, respectively. The other N matrices are the conditional "single dependency" reachability matrices for each of the N components taken one at a time. Typical output from MATRIX is shown in Figure 27. Program NEW2 generates the singletons and doubletons in the most useful and compact format (Figure A-28). The singletons are listed below the doubleton matrix. The doubleton matrix is read as follows:

> Each i,j element with an asterisk presents a doubleton composed of component i and component j.



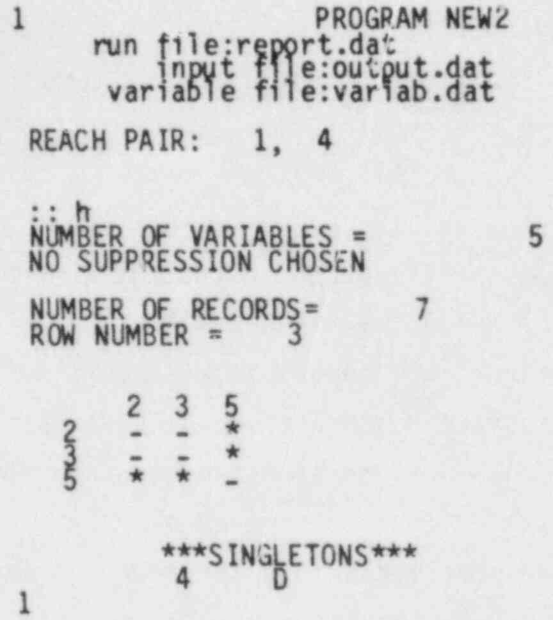
```
WHAT REACH PAIRS DO YOU WANT?,I?J?...1,1 FOR ALL
1,J FOR ALL NODES THAT REACH J
1,4
J=     4I=     3TEMP=     5COND=     0
J=     4I=     5TEMP=     3COND=     0
J=     4I=     4TEMP=     1COND=     1
J=     4I=     2TEMP=     1COND=     5
J=     4I=     3TEMP=     1COND=     5
J=     4I=     5TEMP=     1COND=     3
J=     4I=     5TEMP=     1COND=     2
WHAT REACH PAIRS DO YOU WANT?,I?J?...1,1 FOR ALL
1,J FOR ALL NODES THAT REACH J
1,3
J=     3I=     2TEMP=     1COND=     0
J=     3I=     2TEMP=     1COND=     1
J=     3I=     3TEMP=     1COND=     1
WHAT REACH PAIRS DO YOU WANT?,I?J?...1,1 FOR ALL
1,J FOR ALL NODES THAT REACH J
0,0
```

Figure A-26 Output from Code SHORT



```
                ADJACENCY MATRIX
                    1 00000
                    2 00100
                    3 00000
                    4 00000
                    5 00000
      SINGLE DEPENDENCY REACHABILITY MATRIX
                    1 00000
                    2 00100
                    3 00000
                    4 00000
                    5 00000
 TWO VARIABLE REACHABILITY MATRIX               2 AND
                    1 00000
                    2 00000
                    3 00000
                    4 00000
                    5 00010
 TWO VARIABLE REACHABILITY MATRIX               3 AND
                    1 00000
                    2 00000
                    3 00000
                    4 00000
                    5 00010
 TWO VARIABLE REACHABILITY MATRIX               4 AND
                    1 00000
                    2 00000
                    3 00000
                    4 00000
                    5 00000
 TWO VARIABLE REACHABILITY MATRIX               5 AND
                    1 00000
                    2 00010
                    3 00010
                    4 00000
                    5 00000
```

Figure A-27 Output from Code MATRIX



```
1                  PROGRAM NEW2
     run file:report.dat
         input file:output.dat
      variable file:variab.dat

 REACH PAIR:   1,  4


 :: h
 NUMBER OF VARIABLES =          5
 NO SUPPRESSION CHOSEN

 NUMBER OF RECORDS=      7
 ROW NUMBER =    3


       2  3  5
    2  -  -  *
    3  -  -  *
    5  *  *  -


         ***SINGLETONS***
          4      D
1
```

Figure A-28. Output from Code NEW2

A.7 Partitioning

Once the global digraph has been constructed it is possible to identify complex modules that can be replaced by much simpler digraphs which, to the rest of the global digraph, act like the original module. The process of identifying and replacing these modules is called partitioning and the result is a reduction of the number of nodes in the global digraph.

Partitioning, therefore, is a two step process: 1) Identification of the modules to be partitioned; and 2) Generation of an input/output equivalent digraph to replace the module. A simple approach to the first step is to select unit models as partitions. While this approach most likely wouldn't result in the greatest possible reduction of nodes, it makes unnecessary the development of sophisiticated global search and partitioning algorithms. For the global model of HPSIS, using the valve unit models as partitions reduced the problem size by about 50%.

The second partitioning step requires consideration of how the connections into the partition can affect the output of the partition. The valve partition contains 8 nodes which have inputs from outside the unit model. These "boundary nodes" are inputs from support systems for power and control as well as from human operators. The question that has to be answered is what combinations of these boundary nodes can cause the single output node to fail? This is answered by tying each of the 2**8-1 combinations to a corresponding master node and then calculating the single dependency reachability for the new network. Each of the master nodes which can reach to the output of the partition represents a particular combination of boundary nodes which can cause the valve to fail. Since this combination could arise when the valve is integrated into the global model, the effective digraph which will replace the valve must contain that reachability information. If, for instance, the valve will fail if the master node connected to boundary nodes 1, 3, 4, 6, and 7 fails, then the effective digraph must contain the 5 input AND gate with those nodes as inputs and the valve output node as the output. No information internal to the valve need be carried thus reducing the size of the global model.

Furthermore, if it can be proven that, for a given boundary node, there are no singletons in the global model which can cause it to fail, then it needn't be included in any sets of combinations containing more than itself and one other boundary node. Also, if that same node cannot fail due to a singleton or doubleton in the global model then it needn't be considered in any of the combinations. The caveat here is that the resulting partition cannot be used to calculate tripletons to the valve output, but this can be bypassed by generating partitions with boundary node combinations of desired degree of reachability.

After processing the global partitioned problem, it may be necessary to include details of the valve interior depending upon whether a partitioned valve output appears as a singleton or in a doubleton pair. In the first case, those components within the valve which are singletons to the output node must be included in the global singleton list. Also, those components within the valve which are doubletons to the output are added to the global doubleton array. For the second case, nodes within the valve which are singletons to the partition output must be included along with the output node in the global doubleton array. This post-processing requires a reachability calculation on the valve unit model alone.

A.8 Tripleton Code

The DMA model provides a rich basis for investigation of the effect of various component or system failures For example, the effect of the loss of offsite power could be investigated by "turning on" the node which represents offsite power. A special version of the reachability code was designed and is used to allow these investigations. This code functions in a manner similar to the reachability code described earlier with one difference. After the single dependency reachability calculation is performed, a double dependency reachability calculation is performed using the node to be "turned on" as the first KKK (Figure A-24). The reachability result of this calculation is then used as the result of the single dependency calculation for all subsequent KKK (doubleton) calculations. The resulting doubletons are doubletons if, and only if, the "turned on" node is true (in the failed state). Thus the doubletons are tripletons with the turned on node.

This technique allows a simulation study of the impact of specific failures on the system. For example, the loss of onsite power could be investigated by creating a master node for onsite power and making it adjacent to all onsite power sources. This master node would then be turned on for a tripleton run.

REFERENCES FOR APPENDIX A

A-1. J. L. Peterson, "Petri Nets," Computing Surveys, Volume 9, Number 3, September 1977.

A-2. I. J. Sacks, "Techniques for the Determination of Potential Adversary Success with Tampering (Level 4.1)," Lawrence Livermore Laboratory, October 1978.

A-3. H. S. Warren, "A Modification of Warshall's Algorithm for the Transitive Closure of Binary Relations," Comm. ACM, Volume 18, 218-220, 1975.

A-4. S. Warshall, "A Theorem on Boolean Matrices," Journal of the Association for Computing Machinery, Volume 9, 11-12, 1962.

A-5. M. F. Chamow, "Directed Graph Technique for the Analysis of Fault Trees," IEEE Transactions on Reliability, R-27, No. 1, April 1978.

A-6. P. A. Renard, "Clamor," Lawrence Livermore Laboratory, MC-79-96, January 1979.

A-7. C. J. Patenaude, D. W. Freeman, "Tampering Analysis in the Structured Assessment Approach - A Description of the Level 4 Capability", Lawrence Livermore National Laboratory, November 1980.

A-8. M. N. S. Swamy, K. Thulasiraman, "Graphs, Networks, and Algorithms," John Wiley & Sons, 1981.

NRC FORM 335
(6 83)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by TIDC, add Vol No., if any)
NUREG/CR-3593, Vol. 1

2. Leave blank

3. TITLE AND SUBTITLE
Systems Interaction Results from the Digraph Matrix Analysis of a Nuclear Power Plant's High Pressure Safety Injection System

4. RECIPIENT'S ACCESSION NUMBER

5. DATE REPORT COMPLETED
MONTH January
YEAR 1984

6. AUTHOR(S)
I. J. Sacks, B. C. Ashmore, and H. P. Alesso

7. DATE REPORT ISSUED
MONTH July
YEAR 1984

8. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550

9. PROJECT/TASK/WORK UNIT NUMBER

10. FIN NUMBER
FIN A-0403

11. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Safety Technology
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D. C. 20555

12a. TYPE OF REPORT
Technical Report

12b. PERIOD COVERED (Inclusive dates)
September 1981 to
February 1984

13. SUPPLEMENTARY NOTES

14. ABSTRACT (200 words or less)

The report describes the demonstration of the Digraph-Matrix Analysis on a Nuclear Power Plant's High Pressure Safety Injection System. The demonstration work was beyond the scope of both the methods and the criteria used by the NRC to license nuclear power plants. The analysis discovered components whose failure could jeopardize the High Pressure Injection System given the postulated accident. All these components had been previously considered both in the safety analysis and in the licensing review. The results demonstrate the capability of Digraph-Matrix Analysis to model an accident sequence (including front-line systems, support systems, and operator actions) as a continuously integrated model to discover functional systems interactions. Also, the method is scrutable and can be used on a complex system which contains both a large number of components and dependent loops. Volume 1 is the main report and the description of the method. Volume 2 contains the digraphs, adjacency listings, and data base.

15a. KEY WORDS AND DOCUMENT ANALYSIS
Systems interactions
Digraph Matrix Analysis
Adjacency matrix
Single failures
Paired failures

15b. DESCRIPTORS

16. AVAILABILITY STATEMENT
Unlimited

17. SECURITY CLASSIFICATION
(This report)
Unclassified

18. NUMBER OF PAGES

19. SECURITY CLASSIFICATION
(This page)
Unclassified

20. PRICE
$

☆U.S. GOVERNMENT PRINTING OFFICE : 1984 O - 449-831