NUREG/CR-4179
UCID-20350
Vol. 1

Digraph Matrix Analysis for Systems Interactions at Indian Point Unit 3

Main Report

Prepared by H. P. Alesso, T. J. Altenbach, P. G. Prassinos, D. A. Lappa,
C. Y. Kimura, C. J. Patenaude/LLNL
I. J. Sacks, B. C. Ashmore, D. C. Fromme, M. V. Hershberger/AIPI
C. F. Smith, W. J. Williams/SAI

Lawrence Livermore National Laboratory

Analytic Information Processing, Inc.

Science Applications, Inc.

Prepared for
U.S. Nuclear Regulatory
Commission

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.

The views expressed in this report are not necessarily those of the U.S. Nuclear Regulatory Commission.

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 Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082,
   Washington, DC 20013-7082
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 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-4179
UCID-20350
Vol. 1

Digraph Matrix Analysis for Systems Interactions at Indian Point Unit 3

Main Report

Manuscript Completed: August 1984
Date Published: January 1986

Prepared by
H. P. Alesso, T. J. Altenbach, P. G. Prassinos, D. A. Lappa,
C. Y. Kimura, C. J. Patenaude, Lawrence Livermore National Laboratory
I. J. Sacks, B. C. Ashmore, D. C. Fromme, M. V. Hershberger, Analytic Information Processing, Inc.
C. F. Smith, W. J. Williams, Science Applications, Inc.

Lawrence Livermore National Laboratory
Livermore, CA 94550

Subcontractors:
Analytic Information Processing, Inc.
P.O. Box 966
Danville, CA 94526

Science Applications, Inc.
1811 Santa Rita Road - Suite 104
Pleasanton, CA 94566

Prepared for
Division of Safety Technology
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN A0445

NRC SUMMARY

The NRC staff has been evaluating methods that analyze for intersystems dependencies. The evaluations were both (a) toward resolving Unresolved Safety Issue A-17 (Systems Interaction in Nuclear Power Plants) and (b) toward improving the analysis for dependencies in Probabilistic Risk Assessments. Two methods, Digraph-Matrix Analysis and Fault Tree/Interactive Failure Modes & Effects Analysis, appeared effective although previously not applied on a large scale to nuclear systems. This report describes the demonstration of the Digraph-Matrix Analysis on a large fraction of the systems at one nuclear power plant. The demonstration of the Fault Tree/Interactive Failure Modes & Effects Analysis is described in NUREG/CR-4207.

The objective of the systems interaction analysis was to provide assurance that the independent functioning of selected safety-related systems was not jeopardized by components that cause faults to be dependent. The results reported here came from work beyond the routine criteria used by the NRC to license nuclear power plants. The report should be read as a technical evaluation by the laboratory performing the analysis rather than as a safety evaluation performed by the licensing staff of the NRC. The NRC resolution of USI A-17 will include both a safety evaluation and a regulatory analysis.

The demonstration plant was selected primarily based upon the cooperation extended by the utility toward a resolution of USI A-17. A copy of the draft report was provided to the utility and placed in the Public Document Room on July 3, 1985.

Volumes II through V, containing the supporting digraphs and matrices, are available at the NRC Public Document Room.

FOREWARD

This report consists of five volumes only one of which is being published. The complete document is on file with the authors and Frank Coffman of the Reliability and Risk Assessment Branch of the Division of Safety Technology of the Office of Nuclear Reactor Regulation of the U. S. Nuclear Regulatory Commission. The complete document consists of five volumes. These are:

Volume 1
- 1a Main Report
- 1b Enclosures (contains full set of results)

Volume 2
- Appendix A: Overview of Digraph Matrix Analysis

Volume 3
- Appendix B: DMA Digraphs and Reference Drawings

Volume 4
- Appendix C: Adjacency Lists

Volume 5
- Appendix D: Probability Data Base

In order to make this report more readable, we have included some of the contents of the results volume (1b) in this Volume (1a). We have also included the introduction and the first data base listing from Appendix D. A complete and detailed review of this study will require all five volumes.

ABSTRACT

Digraph Matrix Analysis (DMA) has been under development as a tool to search for systems interactions at nuclear power plants. This report presents the DMA methodology and the results of the analysis of selected safety system combinations at the Indian Point Three nuclear power plant so as to allow a comparison with a competitive analysis performed by Brookhaven National Laboratory. The plant specific results of this study were as follows:

1. No new systems interactions were found in the front-line safety injection or feedwater systems when analyzed separately.

2. The analysis of the complete systems including support systems such as electrical power and service water uncovered the following significant systems interactions:

   a. Improper alignment of a manually set valve in the service water system in conjunction with the loss of offsite power will cause the failure of the diesel generators resulting in a RCP seals failure along with the failure of safety injection leading to reactor core damage.

   b. Failure of an electrical interlock (a set of contacts) in conjunction with the loss of offsite power will cause the loss of multiple trains of front-line systems.

3. A singleton which was found by Brookhaven National Laboratory in the electrical system supporting Low Pressure Injection was verified by the DMA analysis.

4. Several key locations were found which were common to redundant trains of front-line systems. However, we did not find initiating events in these locations.

5. The evaluation of the effects of potential operator actions indicated that:

   a. Operator actions that initiate safety actions such as starting pumps and opening valves, greatly improve system reliability.

   b. Operator overrides that terminate safety actions should be allowed only with the concurrence of a supervisor.

   c. There is a significant difference between operator action dealing with front-line systems and operator actions dealing with support systems.

EXECUTIVE SUMMARY

Studies of the events at Three Mile Island-2 [3], Browns Ferry-3 [4-8] and Crystal River-3 [9] have indicated that complex systems interactions can occur as a result of dependent failures. Methods for identifying these intersystem dependencies have been limited. As a result, the Nuclear Regulatory Commission (NRC) is pursuing a program to define methodologies that will characterize the spatial and functional coupling of nuclear power plant systems.

At present, the NRC is considering two methodologies for system interaction studies. One approach is the expansion of the fault tree analysis portion of Probabilistic Risk Assessments (PRA) by putting additional emphasis on dependence analysis techniques. The second approach is based on graph-theoretic methods utilizing a conditioned matrix representation of logic diagrams called Digraph Matrix Analysis (DMA) [18, 19, 20]. This risk assessment technique is applied in conjunction with an event tree analyses identification of accident sequences or system combinations.

This report documents the analysis of the Indian Point Plant, Unit 3 (IP-3) for adverse systems interactions using DMA. The primary objective of the study was to compare the effectiveness of DMA in finding systems interactions. To this end a parallel study was funded at Brookhaven National Laboratory (BNL). The results of this study and the BNL study will then be compared by NRC to the results of a similar study performed by the Power Authority of the State of New York. A secondary objective of this study was to determine systems interactions in selected combinations of safety systems at IP-3.

In a DMA of a system combination, a large single integrated logic diagram (including AND and OR gates) is created which is then analyzed for single components and pairs of components whose failure can cause safety function failure. This single model includes all front-line systems in the system combination along with all necessary support systems. The logic diagram (digraph) is constructed directly from the plant piping and instrumentation diagrams (P&IDs), electrical one line drawings, and other schematics. Logic connectives (AND and OR gates) are added to these logic diagrams to represent dependence between components. The digraphs thus closely resemble the system schematics. This resemblance to the physical system allows the digraphs to be easily reviewed and corrected, if necessary. Also, changes in plant construction can be readily incorporated into the digraph without reconstructing the entire system digraph. The digraphs are also not limited to the "tree" structure of the more traditional fault tree and can represent cyclic structures. The digraphs are processed through a computer code based on a conditioned reachability calculation which finds the total connectivity of the digraph. Both single components and pairs of components which can affect the operation of other components are found by this reachability calculation, (i.e., failure of A can affect operation of B). By defining a top event component, such as the failure of high pressure safety injection, all single components (Singletons) and pairs of components (Doubletons) can be determined which will cause the top event to occur. Ten combinations of systems were chosen as top events for this study by

NRC. Accident Sequence failure probabilities are determined from the singleton and doubleton failures. These probability calculations were performed to gain a comparison between systems and as a means to compare with other PRAs.

Each system combination consists of several front-line systems along with their support systems and human interactions. Ten system combinations were analyzed. The front-line systems included high pressure injection, low pressure injection and recirculation, accumulators, main and auxiliary feedwater, safety injection actuation, pressure operated relief valve and main coolant pump seals. The support systems included service water, component cooling, control and lube oil, electrical power, instrumentation and control, instrument air, nitrogen to nuclear equipment and city water supply. The analysis also included dependencies resulting from shared locations or environmental conditions within the plant.

The ten system combinations were chosen by the NRC from a list of initiating events and event trees that identified accident sequences that might lead to core melt. The front-line systems that perform vital safety functions were combined with their support systems to form accident sequences that begin with a specified initiating event and lead to "plant damage states". The ten accident sequences analyzed are listed on the following page.

Combination			Description of Systems
1.	S_1D_i	-	Medium LOCA and Loss of Low Pressure Injection
2.	S_1U_i	-	Medium LOCA and Loss of High Pressure Injection
3.	$S_2(Q)U_i$	-	PORV LOCA and Loss of High Pressure Injection
4.	$S_2(P)U_i$	-	RCP seal LOCA and Loss of High Pressure Injection
5.	(TT)ML	-	Turbine Trip and Loss of Feedwater
6.	(LOOP)ML	-	Loss of Offsite Power and Loss of Feedwater
7.	$S_2(P)ML$	-	RCP Seal LOCA and Loss of Feedwater
8.	$S_2(Q)ML$	-	PORV LOCA and Loss of Feedwater
9.	AR	-	Large LOCA and Loss of Recirculation
10.	$S_1U_iD_i$	-	Medium LOCA and Loss of All Injection

Definitions

U_i	=	High Pressure Injection During Injection Phase
D_i	=	Low Pressure Injection During Injection Phase
R	=	Recirculation Cooling During Recirculation Phase
$S_2(P)$	=	Small LOCA (RCP Seals induced)
$S_2(Q)$	=	Small LOCA (PORV induced)
S_1	=	Medium LOCA
A	=	Large LOCA
M	=	Main Feedwater
L	=	Auxiliary Feedwater
TT	=	Turbine Trip
LOOP	=	Loss of Offsite Power

Within the scope and limitations of this Digraph Matrix Analysis to find Systems Interactions at Indian Point-3, we have reached the following conclusions:

1. When we evaluated the front-line systems while assuming that the support systems' probability of failure was zero, we found that the safety injection and feedwater front-line systems were robr c.

2. When we evaluated the interactions of both front-line and support systems, we found the following significant systems interactions:*

   a. ITLBKR3AT6A, the failure of an interlock in the auto closing circuits for breakers EG2 and 2AT3A prevents closure of these breakers unless breaker 3AT6A is open. Physically, the interlock is a "b" contact breaker auxiliary switch. If breaker 3AT6A is closed, or if the "b" contact fails to close when that breaker is open, then the interlock fails and EG2 and 2AT3A will not close automatically. Under loss of offsite power circumstances, this can cause the loss of multiple trains of front-line systems. In particular, auxiliary feedwater pumps 31 and 33 and two of the three safety injection pumps as well as residual heat removal pumps 31 and 32 will not start automatically. Similarly, a "b" contact interlock on breaker 2AT5A prevents diesel supply breakers EG1 and EG3 from closing automatically (see Section 3.2 for details).

   b. The improper alignment of a valve (either SWN-29 or SWN-30) in the service water system can cause all three emergency diesel generators to fail. In the event of a loss of offsite power, the failure of these diesels will cause the loss of cooling to the reactor coolant pump seals resulting in a seal rupture. This seal rupture leads to a LOCA at a rate of about 2000 gpm. The loss of the diesels also will prevent the use of safety injection leading to potential core damage.

3. When we evaluated front-line and support systems with location vulnerabilities, we identified several key locations though we did not find initiating events.

   Locations LOCDP (480 V bus location), LOC001 (AFW pump room), LOCSIPRM (SI pump room) were vitally important and presently secure.

4. When we evaluated front-line and support systems together with their location vulnerabilities and their interactions with operator actions, we concluded:

*Note: In July 1984 Brookhaven National Laboratory identified a safety violation at Indian Point-3 (medium/large LOCA and failure of Battery 32). By changing a modeling assumption in the load shedding model of the electrical system we were able to reproduce this result (See Section 2.4.1).

a. Operator actions that initiate safety actions, such as starting pumps and opening valves, greatly improve reliability and should generally be recommended for both safety injection and feedwater systems.

b. Operator actions that terminate safety actions, such as stopping pumps or closing valves, should only be allowed with the concurrence of a supervisor.

c. There is a significant difference between operator actions dealing with front-line systems instead of support systems.

CONTENTS

2.3 System Digraphs (Continued) Page

2.3 System Digraphs (Continued)

Volume 1b -- List of Enclosures

List of Figures*

*NOTE: See Individual Appendices for their own List of Figures.

List of Tables

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, or location which can significantly impact system operation.

Compression - A computer processing step in the DMA processing sequence in which redundant (repeated) lines of input in the adjacency data are deleted.

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

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 cut sets of the system.

Digraph - A graph consisting of a group of nodes and logical connectives which also indicates the direction of flow of effects.

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

Edge - A directed connection between two nodes.

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

LWR - Light Water Reactor

NRC - U. S. Nuclear Regulatory Commission

Node - The symbol in the digraph which represents a physical component, physical location, plant operating mode, or human interaction.

PWR - Pressurized Water Reactor

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

SI - Systems Interactions

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

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

Strong Component - Consists of a group of nodes which are bi-directionally and unconditionally connected.

Systems Interaction - Spatial and functional coupling (including human actions) between systems that leads to interdependencies.

Unit Model - A detailed digraph model of a specific component of the system. The unit model represents the decomposition of a large component, such as a valve, into its parts. The unit model can be either generic or specific.

List of FSAR/P&ID Symbols and Abbreviations
(Additional Nomenclature is given in Appendix C)

AA	Moisture Alarm
ACS	Auxiliary Coolant System
AE	Moisture Detector
AFWS	Auxiliary Feedwater System
ANPS	Annulus Negative Pressure System
BIT	Boron Injection Tank
BV	Block or Bleed Valve
CARS	Controlled Atmospheric Release System
CCR	Central Control Room
CCW	Component Cooling Water
CFR	Code of Federal Regulations (U.S.)
CHF	Critical Heat Flux
CSS	Containment Spray System
CVCS	Chemical & Volume Control System
D	Local Drain
DH	Drain Header
DNB	Departure From Nucleate Boiling
DPC	Differential Pressure Controller
DPI	Differential Pressure Indicator
ECCS	Emergency Core Cooling System
EPA	Environmental Protection Agency
E/P	Electric to Pneumatic Transducer
EX	Capacitor Discharge Exciters
FC	Fail Closed
FCV	Flow Control Valve
FO	Fail Open
FR	Flow Recorder
FRC	Flow Recording Controller
FE	Flow Element (orifice)
FI	Flow Indicator
FIC	Flow Indicating Controller
FSAR	Final Safety Analysis Report
FT	Flow Transmitter
GA	Gas Analyzer
HC	Hand Controller
HCV	Hand Control Valve
HEPA	High Efficiency Particulate Air Filter
HPIS	High Pressure Injection System
HVAC	Heating, Ventilation, and Air Conditioning
IV	Isolation Valve
IVSWS	Isolation Valve Seal Water System
LA	Level Alarm
LC	Locked Closed; also Level Controller
LCV	Level Control Valve
LG	Level Gage Glass
LFR	Low Fire Return Solenoid
LI	Level Indicator
LIC	Level Indicating Controller
LLT	Low Level Trip

List of FSAR/P&ID Symbols and Abbreviations (Continued)

LO	Locked Open
LOCA	Loss of Coolant Accident
LT	Level Transmitter
MCC	Motor Control Center
MFWS	Main Feedwater System
MOV	Motor Operated Valve
N	Nitrogen Supply Manifold
NC	Normally Closed
NO	Normally Open
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission (U.S.)
OF	O_2 Filter
OR	Orifice Assembly
P&ID	Piping & Instrumentation Diagram
PA	Pressure Alarm
PAB	Primary Auxiliary Building
PCV	Pressure Control Valve
PI	Pressure Indicator
PM	Pneumatic Motor
PORV	Pressure Operated Relief Valve
PR	Pressure Recorder
PRT	Pressurizer Relief Tank
PS	Pressure Switch
PT	Pressure Transmitter
PW	Primary Make up Water
PWR	Pressurized Water Reactor
PWST	Primary Water Storage Tank
RC	Ratio Controller
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RDT	Reactor Drain Tank
RHR	Residual Heat Removal
RWST	Refueling Water Storage Tank
S	Strainer
SIAS	Safety Injection Actuation Signal
SI	Safety Injection
SIS	Safety Injection System
SOV	Solenoid Operated Valve
SRST	Spent Resin Storage Tank
SS	Sample System
ST	Temporary Strainer
T	Containment Isolation Signal
TA	Temperature Alarm
TC	Temperature Controller
TCV	Temperature Control Valve
TI	Temperature Indicator
TIC	Temperature Indicating Controller
TR	Temperature Recorder
TRC	Temperature Recording Controller
TT	Temperature Transmitter

List of FSAR/P&ID Symbols and Abbreviations (Continued)

TW	Thermometer Well
V	Local Vent
VC	Vessel Containment [Building]
VH	Vent Header
VS	Ventilation System
WDS	Waste Disposal System
WHT	Waste Holdup Tank
Δ	Piping Penetration
<>	Seismic Classification

ACKNOWLEDGEMENTS

It is a pleasure to acknowledge the supportive guidance of the NRC contract monitors, Charles Morris and Franklin D. Coffman, throughout this study.

1.0 INTRODUCTION

1.1 Background

Approaches for the assessment of reactor accident risks have evolved over a period of several decades. Early techniques to incorporate accident risks in the design process included the design-basis accident approach; safety assessments, typified by the WASH-740 [1] analysis used very conservative (worst case) assumptions in evaluating the potential consequences of a major reactor accident. More recently, the reactor safety study (WASH-1400) [2] introduced the approach of Probabilistic Risk Assessment (PRA) into the evaluation of reactor safety for generic reactor types. Probabilistic techniques have been extended and refined through subsequent PRAs that have been used to analyze several specific reactors. PRAs to date have been successful in describing and evaluating major accident sequences and the resultant risks. Success in identifying more subtle hidden dependencies between systems or trains designed to be independent has been more limited. Studies of the events at Three Mile Island-2 (TMI-2) [3], Browns Ferry-3 [4-8] and Crystal River-3 [9] have confirmed that complex systems interactions can occur as a result of unanticipated dependent failures.

The Nuclear Regulatory Commission (NRC) Action Plan developed as a result of the TMI-2 accident (NUREG-0660) [10], identified Action Item II.C.3 "to coordinate and expand ongoing staff work on systems interaction [Unresolved Safety Issue (USI) A-17] so as to incorporate it into an integrated plan for addressing the broader question of systems reliability in conjunction with IREP and other efforts." The Division of Safety Technology (DST) has coordinated the ongoing work between the Generic Issues Branch (GIB) and the Reliability and Risk Assessment Branch (RRAB). In February 1983, the activities (primarily USI A-17 and TMI-2 Action Item II.C.3) were combined under the title of USI A-17.

Presently, the NRC systems interaction program is proceeding toward (1) the resolution of USI A-17, and (2) the development of procedures for the consideration of intersystem dependencies in future reactor assessments.

Engineering systems are often designed with redundant trains in order to improve system reliability. However, any common element or coupling between trains can reduce system reliability. The term Systems Interaction (SI) has been introduced by the NRC to characterize the concept of spatial and functional coupling of nuclear power plant systems which can 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. Dynamic human errors are those which occur during the incident.

The Office of Nuclear Reactor Regulation (NRR) of the NRC is pursuing a program to further define and subsequently implement SI regulatory requirements for light water reactors (LWRs). Battelle Columbus/Pacific Northwest Laboratories [11], Brookhaven National Laboratory [12], and Lawrence Livermore National Laboratory [13], assisting the NRC, recommended to the NRC that risk 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 SIs. 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 [14,15]. The method was based on "shutdown logic diagrams" which are success-paths of operation sequences.

At present, the NRC is considering two concepts for a systems interaction study.

One approach holds 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 [16] and minimum cut set common cause/mode analysis [16]. The NRC's initial guidance for this point of view has already been initiated [17].

The second concept is based on graph-theoretic methods utilizing a conditioned matrix representation of logic diagrams and is called Digraph Matrix Analysis (DMA) [18,19,20]. This risk assessment technique would be applied in conjunction with an event tree analysis identification of the accident sequences or system combinations. DMA treats a system combination consisting of several front-line systems along with their support systems and human interactions as a single logic model. Thus, instead of constructing a fault tree for each individual system in an accident sequence, as in the Reactor Safety Study [2], the entire system combination is modeled as a logic diagram (which includes AND and OR gates) that resembles the layout of the actual plant hardware. The advantages of such a model are: (1) the model directly includes the cyclic nature of the physical system; and (2) highly efficient graph based computer processing codes exist for identifying Singletons and Doubleton cut sets.*

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

1. Construction of the logic model is performed directly from plant drawings (piping and instrumentation diagrams, electrical schematics, safety logic drawings). The resulting digraph model can be overlaid on the plant drawings. As a result, the model can be readily understood, reviewed, and corrected.
2. The resulting digraph (directed graph with logic connectives) is not limited to a "tree" structure as are fault trees and hence can represent physical situations which are cyclic. Cycles generally arise from timing and sequencing effects of the failure in a component. Cycles are quite common in piping networks and electrical power and control schematics. Fault tree analysts individually "break" every cycle and

* Technically, the singletons and doubletons found in a DMA are not cut sets of the digraph. They are single nodes or pairs of nodes whose failure can propagate to a terminal node. The term cut set is used only because of its use in fault tree analysis.

construct a logical equivalent representation. Certain types of cycles which arise in DMA must also be broken manually.

3. The digraph is processed through DMA computer codes which are based on a conditioned reachability calculation. This matrix calculational process identifies potential failure paths (reachability) through the system logic model. These codes determine single component failures (Singletons) and pairs of component failures (Doubletons) which would cause system failure. Also selected tripletons can be determined.

4. DMA computer codes can process very large models. System combinations consisting of front-line systems, their support systems and human actions, can be modeled as a single digraph. The model used in this study consisted of about 12,000 components. The ability of DMA codes to process such large models is based on its graph-theoretic approach as opposed to the Boolean equation substitution codes used to find cut sets of fault trees.

A review of the fundamental mathematical aspects of fault tree and DMA risk analysis was presented in Ref. [18]. Initial guidance for DMA was presented in Ref. [19]. A report on the results of a demonstration which evaluated the high pressure safety injection system of a typical pressurized water reactor was presented in Ref. [20].

Figure 1-1 illustrates how an enhanced fault tree systems interaction approach (as suggested by BNL) would compare to the DMA approach. The enhanced fault tree approach would consist of several medium-sized 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 minimum cut sets would include the singleton, doubleton, tripleton, etc., cut sets. Then, a minimum cut set common cause/mode analysis based on Failure Modes and Effects Analysis (FMEA) would be conducted to find higher order cut sets from each fault tree and for the system combination that could be reduced to lower order cut sets (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."

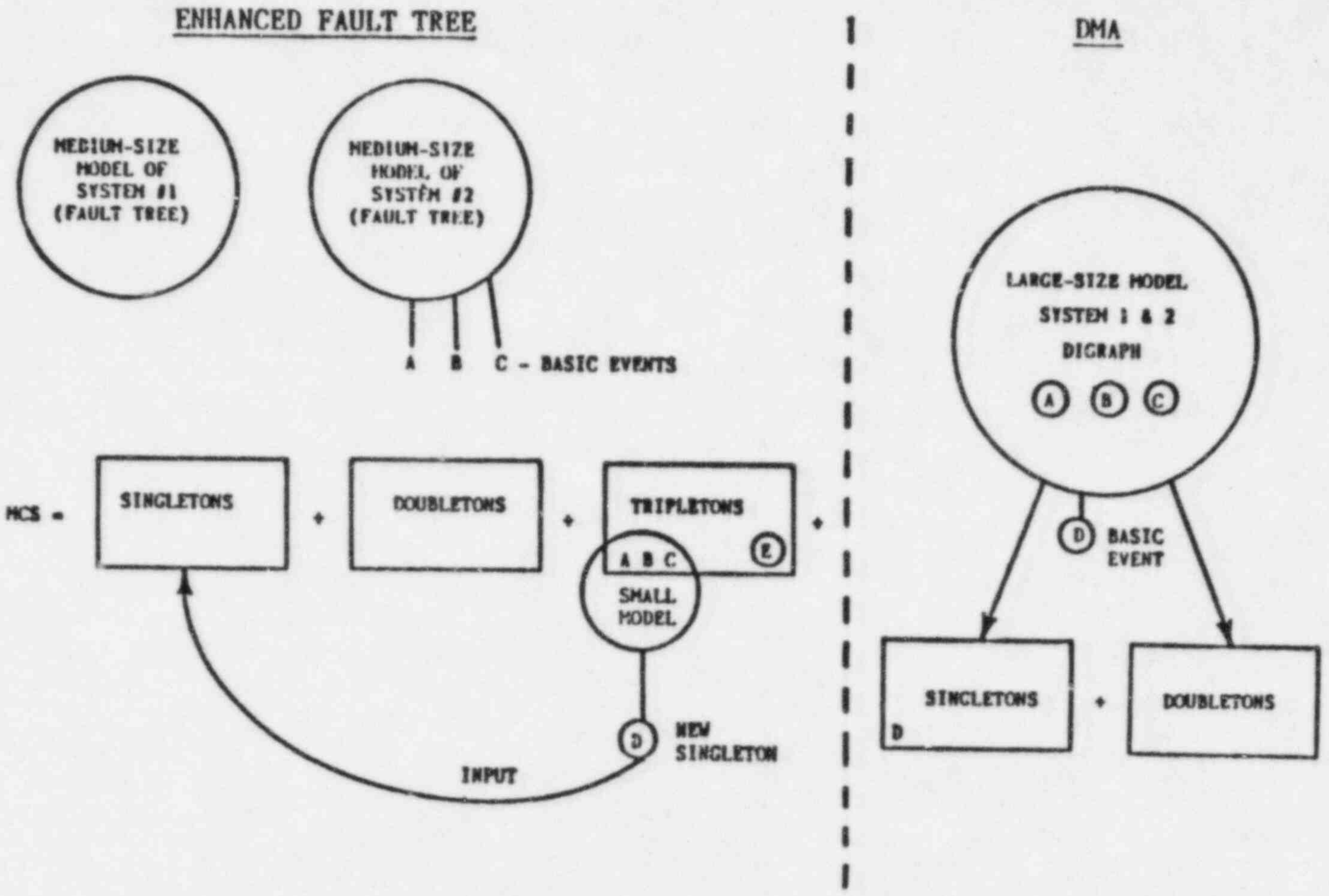


Figure 1-1. Systems Interaction Performed via Enhanced Fault Tree versus DMA

1.2 Objective

The primary objective of this report is to provide a basis for the comparison of effectiveness of the digraph matrix method with other methods, including the method employed by the utility (Power Authority for the State of New York) and the method employed by Brookhaven National Laboratory. The effectiveness parameters to make this comparison are (a) the ability to discover intersystem dependencies hidden within the plant, (b) the ability to rank-order intersystem dependencies that are safety significant, and (c) the resource efficiency.

The secondary objective of this study is to analyze the Indian Point Plant, Unit 3 for adverse systems interactions using Digraph-Matrix Analysis (DMA). The methodology was reported in NUREG/CR 2915 [19]. This effort is intended to aid in the resolution of USI A-17.

1.3 Summary of Results

1.3.1 Overview of Results

The results of the Digraph-Matrix systems interaction study are presented in the form of both minimal cut-sets and point estimate probabilities. The system combinations selected for analysis are presented in Table 1-1. For example, system combination #1 corresponds to S_1D_i (Medium LOCA and loss of Low Pressure Injection). The front-line system is the Low Pressure Injection System and its support systems include: Electrical, Safety Injection Actuation, Component Cooling, Service Water, and Instrument Air, human interactions and locations.

In order to reach productive conclusions about both the safety contributions of functional/spatial coupling and the effectiveness of various methodologies, we evaluate each coupling contribution separately. For each of the ten system combinations, four cases were run to evaluate the contribution of front-line systems, support systems, location and procedures to system failure including unavailability. Each case had its own determination of singletons, doubletons and point estimate probability. Table 1-1 forms a summary of results using the abbreviations listed below to define system combinations.

Definitions

U_i	= Loss of High Pressure Injection During Injection Phase
D_i	= Loss of Low Pressure Injection During Injection Phase
R	= Loss of Recirculation Cooling During Recirculation Phase
$S_2(P)$	= Small LOCA (RCP Seals induced)
$S_2(Q)$	= Small LOCA (PORV induced)
S_1	= Medium LOCA
A	= Large LOCA
M	= Loss of Main Feedwater
L	= Loss of Auxiliary Feedwater
TT	= Turbine Trip
LOOP	= Loss of Offsite Power

In this table, each probability given is the probability that a given system combination will fail to perform its function. This probability includes failure to function due to the effects of component unavailability prior to the accident and to component failure during the incident. In the first case, only the effects of front-line component failures and unavailability were considered. The second case analysis added the effects of failures in the support systems. The third case studied included any additional singleton and doubleton cut sets which arise from common locations of components. In these three cases, both the detrimental and beneficial effects of human intervention during the accident were ignored. These operator effects were considered in Case IV. In Case IVA, the effect of beneficial operator actions were considered. In this case, correct operator actions were included (if permitted by the IP-3 design) to mitigate the effects of component failures. It was assumed that these correct actions would occur with a probability of one. In case IVB, both beneficial and detrimental operator actions were included (again where the IP-3 design would permit). Typical detrimental actions included opening circuit breakers, closing valves, etc. These incorrect operator actions were conservatively given a probability of 10^{-3}.

The numbers of singletons and doubletons presented in this table, indicate the number of first order and second order cut sets which lead to system failure. The numbers listed include only cut sets which contain actual physical components, that is, any cut set containing dummy components used to simplify modeling was not counted. In the majority of cases, most of the cut sets which lead to system failure include the failure of components in support systems.

Table 1-1 Summary of Results

System Combinations	Case I Frontline Systems(FL)	Case II Support Systems(SS)	Case III Spatial FL + SS+ Location(L)	Case IV Human FL + SS+ L+Procedure	
				A	B
#1 S_1 D_i	17 *	17	28	16	18
	84 **	2349	2180	1854	2128
	8.07E-4 +	8.09E-6	N/A	8.08E-4	2.83E-3
#2 S_1U_i	9	28	34	23	23
	535	4426	4552	3482	3862
	7.32E-4	11.49E-4	N/A	2.25E-5	6.31E-5
#3 $S_2(Q)U_i$	0	0	0	0	0
	28	28	63	12	12
	2.30E-6	2.30E-6	N/A	9.87E-7	9.874E-7
#4 $S_2(P)U_i$	0	0	0	0	0
	0	3		0	0
	0	See Text		0	0
#5 $T_{TT}ML$	4	4	8	0	0
	0	0	35	0	4
	1.04E-4	1.04E-4	N/A	0	4.74E-10
#6 $T_{loop}ML$	4	4	8	0	0
	0	942	977	4	4
	1.04E-4	1.09E-4	N/A	4.75E-10	4.75E-10
#7 $S_2(P)ML$	0	0	0	0	0
	228	712	1467	0	0
	4.30E-10	4.80E-10	N/A	0	0
#8 $S_2(Q)ML$	0	0	0	0	0
	21	21	21	0	0
	5.62E-6	5.62E-6	N/A	0	0
#9 AR				7	7
	N/A	N/A	N/A	929	1055
				2.22E-5	3.01E-5
#10 S_1 U_i D_i	6	6	8	4	4
	54	424	430	219	300
	3.34E-5	3.31E-5	N/A	3.29E-12	1.03E-12

* Number of singleton cut sets

** Number of doubleton cut sets

+ Unavailability and failure to function during accident

1.3.2 Summary of Significant Systems Interactions

Within the scope and limitations of this Digraph Matrix Analysis for Systems Interactions at Indian Point-3, we have reached the following conclusions:

1. When we evaluated the front-line systems while assuming that the support systems' probability of failure was zero, we found that the safety injection and feedwater front-line systems were robust.

2. When we evaluated the interactions of both front-line and support systems, we found the following significant systems interactions:*

    a. ITLBKR3AT6A is an interlock in the auto closing circuits for breakers EG2 and 2AT3A. It prevents closure of these breakers unless breaker 3AT6A is open. Physically, the interlock is a "b" contact breaker auxiliary switch. If breaker 3AT6A is closed, or if the "b" contact fails to close when that breaker is open, then the interlock fails and EG2 and 2AT3A will not close automatically. Under loss of offsite power circumstances, this can cause the loss of multiple trains of front-line systems. In particular, auxiliary feedwater pumps 31 and 33 and two of the three safety injection pumps as well as residual heat removal pumps 31 and 32 will not start automatically. Similarly, a "b" contact interlock on breaker 2AT5A prevents diesel supply breakers EG1 and EG3 from closing automatically (see Section 3.2 for details).

    b. Improper alignment of a valve SWN-98 or SWN-99 in the service water system can affect all three diesels (see Section 3.2 for details). On loss of offsite power, misalignment of this valve can cause an RCP seals LOCA and prevent safety injection. This scenario leads to core damage.

3. When we evaluated front-line and support systems with location vulnerabilities, we identified several key locations though we did not find initiating events.

    Locations LOCDP (480 V bus location), LOC001 (AFW pump room), LOCSIPRM (SI pump room) were vitally important and presently secure.

4. When we evaluated front-line and support systems together with their location vulnerabilities and their interactions with operator actions, we concluded:

*Note: In July 1984 Brookhaven National Laboratory identified a safety violation at Indian Point-3 (medium/large LOCA and failure of Battery 32). By changing a modeling assumption in the load shedding model of the electrical system we were able to reproduce this result (See Section 2.4.1)

a. Operator actions that initiate safety actions, such as starting pumps and opening valves, greatly improve reliability and should generally be recommended for both safety injection and feedwater systems.

b. Operator actions that terminate safety actions, such as stopping pumps or closing valves, should only be allowed with the concurrence of a supervisor.

c. That there is a significant difference between operator actions dealing with front-line systems instead of support systems.

1.4 Organization of Report

The complete report consists of five volumes, however only Volume 1 is being published. The remaining volumes are on file with the Systems Interaction branch, Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission. Volume 1 is the main report which includes an executive summary and a summary of results (Section 1.3). Section 2.0 of the main report presents the scope of the study (Sec. 2.1), the descriptions of the systems modeled (Sec. 2.2), and construction of the system digraphs (Sec. 2.3) and system combination digraphs (Sec. 2.4). Then Section 2.4 presents the minimal cut set results for each of the system combinations selected. Section 3.0 gives the general qualitative results. Section 4.0 gives the quantitative results for each system combination selected.

Volume 2 contains Appendix A. Appendix A is an overview of DMA methodology with examples and includes an outline of its computer codes. Volume 3 consists of Appendix B and is the complete set of digraph models and their associated system P&ID, electrical and logical drawings.

Finally, Volume 4 holds Appendix C, the Adjacency Listings (input file) by system, and Volume 5 holds Appendix D, the Probabilistic Data Base used in this study.

1.5 How to Use This Report

There are three basic approaches a reader may take with this report. They are:

I. Just interested in results and conclusions:
Read: Volume I: Executive Summary
Abstract
Introduction
Section 2.1 Scope
Section 2.4 Minimum Cut Set Results
Section 3.0 Qualitative Results
Section 4.0 Quantitative Results
Section 5.0 Conclusion

II. General review of entire study:
Read: Volume II: Review of DMA
then
Volume I: Main Report

III. Detailed Review

In order to perform a detailed review of this study, Volumes III, IV, and V included in the unabridged version will be required. Volume III contains the digraphs and corresponding system schematics (electrical single line and piping and instrumentation drawings). In Volume IV, the DMA adjacency listings for these drawings are given. Volume V contains the probabilistic data base used for the quantitative analysis portion of the study. It is suggested that the reviewer read the documents in the following order:

Volume II: Review of DMA
then
inspect a few digraphs and adjacency listings in
Volumes III and IV.
then
Read Volume I

2.0 DIGRAPH MATRIX APPLICATION TO IP-3

The technical objective of this study has been the application of Digraph Matrix Analysis (DMA) to evaluate potential systems interactions in some systems at the Indian Point-3 plant. To accomplish this objective it was necessary to first identify systems and system combinations for analysis, and to establish procedures for incorporating location, operation action, and maintenance procedures into the assessment.

This section of the report begins in Section 2.1 with a discussion of the scope of the study which includes consideration of system and system combination selection, as well as the incorporation of location, operator action and maintenance. Section 2.2 presents system descriptions for each of the systems selected for incorporation into the analysis. Following the system descriptions, Section 2.3 provides discussions of the system modeling efforts and the resultant digraph models for each of the systems. In Section 2.4, the system combination models and minimum cut set results are presented.

2.1 Scope of the Study

2.1.1 Overview

The purpose of this section is to discuss the scope and limitations of the study and to identify the constraints that led to that scope.

In the selection of a set of criteria to define the scope of this study, we attempted to be both comprehensive (i.e., by including different types of potential SIs involving human, spatial and support systems interactions) as well as complete (i.e., by including as much of the plant as possible). For example, if human procedural interactions were excluded in order to accommodate a greater portion of the physical plant, then an appreciation of the importance of these potential SI candidates would not be achieved.

The selection of the Indian Point-3 system combinations to be included in this study was constrained by: (1) resources and time considerations, and (2) the desire that an SI study be directly integratable into a Probabilistic Risk Assessment (PRA) effort. The resource and scope limitations of this study have constrained us to the 19 individual systems specified in Table 2-3, and to ten system combinations involving these component systems (Table 2-4). The systems and system combinations were selected in agreement with the NRC and with Brookhaven National Laboratory (BNL).

The system combinations which were selected all lead to reactor core damage. In order to limit the scope of the study, we excluded systems which mitigate the effects of a core damage accident.

2.1.2 Initiators

Reactor core damage is a consequence of major concern. In this project, we have attempted to evaluate and identify system combination scenarios that might lead to core damage. In particular, we first identify events which have the potential to initiate such scenarios. We refer to such events as "initiating events" or "IEs." Each IE is the root of a branching family of scenarios, some of which may lead to core damage.

Core damage can occur principally through inadequate heat removal resulting from an excess production of power in the core or a loss of cooling capability.

Excess power would occur if there were an uncontrolled increase in reactivity. Automatic shutdown (SCRAM) systems are designed to quickly shutdown the reactor during off-normal conditions severe enough to require prompt shutdown as detected by the protection systems. The identification of events leading to power excursion incidents can be evaluated from experience and an understanding of the reactor phenomena.

Inadequate heat removal can occur if there is a failure of the primary coolant boundary, or if a loss of heat removal capability leads to opening of pressure relief valves, and thus to a loss of coolant. In order to avoid exceeding a thermal limit following a scram, the rate of decay heat production should be somewhat less than its rate of removal by the various primary and secondary systems. A loss of primary coolant flow, a loss of secondary side heat sink, or a loss of primary coolant itself may upset this heat balance.

The events representing primary coolant boundary failure can be divided into four initiating event categories:

1. Large Loss of Coolant Accident (LOCA)
2. Medium LOCA
3. Small LOCA
4. Leakage to Secondary Coolant

Any primary coolant boundary failure can be assigned to one of the categories based on leak path or size.

One response to a primary cooling system failure is the use of emergency core cooling systems (ECCS) (also termed safety injection systems). The ECCS provides the capability of emergency removal of heat from the core. The provision of such engineered safety features to control postulated accidents is part of the defense-in-depth concept developed to enhance safety.

The emergency core cooling systems must be capable of safely limiting the consequences of a LOCA. Because the primary coolant system contains water and steam under high pressure, a large pipe break would result in rapid expulsion of a large fraction of this coolant into the containment building surrounding the reactor. Immediately after shutdown of the reactor, a substantial amount of residual heat (app. 5%) is still being generated in the fuel from decay of the previously generated radioactive fission products remaining in the fuel. Without provision for removal of this decay heat, elements of the reactor core could melt with severe consequences. Automatic control systems sense the occurrence of a LOCA and coordinate the operation of the different parts of the ECCS as they are needed. After a LOCA, the ECCS would supply water to the core via spray and/or flooding systems as long as needed.

A list of initiating events initially considered for our evaluation of systems interactions at IP-3 is given in Table 2-1.

Table 2-1

INITIAL CHOICE OF INDIAN POINT-3 INITIATING EVENT CATEGORIES

1. LARGE LOSS OF COOLANT ACCIDENT
   (pipe rupture greater than 6-inch)
2. MEDIUM LOSS OF COOLANT ACCIDENT
   (pipe rupture in range of 2 to 6-inch)
3. SMALL LOSS OF COOLANT ACCIDENT
   (pipe rupture less than 2-inch including leakage in reactor coolant pump seals and power operated relief valves)
4. LEAKAGE TO SECONDARY COOLANT
5. LOSS OF REACTOR COOLANT FLOW
6. LOSS OF FEEDWATER FLOW
7. PARTIAL LOSS OF STEAM FLOW
8. TURBINE TRIP
9. REACTOR TRIP
10. STEAM RELEASE INSIDE CONTAINMENT
11. STEAM RELEASE (DEMAND) OUTSIDE CONTAINMENT
12. CORE POWER INCREASE
13. LOSS OF OFFSITE POWER
14. LOSS OF COMPONENT COOLING

2.1.3 Scope of Systems

The basic system functions are necessary to avoid core melt and, failing that, to minimize the chance of offsite release. Unique combinations of the following Indian Point-3 systems can provide the needed functions for particular accident sequences. Typical PRA efforts in the past have concentrated heavily on individual front-line systems. A recent LLNL study [18] demonstrated that detailed studies of support systems are an essential part of any SI effort. As a minimum, the following support systems were included since it was known that they are widely required and potentially involved [18] in systems interactions:

1. Service Water
2. Component Cooling
3. Ac and dc Electrical Power and dc Vital Control
4. Instrumentation and Control
5. Lubrication and Control Oil
6. Safety Injection Actuation.

In addition, LERs have indicated that these support systems may contribute to some important Systems Interactions.

The systems that directly perform a vital safety function are called front-line systems and are listed in Table 2-2 according to safety function [21]. Notice that the last safety function (containment integrity) has numerous associated systems that do not appear as associated front-line systems for other safety functions.

Table 2-2
SAFETY FUNCTIONS

Function	Associated Frontline Systems for IP-3
1. Maintenance of Reactor Coolant Pressure Boundary	Safety Injection Chemical Volume & Control Reactor Coolant & Pressurizing
2. Removal of Decay Heat	Safety Injection Residual Heat Removal Reactor Coolant Auxiliary Feedwater
3. Maintain Reactor Subcriticality	Safety Injection Chemical Volume & Control Residual Heat Removal Auxiliary Feedwater Rod Control Boiler Feedwater Reactor Protection
4. Protect Containment Integrity	Residual Heat Removal Safety Injection Containment Spray Containment Recirculation Containment Isolation Hydrogen Recombiner Containment Fan Coolers

By excluding the fourth safety function from primary emphasis, the choice was made by the NRC to concentrate on core damage as opposed to accident release mitigation scenarios. The systems selected for our assessment are listed in Table 2-3. It should be noted that the selection of subsystems which were included in the study were not arbitrary and in fact result from the basic DMA modeling procedure. That is, required support subsystems are identified as the front-line system components are modeled. As these support subsystems are modeled, additional support subsystems are identified.

Table 2-3

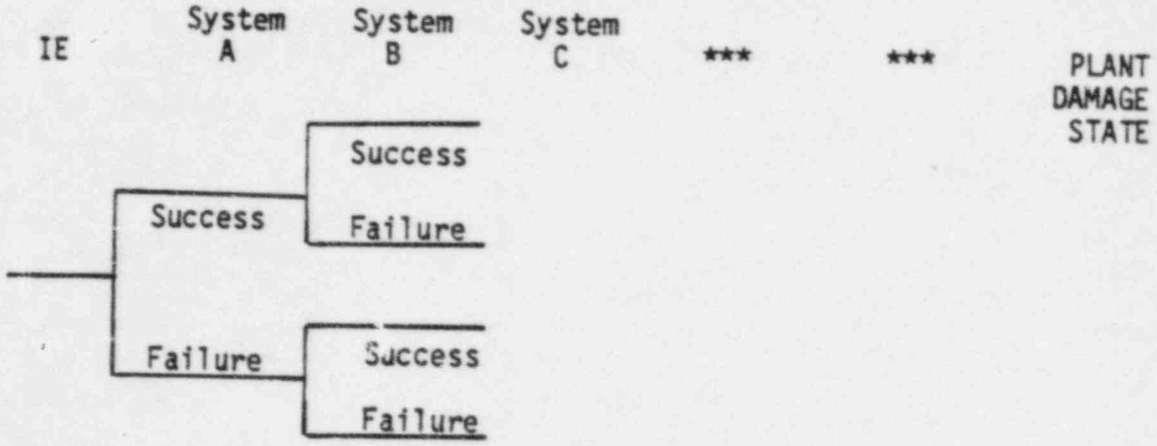
SELECTED SYSTEMS

FRONTLINE:	Safety Injection/Residual Heat Removal
	(1) High Pressure Injection
	(2) Low Pressure Injection
	(3) Recirculation
	Reactor Coolant
	(4) RCP Seals
	(5) PORV and Pressurizer
	(6) Chemical & Volume Control
	Feedwater
	(7) Auxiliary Feedwater
	(8) Boiler Feedwater
SUPPORT:	(9) Instrument Air
	(10) Service Water
	(11) Component Cooling
	(12) Lubrication
	(13) Ac and dc Power
	(14) Dc Vital Control
	(15) Instrumentation and Control
	(16) Safety Injection Actuation
	(17) Feedwater Actuation
	(18) Feedwater Isolation
	(19) Control Oil

2.1.4 Scope of System Combination

How does the initiating event propagate through the plant? The most useful tool for systematically evaluating this question is the event tree diagram. Figure 2-1 illustrates a generalized event tree structure. At the left we identify the initiating event and then ask, "Does system A work or not?" Thus the tree branches at this point, the upper branch representing "system A works" and the lower "system A fails." At system B there is another branching, and so on.

Figure 2-1
GENERALIZED EVENT TREE DIAGRAM



Each path through the tree thus represents a "scenario" -- an envisioned sequence of events beginning with the specified initiating event and leading to a specific "plant damage state."

An earlier safety study of IP-3 (IPSS) Ref. 23 presented event trees for major accident sequences. That study was reviewed by SANDIA[24] and LLNL. The procedure for selecting an accident sequence for DMA through event tree analysis is similar to that of the IPSS approach. The appropriate methodology normally used in the DMA approach is presented in Appendix A.

For this IP-3 systems interaction study, however, resource and scope limitations required us to take certain abbreviating measures. The current study is limited to a portion of the IP-3 plant event trees specified by the systems previously identified in Table 2-3.

The list of system combinations selected by the NRC in conjunction with BNL and LLNL for analysis is compiled in Table 2-4.

In system combinations, 1, 2, 9, and 10, we considered systems interactions that prevented the ECCS (safety injection or recirculation) from responding to a LOCA. In system combinations 3, 4, 7, and 8, we searched for a systems interaction which would both cause the LOCA and prevent a response. For example, in system combination 4 we attempted to find if there was a systems interaction which could cause a reactor coolant pump seal failure and causing a LOCA and also prevent safety injection. (There was!)

In system combinations 5 and 6, we attempted to determine if either loss of offsite power or turbine trip could defeat both the main and auxiliary feedwater systems.

The systems and dependencies which were included in this study were jointly selected by the study teams (BNL and LLNL) and the NRC, and are shown in Table 2-5. The first 19 of these are hardware systems. In this group a system's interaction might arise via a shared component. The

Table 2-4.
SYSTEM COMBINATIONS

System Combination Identifier	Description of System Combination
1. S_1D_i	Loss of low pressure injection during medium LOCA
2. S_1U_i	Loss of high pressure injection during medium LOCA
3. $S_2(Q)U_i$	Loss of high pressure injection during PORV LOCA
4. $S_2(P)U_i$	Loss of high pressure injection during RCP seal LOCA
5. (TT)ML	Turbine Trip with loss of all feedwater
6. (LOOP)ML	Loss of offsite power with loss of all feedwater
7. $S_2(P)$ML	RCP seal LOCA with loss of all feedwater
8. $S_2(Q)$ML	PORV LOCA with loss of all feedwater
9. AR	Loss of recirculation during recirculation phase of large LOCA
10. $S_1U_iD_i$	Loss of all injection during medium LOCA

Identifier key for System Combinations

U_i	= High Pressure Injection During Injection Phase
D_i	= Low Pressure Injection During Injection Phase
R	= Recirculation Cooling During Recirculation Phase
$S_2(P)$	= Small LOCA (RCP Seals induced)
$S_2(Q)$	= Small LOCA (PORV induced)
S_1	= Medium LOCA (2" - 6" rupture)
A	= Large LOCA (>6" rupture)
M	= Boiler Feedwater
L	= Auxiliary Feedwater
TT	= Turbine Trip
LOOP	= Loss of Offsite Power

Table 2-5

Summary of Systems and Dependency Types
Included in the Study Scope

FRONT-LINE:	(1)	High Pressure Injection	Included
	(2)	Low Pressure Injection/Accumulators	Included
	(3)	Recirculation	Included
	(4)	RCP Seals	Included
	(5)	PORV and Pressurizer	Included
	(6)	Chemical Volume & Control	Included
	(7)	Auxiliary Feedwater	Included
	(8)	Boiler Feedwater	Included
SUPPORT:	(9)	Instrument Air	Included
	(10)	Service Water	Included
	(11)	Component Cooling	Included
	(12)	Lubrication	Included
	(13)	Ac and dc Power	Included
	(14)	Dc Vital Control	Included
	(15)	Instrumentation and Control	Included
	(16)	Safety Injection Actuation	Included
	(17)	Feedwater Actuation	Included
	(18)	Feedwater Isolation	Included
	(19)	Control Oil	Included
OPERATOR DEPENDENCY	(20)	Random Human Error Prior to Accident	Included
	(21)	Mitigation by Operator According to Procedure	Included
	(22)	Systematic Diagnosis Error	Excluded
	(23)	Coordinated Incorrect Action	Excluded
LOCATION	(24)	General Location Vulnerability	Included
	(25)	Vulnerability to Fire	Included
	(26)	Vulnerability to Flood	Included
	(27)	Vulnerability to Steam	Included
OTHER	(28)	Common Maintenance	Partially Included
	(29)	Common Manufacturer	Excluded

second group (20-23) considered effects introduced by the human operators of the safety systems. We explicitly considered the effects of human errors prior to the accident by including an unavailability term in the probability data base. This term attempted to capture the probability (given maintenance and inspection policies) that a component would be out of service (when needed) due to a human error. One example of this type of unavailability would be the misalignment of a manually set valve in the service water system. Human operators can also affect the reliability of the safety system during the accident. We also considered the effects of human errors on the failure probability of the system during the incident. The result of this analysis is broken out as a special case in Table 1-1.

2.1.5 Scope of Location Analysis

A "location" is of concern only when the effects which propagate through that location to safety equipment are considered. For example, a flood in a location would not damage piping which passed through that location, but could disable any electrical components in the location. In this DMA we assigned "location types" to each component. That is, a pump in location L would be in a location susceptable to flood, fire, and steam whereas a pipe in the same physical location would not be susceptable to any of these. The adjacency of the various types of locations depends on their type and on the specific mitigator incorporated to limit effects propagation. For example, two locations might be adjacent for the propagation of fire, but not for the propagation of flood. The table below lists some of the effects which could be propagated from location to location and both passive and active mitigators for these effects.

Table 2-6 Location Effects and Potential Mitigators

LOCATION EFFECT	MITIGATOR	
	Passive	Active
1. Fire, Extreme Heat	Fire Walls, Doors	Extinguishers
2. Flood (Water)	Dams, Drains, Walls	Pumps
3. Radiation	Radiation Shields, Radiation Tolerant Components	
4. Impact, Missiles	Missile Barriers, Robust components	
5. Hostile Environment (for humans)	Radiation Shields	HVAC, Protective Gear
6. Steam	Walls	

The effects listed in the above table are not necessarily disjoint. For example, a fire might destroy equipment and also make the environment hostile to humans. These effects also are not necessarily symmetric. That is, an effect which might make the environment hostile to a human might not effect equipment. The propagation of each of the effects must be considered in the context of the actual physical layout of the system being modeled.

The first location effect modeled was that of fire propagation. A fire location node has been assigned to each component in the digraph. The pump room was considered small enough to be treated as one location for the purpose of the analysis of fire propagation. Pipes have been considered to be immune to the effects of fires since they contain no flammable material and are also unlikely to rupture. Thus, there are no connections from fire locations into pipes. On the other hand, pumps, controllers, power wiring, and control wiring have been assumed to be vulnerable to a fire, hence they are connected from their fire locations by an unidirectional edge.

Modeling the effects of flooding is similar to fire.

In this study, we have modeled potential location vulnerabilities, but we have not modeled initiators such as the source of a flood or the cause of a fire.

2.1.6 Scope of Operator Action and Procedures

Scope of Human Intervention Modeling

This model contains nodes for operators who can act beneficially and detrimentally. Beneficial operators generally succeed by backing up failed automatic hardware. They fail by doing nothing; by an act of omission. Detrimental operators degrade system operation by directly affecting a specific component. They cause failure by taking such an action; by act of commission.

Beneficial Operator Intervention

The systems modeled in this study have the ability to succeed with no human intervention. This automatic mode of operation is generally the normal mode (with the exception of the safety injection recirculation phase), however, should hardware failures prevent successful automatic response, credit has been given for potental operator action.

In general, wherever an automatic system can act, an operator can back it up. Many examples of this exist in the automatic safety injection actuation logic. Every component requiring an S.I. signal to initiate a change of state has operator nodes (prefix OPR-) connected to the proper manual actuation hardware in the component control circuitry. Thus, the operator is modeled as redundant to the automatic signal. Operators are also allowed to enable new fluid flowpaths to circumvent a blockage in the normal flowpath. An example of this is in the High Pressure Safety Injection System and is described in Section 2.3.1. No operators are allowed to take actions for controls which are in containment.

Detrimental Operator Action

Allowance has been made for operator errors. These actions constitute acts of commission. In theory, any component in the system could be degraded through such an act, but for the purposes of this study, only manually activated hardware that is accessible (not in a hostile environment) was considered to be susceptable to these errors of commission. Thus, items excluded were check valves, hardware within containment, pipes, and passive electrical hardware. Items included are all externally controllable valves (motor operated valves, gate valves, globe valves, etc.), pumps, electrical breakers, and switches, with controls outside of containment. Operators were not allowed to disassemble anything or, in any way, change the original connectivity of the plant.

2.1.7 Scope of Electrical Analysis

Since the electrical system interacts with all other plant systems, extensive effort went into the electrical model. An electrical block model, where failure of a component is equivalent to an open circuit, was constructed starting with the three 6900 V power sources: offsite power via the station aux transformer, onsite power via the unit aux transformer, and gas turbine backup via the 13.8 kV substation. The model includes the 6900 V system, 480 V system, diesel generators and support systems, 129 V dc system, and 118 V ac instrument bus system.

An electrical break model overlays the block model. In the break model, components fail by a short circuit to ground, and coupled with the failure of mitigators such as breakers failing to trip, the short circuit failure may propagate upstream as well as downstream. The break model includes the 480 V system with diesel generators (excluding support systems), the 129 V dc system, and the unit models for breakers.

Location analysis consisted of identifying common locations for groups of electrical components. Then if a particular location fails, all components in that location fail. Initiators for these postulated location failures were not specified.

2.1.8 Scope of Timing Analysis

The DMA model used for this systems interaction study was quasi-static. That is, detailed timing and sequencing was not accounted for in the model. Some timing analysis was, however, built into the model by the use of switches which prevented failures from propagating until a specific time. To perform an analysis before a specified time, the switches were turned off. To perform analysis valid after this time, the switches were turned on. An example of the use of this type of time switch was in the fuel supply to the diesel generators. For a short time after diesel start, the diesels can draw fuel from their day tanks, but after a longer time the tanks must be refilled. Thus in the early time analysis, the switches between the day tanks and storage tanks were turned off, preventing any failure effects upstream from the day tank from propagating into the diesels. For the long time analysis, the switches were turned on, allowing upstream failures to propagate.

The timing analysis in this study consisted of three steps:

(1) Identification of hardware whose failure will propagate only after a time delay,

(2) Categorization of time delays as either short term (10's of minutes) or long term, (hours)

(3) Creation of a model making it possible to restrict long-term delay failures to the same time frame in which operators are able to act beneficially.

Time delays due to human actions were excluded from the analysis except as per Step 3 above.

2.1.8.1 Identification of Time Delays

Through the course of modeling, the analysts identified 31 components requiring timing consideration. The components all have one common characteristic: each is associated with storage hardware which serves to buffer the failure of a component from the rest of the system. There were four kinds of stored quantities: electrical charge, pressure, fuel (chemical energy), and capacity to cool. An example of electrical-charge storage hardware is a battery. If the charger feeding a battery fails, its failure will not propagate through the battery until the battery drains. Thus, the charger is buffered from battery and downstream components for an amount of time equal to the discharge time of the battery. Similarly, those components which fill or "charge" a pressure tank or fuel tank are also buffered until the tanks are depleted. The final stored quantity, the capacity to cool, is generated by transfer of thermal energy to a heat sink. The heat sink is often composed of at least two parts; (1) for example mass of a pump requiring cooling, and (2) water flowing through a heat exchanger which transfers the heat to the ultimate heat sink, the Hudson River. Thus, loss of cooling water flow will cause the pump to fail but only after a significant time delay.

2.1.8.2 Categorization of Time Delays

There is much uncertainty about the magnitude of the various time delays. It can be difficult to measure such a duration since the availability of a stored quantity is a function of not only its initial conditions and usage but also of how much the storage "vessel" leaks and its use. Decay rates, due to loss of battery charge, tank pressure, and capacity to cool, are often exponential. The leakage factor can dominate assessment of amount stored since the vessels are, in general, assumed to be charged at T_0. Very little information existed to quantify the time delays. After discussion with the IP-3 operator, the delays were determined to fall into two broad time domains: short term (or the order of magnitude of 10 minutes) and long term (at least an order of magnitude longer than short term). Of the 31 time delay components, 16 were short term and 15 were long term.

2.2 Systems Descriptions

The systems selected for analysis were identified in section 2.1.3. In this Section, we provide an overview of the Indian Point-3 plant followed by descriptions of the selected front-line and support systems. Emphasis in these system descriptions is on aspects of each system which have a bearing on the DMA system models. The material presented in these system descriptions closely follows information contained in references [22-24].

2.2.1 General Description* of Indian Point-3

The Indian Point-3 power plant produces about 965 electrical megawatts of power. The Nuclear Steam Supply System (NSSS) consists of a reactor and four closed reactor coolant loops connected in parallel to the reactor vessel. Each loop contains a reactor coolant pump and a steam generator. The NSSS also contains an electrically heated pressurizer and certain auxiliary systems.

High pressure water circulates through the reactor core to remove the heat generated by the nuclear chain reaction. The heated water exits from the reactor vessel and passes via the coolant loop piping to the steam generators. Here it gives up its heat to the feedwater in producing steam for the turbine generator. The cycle is completed when the primary water is pumped back from the steam generator to the reactor vessel. The entire reactor coolant system is composed of leaktight components to ensure that primary coolant radioactivity is confined to the system.

Front-line safety systems that are potentially important in the event of failure of the primary cooling system include the high and low pressure safety injection systems, recirculation systems, the pressure operated relief valve system, the reactor coolant pump seal system, and the chemical and volume control system.

At the steam generators, thermal energy is transferred from the primary cooling system to the secondary cooling system. The secondary cooling system consists of the boiler feedwater and condensate system, the main steam system, and the turbine generator/condenser system.

The condensate and feedwater systems provide water from condensed steam as feed to the secondary side of the steam generators. The main steam system transports thermal energy from the steam generators to the turbine generator where thermal-mechanical-electrical energy conversion takes place.

Front-line safety systems important in the secondary cooling system include the main and auxiliary feedwater systems.

There are several key support systems that are potentially important in maintaining the ability of the front-line systems to operate properly in the event of an incident. Included among these are: the safety injection

* Piping and Instrumentation Drawings and Schematics of systems can be found in Appendix B.

actuation system, the electrical power system, the component cooling and service water systems, the instrument air system, and the lube oil system.

The following sections will describe the individual systems included in this study.

2.2.2 Safety Injection System*

The Safety Injection System Provides emergency core cooling and inserts negative reactivity into the RCS in the event of a Loss of Coolant Accident, a steam generator tube rupture, or a steam line break accident. The system operates in four modes:

(1) High Pressure Injection
(2) High Pressure Recirculation
(3) Low Pressure Injection/Accumulator Injection
(4) Low Pressure Recirculation

2.2.3 High Pressure Safety Injection

The High Pressure Safety Injection System (HPSIS) is designed to provide emergency core cooling in the event of a small or medium LOCA. High pressure flow is required since the depressurization of the RCS is slow for small and some medium sizebreaks. The core cooling process involves injecting borated water from the Boron Injection Tank (BIT) and from the Refueling Water Storage Tank (RWST) with pressurization provided by the Safety Injection Pumps (SIP).

High pressure injection is automatically initiated by the following signals:

1. Low pressurizer pressure
2. High containment pressure
3. High differential pressure between any two steam generators
4. High steam flow in any two of the four steam lines coincident with low T_{avg} or low steam pressure.
5. High-High containment pressure

A safety injection signal starts the three SI pumps and opens the valves which had isolated the BIT. The three pumps deliver borated water to two separate discharge headers (header A and header B) which then flow to each of the four Reactor Coolant System (RCS) cold legs. Header A provides boron injection through the BIT, whereas Header B bypasses the BIT. Each of the four cold leg paths contains a normally open motor-operated valve. Some of these valves receive an SI signal to open (MOV856-C,E,H,K). Injection through two of the four injection paths is needed in response to a medium LOCA and injection through one path is required for a small LOCA.

Approximately 350,000 gallons of water are available from the RWST for delivery during safety injection. This water is borated to a maximum concentration of about 1.4 weight percent boric acid. The RWST is prevented from freezing by steam heat. The water flows from the RWST to

* Piping and instrumentation drawings and their corresponding digraph can be found in Appendix B. Computer input corresponding to the digraphs can be found in Appendix C.

a header where it branches off to a path including valves MOV1810 and VC847. If this path is blocked, the next header in line has an alternate path which can be enabled by an operator opening VGA898.

These two paths terminate at a header consisting of three inputs to the three pumps which lead to the two outputs at the two discharge headers.

The three safety injection pumps are horizontal centrifugal pumps driven by electric motors. With two or three diesel generators functioning, two out of the three SIPs are powered. The pumps are provided with a bypass line back to the RWST in order to provide a recirculation capability in the event that a discharge path is blocked.

The SI pump bearings are cooled by water from the component cooling system. This water is circulated by mini-pumps attached to the main SI pump shaft.

Safety Injection Pump #32 supplies coolant to either header via check valves, whereas pumps #31 and #33 supply only one header each. This arrangement provides sufficient flow in the event of a small LOCA and two failed pumps, or a medium LOCA and one failed pump.

Pumps #31 and #32 provide a direct water supply to the four cold legs of the core through header A. Header B is supplied by pumps #32 and #33 which route water through the BIT.

The BIT is always kept 100% full. This is accomplished by recirculating the water in the tank through the boric acid tanks whenever the plant is at power. The boric acid tanks are at a higher elevation than the BIT and gravity is used to keep the BIT full. There are two sets of parallel valves, which isolate the BIT during normal operation, that are opened by the safety injection signal. During the low pressure recirculation mode these valves are shut again to isolate the BIT.

The BIT is heated by redundant electric heaters and redundant heat tracing to keep the solution temperature above the solubility limit of 130°F at a concentration of 20,000 ppm.

2.2.4 High Pressure Recirculation

The High Pressure Recirculation System (HPREC) is used following safety injection for long term core cooling. Water is drawn out of the recirculation sump by the recirculation pumps and fed into the safety injection pumps. The water is then fed into the RCS cold legs in the same manner as in the injection phase with the HPSIS pumps. Back-up recirculation capability is provided by the Residual Heat Removal (RHR) pumps which draw from the containment sump.

2.2.5 Low Pressure Safety Injection System/Accumulator Injection

The low pressure portion of the Safety Injection System (LPSIS) is designed to rapidly reflood the reactor core following a large or medium LOCA and subsequent blowdown of the primary coolant. The LPSIS is composed of two subsystems, low pressure injection from the RWST and the safety injection tanks (accumulators). The former is an active subsystem; that is, it requires a control signal and electric power to operate; the latter is totally passive, requiring no signal or external power source.

2.2.5.1 Low Pressure Injection

The RHR Pumps are used in the Low Pressure Safety Injection mode. Because of the presence of check valve 881, the system is normally aligned for safety injection, as well as for decay heat removal. A Safety Injection Actuation Signal (SIAS) opens the Residual Heat Loop Discharge Stop Valves 899A, 899B, 746, and 747, starts one of the RHR Pumps, and in coincidence with a loss of offsite power, starts two of the diesel generators. There is approximately a 34 second delay between the receipt of SIAS and full RHR pump operation.

In the safety injection mode the RHR pumps take suction from the Refueling Water Storage Tank. Since the water is at ambient temperature, component cooling is not required and the Component Cooling Water (CCW) pumps may be secured to reduce the electrical load on the 480 V ac diesel generator buses. The design operating pressure of these pumps is only 600 psig. Thus, the safety injection mode of the RHR system is initially most effective for a large pipe break where the primary system rapidly depressurizes from 2235 psig to less than 600 psig. In the event of a small or medium LOCA where low pressure injection is initially unusable, the RHR Pumps can be used as boosters for the low flow (400 gpm) High Pressure (1700 psig) Safety Injection Pumps (HPSIPs) by opening either or both of the two High Head Recirculation Stop Valves (MOV 888A or 888B).

As borated water from the RWST is injected into the core, primary coolant flows out of the break and collects in the two sumps located in the lower level of the Containment Building. When the inventory of the RWST reaches the low level alarm, the operator must realign the system for recirculation. The shift from the injection to the recirculation pha in the case of a large rupture, occurs about 20 minutes after the sta of the accident.

Successful operation of the RHR System in the injection mode requires that at least two of the four injection legs deliver flow to the core for a large LOCA. Injection through one leg is necessary in response to a medium LOCA if high pressure injection is unavailable.

2.2.5.2 Accumulator Injection

The four accumulators are designed to inject emergency coolant into each of the cold legs whenever the primary pressure falls below 650 psig. Each tank contains 700 ft^3 of borated water driven by a nitrogen gas cover. The tanks are filled from the Refueling Water Storage Tank using the High Pressure Safety Injection (HPSI) pumps. The cover gas is supplied by a Nitrogen System. During normal plant operation the accumulators are isolated from the HPSI pumps and the nitrogen system by normally open, fail close, pneumatically controlled gate valves (890A-D,891A-D). Redundant and independent level and pressure indications are displayed in the Control Room for each accumulator. The accumulator tanks are not rated at primary plant pressure. Pressure relief valves are installed on top of each accumulator tank to prevent overpressurization. These valves are set to open at 700 psig.

The accumulators are isolated from the Reactor Coolant System (RCS) by check valves (895A-D) in the discharge path. The 2235 psig primary plant pressure tightly seats these check valves under normal plant conditions. These seats leak somewhat and fluid must occasionally be drained to the Waste Disposal System through normally shut pneumatically controlled valves (896A-D).

Normally open accumulator discharge stop valves (MOV 894A-D) are installed upstream of the accumulator discharge check valves for several reasons. In the event of significant check valve leakage, these valves may be shut; however, a safety injection actuation signal will automatically reopen them, though accumulators isolated in this manner are no longer strictly passive components.

These accumulator discharge valves are also closed during plant heat up and cool down to inhibit undesirable accumulator actuation. In this mode the operator must also set keyed switches to block the SIAS.

2.2.6 Low Pressure Recirculation

The changeover from the injection to the recirculation phase requires operator action and is initiated when the RWST reaches the low level alarm point. The operator has a choice of two sumps, both located in the containment building, from which recirculation water may be drawn. Two pumps take a suction from each sump; however, only one of these four pumps is required to initiate recirculation flow.

The preferred source is the Recirculation Sump, primarily because the recirculation path is completely enclosed by the containment building, precluding the possibility of releasing fission products contained in the sump water to the atmosphere. Two 350 hp, 3000 gpm recirculation pumps are located just above the Recirculation Sump. They are cooled by CCW. In recirculation mode, CCW must also be circulated through the Residual Heat Exchangers.

The two recirculation pumps are connected by a crosstie piping network to the parallel Recirculation Sump Stop Valves (MOV 1802A and 1802B). At least one of these two motor operated valves must be opened by the operator in order for the sump water to reach the Residual Heat Exchangers. The two valves are actuated independently and are powered through separate motor control centers.

The alternate recirculation water source is the Containment Sump. The use of this source is less desirable because part of the recirculation pathway is in the primary auxiliary building, allowing the possibility of radioactive fission product releases to the atmosphere through leaky valve and pump seals. Recirculation from the containment sump is initiated by opening the Containment Sump Stop Valves (MOV885A-B). The RWST Recirculation Stop Valve (MOV883) must be shut in order to prevent the release of fission products to the atmosphere via the RWST. The Residual Pump Suction Stop Valve (MOV882) should also be shut to doubly isolate (with check valve 881) the RWST. An additional level of isolation can be set by shutting the hand operated gate valve (846) on the RWST discharge line. These valves should be closed immediately after recirculation flow is established.

The recirculation phase of residual heat removal is a long term evolution. In a major accident the containment building will be a highly contaminated radiological exclusion area. Personnel will be unable to enter to perform maintenance or cleanup operations. The Primary Auxiliary Building (PAB) may also be a high radiation area if primary coolant has been pumped from the Containment Building. The ability of personnel to operate or repair equipment in the PAB may be affected, especially in the vicinity of the recirculation piping.

2.2.7 Safety Injection Actuation System

The safeguards actuation system receives signals from various primary and secondary plant sensors, processes this input through logic matrices, and sends actuation signals to Engineered Safeguards System (ESS) equipment, based upon plant conditions. The ESS equipment serves to limit damage in the event of pipe rupture in either the Reactor Coolant System or the secondary systems (steam, feedwater, or steam generators).

The signals that the Safety Injection Actuation System receives and the actions that result are presented below:

1. High Steam Line Flow in Conjunction with low T_{ave} or Low Steam Generator Pressure.

This condition is indicative of a steam break downstream of the main steam isolation valves (MSIV). Indications of a steam break are: high steam flow (to generate a signal, two of the four steam lines must indicate high steam flow) in conjunction with (a) low T_{ave} (two of four sensors), or (b) low steam line pressure (two of four sensors). This signal initiates steam line isolation (closure of all four MSIVs) in addition to initiating automatic safety injection.

To generate the high steam line flow signal, a comparison circuit is used to develop a varying setpoint signal based on turbine first stage pressure. Actual steam flow is compared with the programmed setpoint, and a trip signal is generated when actual steam flow exceeds the setpoint. To allow for startup, steam dump, and atmospheric relief valve operation when turbine first stage pressure is not a true indication of actual steam flow, the high steam line flow signal must be in coincidence with either a low T_{ave} signal (sensed by primary loop resistance temperature detectors) generated by a two or four sensing network, or a low steam generator pressure signal generated by two of four pressure sensing networks.

2. Steam Line Differential Pressure.

This condition indicates a steam break upstream of the MSIVs or a large feedwater line break. A break in this location results in the closure of the non-return check valve (located in each steam line). Steam pressure upstream of the check valve now decreases as the associated steam generator feeds the break directly. A comparison network is used in which this steam pressure is compared to the pressure in two of the three remaining intact steam generators. When the pressure in the steam generator feeding the break decreases to the set value below the other two steam pressures, an automatic safety injection signal is generated.

3. Low Pressurizer Pressure.

The pressurizer acts as a surge tank for the reactor coolant system. Pressurizer heaters cycle on and off to maintain RCS pressure within a certain band. Leakage from the RCS in excess of the pressurizer heater and charging pump capability for make up results in a decrease in pressurizer pressure, and consequently RCS pressure. This signal serves to initiate automatic safety injection to protect the core from damage for RCS breaks and excessive leaks. Three channels of pressurizer pressure are monitored and an automatic safety injection signal is generated if any two of the three channels indicate low pressure. This trip is manually blocked by operator action when RCS pressure is below 1,900 psi during a plant shutdown. This block is automatically removed when RCS pressure increases above 1,900 psi and operator action would be required to reinitiate the block if it is required.

4. High Containment Pressure.

In the event of a break in the RCS, or a steam line break inside the containment building, pressure inside the containment building would increase. The rate of the increase is dependent upon the size of the break. Containment pressure is monitored by three pressure transmitters located outside of the containment building. When containment pressure exceeds the setpoint value in two of the three transmitter channels, an automatic safety injection signal is generated.

5. High-High Containment Pressure

A high-high containment pressure is indicative of a large loss of coolant accident or a major steam line break inside the containment building. Containment pressure is monitored by six pressure transmitters located outside the containment building in the piping penetration area. The output of these transmitters is divided into two groups of three. When containment pressure exceeds the high-high setpoint, a signal is developed which energizes the relays associated with that channel. Two out of three channels in both groups are required to initiate automatic containment spray actuation. In addition to the automatic containment spray signal, a main steam line isolation signal is sent to close the MSIVs and an automatic safety injection signal is developed.

The tripping of any of the input channels described above is indicated on supervisory panel "SO" in the control room. In addition the following channel trips listed in Table 2-7 will result in alarms at the locations noted.

Table 2-7
CHANNEL TRIPS

Tripped Channels	Alarm	Location
1. High Steam Line Flow	High Steam Line Flow SI	Safeguards Panel
2. Steam Line Differential Pressure	Steam Line ΔP SI	Safeguards Panel
3. Pressurizer Pressure	Pressurizer Lo-Press Channel Trip	RCS Supervisory Panel
4. High Containment Pressure	Hi Containment Pressure SI Channel Trip	Safeguards Panel
5. High-High Containment Pressure	Pressure (Spray) Channel Channel Trip	No Alarm (High Indicated)

NOTE: All of the trip relays associated with the instrumentation discussed above are "de-energize to trip." That is, loss of power to an instrument channel causes the relays associated with that channel to trip, which results in one of the trip signals required for safety injection actuation.

6. Manual Initiation Signals.

In addition to the automatic signals described above, safety injection or containment spray may be initiated by the operators in the control room.

Manual safety injection is accomplished using the red manual safety injection pushbuttons on panel SB2 in the control room. Pressing one of these pushbuttons initiates the minimum required ESS equipment. Both pushbuttons must be depressed to initiate all ESS equipment. Manual spray actuation is accomplished by depressing both red manual spray actuation pushbuttons on safeguards panel SB1 in the control room. Depressing one spray actuation pushbutton initiates one train of spray equipment.

There are two channels of actuation logic in the safeguards actuation system. These logic channels require dc power for proper operation.

Each logic channel contains seven master relay-slave relay sets. These relay sets are:

- o SI Automatic Actuation
- o SI Manual Actuation
- o Containment Ventilation Actuation
- o Containment Isolation Phase A
- o Containment Isolation Phase B
- o Containment Spray Actuation

The master relays are special relays which contain operating and reset coils. The master relay is normally de-energized. When the proper logic matrix is made up, the operating coil will be energized by auxiliary contacts and command the various safeguards equipment to operate. The master relays, via a mechanical latching mechanism, and the slave relays will remain in the actuated position until the master relay is reset (reset coil is energized). The reset signal is applied through the manual reset pushbuttons.

The safeguards logic relays are located in relay racks behind the reactor trip logic relay panels. These relays are arranged in matrices which develop the necessary logic for safeguards initiation. Each logic relay is fed from a safeguards actuation bi-stable located at the analog racks. The signal from each analog bi-stable feeds a safeguards logic relay in each safety injection channel.

2.2.8 Feedwater Systems

The nuclear reactor at Indian Point Unit 3 produces 965 electric megawatts of power. Cooling of the reactor core is provided by four independent primary cooling loops. Each of these loops circulates pressurized, superheated water from the reactor vessel to a steam generator. In the steam generator, the heated primary water is passed through a bundle of U-shaped tubing. This tubing is immersed in water in the lower half of the steam generator. As the heated primary water passes through the tubing, it exchanges heat with the cooler water on the outside of the tubes never coming in direct contract with that cooling water. After passing through the steam generator tubes, the primary water is returned to the reactor pressure vessel to carry away more heat.

The four steam generators provide the initial sink for the heat produced in the reactor vessel. Heated primary water enters the steam generator from the bottom, passes through a bundle of inverted U-tubes, and then exits the steam generator from the bottom. The inverted U-tube bundle occupies the lower half of the steam generator. This lower half is filled with secondary cooling water. The secondary feedwater enters the shell side of the steams generator through a fill ring. The water is heated by the primary water passing through the U-tube bundle and, eventually, reaches boiling temperature. The steam produced fills the upper half of the steam generator and exits at the top through main steam line.

Once the steam leaves the steam generator, most of it goes directly to the high pressure side of the main turbine. Some steam is drawn off prior to and after this point for use as auxiliary steam in various processes. After performing the mechanical work of driving the turbine, the steam enters the condensate system.

The purpose of the Condensate System is to condense the turbine exhaust steam, remove air from the condensate, and deliver the condensate to the feedwater system. The condensate system consists of three condensers (7,230,000 lbs. of steam/hr capacity, each) taking steam from the turbine and condensing it with cooling water from the circulating water system. The three eight-stage, vertical, pit-type condensate pumps (7860 gpm, each) are rated at 7860 gpm and 1150 ft TDH when operating at 1170 rpm. The pump bearings are lubricated by the pumped liquid. Each pump is driven, through a solid coupling, by a 3000 hp vertical solid shaft induction motor that has an open drip proof enclosure. These pumps are operated by manual controls on the main control board. The pumps take the condensate and discharge it to their air ejectors. From there, the condensate flows to the feedwater heaters via the gland steam condenser.

The only other major component of the condensate system is the condensate storage tank (600,000 gal), which is used primarily for condenser hot well surge and make up. The tank also provides suction for the auxiliary feedwater pumps. For that reason, the tank has an assured reserve of 360,000 gallons of water.

The Main Feedwater System takes the condensate from the condensers and returns it to the steam generators as secondary cooling water. The system consists of 15 feedwater heaters, taking discharge from the condensate pumps and delivering it to the two steam driven main feedwater pumps (15,300 gpm at 1830 ft TDH, each). Heating in the feedwater heaters is provided by the auxiliary steam supply system, using steam taken from various stages of the turbine generator. The drainage from the heaters flows to the heater drain tank where it is then pumped by the heater drain pumps tc the intake of the main feedwater pumps.

There are two main feedwater pumps that provide feedwater for the four steam generators. The discharge from each feedwater pump passes through one heating stage before it enters the steam generators. The main feedwater pumps, also referred to as the boiler feedwater pumps, are single-stage horizontal centrifugal pumps with barrel casings. Each pump is rated at 15,300 gpm and 1830 ft TDH when operating at 4875 rpm. Seal water injection is used for shaft sealing. Bearing lubrication for both the pump and its turbine drive is accomplished by an integral lubricating oil system mounted on the pump base. Normal circulation for the lubricating oil system is provided by two motor-driven pumps. The lubricating oil system also includes a reservoir and a cooler.

Each main feedwater pump is driven, through a flexible gear type coupling, by an 8350 hp horizontal steam turbine using steam from the discharge of the three reheater moisture separators. The main feedwater pumps are operated automatically by the feed control system. Manual controls are also provided on the main control board for remote operation and testing during normal operation. During normal startup of the plant, the pumps are started locally. A minimum flow control system is provided to ensure that each pump is handling at least a 3000 gpm flow at all times.

The speed of the pump turbines is controlled by the totalized steam flow. When there is low main feedwater pump suction pressure, the pump turbine speed is reduced to prevent excessive pressure in the feedwater piping.

The design loss of main feedwater transients are those caused by:

- o Interruptions of the Main Feedwater System flow due to malfunction in the feedwater or condensate system, and
- o Loss of offsite power or blackout with the consequential shutdown of the main feedwater system pumps, auxiliaries, and controls.

Loss of main feedwater transients are characterized by a rapid reduction in steam generator water levels. This results in a reactor trip, a turbine trip, and auxiliary feedwater actuation by the protection system logic. The reactor power quickly falls to decay heat levels following reactor trip. The steam generator water levels continue to decrease, progressively uncovering the steam generator tubes as decay heat is transferred and discharged in the form of steam through the steam dump valves to the condenser or through the steam generator safety or power-operated relief valves to the atmosphere. The reactor coolant temperature increases as the residual heat, in excess of that dissipated through the steam generators, is absorbed. With increased temperature, the volume of reactor coolant expands and begins filling the pressurizer.

Without the addition of sufficient auxiliary feedwater, further expansion will result in water being discharged through the pressurizer safety and relief valves. If the temperature rise and the resulting volumetric expansion of the safety valve capacities may be exceeded causing (1) over-pressurization of the RCS and/or (2) the continuing loss of fluid from the primary coolant system.

Sufficient auxiliary feedwater is necessary to arrest the decrease in the steam generator water levels, to reverse the rise in reactor coolant temperature, to prevent the pressurizer from filling to a water solid condition, and eventually to establish stable hot standby conditions. Subsequently, a decision may be made to proceed with plant cooldown if the problem cannot be satisfactorily corrected.

The blackout transient differs from a simple loss of main feedwater in that emergency power sources must be relied upon to operate vital equipment. The loss of power to the electric driven condenser circulating water pumps results in a loss of condenser vacuum and condenser dump valves. Hence, steam formed by decay heat is relieved through the steam generator safety valves on the secondary side or the power-operated relief valves on the primary side.

Assuming that the reactor protection system operates to reduce core power level, a total lack of feedwater delivery to the steam generators to remove heat generated by the core would result in the steam generators boiling dry on the order of about 1/2 hour. However, an alternate feedwater supply is provided by the Auxiliary Feedwater System (AFWS). Operation of this alternate feedwater system, in conjunction with steam relief to the atmosphere through safety valves, would result in successful cooling of the core following all transient events involving the interruption and loss of normal RCS heat removal capability. Should the auxiliary feedwater system fail on demand, the time available for the plant operator to restore operation of either the RCS or the AFWS, without risking an excessive loss of RCS coolant from the RCS pressurizer safety and relief valves and, thus, a core melt, would be approximately 1 to 1 1/2 hours.

The Auxiliary Feedwater System provides emergency feedwater to the steam generators in the event of loss of main feedwater. The system consists primarily of one steam turbine driven pump and two electric motor driven pumps. These pumps take suction from the condensate storage tank. The tank has a reserve of 360,000 gallons of water for this specific purpose. This water level is sufficient to provide residual heat removal for 24 hours at hot shutdown conditions.

In the event of the loss of the condensate storage tank water supply, the auxiliary feedwater pumps can take suction from the 1.5 million gallon city water storage tank.

There are two independent loops for auxiliary feedwater delivery to the steam generators. One loop utilizes the two motor driven pumps. Each of the pumps supplies feedwater to two of the four steam generators. Thus, all four steam generators are supplied. The other loop utilizes the turbine driven pump, supplying feedwater to all four steam generators. The capacity of each loop is sufficient to insure that at least two of the four steam generators will not boil dry.

The motor driven pumps are Ingersoll-Rand nine stage horizontal split case centrifugal units, each of which supplies 400 gpm of water at a head of 1350 psi. The pumps have grease lubricated ball bearings. The motor drives are manufactured by Westinghouse Electric Corporation.

The power for the pump motors is taken from 480 V bus 3A for pump No. 31 and from 480V bus 6A for pump No. 33. In the event of complete loss of electric power, power is restored automatically from the diesel generators.

The steam turbine driven auxiliary feedwater pump is a Worthington Corporation horizontal multi-stage centrifugal pump with a capacity of 800 gpm at 1350 psi. The turbine drive for the pump is a Worthington Corporation horizontal axial flow non-condensing unit rated at 970 hp at 3570 rpm. The turbine steam supply is taken from the main steam lines of steam generators No. 32 and No. 33, ahead of the isolation valves. There are two temperature controlled shutoff valves mounted in series in the steam supply line. These valves will close when the temperature reading in the Auxiliary Boiler Feed Pump Room reaches 120°F.

Cooling of the pump thrust bearing and the turbine inboard and outboard bearings is accomplished with water from the pump discharge. The cooling return water is piped to the condensate storage tank. Bearing flow rates and the combined return temperature are indicated locally.

The condensate pumps could potentially be used to deliver water to the steam generators in the event of failure of the condenser vacuum occurs and affects operability of the main feedwater pumps. In this case, action by the plant operator would be needed to depressurize the steam generators. This is necessary because the design of the condensate pumps would not permit water delivery against the high steam pressure conditions (less than or equal to about 1100 psi).

2.2.9 Electric Power System

The primary functions of the electric power system during an accident scenario are to:

- o Provide a reliable electrical power supply to those components whose operation is needed to mitigate any abnormal event affecting the reactor core, its heat removal systems, or systems which could affect the release of radioactivity to the environment.

- Provide a reliable control power supply for the operation of these systems and for the initiation of safeguards systems actuation signals.
- Provide a reliable source of power to instrumentation necessary for monitoring emergency system functions, for monitoring key plant parameters, and for inputs to safeguards systems actuation logic.

A reliable Offsite Power Supply network connected to the station power system through redundant supply paths normally performs these functions. In addition, one onsite gas turbine-generator unit and two additional gas turbine-generator units located at the Buchanan substation may be connected to the station power system through the offsite power supply tielines. Although procedures exist for using the onsite Gas Turbine Unit 1 to power IP-3, the operators to which we spoke were not familiar with them. It is also unclear how long it would take to start and load this turbine.

If all offsite power sources fail, three diesel generators, each capable of supplying 50% of the power requirements of the safeguards systems components, provide independent onsite power generation capabilities.

The dc power system, supplied from four onsite storage batteries, provides power supplies to vital controls and instrumentation and is the primary source of power to all safeguards actuation and reactor protection system circuits.

During normal operation, power is supplied to 6.9 kV buses 1, 2, 3, and 4 from the main generator output through the unit auxiliary transformer. Power is supplied to 6.9 kV buses 5 and 6 from the offsite power grid through the 138 kV substation and the station auxiliary transformer. Following a trip of the main generator, automatic crosstie breakers connect buses 1 and 2 to bus 5 and connect buses 3 and 4 to bus 6, thereby maintaining all six 6.9 kV buses powered from the offsite grid. The redundant source of offsite power from the 13.8 kV substation and gas turbine-generator Unit 1 may be manually connected to buses 5 and 6 only if these buses are de-energized and their normal supply breakers from the station auxiliary transformer are open. Although no essential safeguards components are supplied directly from the 6.9 kV buses, buses 2, 3, 5, and 6 supply power to the 480 V essential power buses 2A, 3A, 5A, 6A, 312* and 313*, through their respective station service transformers.

They also provide power to auxiliary equipment rated at 400 horsepower and above. An overcurrent condition on any of the 6.9 kV buses actuates the associated bus protection lockout relays, which isolate the bus by tripping and locking out the normal supply breaker and the 6.9 kV tie breaker for that bus.

Components rated between 100 and 400 horsepower are supplied directly from the station 480 V Switchgear Buses 2A, 3A, 5A, and 6A. Individual

* These buses were added for an Appendix R upgrade.

loads of 100 horsepower and below are supplied from 480 V motor control centers (MCCs) fed from the 480 V switchgear buses. The normal power supply to each of the 480 V buses is from its associated 6.9 kV bus through a station service transformer. If this normal power source is unavailable, an independent source of emergency onsite power is provided to each of these buses from the three emergency diesel generator units.

The load from the station safeguards systems components are designed to be distributed among the four 480 V switchgear buses in a manner such that, with coincident loss of all offsite power sources and failure of any one of the diesel generators, power will remain available to the minimum number of components needed to mitigate any of the design basis accident scenarios.

If a fault occurs on one of the 480 V switchgear buses, lockout relays are actuated which trip and prevent reclosure of all breakers associated with the bus. The bus lockout relays must be manually reset after the fault is cleared to allow the tripped breakers to be reclosed.

In addition to the normal and emergency power supplies to each of the 480 V switchgear buses, crosstie breakers between buses 2A and 5A and between buses 3A and 6A provide manual interconnections for these buses, and a crosstie breaker between buses 2A and 3A provides automatic interconnection. These crosstie breakers are administratively controlled to remain open during normal unit operation. Breakers 2AT5A and 3AT6A may be closed manually from the control room only if no fault exists on either of the associated buses and one of the buses is de-energized. These breakers trip automatically on any of the following conditions:

- o Bus lockout relay actuation on either associated bus
- o Undervoltage on either associated bus
- o Safety injection signal
- o Overcurrent

Breaker 2AT3A closes automatically when the following interlocks are satisfied:

- o Undervoltage on bus 3A
- o Breaker 3AT6A open
- o Feedbreaker 3A open
- o Diesel output breaker EG1 closed
- o No faults on buses 2A or 3A.

Breaker 2AT3A is tripped only by bus lockout relay or overcurrent relay activation. Besides the four 480 V switchgear buses, two extra 480 V buses were added as part of the Indian Point-3 modifications for emergency shutdown. Buses 312 and 313 are powered from 6900 V Buses 1 and 3, respectively. A manual crosstie also allows these two 480 buses to be connected.

Each of the Emergency Diesel Generators is powered by a 16-cylinder, four-cycle, turbo-charged diesel engine rated at 2,450 horsepower at 900 rpm. The generators are self-excited, three-phase, 60 Hertz, 480 V units rated at 2,188 kVA at 0.8 power factor. The output ratings of each diesel generator unit are 1,750 kW for continuous service and 1,950 kW for a maximum of 2,000 hours. Each unit is capable of supplying sufficient power to maintain the operation of at least 50% of the safeguards systems components required for mitigating any of the design basis accident scenarios analyzed in the Indian Point Unit 3 Final Safety Analysis Report (FSAR).

Each diesel generator receives an automatic starting signal under either of the following conditions:

- o Undervoltage at its associated 480 V bus (diesel generator 31 starts automatically on undervoltage at bus 2A only)
- o Safety injection signal.

However, for a diesel generator to be available for auto starting, the engine starting mode control switch located at the diesel generator control panel in the diesel generator building must be in the "Auto" position. (Two other positions are available: "Off," which prevents the engine from starting, and "Manual," which allows manual starting from the local panel start pushbutton only.) An alarm is received in the control room if the switch is moved from the "Auto" position.

Each diesel generator can attain full speed and voltage within ten seconds and can be fully loaded within 30 seconds from the time of the starting signal. A fast acting electro-hydraulic governor maintains a constant diesel engine speed as load is applied to the unit. The generator output breaker will close automatically to load the diesel generator onto its associated bus only if an undervoltage condition is detected at that bus and the normal bus feed breaker is open. For successful starting or continued operation of the diesel generators, four auxiliary systems are needed: starting air system, the diesel fuel oil transfer system, the station service water system, and 125 VDC control power.

The Indian Point Unit 3 DC Power System consists of four independent battery installations. Each is connected to a dc power panel and is maintained under continuous charge by a self-regulating battery charger. The system is ungrounded, with the positive and negative legs maintained at potentials of approximately 129 volts with respect to ground. Ground detection is provided for each battery division, with a common alarm in the control room.

Three of the dc power panels supply control power to each associated essential ac power division while the fourth dc power panel provides only the normal source of power to ac instrument bus 34. The dc system also supplies power to all safeguards actuation and reactor protection logic matrices. A bus tie breaker is available to connect power panel 31 to power panel 32 in the event of failure of the battery or battery charger for either of these panels. This breaker is administratively controlled to remain open during normal operation and is only permitted to be closed when the plant is in the cold shutdown condition.

Each of the Battery installations is composed of 60 individual lead antimony storage cells that are connected to provide a nominal terminal voltage of 129 VDC. Battery 31 is rated at 1,320 ampere hours, battery 32 is rated at 960 ampere hours, battery 33 is rated at 425 ampere hours, and battery 34 is rated at 440 ampere hours (each at an 8-hours discharge rate). Batteries 31 and 32 are connected to their respective power panels through 800 ampere fuses; battery 33 uses a 600 ampere fuse, and battery 34 has a 600 ampere circuit breaker.

During normal operation, the loads from each of the power panels are supplied from the output of the associated battery charger, which also provides a constant trickle charge to maintain the battery in a fully charged condition. Each of the battery chargers is a silicon-controlled rectifier self-regulating unit cooled by forced air circulation.

All station 480 V loads rated at 100 horsepower and below are supplied from Motor Control Centers powered from the 480 V switchgear buses. All safeguards system motor-operated valves are powered from either MCC 36A or MCC 36B, which remain energized wherever their associated supply buses (5A and 6A, respectively) are energized. The supply breakers to MCCs 36A, 36B, and 36C receive automatic closing signals on any safety injection actuation and may be operated from the Unit 3 control panels. The supply breakers to all other MCCs are operated locally at the 480 V switchgear by manual close and trip pushbuttons.

All instrumentation that monitors vital plant parameters and provide input signals to the reactor protection and safeguards actuation systems is supplied from 118 V AC Instrument Power Buses. Instruments providing redundant input signals to the reactor trip and safety injection logic are supplied from separate buses so that failure of any one bus will not prevent a protection function from actuating or cause an inadvertent trip.

Because these instruments require an extremely stable and reliable source of power, all four instrument buses are normally supplied by static inverters, which convert dc power into a very smooth, noise-free ac power signal. Each inverter is rated at 7.5 kVA with an output voltage of 118 V ac at 60 Hertz. This output will be maintained over a range of input voltage fluctuations from 105 V dc to 140 V dc.

A reserve power supply for each of the instrument buses is provided from 120 V ac lighting bus 32 through a manual transfer switch located at each instrument bus. These transfer switches are provided with mechanical interlocks to prevent both supplies to a given bus from being connected in parallel. The transformer supplying lighting bus 32 is sized such that only one instrument bus may be supplied from the reserve power source at a time. Instrument bus 34 also has its own backup power supply provided by Motor Control Center 36B through a Solatron transformer and controlled by another manual transfer switch located at the transformer in the cable spreading area of the Control Building.

The safeguards actuation, reactor protection, main turbine-generator protection, and offsite tieline fault protection systems provide signals to the station electric power system for the initiation of automatic bus transfer operations, bus load shedding, diesel generator starting, and automatic bus load sequencing under a variety of transient conditions.

Within the system, the ac and dc subsystems are strongly dependent on one another through the ac-powered battery chargers and dc control power supplies to the diesel generators and 6.9 kV and 480 V switchgear.

The control room and local plant operators interface directly with the electric power system for remote and local manual circuit breaker operations and manual operation of the diesel generators. Although the system is designed to automatically provide a reliable source of onsite power during a wide range of anticipated events, these manual operations provide the ability to realign power supply flow paths to compensate for failures of individual components and subsystems. These operator inputs also provide an opportunity for systems interactions.

2.2.10 Chemical and Volume Control System

The Chemical and Volume Control System (CVCS) performs many functions through the various phases of plant conditions. During normal operation it performs 6 functions: 1) provides the required seal water flow for the reactor coolant pump shaft seals, 2) maintains the proper water inventory in the Reactor Coolant System, 3) adjusts the concentration of the chemical neutron absorber for chemical reactivity control, 4) processes reactor coolant effluent for reuse of boric acid and reactor make up water, 5) maintains the proper concentration of corrosion inhibiting chemicals in the reactor coolant, and 6) maintains the reactor coolant and corrosion product activities to within design levels.

The CVCS connects directly into the reactor coolant system. A portion of the high pressure charging flow is injected into the reactor coolant pumps between the thermal barrier and the shaft seal so that the seals are not exposed to high temperature reactor coolant. Part of the flow is the shaft seal leakage flow and the remainder enters the RCS through a labyrinth seal on the pump shaft. Part of the shaft seal injection flow cools the lower radial bearing, and part passes through the seals and is cooled in the seal water heat exchanger, filtered, and returned to the volume control tank.

Seal water injection to the RCS requires a continuous letdown of reactor coolant to maintain the desired inventory. In addition, bleed and feed of reactor coolant is required for removal of impurities and adjustment of boric acid in the reactor coolant.

During plant operation, reactor coolant flows through the letdown line from the reactor coolant loop 1 cold leg on the suction side of the pump and is returned to the same cold leg on the discharge side of the pump via a charging line. An alternate charging connection is provided to the hot leg of loop 2. An excess letdown line is also provided in the discharge side of the reactor coolant pump in loop 1.

Each of the connections to the RCS has an isolation valve located close to the loop piping. In addition, a check valve is located downstream of each charging line isolation valve. Reactor coolant entering the CVCS flows through the shell side of the regenerative heat exchanger, where its temperature is reduced. The coolant then flows through a letdown orifice which reduces coolant pressure. The cooled, low pressure water leaves the Reactor Containment and enters the Primary Auxiliary Building where it undergoes a second temperature reduction in the tube side of the non-regenerative heat exchanger followed by a second pressure reduction by the low pressure letdown valve. After passing through one of the mixed bed demineralizers, where ionic impurities are removed, coolant flows through the reactor coolant filters and enters the volume control tank through a spray nozzle. The cation bed demineralizer, located downstream of the mixed bed demineralizers, is used intermittently to control cesium activity in the coolant and to remove excess lithium. The deborating demineralizers can be used intermittently to remove boron from the reactor coolant near the end of the core life. When the deborating demineralizers are in operation, the letdown stream passes from the mixed bed demineralizers and then through the deborating demineralizers and into the volume control tank after passing through the reactor coolant filter.

Hydrogen is automatically supplied, as determined by pressure control, to the vapor space in the volume control tank, which is predominantly hydrogen and water vapor. The hydrogen within this tank is, in turn, the supply source to the reactor coolant. Fission gases are periodically removed from the system by venting the volume control tank to the Waste Disposal System prior to a cold or refueling shutdown.

The CVCS volume control tank, CVCS holdup tanks, and associated piping were all designed to accommodate up to 100% hydrogen in the vapor space. Flammable mixtures are precluded by excluding oxygen. The gas analyzer samples these vapor spaces automatically and alarms any sample point where an oxygen concentration of 2% is detected. Exclusion of oxygen is accomplished by leak tight construction of tanks and piping systems and by maintenance of positive pressure inside these tanks and piping systems.

From the volume control tank, the coolant flows to the charging pumps which raise the pressure above that in the RCS. The coolant then enters the containment, passes through the tube side of the regenerative heat exchanger, and is returned to the RCS. The three positive displacement, variable speed drive charging pumps used to supply charging flow to the RCS can be controlled manually or automatically. During normal operation, only one of the three pumps is automatically controlled with the speed modulated in accordance with pressurizer level. During load changes the pressurizer level set point is varied automatically to compensate partially for the expansion or contraction of the reactor coolant associated with temperature changes. The level set point is varied between 20 and 60 percent of the adjustable range depending on the power level. Charging pump speed does not change rapidly with pressurizer level variations due to the reset action of the pressurizer level controller.

The concentration of the boric acid neutron absorber (for chemical reactivity control) is controlled by adding the mixture of boric acid and primary water upstream of the charging pumps. Small quantities of boric acid solution are metered from the discharge of an operating boric acid transfer pump for blending with make up water as make up for normal leakage or for increasing the reactor coolant boron concentration during normal operation. The boric acid is stored in two boric acid tanks after being prepared in the boric acid batching tank.

During plant startup, normal operation, load reductions, and shutdown liquid effluents containing boric acid flow from the RCS through the letdown line are collected in the holdup tanks. As liquid enters the holdup tanks, the nitrogen cover gas is displaced to the gas decay tanks in the Waste Disposal System through the waste vent header. The concentration of boric acid in the holdup tanks varies throughout the core life from the refueling concentration to essentially zero at the end of the core cycle. A recirculating pump is provided to transfer liquid from one holdup tank to another.

2.2.11 Component Cooling Water System

The Component Cooling Water Loop System is a system designed to remove heat from the RCS components, heat exchangers (HXR), and pumps. The water flows through these components in parallel lines of piping, which stem from two main headers.

The component cooling loop is necessary to provide adequate cooling for certain active components. In order to insure that the loop is functioning properly, the loop is monitored by the following instrumentation:

1. A pressure detector on the piping between the component cooling heat exchangers and the component cooling pumps.
2. Flow indicators and temperature indicators at the outlet of the heat exchangers.
3. Radiation monitors in the inlet and outlet piping from the heat exchangers.
4. Temperature indicators on the main inlet line to the component cooling pumps.

The component cooling system transfers the heat to the Service Water System. This arrangement reduces the extent of radioactive leakage by providing a double barrier.

During normal operation, two Component Cooling Pumps (CCP) and one Component Cooling Heat Exchanger (CCHXR) serve necessary loads. This leaves one standby pump and one standby HXR. All five components are utilized during normal plant shutdown, but safe shutdown is not affected by the loss of one pump or HXR.

Two Surge Tanks, one for each header, are used to allow for expansion and contraction of water until a leak can be located and isolated. These tanks are monitored for high radiation. The surge tanks are also used to receive make up water from the Primary Water Treatment Plant.

The cooling load from either of the headers can be split up such that each header, alone, can supply necessary cooling for long term recirculation following a LOCA in the event of a large break. This means that at least one of each of the following is supplied by each header:

1. Residual heat exchangers
2. Residual heat removal pumps
3. Recirculation pumps
4. Safety injection pumps

The three CCPs are horizontal, centrifugal pumps and were designed to withstand mechanical damage. These three pumps serve to circulate the cooling water around the loop.

CCHXRs are the shell and straight tube type. Service water circulates through the tube section at the same time that the CCW flows through the shell section.

There are four Component Cooling Booster Pumps (CCBPs) (two for each Recirculation Pump) which are used to protect the internal Recirculation Pump motors from the atmosphere inside containment. Only one CCBP is necessary for each rec'rculation pump. These CCBPs are started during the injection phase of accident recovery.

Component Cooling is provided for:

1. Residual heat exchangers
2. Reactor coolant pumps
3. Non-regenerative heat exchanger
4. Excess letdown heat exchanger
5. Seal water heat exchanger
6. Boric acid evaporator
7. Sample heat exchangers
8. Waste evaporator condenser
9. Waste gas compressors
10. Reactor vessel support pads
11. Residual heat removal pumps
12. Safety injection pumps
13. Recirculation pumps
14. Spent fuel pit heat exchanger
15. Charging Pumps

2.2.12 Service Water System

The Service Water System (SWS) provides essential heat transfer for many front-line and support systems. It accomplishes this by drawing cooling water from the Hudson River and pumping it through heat exchangers which interface with the other systems. The water is pressurized by nine Service Water Pumps (SWP) each capable of pumping 5000 gpm. During various plant conditions, flow requirements may vary. In the case of a LOCA coincident with a blackout, initially two pumps must be operating which supply flow to Nuclear and Conventional Services.

Of the nine service water pumps, six are used as main and three are used as back-ups. An automatic strainer flushes debris out of the downstream side of each SWP. Each of the nine SWP piping legs has identical piping. The SWPs are divided into 3 groups, each with a header:

Main pumps
SWP31, SWP32, SWP33 - Conventional Services Header
SWP34, SWP35, SWP36 - Nuclear Services Header
Backup pumps
SWP37, SWP38, SWP39 - Backup SWP Header

During safety injection, all essential loads can be adequately cooled by two of the three pumps normally on.

The diesel generators and the Central Control Room Air Conditioning Units (CCR ACUs) are considered part of the "Nuclear Services" section of the SWS. They lie downstream of the conventional, nuclear, and backup pump headers.

Each of the three headers is fed by three service water pumps. The three normally operating pumps are those which feed the nuclear header which is upstream of all essential loads. It is possible, however, to start other pumps should any of these three be unavailable.

For the case of unit trip with blackout and safety injection, the success criteria states that fór the recirculation phase only one additional pump is required for removal of the additional load. Should offsite power or all three diesels be available, another pump is activated.

Water is drawn from the Hudson River through "traveling screens" which strain out objects in the river water. These screens are constantly in use and require electrical power and a supply of water to flush away accumulated debris. After the water passes through these screens, it is drawn to the main service water pumps through three normally open routes. Two of these are via circulating water pump wells through normally open sluice gates connecting them to the SWP well. A third path is through the traveling screen path which connects directly into the SWP well. Debris flushing water for the traveling screens is supplied by the six main SWPs. Both the Conventional and Nuclear Services Headers supply water to the traveling screens through a crosstie via VB4 and VB5, respectively, into a single pipe. All outside piping is heat traced.

The backup service water pumps (SWP37, SWP38, SWP39) draw water directly from the discharge canal without any apparent screening of material before it is drawn into the pumps. There are three identical SWP legs, each with an automatic strainer downstream of the pumps.

The automatic strainers downstream of each backup SWP regularly flush out debris. The destination of material flushed by backup SWP automatic strainers is a trash trough.

Flow to the Conventional Services (e.g., boiler feed pump lube oil coolers) can come from the Nuclear or Conventional Service Water Headers. The backup pumps, however, are downstream of the path to those components and cannot circulate water through them. Flow to the Nuclear Services (diesels and CCR ACUs) can come from the main pumps or the backup pumps.

Flow is directed to the Nuclear Services from the two junctions of the main and backup pump fed paths. Part circulates through the essential loads and part flows through the component cooling heat exchangers (a non-essential load). Flow to the CCHXRs first passes through a crosstie just upstream of them. This crosstie enables routing of flow from any combination of the service water pump headers to the component cooling heat exchangers. There are two valves in the crosstie.

After flowing through the CCHXRs, the water flows through a single path to the river.

Flow to Nuclear Services passes by outlets to an essential load, the instrument air compressor coolers. Flow next passes to the CCR ACUs which are defined essential loads. There are two parallel trains, one for each air conditioning condenser. The trains can be crosstied via VGA1297K. After passing through the condensor, the water flows out to the river on a single path. Flow through the diesel generator lube oil and jacket water coolers also exits the system along a single path. Many components on the discharge path are shared by the diesel and CCR ACU heat transfer circuits.

Flow to the Conventional Services cools the essential load of the feedwater pump lube oil as well as non-essential loads. The feedwater pump cooling is along a simple path with no crossties and dumps into the discharge channel. The non-essential loads in Conventional Services all lie in the Conventional Plant Closed Cooling System, which is a circuit that interfaces with the rest of the SWS at the two Closed Cooling System Heat Exchangers. Non-essential loads on this circuit include the boiler feed pump pedestal coolers and the boiler feed pump bearing coolers.

2.2.13 Pressure Operated Relief Valves

The function of the pressure operated relief valves (PORVs) is to provide pressure relief as part of the pressurized Overpressure Protection System (OPS).

The OPS is designed to prevent the reactor vessel pressure from exceeding the Technical Specifications (Appendix G) limits. These specifications take into account the fact that the reactor vessel steel has less ductility at low temperatures and that as the reactor vessel is irradiated during its lifetime, the limitations on pressure become even more stringent.

The OPS is based on a three-channel analog curve tracking arrangement which can initiate an appropriate chain of coincidence logic. This arrangement has the purpose of automatically preventing violations of the operating technical specification temperature/pressure limit curve for the reactor vessel.

Wide range RCS temperature signals are used to perform two primary functions in this system:

1 Provide the arming and disarming function, and
2 Serve as the independent variable in computing the system pressure limit that must be adhered to.

The arming function of the Overpressure Protection System is activated when the RCS temperature is below a predetermined value (300°F).

The temperature signals are fed into three respective signal processors whose task it is to provide maximum RCS pressures allowed as a function of the input temperature. The difference between the Appendix G curve pressures and the actual RCS pressure transmitted by three (0 to 1500) psig transmitters is computed in each of the three channels. If any two-out-of-three of these differences is smaller than a preset minimum, a trip open condition will be initiated for each pressurizer power operated relief valve.

The pressure operated relief valves are operated using a N_2 system with local accumulators at each valve. The main function of the pressure operated relief valves is to protect against overpressure by opening automatically at 2335 psig. The PORVs will also open automatically when the reactor coolant temperature is between 0°F and 300°F, to relieve the RCS pressure to valves below the Appendix G curves. Under this mode of operation, the PORVs will relieve solid water rather than steam-water mixture at 2335 psig.

Westinghouse conducted a generic reactor vessel overpressure study and the analytical results showed that only one PORV is necessary for the design mass input overpressure incident and the design thermal input overpressure incident.

The motor operated valves and power operated relief valves feed to the pressurizer relief tank. The tank has sufficient capacity to accept the expected short term flow from the OPS.

2.2.14 Instrument Air System

The primary function of the Instrument Air System is to supply clean, oil and moisture free compressed air to the instruments, controls, and other required services in the conventional and nuclear plants.

Instrument air is supplied by two single stage compressors located in the control building. Each compressor discharges through its individual aftercooler and moisture separator to a common air receiver whose discharge is arranged in parallel paths, each containing an air filter and refrigerant dryer. Headered flow is then split. The first leg supplies the air requirements of the conventional plant. The second leg supplies the air requirements of the nuclear plant and other services located outside the buildings. In the latter case, further reduction of the air dew point is necessary to prevent freezing in the lines. This is accomplished by desiccant dryers in the air lines which leave the control building. Outside services include lines supplying the Auxiliary Feed Pump House and the Intake Structure. Another line supplies nuclear services which include the Penetration and Weld Channel Pressurization System.

Backups to the Instrument Air System are supplied by the Station Air System and the Administrative Building Air System through connections downstream of the instrument air receiver. Off of the Station Air backup supply is also an emergency supply to the Penetration and Weld Channel Pressurization System through an oil filter set and desiccant dryers.

Ambient air is supplied to the compressors through individual air filters and silencers. A sight glass indicator will show red when an air filter needs to be replaced. Air is compressed by the action of the piston and exits to the aftercooler. Air compressor cylinder and aftercooler jacket water cooling are supplied by the service water system through the Instrument Air Closed Cooling Water System. Air from the aftercoolers discharges to a common receiver where it is stored until used.

The compressors are designed to run continuously. Normally, however, one compressor runs (HAND mode) while the other is in a standby (AUTO mode) condition. The compressor operating in HAND mode is controlled to maintain the receiver air pressure between 100 and 110 psig. Should air pressure decrease to 95 psig, the standby compressor will automatically start and continue running until air pressure reaches 105 psig.

Each compressor is controlled by an unloader, a device which vents the air compressor's cylinders to atmosphere, thus allowing air to pass freely in and out of the suction valves without compression. Air pressure from the receiver is fed back to a pressure switch for each controller operating in HAND mode. When receiver pressure exceeds 110 psig, the pressure switch opens. The pressure switch controls a three-way solenoid valve (SOV1198/1199) which is normally energized to vent the unloaders. When the solenoid deenergizes, the full receiver pressure passes through the three-way valve and is applied to the suction valve unloaders causing them to open, thus unloading the compressor. Failure of this solenoid valve to fully reset or the pressure switch to close could result in a continuous unloading of the compressor. When receiver pressure drops below 30 psig, the unloader valves shut and the compressor is loaded regardless of the three-way valve's position.

On the discharge side from each compressor are temperature controllers (TC 1104S/1105S and TC 1106S/1107S) which trip the associated compressor on high discharge air temperature at 375°F or high cooling water return temperature at 150°F. The tripped compressor will not restart until the temperature sensor cools and the controller resets. A fire in the compressor room could cause both of the air temperature controllers to trip because of high intake temperature.

The receiver provides sufficient storage space for the compressed air to prevent pulsations produced by the compressors. The receiver relief valve is set to lift at 135 psig to protect the system from overpressurization.

The main header, after the 3-inch Station Air backup supply tie, splits into parallel streams, each containing an air filter set and a refrigerant dryer. A differential pressure controller energizes a normally shut 3-way solenoid valve when the air flow through the refrigerant dryers is low enough that the differential pressure across the dryers is greater than 12 to 20 psig. Energizing this solenoid causes the 3-way valve to pressurize the top of a fail shut diaphragm valve. The diaphragm valve then opens allowing flow to bypass the regenerative dryers through a filter. Manually opening the differential pressure controller's equalizing valve (IA-65) will also bypass air around the refrigerant dryers; however, the piping is much smaller in diameter than the normal flow path. The dew point of the bypassed air will be considerably higher than the 35°F dew point of the refrigerant dryers. Rapid air expansion could cause air line freeze up when the dryers are bypassed.

After the dryers, the air header splits. The 2-inch branch through IA-4 supplies the steam dumps and other loads in the conventional plant building Instrument Air System. The other path is to the desiccant dryers and the nuclear plant Instrument Air System.

The regenerative dryers further reduce the dew point to -40°F so that compressed air leaving the control building will not freeze under the lowest expected outdoor temperature. A 4-way valve on the regenerative dryer inlet directs air up through the desiccant bed in service. A small portion of the dried gas is diverted to the other bed where it is electrically heated and passed downward through the wet desiccant for regeneration. This air then exhausts to atmosphere through the 4-way valve. The 4-way valve and heaters are controlled by a timing circuit.

A nonregenerative desiccant dryer is provided in the bypass line around the regenerative dryers. The solenoid valve (SOV1143) deenergizes when pressure switch PC1170S on the regenerative dryer discharge drops below 90 psig. In the deenergized position the 3-way solenoid valve vents the diaphragm of the fail open valve (PCV1143) to atmosphere. When the diaphragm valve opens, air flows through the nonregenerative desiccant dryer. Once tripped, the solenoid valve must be manually reset to restore the bypass line to the standby condition. An alarm sounds in the control room whenever the valve is open.

Parallel afterfilter sets on the discharge of the desiccant dryers remove any desiccant which may have been carried over. Only one filter is in service at a time. Local operator action is required to reposition the 3-way selector valves (IA-12) when the differential pressure gage (DPI1132) reaches 5 psig.

A 3-inch tie from the station air system supplies emergency make up to the refrigerant dryers. Parallel filter sets, similar to those described previously, remove oil and particulates from the station air supply. A pressure controller (PCV1169S) and 3-way solenoid valve (SOV1142), similar to those described previously, cause the make up valve (PCV1142) to open when the refrigerant dryers suction pressure drops below 90 psig. The make up valve will remain open until the solenoid valve is manually reset. An alarm in the control room warns the operator that the make up valve is open.

An emergency make up to the Weld Channel Pressurization System is provided from the same line which supplies backup instrument air from the conventional plant header, through manual stop valve IA-56. A parallel set of oil filters, desiccant dryers, and afterfilters are provided in this line. Their operation and functions are the same as previously described for the normal instrument air supply.

A blackout strips the Instrument Air System Motor Control Centers (MCC34 & MCC39) from their electrical buses. A local nitrogen backup supply is provided to equipment in the Service Water and Auxiliary Feedwater Systems.

During blackout, all solenoid operated valves fail in the deenergized position to vent the tops of their associated diaphragm valves. The emergency tie isolation valve (PCV1142) fails open to make the stored pressure of the Station Air System available to the instrument air header. The refrigerant dryer bypass valve (PCV1542), however, fails shut to prevent flow from bypassing the refrigerant dryers. Thus, operator action is necessary to bypass the refrigerant dryers during blackout. The nonregenerative desiccant dryer isolation valves (PCV1141/1143) open to bypass air around the inoperative regenerative desiccant dryers. The exhaust valves (SOV1101/1105) in the regenerative desiccant dryer purge air outlets fail shut to conserve the remaining system air inventory.

When the instrument air pressure in the AFW System falls below 50 psig, a pressure regulating valve (PCV1276) automatically opens to supply nitrogen from three backup bottles. This backup supply services:

1. The Auxiliary Feedwater regulators (FCV405A/B/C/D and FCV406A/B/C/D), normally shut, fail open
2. The turbine speed (HCV1118), steam isolation (PCV1310A/B), steam pressure (PCV1139), and the bearing cooling water flow (PCV1213) regulators of Auxiliary Feedwater Pump No. 32
3. The AFW Pump City Water emergency tie isolation valves (PCV1187/1188/1189), normally shut, fail open
4. The Condensate Storage Tank (CST) fill isolation valves (FCV1121/1123), normally shut, fail shut.

The steam isolation valves (PCV1310A/B) are temperature controlled and automatically shut to protect the motor driven AFW pumps from a steam line rupture if the air temperature in the Auxiliary Feedwater Pump Room exceeds 180°F. Air pressure is required to open these isolation valves.

2.2.15 Lube Oil System

The Lube Oil System is used to circulate warm, purified, control and lubricating oil to the main turbine and the boiler feed pumps. The system consists of many large vented tanks, i.e., Main Turbine Oil Conditioner, Turbine Lube Oil Reservoir, Dirty and Clean Oil Storage Tanks, Boiler Feed Pump Oil Console, and Boiler Feed Pump Turbine Oil Conditioner. A potential fire hazard exists upon the loss of tank ventilation; however, carbon dioxide and foam fire suppression systems are installed to control such fires.

The Oil Resevoir Heater Pump takes suction from the Boiler Feed Pump Oil Console when the locked closed valve LO-42 is opened. This pump is used to warm up the oil in the Boiler Feed Pump Oil Console when the system has been shut down for an extended period of time. Part of this flow is diverted to the sludge separator, R2D2, before returning to the Boiler Feed Pump Oil Console.

The Boiler Feed Oil Console Transfer Pump is used to transfer oil to either the Dirty or Clean Oil Storage Tank. Makeup oil is taken from the Clean Oil Storage Tank via the Oil Storage Tank Transfer and Cleanup Pump or the Turbine Oil Reservoir Transfer Pump.

The Boiler Feed Oil Console Circulating Pump is used to circulate oil through the Boiler Feed Pump Turbine Oil Conditioner. The Boiler Feed Pump Oil Conditioner Circulating Pump circulates the oil contained in the Boiler Feed Pump Turbine Oil Conditioner through the polishing filter.

The Main Turbine Oil Conditioner Circulating Pump circulates oil between the Main Turbine Oil Conditioner, its polishing filter, and the Turbine Lube Oil Reservoir. Oil from the Turbine Lube Oil Reservoir may be transferred to the Clean or Dirty Oil Storage Tank by opening the Locked closed valve LO-15 and by running the Turbine Oil Reservoir Transfer Pump.

Lube oil from either the Dirty or Clean Oil Storage Tanks may be cleaned up by the Main Turbine Oil Conditioner by repositioning the LO-1 swing connection and running the Oil Storage Tank Transfer and Cleanup Pump.

A truck loading connection is provided for filling or draining the system. Various valves and blank flanges can be repositioned to accomplish the desired truck loading/unloading elevations.

The R4D4 sludge separator can also be used to clean up the contents of the Dirty and Clean Oil Storage Tanks. A bank of six heaters can be valved into the system to warm up the lube oil.

The Boiler Feed Pumps are lubricated by oil from the Boiler Feed Pump Oil Console. Two 480 V ac Main Lubricating Oil Pumps take suction from the console and discharge through check valves to the high presssure oil header. One pump provides sufficient flow to supply the needs of both Boiler Feed Pumps and their turbines.

The standby pump will automatically start if the running pump's circuit breaker opens or the discharge header pressure drops below 115 psig. In the event that bearing oil pressure decreases below 50 psig, the emergency dc Lube Oil Pump will automatically start. Test switches which open the solenoid dump valves may be used to verify the operation of the automatic low pressure starting circuitry.

Oil from the high pressure header passes through an orifice and filter before entering a set of parallel coil coolers. Locally mounted pressure gauges indicate when the filter should be replaced. Heat from the oil coolers is removed by the Service Water System. Each cooler is independently capable of supplying oil to both feed pumps and their turbines. Oil from these components is returned to the oil console reservoir for reuse.

2.2.16 Reactor Coolant Pump Seal System

The Indian Point-3 plant is a four-loop Westinghouse PWR. Each loop contains a reactor coolant pump that is designed to circulate large volumes of reactor coolant at high temperature and pressure. These pumps facilitate the transport of energy produced in the nuclear core to the tube side of the four steam generators for the production of steam that is used to power the turbine-generator.

Each reactor coolant pump is a vertical single-stage centrifugal pump which employs a controlled leakage seal assembly. Each pump is designed to pump 89,700 gpm of reactor coolant at a temperature of 555°F and a pressure of 2235 psig. Each pump consists of three general areas; the hydraulics package, the shaft seal package, and the motor package.

2.2.16.1 The Hydraulic Package

The pump hydraulics area consists of a casing, impeller, diffuser, thermal barrier, thermal barrier heat exchanger, lower radial bearing, main flange and pump shaft.

The casing has a bottom suction and a side discharge nozzle. Reactor coolant is drawn up through the casing adaptor which directs the coolant flow to the impeller. The impeller is designed for counterclockwise rotation. Labyrinth type seals are provided on the top and bottom impeller guide structure to minimize recirculation flow. Coolant leaves the pump through a diffuser which converts the velocity head to pressure head. The casing adapter and diffuser act to impede backflow through an idle pump, and in case of a cold leg break to restrict flow through the break.

Located immediately above the impeller and diffuser is a thermal barrier assembly. During normal operation, the thermal barrier minimizes the heat flow from the reactor coolant to the pump lower radial bearing and the shaft seal area. The thermal barrier assembly is made of all welded construction consisting of a heat exchanger fabricated of layers of coiled tubing in a pancaked fashion. A separation plate with drilled passages on its outer periphery is installed between the tubing layers. Labyrinth seals are installed where the top, separation and bottom plates surround the pump shaft to minimize thermal barrier heat exchanger bypass flow.

Cooling water for the thermal barrier heat exchanger comes from the component cooling system, passing through a check valve before separating to each pump. This same cooling water also goes to the motor bearing oil cooler which will be discussed later. After the flow junction to motor oil coolers, 25 gpm passes through a reducer and a check valve to the thermal barrier heat exchangers. Piping from the check valves to the flange connection on the pump is designed for high pressure since it may be subjected to reactor coolant system pressure. After the coolant passes through the heat exchanger, it flows through a local flow indicator and a manual isolation valve. The heat exchanger exit flow also has a safety valve (local) prior to the manual isolation valve to relieve excessive pressure that may be caused by heating. This valve is set at 2485 psig and relieves directly to the containment sump. Following the manual isolation valve, flow from all the pumps combine and penetrate the containment. The flow then passes through a local orifice metering device which controls the motorized valve directly upstream. If a rupture in a heat exchanger should occur, high flow would result, and the motorized valve would close. Thus, isolating all thermal barrier cooling flows. Following the flow metering device is another motor operated valve (MOV). High pressure piping is used from the MOV to all the pump thermal barriers since they may be subjected to RCS pressure. The combined thermal barrier return flow is then routed back to the component cooling system. Low flow and high temperature are alarmed on the SG panel in the Central Control Room (CCR).

Above the thermal barrier upper labyrinth seal, on the inside diameter, is a stellite-overlayed valve seat which mates with a similar seat on the bottom of the lower pump radial bearing journal. This acts as a low pressure valve capable of holding a 30-foot head of water. The lower radial bearing is cooled and lubricated by pump seal injection water. It consists of a two-piece horizontally split housing, a bearing cartridge and a journal. Graphiter-4 rings are shrunk into a bearing cartridge and form the bearing surface. The bearing operates against a stellite-overlayed journal which is shrunk on to the pump shaft. A resistance temperature detector, located in the thermal barrier housing, senses water temperature and provides indication in the CCR on the RCS supervisory panel (SAF). This is indicated on the panel as "No. 1 Seal Inlet Temp."

2.2.16.2 The Shaft Seal Package

The pump shaft seal area consists of the No. 1 controlled-leakage film riding face seal and the No. 2 and No. 3 rubbing face seals. These seals are contained within the main flange and seal housing between the hydraulics area and the motor area. The pump seal assembly restricts leakage from the primary coolant system along the pump shaft.

The No. 1 pump seal, the main seal of the pump, consists of a runner which rotates with the pump shaft and a non-rotating seal ring attached to the lower seal housing. The seal ring and runner have aluminum oxide surfaces. A flow path is formed between the seal ring and runner with a separation of about 0.00045 inches which depends on seal geometry and pressure distribution. The seal ring is allowed to move axially to accommodate changes in pump shaft position.

The No. 2 seal, located above the No. 1 seal, consists of a graphiter-39 insert shrunk into a stainless steel seal ring. The seal ring insert rubs on an aluminum oxide surface runner which rotates with the pump shaft. The No. 2 seal ring is also allowed to move axially.

The No. 3 seal, located above the No. 2 seal, is of similar design and construction as the No. 2 seal. This seal is also allowed to move axially.

High pressure injection water is supplied to the pump seal assembly from the chemical and volume control system by the charging pumps. The seal injection flow from the charging pumps passes through two injection filters and manifolds with associated isolation, vent and drain valves and a valve bypass line to all the RC pumps. The two filters are provided outside the containment so that a single filter change can be effected without interrupting the injection flow. A differential pressure indicator is provided across the filters inlet and outlet manifolds to register filter fouling. High RCP seal injection filter differential pressure is indicated on the SFF panel in the CCR.

Each RC pump is provided with an orifice type inlet flow indicator and transmitter for local and CCR indication followed by an adjustable valve, both located outside containment so that injection flow can be adjusted. Just prior to entering the containment, each injection line is provided with a manual isolation valve. After the injection flow enters the containment, three check valves are provided to prevent backflow from the RCS if injection flow is lost. The injection line is also provided with a drain valve between the check valves and the pump connection so that the pump seal cavity can be drained.

The seal injection flow, 8 gpm, enters the pump in the thermal barrier region where the flow splits with a portion, 3 gpm, passing through and around the lower radial bearing to the controlled-leakage seal package. The remaining portion, 5 gpm, passes down through the thermal barrier heat exchanger and into the reactor coolant system where it constitutes a portion of the make up water and acts as a buffer to prevent RCS coolant from entering the radial bearing and seal section of the pump. In the event of seal injection water loss, the thermal barrier heat exchanger will cool the RCS coolant passing upward through it.

To assure sufficient flow through the thermal barrier labyrinth seal into the RC system, a pressure drop indicator is provided. This pressure drop measurement is indicated in the CCR on the SFF panel as "RCP thermal barrier to delta p" and only gives an indication when positive downward flow is provided. No indication of negative flow or RCS leakage is given other than the low delta p signal.

During normal operation, the No. 1 seal injection flow passes through the No. 1 seal and splits with a small portion (3 gph) going to the No. 2 seal and the remainder leaving the pump. This outlet's flow passes through a remotely operated valve, two flow meters in series and then combines with the flow from the other pumps before returning to the CVCS volume control tank. The flow meters are provided with isolation valves, a valved bypass line and a valved drain line and give a low or high flow alarm in the control room on the SSF panel.

To operate the RC pumps at low reactor coolant pressure, additional seal flow is required to remove friction heating which is provided by the No. 1 seal bypass line. This line, which is on the high pressure side of the No. 1 seal, consists of a vent connection, a check valve, a letdown orifice and a flow indicator. In the circuit following the flow meter all pump bypass lines combine, pass through a flow control valve and return to the volume control tank. The bypass line normally remains closed at RCS pressure above 1500 psi or when the flow through the No. 1 seal is greater than 1 gpm. Combined low bypass flow is alarmed on the SFF panel in the CCR only when the bypass flow control valve is open.

Between the No. 1 seal leak-off line and the bypass line a differential pressure indicator is provided which indicates pressure drop across the No. 1 seal. This measurement is indicated in the CCR with an alarm if the pressure drop falls below 275 psi.

The No. 2 seal injection water passes through the seal and then splits where a small portion (100 cc/hr) goes to the No. 3 seal and the remainder goes to the No. 2 seal leak-off system. The No. 2 leak-off water leave the pump and goes to a six-inch diameter standpipe that provides the seal with a seven-foot water head back pressure. The standpipe outlet line has an orifice restriction that is designed to permit the normal No. 2 seal leakage to pass. After the orifice on the standpipe outlet line, it junctions with the standpipe overflow line, then passes through an isolation valve and combines with the flow from the other pumps before going to the reactor coolant drain tank. The standpipe has a valved high point vent line, a drain valve, two level indicators and can receive make up water from the reactor coolant make up system via the charging pumps. The two level instruments are provided to indicate both high and low level in the tank. Their signals activate low and high level alarms and indicator lamps on the SA panel in the CCR. A high standpipe level indicates excess leakage through the No. 2 seal while a low level signal indicates excess leakage through the No. 3 seal, the standpipe make up water circuit consists of a remotely operated valve (switch on the SA panel in the CCR), an adjustable flow valve and a check valve.

The No. 3 seal water passes through the seal and then drains into the floor trench in the annulus area below the reactor vessel. There is no valve in the drain line. The No. 2 seal standpipe provides the back pressure which insures leakage flow through the No. 3 seal.

2.2.16.3 <u>The Motor Package</u>

The Motor Package is located on the top of the pump and is separated from the RCS by the seal package. The motor is a vertical, solid shaft, six pole class b thermal elastic epoxy-insulated, squirrel cage induction motor of drip proof design. The motor is equipped with upper and lower radial guide bearings, a double Kingbury type thrust bearing, thrust bearing oil lift system, flywheel, bearing oil coolers, space heaters, anti-rotation device and appropriate instrumentation.

The motor windings are air cooled and have six resistive temperature detectors embedded in the stator winding. The motor shaft is connected to the pump shaft by two solid carbon steel flanges. The flywheel is located on the upper portion of the motor shaft and provides additional inertia to extend the coast down time of the pump. On each side of the motor windings are the upper and lower guide bearing.

The lower guide bearings, with a babbit-steel surface, operates against a 0.5 carbon alloy steel journal. The entire bearing assembly is immersed in a 25-gallon oil reservoir and the oil is circulated by convection currents and agitation due to the shaft rotation. An integral one-pass, coiled-finned tube heat exchanger is located within the oil reservoir. Local oil level indication along with high and low oil level alarms, annunicated in the CCR on the SAF, are provided. A bearing temperature detector provides indication and alarm in the CCR via the plant computer.

The upper bearing assembly consists of a combination upper guide bearing and thrust bearing. The babbit-on-steel bearings operate against an alloy steel journal shrunk onto the motor shaft. Both bearings have a 175 gallon oil reservoir with the oil being circulated by the thrust bearing runner. The upper bearings oil is cooled by a two-pass heat exchanger mounted on the side of the motor. Local oil level indication, along with high and low oil level alarms are annunicated on the SA panel in the CCR.

Both the upper and lower bearing oil heat exchangers have component cooling water as the cooling medium. Each heat exchanger cooling water line junctions with the component cooling water inlet line separately prior to the check valve in the line that goes to the thermal barrier heat exchanger. The lower bearing oil cooling water passes through an isolation valve, the heat exchanger, a local flow meter, another isolation valve and junctions with the upper bearing oil cooling water. The upper bearing oil cooling water line has two isolation valves, one on each side of the heat exchanger before it junctions with the lower bearing oil cooling water line. Both cooling water lines have a valved vent connection between the isolation valves. After the two cooling lines come together, the cooling water passes through a flow meter and a valve before returning to the component cooling water system. Bearing coolant return low flow and high temperature alarms are provided on the auxiliary coolant supervisory panel (SG) in the CCR.

2.3 System Digraphs

In the previous sections, the systems to be analyzed in this study were identified and described. In this section we discuss the digraph modeling efforts resulting in the construction of system digraphs for each of these previously described systems.

For each system, the modeling effort involved the establishment of system boundaries, the modeling of major components and their interrelationships, and the unit model expansion of selected major components within the system. Appendix A provides a more detailed discussion of Digraph Matrix Analysis and the digraph modeling procedures.

The establishment of system boundaries is particularly important for two reasons. First, it is necessary to bound each system and identify the precise nature of the boundaries so that when systems are combined, the mutual boundary nodes are properly taken into account. Secondly, system failure criteria must be identified and expressed at modified boundary nodes.

A feature of the DMA approach that results in enhanced clarity of the modeling approach is the use of the actual plant drawings and component identifiers as a basis for the resultant model. Thus, the plant schematics are used as a template for the digraph model which is sketched as an overlay drawing. In addition, node names based on the schematic identifiers are used to the greatest extent possible.

Drawings of the plant schematics (P&IDs) together with overlay drawings of the corresponding digraph models are assembled in Appendix B, found in Volume 3 of this report. Node names, as discussed previously, are based on schematic identifiers found in the P&IDs, and are also identified generically in the glossary of this report and in the glossary of Appendix B. The computer input file and symbolic description of the digraph models in the form of adjacency input listings can be found in Appendix C (Volume 4). All of these information sources can be used in conjunction with the following system-by-system discussions of the construction of the system digraph models.

2.3.1 Safety Injection System Digraphs

2.3.1.1 Overview

The Safety Injection System (SIS) Piping and Instrumentation Drawing (P&ID) is provided in Fig. B.1. of Appendix B. The safety injection system operates in four modes; high pressure injection, low pressure injection, high pressure recirculation and low pressure recirculation. Despite operating in a variety of modes, the SIS was modeled as a single digraph (with appropriate computer flags to distinguish the differences of the system under alternative modes of operation).

The safety injection and recirculation phases are included in one complete model (see Figs. B.1.1 and B.1.2) which consists of two digraphs traced over two P&IDs. Three separate failure criteria were used for different conditions. Since a significant portion of the piping is shared by the injection and the recirculation phases, this method of modeling the hardware and flagging different modes and phases gives a very complete visual picture. Only three of the five possible injection/recirculation phases are included in the chosen system combinations. High Pressure Recirculation (HPR), and Accumulator Injection (ACC) were excluded from the scope of this study by the NRC, although the piping exists on the drawings. The three which are included are:

1. High Pressure Injection (HPI)
2. Low Pressure Injection (LPI)
3. Low Pressure Recirculation (LPR).

The terminal nodes representing system failure criteria are shown on the Phase and Path Interconnection Digraph (see Fig. B.1.3). The terminal nodes SLOCA, MLOCA, and LLOCA are used to identify small, medium and large LOCA respectively. Each system combination uses only one of these terminal nodes.

2.3.1.2 Path Criteria

The Phase and Path Interconnection Digraph is based on the fact that eventually all injection legs come together to form four cold injection legs. Therefore, the digraph (see Fig. B.1.3) starts with 14 legs on the right hand side and leads to four terminal nodes on the left hand side. The input consists of four cold legs and one hot leg dedicated to the high pressure injection path that bypasses the Boron Injection Tank , and four cold legs and one hot leg dedicated to the path through the BIT. The four cold legs of the non-BIT path and the four legs of the residual heat exchanger (RHXR) path meet first, followed by the BIT path which connects in later. No boron injection is necessary since the reactor is assumed to be scrammed at the start of the accident. For this reason, the BIT and non-BIT paths are redundant. Since a break in any reactor cold loop renders that path useless for injection, common loop nodes are introduced to propagate the break to the non-BIT path, the BIT path, and the RHXR path.

The failure criteria for paths into the core varies with the size of the LOCA. A small LOCA with the reactor scrammed requires only one high pressure leg of the 10 legs (eight cold legs or two hot legs) into the core provided that the path is not connected to the leg with the break in it. This path can go either through the BIT or around it. A medium LOCA requires two of the ten high pressure legs through the BIT or around it, or a low pressure leg through the RHXRs. These high pressure criteria are based on the assumption that the hot leg injection paths are sufficient alternate paths if all cold leg paths are blocked in High Pressure Injection. In the event of a large LOCA, the Low Pressure Injection System must provide two unbroken legs through the RHXRs.

2.3.1.3 Pump Criteria

The Safety Injection Pumps are required for High Pressure Injection. In the event of a small LOCA, only one SIP is necessary to supply injection cooling to the core. Two pumps are needed for a medium LOCA. This is shown in the Pump Criteria Digraph (See Fig. B.1.3). The functioning pump or pumps must be able to supply cooling to the functioning path or paths.

There are two Residual Heat Removal Pumps (RHRPs) to supply Low Pressure Injection and one alternate path for Low Pressure Recirculation from the containment sump. One pump is sufficient for all phases and the other provides backup.

Two Recirculation pumps (RECPs) are provided for LPR from the recirculation sump. Only one is necessary for all phases.

2.3.1.4 Cooling Requirements for Recirculation

In either a medium or large LOCA recirculation phase, some cooling is necessary since the water that is being used to cool the core starts out hot from its last pass through the core. This cooling can take place by means of the RHXRs. There are two redundant RHXRs. The assumption is made that the valves downstream toward the core from the RHXRs do not necessarily need to be closed to force the water back up to the SIPs for the alternate path during HPI. It is assumed that the suction on the SIPs combined with the high pressure in the core is sufficient to divert the flow.

In recirculation, flow from the functioning pump (either RECPs or RHRPs) must be piped through the functioning RHXR and into the available path or paths to the core.

2.3.1.5 Safety Injection Actuation Signal

Upon the receipt of an SI signal the SIPs and the RHRPs start. In addition, isolation valves on both sides of the BIT open, and the valves which allow the recycling of the BIT close.

Along with the BIT isolation valves, there are a number of valves which are already open and also receive a confirmatory SI signal to open. The valves which receive an SI signal are listed in Table 2-8.

TABLE 2-8
Valves Receiving an SI Signal

Identifier	Description	Initial State
1. MOV1852A/B	BIT Isolation	Normally Closed
2. MOV1835A/B	BIT Isolation	Normally Closed
3. MOV856C/E/H/J	High Head Cold Legs	Normally Open
4. MOV851A/B	High Head SIP Discharged	Normally Open
5. FCV1851A/B	BIT Recycle	Normally Open

After SI has been initiated and the automatic systems take over, the operators check various indicators and determine what type of accident (if any) is taking place and what operator action is required. If all systems are functioning normally, either the RHRPs or the SIPs can be shut down (the other remains in use). If there is a problem, however, the operator must repair it or re-route the flow.

There are three paths for high pressure injection - two of these are normal flow paths either through MOV1810 or by opening VGA898 if the MOV1810 line is blocked. The third choice involves routing flow through the RHRPs and RHXRs, then back to the SIPs through MOV888A/B. Either of the last two alternate paths require operator intervention as denoted by OPRs (operators doing the right thing during the accident). These OPRs are OPR898 and OPR888. In addition to MOV888A/B, OPR888 is responsible for closing MOV899A/B or MOV746/747 to insure flow is routed back to the SIPs.

Low pressure injection has its only path as the normal flow through the RHRPs and the RHXRs, and then flowing out through the Low Pressure Injection legs. There is no way to re-route flow.

Flow paths for low pressure recirculation are varied mainly due to the fact that there are two sources of water - the Recirculation Sump and the Containment Sump. Normal flow is routed from the RECPs (drawing from the Recirculation Sump) to the RHXRs to the Low Pressure piping, with back-up capability provided by the RHRPs drawing from the Containment Sump. In the case where back-up capability is required, but the path from the RHRPs to the RHXRs is blocked, there is an alternate route through MOV883 up to the SIPs, then through MOV888A/B and backwards through one heat exchanger then forward through the other heat exchanger and out the Low Pressure Injection legs.

2.3.1.6 Crossties

There are several groups of pipe junctions near headers which require a crosstie model. These junctions include input to the SIPs (three inputs and three outputs), input and output of the RHXRs (two inputs and two outputs) and a pipe crossing between the two headers leading to the Low Pressure Injection legs (two inputs and two outputs). Crossties are discussed in more detail in Section A.4.2.

The crossties can lead to cycles (see Section A.4.3 for a discussion of cycles and loops) between phases because the direction of flow is dependent on hydraulic conditions and not hardware restrictions. This problem can usually be solved by the judicious placement of "boundary nodes". Alternatively, situations exist where greater effort to break the cycle is required. This occurs once in high pressure injection and once in two different directions in low pressure recirculation. For high pressure injection, the cycle is in Fig. 2-2.

The problem arises because in the digraph of Figure 2-2 failure cannot propagate to each of the SIPs from the RWST. Should the RWST be emptied of water, that failure should propagate to all three SIPs. For example from RWST to SIP31, note that failure reaches the first AND-gate (A) on the right side, but can't reach through because in order for the left side of AND-gate (A) to fail, the failure must have already propagated through AND-gate (A). (Tracing back from the second side of AND-gate A leads to AND-gate B. The left sides of AND-gate B can only fail through the RHXRs and RHRPs back to AND-gate A.) This is the type of conditioned cycle which must broken.

The procedure for breaking the cycle involves considering each sink separately. In this case, SIP31 is a different case from SIP32 and SIP33. This is because shorting AND-gate A from RWST to the output of the gate only makes sense for SIP32 and SIP33, since flow to the left side of the AND-gate must have passed by both SIPs already. Similarly,

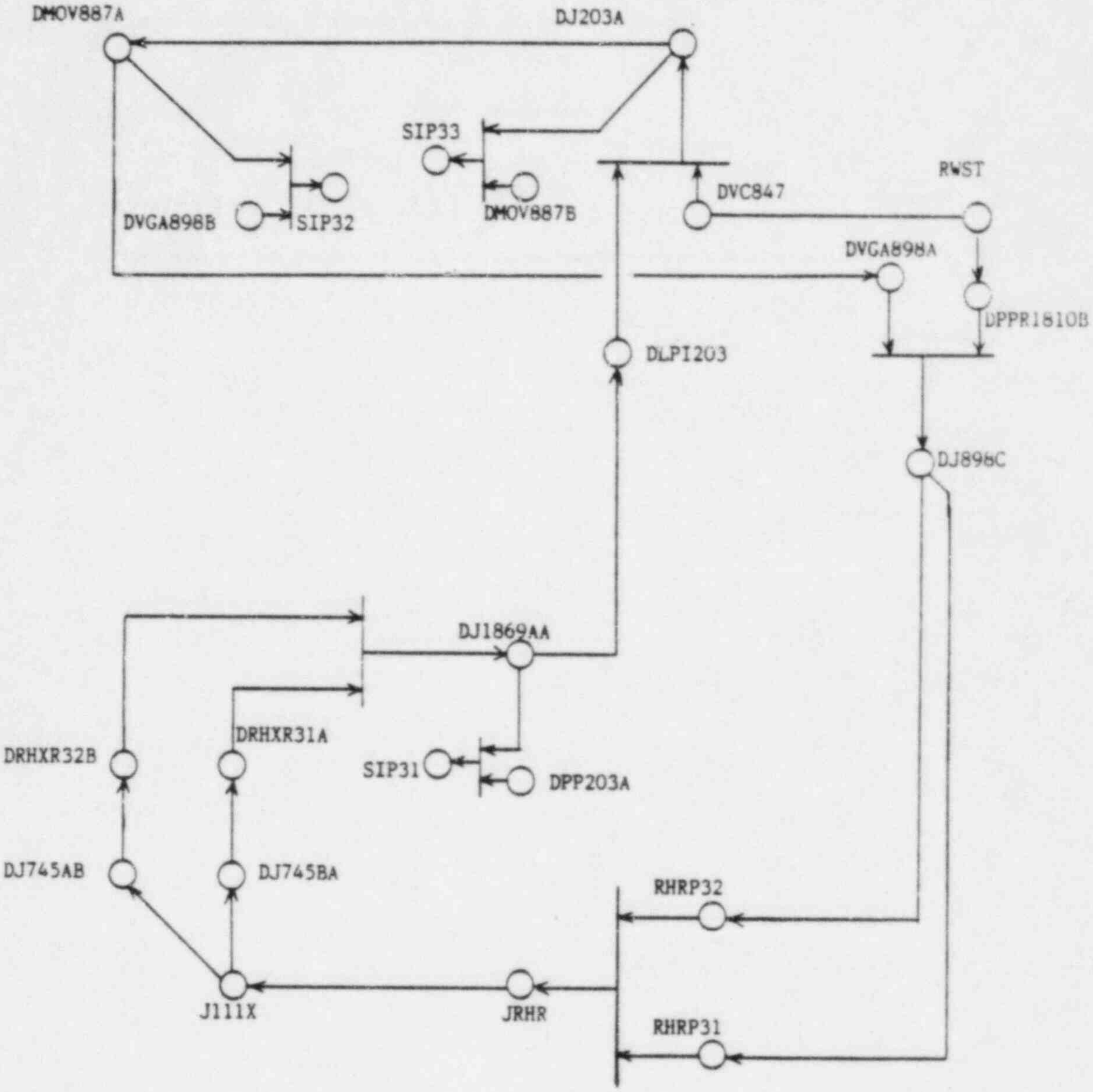


Figure 2-2 High Pressure Injection Cycle

flow to SIP31 indicates that a short from the RWST to the output of AND-gate B would solve that cycle problem.

These two different shorts require dummy nodes representing each node on the cycle path for each solution. These paths will be designated as primed (to sinks SIP32 and SIP33 - shown in grey) and double primed (to sink SIP31 - shown in red). This is shown in Figure 2-3.

There are two conditioned cycles in low pressure recirculation which exist because flow can circulate around the heat exchangers. This time there are two AND-gates which must be shorted for each sink. Figures 2-4 and 2-5 show the cycle and its solution respectively.

In Figure 2-3, the red and green lines represent flow in one direction and the blue and black lines represent flow in the other direction.

Unit models of various pumps and valves in the Safety Injection System are included in Appendix B in Figs. B.1.4 - B.1.5.

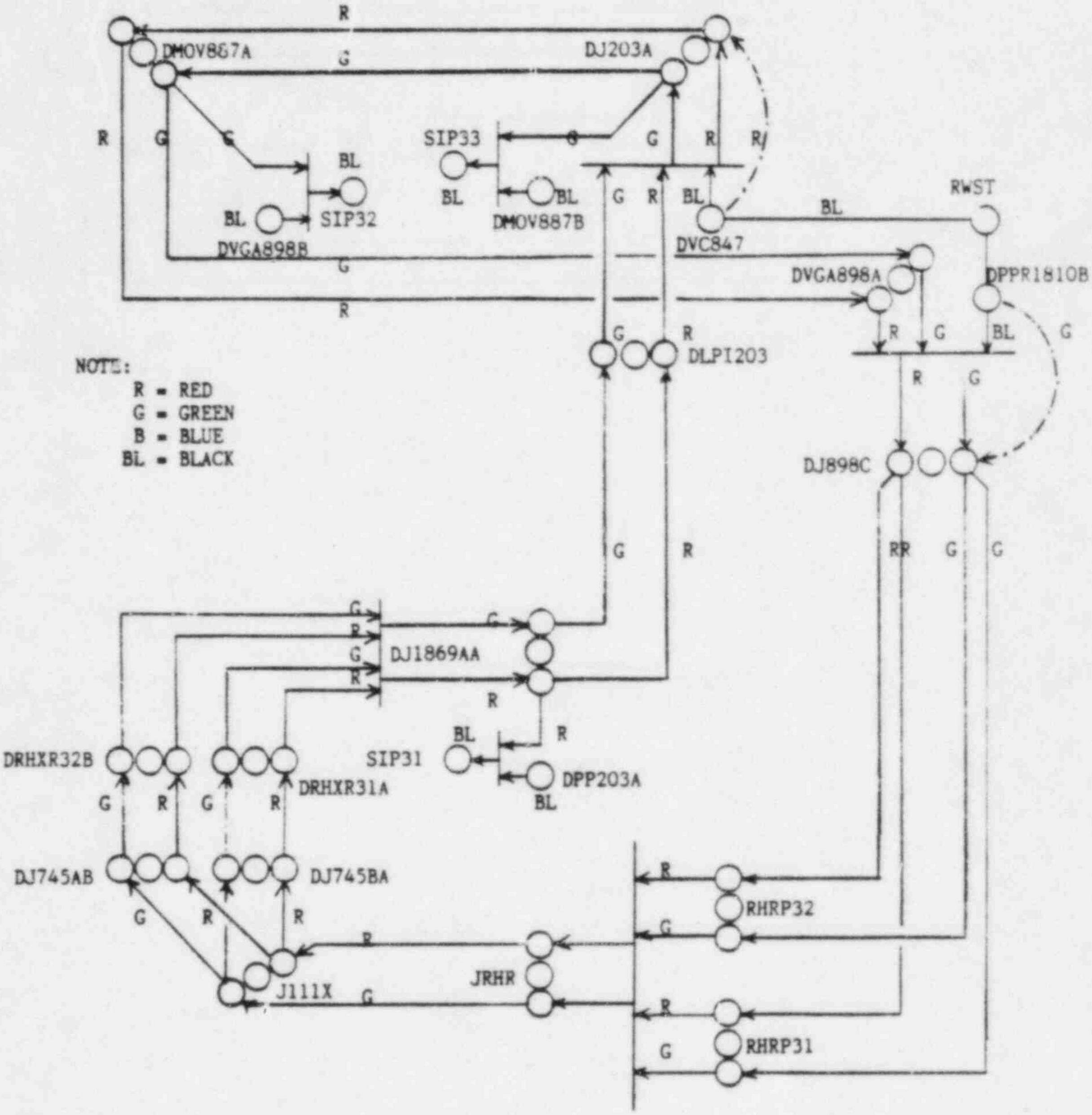


Figure 2-3 Dummy Nodes for Safety Injection Cycle

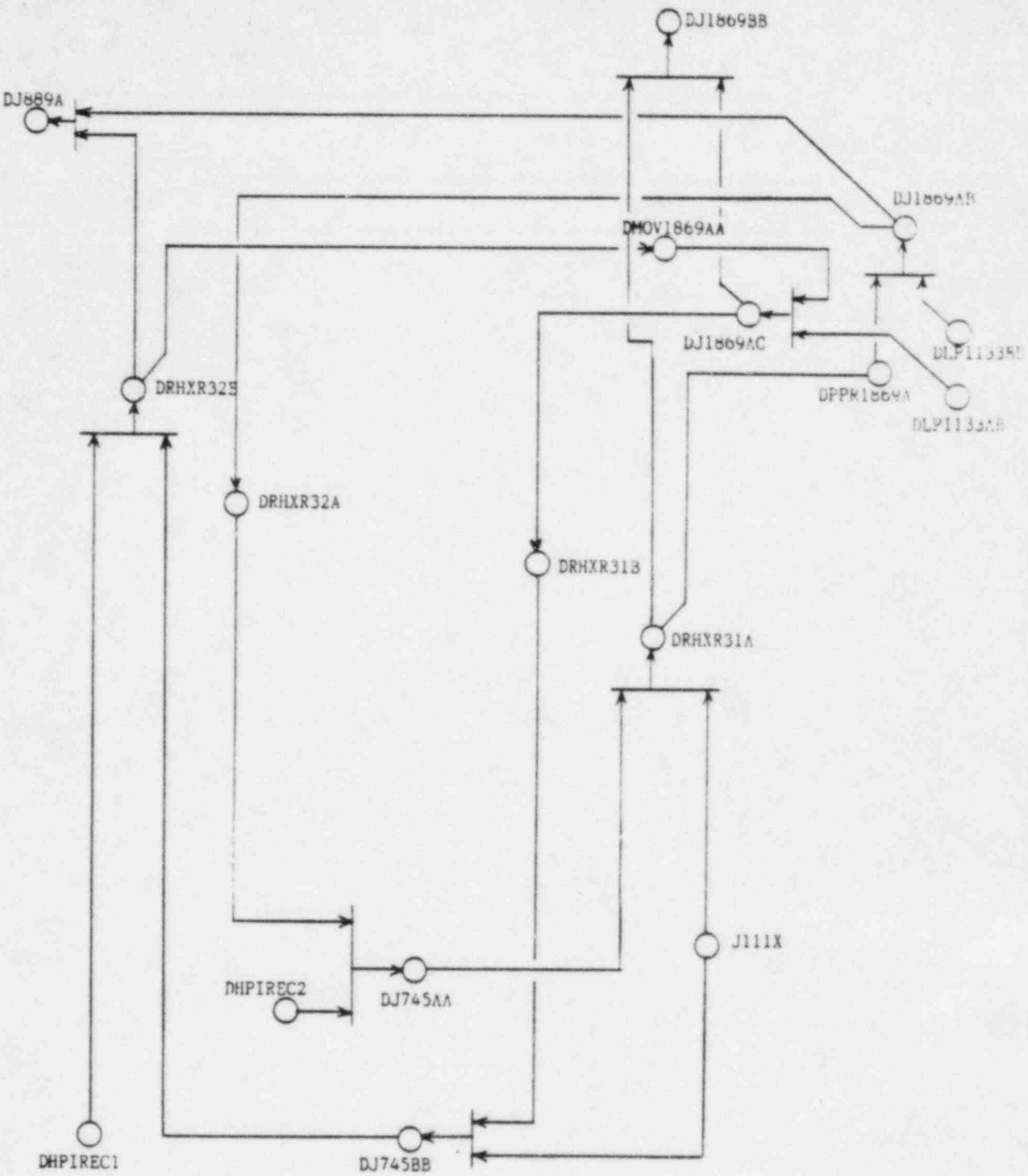
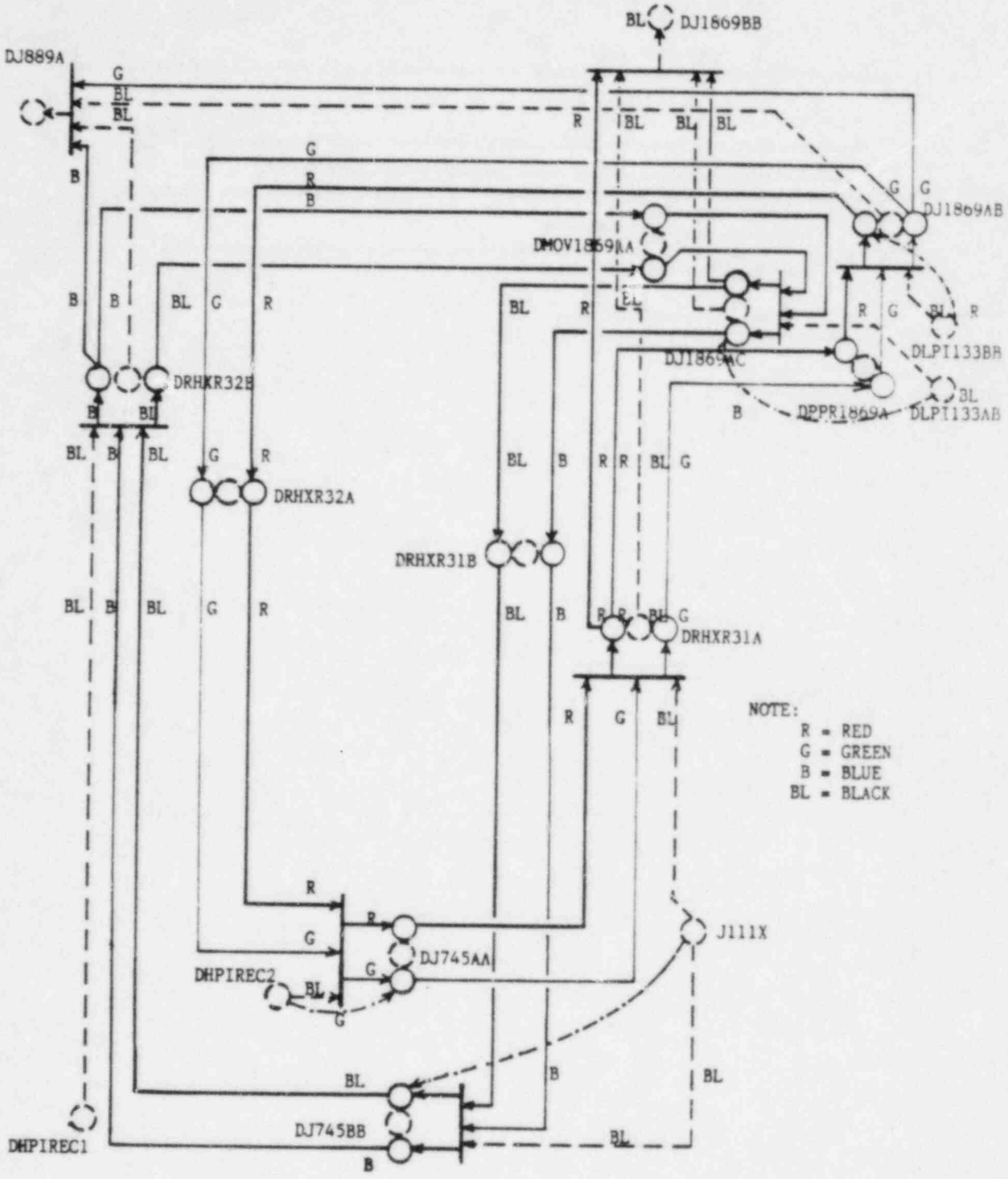


Figure 2-4 Low Pressure Recirculation Cycle



NOTE:
R = RED
G = GREEN
B = BLUE
BL = BLACK

Figure 2-5 Dummy Nodes for Recirculation Cycle

2.3.2 Safety Injection Actuation Digraphs

The Safety Injection Actuation System (SIAS) detects faults in the primary or secondary reactor coolant systems and initiates engineered safeguard component operation. The successful operation of the SIAS will: 1) trip the reactor, 2) initiate a generator trip and bus transfer 30 secs after reactor trip, 3) initiate the safequards equipment sequence signal, including starting of the diesels, 4) initiate containment ventilation isolation, 5) initiate containment "phase A" isolation, and 6) place the isolation valve seal water system into service.

A SIAS signal is initiated by any one of the following six signals: 1) low pressurizer pressure, 2) steam line break upstream of the main steam isolation valves (MSIVs), 3) steam line break downstream of the MSIVs, 4) high containment pressure, 5) high-high containment pressure, and, 6) manual actuation.

The SIAS signals originate at various instruments which transmit information to bistables that trip when out of tolerance conditions occur. This instrumentation is powered from the ac instrument buses. The bistables control ac relays that open contacts arranged in a logic matrix that de-energizes dc master relays in the SIAS circuit. The master relays, when de-energized, close contacts that energize auxiliary relays in the same circuit. The auxiliary relays control contacts on the various equipment or actuate still other slave relays that control contacts on equipment. These slave relays are located at the equipment switchgears along with the switchgear and bus interlocking and undervoltage relays.

Two safety injection actuation logic trains "a" and "b" are utilized for redundancy. The duplication begins at the bistables and continues to the various equipment. SIAS logic train "a" is supplied with power from the 125 V dc distribution panel 31 and logic train "b" from the 125 V dc distribution panel 34.

The SIAS was modeled for failure to initiate or transmit a signal to the various equipment. A brief discussion of the models for each of the initiation signals is given below.

The low pressurizer pressure signal is activated whenever any two of three pressures indicate below 1720 psig. The pressure signals are derived from the same pressure channels used for the low pressure reactor trip, however, lead-lag amplifiers are not used. This trip logic can be manually bypassed using a "block SI" switch in the control room to allow for normal reactor coolant system cooldown and depressurization. This SIAS initiation signal would fail whenever any two of the three pressure sensor channels fail or by the manual bypass.

The steam break upstream of the Main Steam Isolation Valves logic uses a comparison logic circuit whereby each of the steam generator's pressure is compared to the steam pressure in each of the other three steam generators. A 2 out of 3 logic is used such that if a given steam generator pressure is more than 125 psi lower than 2 of the 3 remaining steam generators, a safety injection actuation trip signal will be generated. The comparison logic would fail whenever any 2 out of 3 steam generator pressure inputs fail. The SI trip logic would fail when all 4 comparison logics fail.

The steam break downstream of the main steam isolation valve logic uses the steam flow as measured by sensing the differential across a steam flow element in the main steam line. One flow element and two delta-p transmitters are used for the main steam line associated with each steam generator. The output from each delta-p transmitter is compared to a reference signal based on the turbine first stage pressure in flow control comparison bistables. The comparison bistables (2 per steam line) feed into a 1 out of 2 logic circuit (1 per steam generator). The 1 out of 2 logic circuits would fail whenever both inputs fail. The four 1 out of 2 logic circuits then feed into a 2 out of 4 logic circuit for the generation of the steam break signal. Thus, steam break downstream of the MSIVs must be sensed by 2 out of 4 flow channels to initiate a safety injection trip. This logic circuit would fail whenever any 3 out of 4 inputs fail. The SI actuation signal is also interlocked with either a low t_{avg} signal (2 out of 4 steam pressure channels below 544°F) or a low steam generator pressure signal (2 out of 4 steam pressure channels below 600 psig). These interlocks are provided in order to allow for startup, steam dump or atmospheric relief valve protection.

The high containment pressure logic is activated whenever any 2 out of 3 containment pressure channel inputs register a containment atmosphere pressure of 2.0 psig or greater. This logic exists to limit the maximum atmospheric pressure within the containment due to a primary or secondary leak. This system would fail whenever any 2 out of 3 containment pressure channel inputs fail.

The high-high containment pressure trip logic is activated whenever any redundant 2 out of 3 containment pressure channel inputs register a containment atmosphere pressure of 28 psig or greater. This SI actuation trip logic acts as a backup to the high containment pressure trip logic. In addition to initiating safety injection, high-high containment pressure will also result in a phase "b" containment isolation, a containment ventilation isolation, containment spray actuation and steam line isolation. This trip logic exists to close the steam line air operated check valves to prevent overpressurization of the containment due to a steam break inside the containment with simultaneous failure of the nonreturn check valve in that loop. A second reason for this trip logic is to block the path of the steam line rupture since that path connects the containment atmosphere with the secondary plant or the outside atmosphere. Since the containment spray system uses highly corrosive NaOH additive, redundant logics are used to trip the high-high containment pressure signal to prevent actuation of the sprays on a spurious signal.

The SIAS initiation signal could fail to be transmitted in the circuitry. The contacts in both SI actuation trains for all of the master relays are normally energized and de-energize when tripped except for the high-high containment pressure trip. Therefore, only the ac power for the high-high containment pressure trip need be modeled since loss of ac power to all other SI actuation trips will lead only to a spurious SI signal. The SI master relays will trip on loss of dc power in each train. However, since the auxiliary relays are also powered by the same dc bus, they will not energize to transmit the SI actuation signal.

The SI slave relays were modeled along with the bus interlocking and undervoltage relays. The connection to their associated equipment could fail due to relay failure or failure of their associated dc power supply.

The bus undervoltage relays associated with the switchgears were modeled to respond to an inadvertent undervoltage signal in their respective bus. This was done because the undervoltage relays trip various equipment off line. A more detailed discussion of the undervoltage relays and their association with load shedding and re-energizing is given in the discussion of the electrical system (Sections 2.2.9 and 2.3.6).

In some instances, the failure of the SI signal or the transmission of an inadvertent undervoltage signal has a beneficial effect. (For example: blocking the trip of a certain pump.) These "success" paths were included in the SI model.

2.3.3. Main Feedwater Digraphs

2.3.3.1 Introduction

The main feedwater system is designed to supply coolant to the secondary side of the four steam generators (SGs). This secondary coolant removes heat from the primary coolant system and is converted to steam that drives the turbine generator. Once through the main turbine, the steam is condensed and returned to the SGs as secondary coolant.

The successful operation of the main feedwater system requires normal levels be maintained in all four steam generators. Thus, the failure criterion for the main feedwater system is failure to supply sufficient coolant flow to any one of the steam generators.

The main feedwater system can be considered as having four functional divisions: 1) two turbine-driven main boiler pumps, 2) secondary coolant delivery to the SGs, 3) main steam from the SGs to the turbine generator, and 4) condensate make up to the boiler feed pumps. A discussion of the main feedwater system models following the four functional areas is given below. (See associated P&IDs and Digraphs in B.3 in Appendix B.)

2.3.3.2 Main Boiler Feed Pumps

The two main boiler feed pumps facilitate the transport of secondary coolant to the four steam generators. Both pumps are required to operate to maintain normal SG levels. Therefore, failure of either pump will result in the failure of the main feedwater system.

Each boiler feed pump (BFP) assembly consists of a horizontal steam driven turbine coupled to a horizontal single-stage centrifugal pump, a control and lubrication system and associated control circuitry. Both pumps are supplied with a single seal-water injection system. The model for these pumps consists of a set of unit models which include their support systems.

Each BFP turbine is controlled by a control oil system that consists of several servomotors and controllers, an oil collection tank and interconnection with the turbine and pump lubrication oil and the BFP oil console. The various servomotors and controllers are listed below:

1) High pressure stop value controller and servomotor,
2) High pressure governor valve servomotor,
3) Low pressure stop valve controller and servomotor,
4) Low pressure governor valve servomotor,
5) Auto-stop trip system that trips the turbine on overspeed (5800 rpm), low bearing pressure (< 10 psig), low condenser vacuum (< 16.2 inch H_2O), manual trip and solenoid trip. The solenoid trip shuts down the turbine on bearing wear indications and local or remote manual trip.

The servomotor and controller assemblies control contacts in the turbine trip, reset, governor and stop valve circuitry. All BFP control circuitry is designed such that loss of dc control power will not trip the BFP turbine.

The oil pressure to the each control oil system is supplied by the BFP main oil pumps.

The assumptions used to model the BFP control oil system were:

1) loss of oil pressure to any controller or servomotor will change the state of the associated contacts in the control circuity,
2) no flow or low oil level in the oil collection tank will send a signal to the BFP main oil pumps,
3) loss of oil return from any assembly in the control oil system will not fail the tanks delivery to the main oil pumps, and
4) loss of oil return from the BFP turbine or pump bearings will fail the tanks delivery to the main oil pumps (low tank level).

In addition, loss of oil pressure to either turbine or pump bearings will trip the associated boiler feed pump.

Each BFP turbine trip and reset circuit actuates a solenoid that vents instrument air and closes the steam inlet valve. This solenoid is normally de-energized and is energized by closure of several contacts, some in a logic matrix, from the bearing protective device, the overspeed trip device, the BFP discharge valve, a remote control switch and a local trip pushbutton on the BFP control console.

The governor valves control the turbine speed by adjusting the amount of steam into the turbine. There are two governor valves; one on low pressure steam and one on high pressure steam. Both governor valves are controlled by the BFP control oil system and close on loss of oil pressure.

The high and low pressure stop valves shut off the high and low pressure steam from entering the turbine, upsteam of the governor valves. These valves are also controlled by the BFP control oil system and operate to trip the turbine loss of oil pressure.

The BFP seal water injection system consists of two pumps that take suction from the condensate system and inject water into the seal area of each pump. Only one injection pump is necessary to produce sufficient seal water pressure. Therefore, failure of both pumps will cause a failure in seal water injection and ultimately, failure of the boiler feedwater pumps.

Both boiler feed pumps and turbines are cooled by the service water system. Failure of service water cooling will cause the boiler feed pumps and turbines to trip. In addition, service water also cools the BFP control and lubrication oil through two heat exchangers. One heat exchanger will provide sufficient cooling. Therefore, failure of cooling to both heat exchangers is necessary to cause high oil temperature that would fail (or trip) the main BFP oil pumps.

2.3.3.3. Secondary Coolant

Both boiler feed pumps deliver secondary coolant to a common header that supplies flow to three feedwater heaters (36A,B,C) and a bypass line. The discharge from the heaters and bypass line feed a header that goes to the four steam generator feed lines.

The model for flow to the four steam generators is based on the two following assumptions:

1) flow through any 3 of the 4 heater paths (3 heaters, 1 bypass) is sufficient to supply the four steam generators with feedwater. Therefore, failure is defined as failure of any two paths, and
2) the feedwater heaters contribute to the failure of the flow path only if they are blocked and do not pass flow. Failure of the heaters to provide heating of the feedwater is not considered to contribute to the failure of the flow path.

Flow is supplied to each steam generator through a main feed line or a low-flow bypass line. Each line is capable of supplying sufficient flow to maintain normal steam generator level. Therefore both lines must fail to deliver flow before secondary coolant make-up is lost to each steam generator.

Both the main feed and low-flow bypass lines are equipped with pneumatically operated feed regulator valves. These valves will fail closed on loss of instrument air. The main feed regulator valves are automatically controlled by the feedwater control system. The low-flow bypass regulator valves are manually controlled.

2.3.3.4 Main Steam

The main steam system supplies the main turbine with high pressure steam. This system also supplies the two boiler feed pump turbines and the turbine-driven auxiliary feedwater pump with steam. The main steam system was not modeled except for the connections to these three turbine-driven pumps.

2.3.3.5 Condensate System

The condensate system supplies coolant to the boiler feed pumps suction. This system consists of three main condensers, three condensate pumps, heater drains return, flash evaporator, steam-jet air ejector condenser, gland-steam condenser, three low pressure feedwater heater trains (31A,B,C and 32A,B,C), three feedwater heater trains (33A,B,C;34A,B,C;35A,B,C) and associated piping.

Each main condenser supplies coolant to the condensate pumps inlet header with two lines. The model assumes that any of the six lines provide adequate suction to the condensate pumps.

During full power operation, all three condensate pumps must be operating. Therefore, failure of any one condensate pump will fail boiler feed pump suction requirements.

Condensate pumps 31, 32 and 33 are supplied with ac current from the 6.9 kV buses 2, 3 and 4, respectively. The condensate pumps deliver coolant to a discharge header which branches into three flow paths; 1) flow path A, through the steam-jet air ejector condenser and the gland steam condenser to the low pressure feedwater heater train inlet, 2) flow path B, which flows directly to the low pressure feedwater heater train inlet where it combines with flow path A, and 3) flow path C, which is a recirculation path back to the main condensers.

The combined flow of paths A and B goes through three parallel sets of low pressure feedwater heaters. The heater train is also equipped with a valved bypass line. Flow is required through 3 of the 4 heater train flow paths (3 heater sets and 1 bypass line). Therefore, insufficient flow will result if any combination of two paths fail.

After passing through the low pressure feedwater heater train, the condensate flow splits into two paths. One path goes directly to the inlet of the feedwater heater train with the other passing through the flash evaporator. These two paths recombine before going to the feedwater heater train. Both the direct and flash evaporator paths are capable of supplying sufficient flow to the feedwater heater train. Therefore, both paths must fail to pass flow for this subsystem to fail.

The boiler feed pumps normally receive flow from a header connected to pump 31 that continues to pump 32. This is the normal flow path from the feedwater heater train. However, there is a bypass line that connects to pump 32 first then continues to pump 31 via the same header used for the normal flow path. Thus, there is a crosstie situation for the adjoining header. The only other pathways for flow to the boiler feed pumps are from the heater drains tank or the "dynamite" valve, FCV1150. Valve FCV1150 could be used to bypass all components between the condensate pumps and the boiler feed pumps, however, operators are under strict orders not to use this valve. Additionally, the valve is reportedly going to be removed. Thus, valve FCV1150 and its flow path were not modeled.

The boiler feedpumps require 3 of the 4 incoming feedwater heater lines (3 from the heaters and the 1 bypass) to fulfill suction requirements.

Also, there must be flow from the heater drains tank, which supplies 35% of the feedwater suction requirements. Therefore, failure of condensate make up to the boiler feedpumps is failure of any 2 of the 4 incoming feedwater lines, or, failure of the heater drains return.

Coolant from the No. 35 and 36 heater drains and the main stream drains tank is collected in the heater drains tank and pumped to the boiler feed pumps inlet header. The piping from the heater drains tank to each heater drains pump has a level control valve operated by a pneumatic tank level controller. The unit model for the tank assumes loss of instrument air to the tank level controller will shut both level control valves.

The two centrifugal heater drain pumps are remotely controlled from the central control room. Pumps 31 and 32 are powered from the 6.9 kV buses, 3 and 4 respectively. These pumps will trip from:

1) motor thermal overload,
2) overcurrent, instantaneous and time delayed,
3) low-low discharge flow
4) low-low heater drains tank level, and
5) main generator primary and backup trips.

The heater drain pumps will not trip on loss of dc control power. In addition, the instrumentation bistables associated with the pumps are considered normally de-energized so that a loss in an instrument bus will not trip the pumps.

2.3.4 Auxiliary Feedwater System Digraphs

The auxiliary feedwater system provides secondary coolant to the four steam generators in the event of failure of the main feedwater system. During reactor shutdown conditions, the auxiliary feedwater system must supply at least one steam generator with secondary coolant using at least one auxiliary feedwater pump to remove core decay heat. Therefore, failure of the auxiliary feedwater system is a failure to supply at least one steam generator with secondary coolant flow. (See associated P&IDs and digraphs in B.4 of Appendix B.)

The auxiliary feedwater system consists of three auxiliary feedwater pumps, two electric motor-driven and one turbine-driven, feedwater coolant supply and secondary coolant delivery piping to the steam generators. The feedwater coolant supply is from two sources: the condensate storage tank or a piping bridge from Unit 1 that connects to the 1.5-million gallon water storage tank and the Buchanan City Water System. The city water supply is considered an infinite supply of coolant.

The two motor-driven Auxiliary Feedwater (AFW) pumps 31 and 33, are powered by the 480 V buses 3A and 6A, respectively. AFW pump 31, supplies secondary coolant to steam generators #31 and #32 through individual pipes connected to the pump discharge header. AFW pump 33 feeds steam generators #33 and #34. All four of these steam generator supply lines are equipped with pneumatically operated, manually controlled AFW regulator valves (FCV406A,B,C,D). These valves require instrument air to close and fail "as is". Therefore, loss of instrument air will not result in their failure. Additionally, the ability to regulate feedwater to limit steam generator thermal loading and excessive primary coolant system cooldown is needed. Therefore, all feedwater regulator valves, both main and auxiliary, are supplied with a backup nitrogen system.

The turbine-driven AFW pump, 32, supplies all four steam generators through four lines connected to the pump's discharge header. Each line is equipped with a pneumatically operated, manually controlled feedwater valve (FCV405A,B,C,D). These valves also require instrument air to close.

The four auxiliary feedwater supply lines from the motor-driven pumps combine with the lines from the turbine-driven pump before going to the steam generators. These auxiliary feedwater supply lines join with the main feedwater lines downsteam of the main feed and low-flow bypass regulator valves and the steam generator inlet flow instrumentation.

Suction to the three AFW pumps is supplied by the condensate storage tank (600,000 gal) or the Buchanan City Water System. The condensate storage tank feeds a header that supplies the three pumps. The city water supply also feeds a header. The suction lines from both headers combine before entering each pump's intake. Each pump suction line from the city water header is equipped with a pneumatically operated valve that fails in the open position. The suction line from the condensate storage tank and the three lines from the associated header are equipped with manually operated valves.

The unit models for the AFW pumps consist of the AFW auto-start circuitry, the 480 V feed breakers for pump 31 and 33, and the steam supply and control for pump 32.

The AFW auto-start circuitry receives signals from the AFW actuation system, and the main boiler feed pumps and discharge valves and actuates contacts in the 480 V feed breaker circuitry for pumps 31 and 33 and the steam supply circuitry for pump 32. The auto-start circuit was modeled such that it fails to start any of the three pumps.

For the AFW pumps 31 and 33, the auto-start circuitry fails to transmit the signals from the actuation circuitry or the boiler feed pumps by not closing the appropriate contacts in the 480 V feed breaker circuitry. For the AFW pump 32, failure to transmit the actuation signal results in failure of a solenoid to be de-energized and vent instrument air from the AFW turbine inlet steam control valve, PCV1139. In addition, AFW pump 32 can be tripped by inadvertently energizing this same solenoid since instrument air is needed to close the valve. Therefore, failure in instrument air will not fail PCV1139.

The 480 V feed breaker circuitry controls the ac circuit breaker that connects the pump motor to the ac buses. This circuitry has several control switches and sets of contacts that actuate the breaker closing and trip coils. The model of this circuit was developed such that the switches or contacts would fail to actuate the closing (close the ac breaker) or would actuate the trip coil (trip the breaker open). Operator errors include either failure to turn on the pump or to inadvertently trip it.

The AFW pump 32 turbine steam supply control system was not modeled extensively. However, nodes for the local hand controller of valve PCV1139 were included along with operator interaction. The steam supply to the AFW turbine comes from the main steam system which was not modeled. However, the inlet steam line contains two pneumatically-operated temperature control valves (PCV1310A & B) that close in the event they sense a high temperature in the AFW pump room or the room just above, where the main steam lines leave the containment building. These two valves were included in the model since they require instrument air to open and will fail closed.

The AFW turbine has four drain lines on the turbine exhaust. If all four lines become blocked, the turbine will trip.

The AFW pumps 31 and 33 are cooled by an internal cooling system that use the pump suction as coolant. This internal cooling was not modeled. The AFW pump 32 and turbine has a self-pumped external cooling system that was included in the model.

2.3.5 Feedwater Actuation Logic Digraphs

2.3.5.1 Overview

The feedwater actuation logic consists of two systems: the main feedwater isolation system and the auxiliary feedwater actuation system. Both of these systems were designed using the same philosophy as the Safety Injection Actuation System. That is, a normally energized ac circuit containing an instrument, an amplifier, test points and a bistable. The bistable de-energizes two ac relays in different trains (A & B) for redundancy.

Each ac relay controls contacts arranged in a logic matrix on a dc circuit that de-energizes master relays. The master relays control contacts that energize auxiliary relays. The auxiliary relays control contacts on the specific equipment. (See associated Schematics and Digraphs in B.5 of Appendix B.)

2.3.5.2 Main Feedwater Isolation

The main feedwater isolation system is part of the plant protective system and trips the main boiler feed pumps by closing the boiler feed pumps discharge valves. This isolation system also closes the main feed regulator valves (FCV 417, 427, 437 and 447) and trips the main turbine. The main feedwater isolation signals are:

1. high-high steam generator level (>70% of span) sensed by two of three level instruments on any steam generator,
2. low steam generator temperature coincident with a reactor trip signal when the steam generator level control is in automatic, and
3. a safety injection signal.

Success of the main feedwater system is continued operation. Therefore, the model was developed for isolation of main boiler feed resulting from failures in the isolation system. Additionally, successful transmission of any signal that would isolate main feedwater was also modeled. Since main feedwater isolation results from successful operation of the isolation system, this digraph is a model of how the system was designed to succeed and modeled in success space with faults as initiators.

The model consists of two parts. The first part models the logic signal through its transmission to isolation of the main feedwater (signal model). This model is overlayed on the logic diagram (VE&C Dwg #5651D72). The diagram does not, however, represent the actual hardware wiring of the many relays and contacts that make up this system. The second part of this model represents the actual physical make up of this system, trying to adhere to the representation of the signal model. The second part of the model also models the hardware as unit models of the logic gate nodes on the signal model. The model assumes that the steam generator levels are being controlled by the automatic level control system.

2.3.5.3 Auxiliary Feedwater Actuation

The auxiliary feedwater actuation system closes the main ac circuit breakers on the motor-drive AFW pumps and starts the turbine-driven AFW pump. The two motor-driven AFW pumps will be automatically actuated under any of the following conditions:

1) loss of voltage on the 480 V bus 3A (AFW pump 31) or bus 6A (AFW pump 33) without a safety injection initiation signal (this action is time delayed for 28 seconds until the diesel generators load onto the 480 V buses),
2) very low level in any steam generator (< 15% span), sensed by two of three level instruments,
3) trip of either main boiler feed pumps through the main boiler feed pump turbines auto-stop oil pressure signals,
4) a safety injection signal.

The turbine-driven AFW pump will automatically start if either:

1) a very low level exists in any two of the four steam generators (<15% of span), or
2) normal power to the 480 V buses 6A or 3A is lost (if a safety injection signal does not exist).

This system was modeled for failure to detect or transmit the actuation signal. For the two motor-driven AFW pumps, for condition 2 above, the pumps first trip and are then brought back on line. This tripping was included in the model. The turbine-driven AFW pump requires that its remote trip pushbutton be in the reset position or it will not start. This includes failure of the trip switch contacts to open and operator error for tripping the turbine.

2.3.6. Electrical Power System Digraphs

2.3.6.1 Introduction

This section describes the electrical system models, including 6900, 480 and 118 V ac power and 129 V dc power. A fundamental assumption in the modeling is that the reactor is operational at power and all components are in their normal operational state prior to a postulated accident sequence. In this state, all electrical buses are powered from their normal supply, and all bus tie breakers are open.

Since the electrical system interacts with all of the other plant systems modeled, extensive effort went into developing a large detailed model. The system combinations involving loss of offsite power with unit trip are especially interesting from the standpoint of systems interactions with the electricalsystem, and the models are designed to capture these interactions.

Several features of the model are important in understanding its overall design. First, the primary model is known as a "block" model, meaning than when a component fails the effect is to block the flow of electrical power downstream. An example of such a failure is the inadvertent trip of a normally closed bus feed breaker. A "break" model then overlays portions of the block model. In the break model a component fails via a short circuit from itself to ground, thereby blocking the flow of electrical power downstream as in the block model. However, the failure can also propagate upstream if the appropriate circuit breaker or fuse fails to open. Another feature of the model is the extensive development of electrical crossties, including automatically actuated crossties, manual crossties, and available manual crossties which have no procedures allowing their use. Finally, since the electrical system is organized into trains with many similar components, extensive use was made of unit models in constructing the digraphs. Node names on the unit model digraphs will contain generic characters, to which an accompanying table of specific characters is applied depending on the train of interest.

2.3.6.2 Block Model

2.3.6.2.1 Overview of Block Model

A block model was constructed for all portions of the electrical system of interest to this study. A single digraph (Appendix B.6.1.A) overlays the corresponding electrical drawing (9321-F-33853-1) and shows a simplified logical representation of the main components in the system. The purpose of this digraph is to present the basic hardware layout of the electrical system, without the clutter of support systems, unit models, and rigorous modeling of bidirectional flows.

The electrical system model includes 6900, 480, and 118 V ac power supplies as well as 129 V dc power. The 6900 V power is normally supplied from offsite power through the Station Auxiliary Transformer (STAUXXFMR) to Bus 5 and Bus 6, and from the main generator through the Unit Auxiliary Transformer (UAUXXFMR) to Buses 1, 2, 3, and 4. An alternate supply of 6900 V power is available from the 13.8 KV substation (13.8SUB) which includes gas turbines #1 and #2. These three nodes represent incoming 6900 V power on the digraph.

The six 6900 V buses are crosstied with four breakers (BKRUTIST5, BKRUT2ST5, BKRUT3ST6, BKRUT4ST6). The combination of these crosstie capabilities and the use of three input power sources gives a large variety of possible circuits to power each bus. The only restriction placed on potential use of these circuits is an interlock preventing simultaneous closure of BKRST5 with BKRGT5, and BKRST6 with BKRGT6. In digraph B.6.1.A, the 6900 V crosstie network model is simplified to illustrate possible power flows without the emcumbrance of a myriad of dummy nodes needed to rigorously model the bidirectional flows. Each 6900 V bus, feed breaker, and tie breaker is fed by an AND gate whose inputs represent each of the possible power sources. The bidirectional edges from these components to the AND gates represent power flow through the components and into other components. For example, the STAUXXFMR node suplies BKRST5 through an AND gate. From BKTST5, power flows to BUS 5 through a 3-input AND gate.

From the 6900 V buses, power flows through the six station service transformer feed breakers to the transformers, which supply 480 V power through feed breakers to the six 480 V buses. Simplified crossties are again shown between BUS312 and BUS313, and BUS2 and BUS3. Crossties also exist between buses 5A and 2A, and 3A and 6A; but since plant technical specifications prohibit their use when the plant is above cold shutdown conditions, only the breakers themselves (BKR2AT5A, BKR3AT6A) are sh wn on digraph B.6.1.A.

Three diesel generators (GENSDL33, 31, and 32) are modeled as redundant power feeds through their output breakers to their respective 480 V buses (BUS5A, 2A, and 6A). The 480 V buses then supply an assortment of motor control centers (MCC) through individual MCC feed breakers, and also supply lighting bus 32 (L1BUS32) through a breaker (BKRLTBUS32) and transformer (XFMRLT32). The 480 V buses and MCCs power the plant safeguards components. Modeling for these connections is contained in the individual component unit models for each system.

Four trains of 129 V dc power supply the dc powerpanels (PWRPNL31, 33, 34, 32). Each powerpanel receives redundant power from its charger through the charger output breaker and from its battery through the battery output breaker or fuse. The chargers are supplied by MCCs through charger input breakers. Although the chargers do provide continuous charging to the batteries during normal operation, this connection was not modeled since the battteries will last approximately 8 hrs without charging. Therefore, the batteries are treated like an independent source of dc power in the model. DC powerpanel 31 supplies dc distribution panels 31 and 33 (PNLDIS31, 33) through breakers, and powerpanel 32 supplies distribution panels 32 and 34.

Each dc powerpanel provides the normal power supply to its associated 118 V instrument bus (IBUS31, 32, 33, 34) through a static inverter (STATINV31, 32, 33, 34). Instrument buses 31, 32, and 33 have a backup power supply through individual switches from lighting bus 32 (LTBUS32), which is powered from bus 3A through a breaker and lighting transformer 32 (XFMRLT32). Instrument bus 34 has this same backup supply, plus another backup from MCC36B through the Solatron transformer (XFMRSOLA) and another switch. Therefore, a 3-input AND gate connects to IBUS34.

Note that digraph B.6.1A does not show unit models for the breakers and the diesel generator support systems. The modeling of operator actions and dc control power is contained in those unit models to be described in the next section. Also included there are the detailed models of the electrical crossties.

Figure B.6.1.B overlays digraph B.6.1.A and shows how the digraphs in the block model are organized. Groupings consist of: the 6900 V crosstie (digraphs B.6.2.A - B.6.2.B, B.6.3.A - B.6.3.D); the 480 V crosstie including diesel generator support systems (digraphs B.6.4.A-B.6.4.B, B.6.5.A - B.6.5.E, B.6.6.A - B.6.6.G); motor control centers (B.6.8 - B.6.9); dc system (digraphs B.6.10, B.6.23 - B.6.24); and 118 V ac system (digraphs B.6.25 - B.6.26). Associated with each component in digraph B.6.1.A is a letter designating the location of that component according to the key provided.

2.3.6.2.2. 6900 V Crosstie Model

The block model for the 6900 V crosstie consists of two complex unit model digraphs, digraph B.6.2.A for buses 1-4, and digraph B.6.2.B for buses 5-6. In each of these models, the terminal mode is labeled DUMBUS*, where * refers to the bus of interest. This node represents power flowing from the bus to the station service transformer. Many other "dummy" nodes appear on the digraphs beginninig with DUM..., representing power flows through the crosstie in various directions from each possible source.

Let us examine digraph B.6.2.A for bus 1 in detail, using the key, * = 1, $ = 2, ? = 4, + = 3, # = 5, and / = 6. Node DUMBUS1, the output of bus 1, fails if the bus itself fails (BUS1), or if all power into bus 1 fails (DUM691 and DUMCT12B). Node DUMCT12B represents power from bus 2 to bus 1 through tie breakers UT1ST5 and UT2ST5. This path fails if either tie breaker fails open, or if bus 2 fails, or if the power supply to bus 2 fails (UAUXXFMR and DUM2Z34). Node UAUXXFMR represents the power source form the unit aux transformer. Node DUM2Z34 represents power to bus 2 from bus 3 (DUM123) and to bus 2 from bus 4 (DUM124), both through breaker UT2. Node DUM123 fails if breaker UT3 fails open, or if bus 3 fails, or if bus 3 fails to receive power (DUM36). Similarly, node DUM124 fails if breaker UT4 fails open, if bus 4 fails, or if bus 4 fails to receive power (DUM46). Node DUM36 represents the power supply to bus 3 from bus 6 through breaker UT3ST6. It fails if the breaker fails open, if bus 6 fails, or if bus 6 fails to receive power (DUM6FEED). Similarly, node DUM46 represents the power supply to bus 4 from bus 6 through breaker UT4ST6. Refer to digraph B.6.2.B for the development of node DUM6FEED. It fails if its two power sources fail (DUM138KV6 and DUMGT6). Node DUM138KV6 represents power to bus 6 from the station aux transformer through breaker ST6 (the normal feed). Node DUMGT6 represents power to bus 6 from the 13.8 kV substation through breaker GT6 (a backup source). Now this crosstie from bus 2 to bus 1 has been fully developed back to all three possible sources.

Following the top branch of the AND gate for power feed to bus 1, node DUM691 represents all other possible power feeds and fails if DUMUT1 and DUMCT15 fail. Node DUMCT15 represents power from bus 5 to bus 1 through breaker UT1ST5. This path fails if the breaker fails open, bus 5 fails, or if bus 5 fails to receive power (node DUM5PWR). Refer to digraph B.6.2.B for the development of node DUM5PWR.

Node DUM5PWR fails if bus 5 fails to receive power through breaker ST5 (node DUMST5PWR) and if bus 5 fails to receive power through breaker GT5 (node DUMGT5PWR). Node DUMST5PWR fails if the power feed from the station aux transformer fails (normal supply) and crosstie power feed from bus 6 through breaker ST6 fails (node DUMCT56S). Node DUMGT5PWR fails if the power feed from the 13.8 kV substation fails and crosstie power feed from bus 6 through breaker GT6 fails (node DUMCT56G). Both nodes DUMCT56S and DUMCT56G fail if bus 6 fails, their respective bus 6 feed breakers fail open, or if bus 6 fails to receive power. Since breakers ST6 and GT6 may not be closed simultaneously, then in this case bus 6 fails to receive power if the crosstie from bus 3 through breaker UT3ST6 fails (DUMCT563) and if the crosstie from bus 4 through breaker UT4ST6 fails (DUMCT564). Both of these crossties fail if their respective buses or tie breakers fail, or if the source power feed from the unit aux transformer fails.

Refer back to node DUMUT1 on digraph B.6.2.A, which represents power feed to bus 1 through breaker UT1. This fails if the crosstie from bus 4 to bus 1 through breaker UT4 (DUMCT14) fails, and if the crosstie from bus 3 to bus 1 through breaker UT3 (DUMCT13) fails, and if the crosstie from bus 2 to bus 1 through breaker UT2 (DUMCT12T) fails, and if the normal feed from the unit aux transformer fails.

Developing these crossties, node DUMCT14 fails if bus 4 or breaker UT4 fail, or if bus 4 fails to receive power from bus 6 (DUM46) through breaker UT4ST6. Similarly, node DUMCT13 fails if bus 3 or breaker UT3 fail, or if bus 3 fails to receive power from bus 6 (DUM36) through breaker UT3ST6. Both DUM46 and DUM36 fail if bus 6 or their respective tie breakers fail, or if bus 6 fails to receive power from the station aux transformer and 13.8 kV substation (node DUM6FEED which was developed earlier). Finally DUMCT12T fails if bus 2 or breaker UT2 fail, or if bus 2 fails to receive power from bus 5 (DUM5FEED). Node DUM5FEED fails if the power feed from the station aux transformer through breaker ST5 fails, and if the power feed from the 13.8 kV substation through breaker GT5 fails (digraph B.6.2.B).

Now we have shown the detailed model for power feed to bus 1 directly from the unit aux transformer, with alternate paths from bus 5, bus 3, bus 4, bus 6, and two paths from bus 2, and two alternate power sources (station aux transformer and 13.8 kV substation).

Let us now examine digraph B.6.2.B, using bus 5 as an example. Power supply to bus 5 fails if crosstie power from bus 2 through breaker UT2ST5 fails (DUM52), and if crosstie power from bus 1 through breaker UT1ST5 fails (DUM51), and if the power feeds through breakers ST5 and GT5 both fail (DUM5PWR). Node DUM5PWR was developed earlier. Node DUM52 fails if bus 2 fails, or if breaker UT2ST5 fails open, or if breaker UT2 fails open, or if bus 2 fails to receive power (node DUMCTA5). Similarly, node DUM51 fails on the same respective situations, and has the same power feed as DUM52 in this case. Node DUMCTA5 fails if its direct power feed from the unit aux transformer fails, and if crosstie power from bus 3 (DUM5Z3) and bus 4 (DUM5Z4) fail. Each of these crossties fail if their respective bus or feed breaker fails, or if the power feeds from the station aux transformer and the 13.8 kV substation (DUM6FEED) to bus 6 fail.

2.6.2.3 Main Generator/Unit Aux Transformer Trip

The detailed model of the 6900 V crosstie network described above contains three power sources, the station aux and unit aux transformers and the backup supply from the 13.8 kV substation. However, all system combinations require a main generator (and unit aux transformer) trip soon after accident initiation. Therefore, the 6900 V crosstie model was revised in order to remove the unit aux transformer as a power source. To this extent, the model no longer represents the plant in its normal state.

In order to remove the effects of the unit aux transformer while still leaving it in the digraph, the following changes were made. Every place node UAUXXFMR enters digraphs B.6.2.A and B.6.2.B, the entry is into one side of an AND gate. Then for each of these gates, the other input is directly connected to the gate output, effectively "shorting out" the UAUXXFMR node. These connections are shown on the digraphs as dashed lines.

2.3.6.2.4 Unit Models for 6900 V Breakers

The circuit breakers modeled in the 6900 V system can be divided into three groups depending on their function. These groups are: normal bus feed or station service transformer feed breakers (ST5, ST6, UT1, UT2, UT3, UT4, SS2, SS3, SS5, SS6, SS312, SS313); bus tie breakers (UT1ST5, UT2ST5, UT3ST6,. UT4ST6); alternate bus feed breakers (GT5, GT6). A unit model digrap'ı for each breaker group is described next.

The unit models for breakers normally feeding the 6900 V buses and station service transformers are shown in digraphs B.6.3.A, B.6.3.B, and B.6.5.A. These breakers are normally closed and fail in the block model by opening inadvertently. This will occur if the lockout relay causes a spurious trip (R86...), if the operator errors by opening the breaker from the control room (OPWD...), or if the operator errors by opening the breaker locally (OPWA...).

The unit model for the bus tie breakers is shown in digraph B.6.3.C. These breakers are normally open and the block model depicts failure to close. This will occur if the automatic closing device fails (AXFR...), and if the operator fails to close them (OPRD...) via the switch in the control room (SW...), and if the operator also fails to close them locally. Both the switch and the automatic closing device require dc power (PWRPNL...) to operate, and an operator could err (OPWADC...) by removing the dc power feed at the breaker. The automatic closing device was not modeled in any greater detail.

The unit model for the alternate bus feed breakers is shown in digraph B.6.3.D. These breakers are normally open, so failure to close is modeled. This happens if the operator (OPRDGT...) fails to use the switch (SWGT...) in the control room, and if the operator fails to close the breakers locally. The switch will not function if dc power fails or if the operator removes the dc power feed. It will also fail if any of three interlocks fail. The interlocks require the associated normal feed breaker to be open (ITLST...), an undervoltage condition on the bus (ITLUV'BUS...), and the sync switch to be on (ITLSYCGT...). This latter interlock will fail if the switch itself fails (SWSYCGT...) or if the operator fails to turn it on (OPRDSWSYCGT...).

2.3.6.2.5 480 V Crosstie Model

The 480 V crosstie model consists of 4 trains of power from 6900 V buses 5, 2, 3, and 6 to 480 V buses 5A, 2A, 3A, and 6A. Each train in digraph B.6.4.A begins with the power output node of the associated 6900 V bus, DUMBUS*, goes through the station service transformer feed breaker (BKRSS*), the station service transformer (XFMRSS*), and the 480 V bus normal feed breaker. Diesel generators supply three of the 480 V buses through the generator output breakers. The other components in the model are the three 480 V bus tie breakers, between buses 5A and 2A (BKR2AT5A), between buses 2A and 3A (BKR2AT3A), and between buses 3A and 6A (BKR3AT6A).

The complex series of AND gates between the power sources for each train and the 480 V bus output node (DUMBUS*A) were constructed to model all possible crosstie power flows. In this model, a bus output will fail if the bus itself fails, or if all power into the bus fails. Power into the bus fails if normal power fails, backup power fails (except bus 3A), and all crosstie power fails. Crosstie power fails if the supplying bus fails, or if all power supplies to that bus (normal, backup, and other crossties) fail, or if the appropriate crosstie breaker fails to close.

For example, consider node DUMBUS5A in digraph B.6.4.A. This node fails if BUS5A fails, or if DUMAND1 and DUM2 fail. Node DUMAND1 represents normal power (BKR5A) and backup power (DUMDG33). Node DUM2 represents crosstie power from 2A, and fails if the tie breaker is open (BKR2AT5A), or if bus 2A fails, or if the normal and backup feeds for bus 2A fail (DUMAND2) and crosstie power to bus 2A from bus 3A fails (DUM4). Similarly, DUM6 represents crosstie power from bus 6A to bus 3A, DUM5 from bus 3A to 6A, DUM3 from 2A to 3A, and DUM1 from 5A to 2A.

The preceeding description of the 480 V crosstie model assumes that all three crossties can be used, giving each 480 V bus a choice of four 6900 V buses and three diesel generators to supply its power. However, plant technical specifications [Ref. SOP-EL-5 Rev. 5, Operation of On Site Power Sources, dated 5/27/83] prohibit breakers 2AT5A and 3AT6A from being closed when the plant is above cold shutdown conditions. A simple modification to the model disables these two crossties. This modification can be seen as the dashed line connections in digraph B.6.4.A. A connection was made from the allowable power sources to each bus outlet, eliminating the effects of nodes DUM1, DUM2, DUM5, and DUM6.

The modifications made to the 480 V electrical system to comply with "Appendix R" requirements are modeled in digraph B.6.4.B. These modifications include the addition of two trains, one each from 6900 V buses 1 and 3, through station service transformers to 480 V buses 312 and 313. Bus 313 then feeds MCC312A through a breaker. A simple crosstie was also modeled between buses 312 and 313.

2.3.6.2.6 Unit Models for 480 V Breakers

The breakers serving the 480 V crosstie can be divided into four functional groups. These are: normal bus feed breakers (5A, 2A, 3A, 6A, 312, 313); manual tie breakers (2AT5A, 3AT6A, 312T313); automatic tie breaker (2AT3A); and diesel generator output breakers (EG3, EG1, EG2). Following is a description of the unit model for each group.

The bus feed breakers are normally closed and fail by inadvertent opening in the block model. As seen in digraph B.6.5.B, failure occurs on a spurious overcurrent detection (OIBUS#A) or on a spurious undervoltage detection (UVBUS#A), or by the operator opening the breaker locally (OPWABKR#A), or via switches in the control room (OPWDSWCRBKR#A) or diesel building (OPWDSWDBBKR#A).

The manual tie breakers are modeled in digraph B.6.5.C. These breakers are normally open and failure to close is modeled. However, since breakers 2AT5A and 3AT6A are not used, this unit model does not normally apply. Also, no information was available on breaker 312T313. Therefore, it was assumed that this model applies. Nevertheless, should any of the breakers be used, they will fail to close if the operator fails to close them locally (OPRABKR#AT$A) and remote closure fails

(DUMBKR#AT$A). Remote closure fails if the switch fails (SWBKR#AT$A), its dc power supply fails (PWRPNL*), or if the operator fails to use the switch (OPRDBKR#AT$A), or if any of four interlocks fail. An interlock will fail if a spurious bus fault is detected (ITLBFBUS...), or if an undervoltage relay does not detect the undervoltage condition (ITLUV'BUS...). The undervoltage relay fails if its dc power supply fails.

Automatic tie breaker 2AT3A (digraph B.6.5.D) is normally open and fails to close and remain closed in the block model. This occurs if the automatic closing device fails (AXFRBKR2AT3A), remote closing fails (DUMBKR2AT3A), and local closing fails (OPRABKR2AT3A). The automatic closing device fails if any of six interlocks fail. An interlock fails if a spurious bus fault on bus 3A or 5A is detected (ITLBFBUS3A, ITLBFBUS5A), if the undervoltage relay fails to detect an undervoltage condition on bus 3A (ITLUV'BUS3A), if breaker 3A is not detected to be open (ITLBKR3A), if breaker EG1 is not detected to be closed, or if breaker 3AT6A is not detected to be open. The undervoltage and breaker EG1 interlocks fail if the dc power supply fails (PWRPNL33).

Remote closing of the breaker fails if the operator fails to use the switch in the control room (SWCRBKR2AT3A) and in the diesel building (SWDBBKR2AT3A). Both switches fail on loss of dc power. Remote closing also fails on any of four interlocks. A spurious bus fault detection on buses 2A or 3A fails the interlocks, as does failure of the undervoltage relay to detect an undervoltage on buses 2A or 3A.

A similar model was developed for the diesel generator output breakers (digraph B.6.5.E), which are also normally open and fail to close and remain closed in the block model. The basic failure modes are the same as breaker 2AT3A, but the interlocks are different. Automatic closure fails on any of six interlocks: failure to detect normal voltage on the diesel generator (ITLVDG3#), detection of a spurious fault on the diesel generator (ITLFDG3#); failure to detect an undervoltage on the bus; detection of a spurious fault on the bus; failure to detect the bus feed breaker being open (ITLBKR*A); and failure to detect the manual tie breaker being open (ITLBKR$). The first four interlocks also fail remote manual closure of the breakers. Failure of dc power fails the first three interlocks.

2.3.6.2.7 Diesel Generator Support Systems

Each diesel generator depends on a set of support systems for successful starting and continued operations (digraph B.6.6.C). The support systems are primarily dedicated to each diesel, but some commonalities do exist. The systems needed for starting are: diesel engine starting air system (digraph B.6.6.A) and its support system, diesel generator start signal (digraph B.6.6.E); and the diesel generator exciter (digraph B.6.6.F). The station service water hookup to the diesel engine cooling system (digraph B.6.6.G) is needed for continued operation, and the diesel engine fuel oil transfer system (digraph B.6.6.D) is needed for both starting and operation. Modeling descriptions for each support system follow.

Starting Air System

Each diesel generator has its own starting air system (STAIR$), but the air supplies can be crosstied. The air system fails to start the engine if both start motors (STMOT1$, STMOT2$) fail. Each start motor has an independent train back to the common air receiver. A start motor fails if its solenoid operated valve fails to open (VSOL...). This happens if the automatic start signal fails (STSIG...) and the operator (OPRAPB...) fails to use the local manual pushbutton (MPB...). It is assumed the solenoid valve fails to pass flow if the pressure reducing valve fails closed (VPR...). Flow to the pressure reducing valve fails if the receiver exit valve (VRCVR...) fails closed. The air supply to the exit valves fails if the receiver itself fails (RCVR$)) or if flow into the receiver fails. The receiver fails if it is not charged by its compressor (CMPSR$) and by the crosstie with the other two receivers (DUMAIR+). The compressor is powered by a motor control center. However, since the receiver is assumed to be charged initially, failure of the compressor will not fail the receiver until it is discharged. Therefore, a time transition node is placed between the compressor and the AND gate to the receiver (TTRCVR$). This node indicates that the failure is propagated only after a significant time delay. In addition, the connection from node CMPSR$ to TTRCVR$ is shown as dashed in digraph B.6.6.A because it is not included in the adjacency computer input in order to reduce problems with conditioned cycles (Section 2.3.6.3).

Crosstie flow into the receiver fails if an operator fails to open the equalizing valve (VEQL$) or if air is not available from both of the other receives (DUMAIR+-, DUMAIR+*). An alternate pathway from another receiver fails if that receiver fails, if its equalizing valve fails, or if the receiver is not charged by its compressor.

Diesel Start Signal

The diesel start signal logic supports the starting air system. The start signal to one of two start motors in a diesel engine fails if both the automatic (DUMSTAUTO+$) and manual (DUMSTMAN+$) signals fail. The automatic signal fails if the start switch (STSWDG+$) is not in the "auto" position, or if an undervoltage condition on the 480 V bus is not detected and the appropriate contacts from the Safety Injection Actuation System (RSISIG'Z+$) fail to generate a SI signal. The manually-activated start signal fails if the start switch is not in the "manual" position, or if the operator fails to push the start button (MPBDG+$). Loss of dc power supply to the start switch fails both the manual and automatic starting signal.

Diesel Generator Exciter

The diesel generator exciter was not explicitly modeled, with the exception of the connection from dc power. This connection is important, since loss of dc power fails the exciter which fails the diesel generator by preventing it from starting. Once started, however, the exciter no longer requires dc power.

Station Service Water Cooling

Once started, the diesel engines require immediate cooling from the station service water system. Diesel cooling fails (STSVW$) if either the jacket heat exchanger (JKTHX$) or oil coolers (OILCLR$) fail. These nodes are not modeled in detail, but are treated as boundary nodes which connect to the service water system. Failures in that system will propagate through to the diesels through these nodes.

Diesel Fuel Oil Transfer System

Each diesel engine has its own fuel oil transfer system, although all three systems are normally crosstied. Fuel oil supply to a diesel (OILXFR$) fails if the secondary duplex filter fails (FLTRB$), if the booster pump fails (PBSTR$), if the primary duplex filter fails (FLTRA$), or if the day tank exit valve fails to pass flow (VDF18#). This will happen if that normally open valve is erroneously closed by an operator (OPWADF18#) or if the day tank fails to provide flow (TKD$). Since the day tank is assumed to be full initially, a time transition node (TTTKD$) connects to it indicating that loss of fuel supply to the day tank fails flow from the tank only after the time interval needed for the tank to empty (approximately 1.4 hr). Therefore, for diesel engine starting and short term operation, the fuel supply to the day tank is not needed and any singleton or doubleton results which include nodes upstream of TTTKD$ can be disregarded. However, for accident sequences requiring longer term operation of the diesels, that supply is necessary.

The day tank fails to receive flow if all four valves feeding it fail to pass flow (LCV+A, VDF17#A, LCV+B, VDF17#B). Valves LCV+A and LCV+B are normally open and fail if operators erroneously close them or if the automatic closing device fails. Valves VDF17#A and VD17#B are normally closed and fail to pass flow if the operator fails to open them. Valves LCV+A and VDF17#A both connect to the normal fill line and fail to receive flow if the three normally closed valves to the line from each fuel train (VDF8A, VDF8B, VDF8C) fail to be opened by an operator. Valves LCV+B and VDF17#B both connect to the emergency fill line and fail to receive flow if the three normally open valves to the line from each fuel train (VDF9A, VDF9B, VDF9C) are erroneously closed by an operator. Note that the normal fill line acts as a backup to the emergency fill line in the system.

Flow to both fill line valves for a particular train fails if check valve VDF15# fails. Flow to this valve fails if check valve VDF15# fails. Flow to this valve fails if check valve VDF3# fails and alternate supply valve VDF20 fails (on train 33 only). The normally closed alternate supply valve fails to pass flow if an operator fails to open the valve, or if the diesel fuel truck fails to deliver fuel (TRUCK).

Valve VDF3# fails to receive flow if the transfer pump fails (PXFR$). The transfer pump fails to supply fuel if its power supply fails (MCC36*), if its start signal fails, or if the fuel oil storage tank fails (FTK$). The transfer pump fails to start if the automatic start switch (STPXFR$) fails or if the low level detector fails, and if the operator fails to manually start the pump (OPRAPXF$).

Since the underground fuel tanks are assumed to be full initially, they will have sufficient fuel for the duration of the accident sequences modeled (approx. 72 hr). Therefore, failure to fill the tanks is not included in the adjacency input, but is shown as a dashed connection on digraph B.6.6.D. Node TTFTK$ represents the time needed for the tank to empty. Once empty, the tank fails to receive fuel if its normally open inlet valve (VDF2#) fails or if an operator erroneously closes it. The inlet valves for all three tanks fail to receive fuel if valve VDF1 fails or if the operator fails to open it. Finally, valve VDF1 fails to pass fuel if the diesel fuel truck fails to deliver it.

2.3.6.2.8 480 V Motor Control Centers

The motor control centers supply 480 V power to various pumps, valves, and battery chargers, and other equipment throughout the plant. The MCCs are directly connected to the 480 V buses through MCC feed breakers (digraph B.6.8.A). Bus 5A supplies MCCs 36A,38, and 39; bus 6A supplies MCCs 36B and 37; bus 2A supplies MCCs 31, 33, 34, 36C, and 310; and bus 3A supplies MCCs 32 and 35. Connections from the MCCs to power the various plant components outside of the electrical system are made in the individual unit models for the system of interest.

There are two basic types of unit models for the MCC feed breakers (digraph B.6.9.A), depending upon their function during an accident. All MCC feed breakers are normally closed and fail by opening inadvertently. Breakers 36A, 36B, and 36C power the safeguards equipment and their loads are not stripped off on a safety injection signal. In fact, the SI signal closes them, should they be inadvertently opened. In the model, these breakers fail if the overcurrent device inadvertently opens them (OIBKRMCC#), or if the operator erroneously opens them either locally or from the control room after the accident has started. They also fail if they have been opened before the accident (STATUSMCC#), and the operator fails to close them either locally or from the control room, and the SI signal fails to close them automatically (RSISIG'Z).

The other breakers are tripped on SI signal and/or supply bus undervoltage. These breakers fail open if the overcurrent or undervoltage devices inadvertently open them, or if a spurious SI signal (RSISIGZ) inadvertently opens them (except for MCC34 and 39).

2.3.6.2.9 129 V dc System

There are four trains of dc power, each getting its normal supply through a battery charger from a different 480 V bus, and its backup supply from a dedicated battery. The dc power is distributed to components throughout the electrical system and the rest of the plant from distribution panels 31, 32, 33, 34 (PNLDIS...) and power panels 31, 32, 33, 34 (PWRPNL...). In digraph B.6.10.A, each distribution panel fails if the normally closed breaker from the power panel fails open, or if the power panel fails. The power panel fails if normal and backup power from its own train fails (DUMANDDC...) and crosstie power from the other train fails (DUMDC...). Normal power fails if the charger fails, if the charger input breaker fails open, or if the motor control center fails to supply power to the train. In addition, a spurious undervoltage signal trips the charger input breaker, and erroneous operator action can open the input and output breakers.

Backup power to the power panels fails if the battery output fuse (FUSEPNL#) or breaker (train 34 only) fails open, or if the battery fails, or if the battery is discharged after a period of use (TTBATTERY#). The battery is assumed to be charged initially, therefore, a time transition node indicates the latent failure. A dashed connection is shown from the charger output breaker to node TTBATTERY#, representing the continuous charging function of the charger. This connection is not included in the adjacency input, since we wish to treat the battery as an independent source of dc power in the model.

Although the crosstie between trains 31 and 32 is modeled in digraph B.6.10.A, the tie breaker is administratively controlled to allow closure only during cold shutdown conditions [Ref. System Description 27.1 Page 78]. Therefore, the dashed line connections from DUMANDDC1 to PWRPNL31 and from DUMANDDC3 to PWRPNL32 were added to the adjacency input to eliminate the effects of the crosstie in the model.

DC power trains 33 and 34 are modeled in digraph B.6.10.B. These trains do not power distribution panels, and there is no crosstie between trains. With these exceptions, this model is the same as the one for trains 31 and 32.

2.3.6.2.10 118 V ac System

There are four trains of 118 V ac power, one from each dc power panel through a static inverter to an instrument bus. For trains 31, 32, and 33 (digraph B.6.11.A), an instrument bus fails (IBUS$) if its normal supply and backup supply fails. The normal supply fails if the static inverter (STATINV$) or the dc power panel fails. The backup supply fails if an operator fails (OPRSWIB$) to switch over to the backup supply, if the switch itself fails (SWIBUS$), if lighting bus 32 fails (LTBUS32), if lighting transformer 32 fails (XFMRLT32), if the transformer feed breaker fails open (BKRLTBUS32), or if the 480 V power supply fails (DUMBUS3A). From digraph B.6.7.A, the feed breaker will also fail if load stripping relay R3-33A trips it spuriously, if a spurious undervoltage is detected on bus 3A, or if a spurious SI signal is detected. The back up supply is also assumed to fail, due to overloading lighting bus 32, if an operator attempts to use it to power more than one instrument bus at any time. This action is represented by node OPWLTBUS.

Instrument bus 34 (digraph B.6.11.B) has the same model for normal and backup power, but has a secondary backup system as well. The secondary backup fails if the operator fails to switch over to it (OPRASWXFR), if the switch itself fails (SWXFRIBUS34), if the Solatron transformer fails (XFMRSOLA), if the breaker supplying it fails open, or if the power supply from MCC36B fails.

2.3.6.2.11 Node Locations

The electrical system component locations were determined on a physical inspection of the plant and through use of arrangement drawings for components in high radiation areas. The major effort in the location analysis was to define common locations for groups of components. A location node is then connected to every major component in the electrical system (digraph B.6.12). Failure of a location node then fails all components in that location. Initiating events to these location failures were not specified however, since the intent of this analysis is to show the sensitivity of locations to some catastrophic event in general.

Electrical locations are designated by letters from A through S. Where other system components appear in electrical locations, the same location node will be used in that system's location digraph. Following is a list of locations and the components in each.

TABLE 2-9
ELECTRICAL LOCATION DESIGNATIONS

LOCATION	DESCRIPTION	COMPONENTS
A	Outside, Next to Primary Auxiliary Building	Station Aux and Unit Aux Transformers
B	Outside (different from A).	13.8 kV Substation
C	Turbine Building, 15 ft. elev., 6900 V Switchgear Area	6900 V Buses, & Breakers, Station Service Transformers, Appendix "R" modifications, MCC34.
D	Control Building, 15 ft elev.	480 V Buses and Breakers; Charger 33, Power Panel 33, MCC36C.
E1, E2, E3	Turbine Building, 15 ft elev., Different Locations	MCC32, 33, 35
F	Containment Building, 68 ft. elev.	MCC38
H	Primary Auxiliary Building, 55 ft. elev.	MCC36A, 36B, 37 Lighting Transformer and Bus 32
I	Outside, Near Intake Structure	MCC31
J	Unit 1 Superheater Building	MCC310
K	Diesel Generator 33 Room	D.G. 33
L	Diesel Generator 32 Room	D.G. 32
N	Diesel Generator 31 Room	D.G. 31, Battery 33
O	Battery 31 Room	Battery 31
P	Battery 34 Room	Battery 34
Q	Battery 32 Room	Battery 32
R	Control Building, 33 ft elev. Cable Spreading Area	Charger 31, 32, 34; Static Inverter 31-34; Power Panel 31, 32, 34; Solatron Transformer; MCC39
S	Control Room	Instrument Buses and dc Distribution Panels

2.3.6.3 Break Model

The electrical break model was developed as an addition to the block model to account for failures such as short circuits within components, and breakers or fuses failing to open. The break model not only treats failure to conduct power downstream through the electrical model, but also treats the propagation of a short circuit failure upstream and even across one train to another train via tie breakers or common power sources. Each component node from the block model will have a corresponding break model node designated by the suffix "/" which represents a short to ground within that component. This short circuit break node is directly connected to its corrresponding block model node. Then a short in the component fails that node in the block model. The short will also propagate both upstream and downstream through AND gates to the neighboring components. The other half of each AND gate represents a circuit breaker or fuse failing to trip. This node is designated by the suffix ":". Then for a short in one component to cause a short in the next component, the breaker between them must fail to trip. In general, each short circuit node in the break model is connected bidirectionally to adjacent short circuit components, with each connection passing through an AND gate with the failure of a short circuit mitigating device (breaker fails to trip).

Due to resource limitations, only the most important parts of the electrical system were included in the break model. Comprising the break model are the feeds from the 6900 V buses and diesel generators to the 480 V buses, then down through some of the motor control centers to the dc system. Unit models for the 480 V breakers are also included.

2.3.6.3.1 Feeds to 480 V Buses and Crossties

Digraph B.6.13.A shows short circuit failures for the 480 V buses. A 480 V bus shorts (BUS#A/) if another break failure propagates through the normal power feed train or through the diesel generator feed. Three breakers will mitigate potential shorts, and at least one of these must also fail to trip (BKR#A:, BKRSS#:, BKREG*:) to propagate the failure.

Short circuits can also propagate through crossties from one train to another. For the manual 480 V crossties (digraph B.6.13.B), a short on one bus (BUS#A/ or BUS$A/) or tie breaker (BKR#AT$A/) propagates to the adjacent bus if the tie breaker has been erroneously closed by an operator (OPWBKR*AT%A) and the tie breaker fails to trip (BKR#AT$A:). For automatic crosstie breaker 2AT3A, the operator error does not apply.

2.3.6.3.2 Circuit Breaker Unit Models

A unit model of failure to trip was developed for each breaker used in the break model. For the station service transformer feed breakers (digraph B.6.13.C), failure to trip occurs if the operator fails to trip the breaker locally (OPRABKRSS#) and remotely (OPRDSWBKRSS#) with the switch (SWBKRSS#), and the 86 device for automatic breaker trip fails (R86SS#:). Both the switch and 86 device fail on loss of dc power.

The 480 V bus feed breakers fail to trip (digraph B.6.13.D) if the operator fails to trip the breaker locally and remotely from the diesel building switch and control room switch, and the undervoltage and overcurrent relays fail to trip. All of these except for manual local trip fail on loss of dc power.

The same operator failures apply to the diesel generator supply breakers failure to trip (digraph B.6.13.E). Besides these errors, failure won't occur unless the overcurrent and bus fault relays also fail. However, all the trips except manual local require dc power.

The 480 V manual crosstie breakers fail to trip (digraph B.6.13.F) if the operator erroneously closed them, and the operator fails to trip them locally and through the control room switch, and the safety injection signal fails to trip them through both contact sets, and the overcurrent trip fails. The overcurrent trip and remote switch both fail on loss of dc power.

The model for the 480 V automatic crosstie breaker failure to trip (digraph B.6.13.G) is the same as the bus feed breaker unit model, except that the tie breaker does not trip on bus undervoltage.

2.3.6.3.3 DC Power System

The break model digraph for the dc supply to the power panels (digraph B.6.13.H) shows that shorts can propagate through the power panels either from the charger feed or from the battery feed. There are four break mitigators included in the model, the charger input and output breakers, the MCC feed breaker, and the battery output fuse. Note that since the battery receives constant charging through the charger output breaker, shorts can propagate between the battery and the charger. It was also assumed that shorts could not propagate upstream from the charger to the input breaker.

The break model continues in digraph B.6.13.I with feeds from the power panels to the distribution panels. The distribution panel feed breakers mitigate shorts between panels.

Also included in the dc system break model is the manual crosstie between power panels 31 and 32 (digraph B.6.13.J). Shorts propagate between power panels if an operator has erroneously closed the tie breaker (OPWDBKR31T32:) and the breaker fails to trip. The breaker will fail to trip if the overcurrent trip fails and the operator fails to trip it.

2.3.6.4 Electrical System Interactions

The electrical system model interacts with all of the other systems modeled, besides feeding back into itself from one subsystem to another. The interactions from electrical to other systems consist of various power feeds from the 6900 and 480 V buses and motor control centers to equipment, from the instrument buses to power plant sensors, and from the dc power panels and distribution panels to control component actuation and relay logic.

Interactions from other systems to electrical are limited to the service water system and safety injection actuation system. Service water is needed to cool the diesel engines, and loss of service water quickly causes loss of the diesel generators. During an accident condition with loss of all offsite power, loss of service water then causes loss of all ac power and plant safeguards equipment will not function. This interaction appears as an important result in some of the system combinations studied.

The safety injection actuation system interacts with the electrical system by operating logic or interlocking relays, which open or close breakers and control diesel generator automatic starting. Failures in the SI actuation system can prevent the electrical system from automatically responding properly to an accident. However, all of these functions can be performed by an operator as backup to the automatic system.

There are two interesting types of interactions within the electrical system, both involving the construction of conditioned cycles within the models. The three fuel oil transfer pumps which supply diesel fuel to the day tanks for each diesel generator are powered from motor control centers. These motor control centers are powered from the 480 V buses, which under accident conditions, are powered by the diesel generators. This type of cycle presents no particular problem for the DMA codes to solve, since the pumps do not need to be running until well after the diesel generators are started.

More pervasive cycles are created through the inclusion of dc power feeding back into the electrical system. DC power is required for the remote operation of all 6900 and 480 V breakers, both through operator acutated switches and through automatic relay actuation. These dc power connections are included in the unit models for the various breakers. Loss of dc power renders most breakers inoperable, except via manual control locally. Again, these cycles in the digraph models are easily handled by the DMA codes.

The only problem involving conditioned cycles in the electrical model concerns the dc power feed to the diesel generator exciter. However, with the proper connections in the model, some solutions in the double dependency calculations are incomplete. For example when considering the 480 V buses, the model correctly produces a doubleton of the 6900 V buses and diesel generators. But since the batteries must supply dc power for diesel starting, the 6900 V buses and batteries are also a doubleton. The conditioned cycle prevents this doubleton form appearing in the DMA code results.

Similarly when considering the dc power panels, the model correctly produces a doubleton of the 480 V buses and batteries. But since the power panels start the diesels which supply the 480 V buses, the 6900 V buses and batteries are also doubletons to the power panels. The conditioned cycle also prevents these doubletons from appearing.

Although the digraphs are constructed with the electrical system under normal operating conditions and the diesel generators off, the conditioned cycles fool the DMA codes into producing results which represent the system with the diesels already operating. A theoretical solution to this problem has been developed, but computer size limitations, due to the enormous size of the electrical model, prevented its implementation. The missing doubletons were included in the system combination results in an extra post-processing step so that no important interactions are missed.

2.3.7 RCP Seals and Chemical and Volume Control Digraphs

2.3.7.1 Reactor Coolant Pump Seals

The Reactor Coolant (RC) pump is an integral part of the Reactor Coolant System and facilitates the transport of heat produced in the nuclear core to the primary side of the steam generators. The RC pump consists of three general areas: the hydraulics package, the shaft seal package, and the motor package. Failures of several of the many components within these packages could result in a breach of the reactor coolant system that would challenge the emergency core cooling system. For a RC pump LOCA to occur, failures that result in allowing reactor coolant out of the RCS and into the pump must occur along with an uncontrolled path for the coolant to leave the RC pump. The failure criterion for a RC pump LOCA was developed as a digraph overlayed on a schematic of the RC pump shaft seal area and is presented in B.7 of Appendix B. The model was developed such that failure is allowing flow to pass out the RCS and through the pump to the containment (break model). A discussion of the failure modes and assumption used in this analysis is given below.

2.3.7.1.1 Hydraulic Package

The pump hydraulic package is the part of the pump that does the actual pumping of the reactor coolant. The pump casing, impeller and other hydraulic components are separated from the shaft seal package by a thermal barrier. This thermal barrier consists of a labyrinth seal and a heat exchanger. The heat exchanger isolates the hot reactor system from the remainder of the pump. The thermal barrier heat exchanger cooling medium is supplied by the component cooling system. A rupture in this heat exchanger would constitute a path for the reactor coolant to leak from the reactor coolant system. This rupture is considered a random failure since loss in cooling flow would not result in failure of the heat exchanger tubing which is designed for high pressure and temperature. The heat exchanger rupture has to be accompanied by either the cooling water inlet or outlet line being open for a LOCA to occur. The inlet line has high pressure piping up to a check valve just before the pump. The outlet line has high pressure piping up to a flowmeter controlled isolation valve outside of containment.

The labyrinth seal rubs on the pump shaft and has high pressure seal water injection on the side opposite the reactor coolant system. A failure of the labyrinth seal along with a loss in seal water injection flow or pressure would allow reactor coolant to leak from the reactor coolant system. Failure of the labyrinth seal can be either a random failure or can be caused by excessive shaft vibration which would be caused if the pump lower radial bearing were to fail or if either of the motor bearings were to fail.

2.3.7.1.2 Shaft Seal Package

The shaft seal package separates the pump hydraulic components from the motor components and prevents reactor coolant from leaving the impeller region of the pump. High pressure seal water is injected into the pump from the charging system where a portion of it flows into the reactor system as make up water and the remainder flows up through the pump seals. The seal package consists of three seals, the No. 1 seal, No. 2 seal and the No. 3 seal, with respective leak-off systems and a No. 1 seal bypass line. The No. 1 seal is designed to provide a large pressure drop so that a portion of the seal injection water will enter the reactor system. In addition, the pump lower radial bearing is located on the high pressure side of the No. 1 seal so that cooling is provided by the seal water injection. The No. 1 seal leak-off flow is directed to the volume control tank of the charging system. The No. 2 seal is located above the No. 1 seal and is designed to provide the same pressure drop as the No. 1 seal in the event that the No. 1 seal should fail. The No. 2 seal leak-off system is constructed of low pressure piping and flow is directed to a standpipe and then to the waste disposal system via the loop drains at the RC pumps. The No. 3 seal is located above the No. 2 seal and is a vapor seal capable of holding only a 5 psi differential pressure. The No. 3 leak-off flow goes directly to the floor trench below the reactor vessel. The No. 1 seal bypass line is provided to give additional flow to the lower radial bearing region during pump start up and when the reactor coolant system pressure is below 1500 psi.

Failure of the No. 1 shaft seal will allow seal water injection pressure into the No. 2 seal inlet cavity. If the No. 1 leak-off line provides an uncontrolled flow path out the pump, the seal water injection pressure will be decreased, allowing coolant to flow out of the reactor coolant system and into the containment. The No. 1 shaft seal leak-off path fails when it is open to the low pressure piping (151 psig) downstream of either valves 243A, B, C, D, or valves 244A, B, C, D.

In the event of a No. 1 shaft seal failure and closure of the No. 1 seal leak-off lines, (FCV261A,B,C,or D) the No. 2 seal is designed to provide the same pressure drop as the No. 1 seal and force seal injection water into the RCS. In this case, failure of the No. 2 seal will reduce the seal water injection pressure and provide a leak path out the pump, since neither the No. 2 seal leak-off system nor the No. 3 shaft seal can hold seal water injection or RCS pressure.

Another possible flow path out the pump is provided by the No. 1 seal bypass line. This flow path fails when it is open to the low pressure piping (151 psig) following the flow control valve FCV246. For this path to be open, an orifice which provides sufficient pressure drop to the No. 1 seal inlet cavity must fail and the flow control valve, FCV246, must be open.

Loss of seal water injection will allow the reactor coolant to leave the RCS. It is assumed that the thermal barrier heat exchanger does not provide sufficient cooling to prevent this hot coolant from flashing to steam and failing the pump lower radial bearings and all the shaft seals. The failure of the seal water injection system is discussed in the section on the modeling of the chemical and volume control system.

One failure in seal water injection is a vent or drain valve opening on the seal inlet piping. This failure would also result in a flow path out the pump. It was assumed that this failure would have to occur between the third check valve and the RC pump on the inlet piping.

The pump motor provides the motive force to turn the pump shaft and impeller. The rotor is attached to the pump shaft by a flange above the shaft seals. The rotor is supported on both sides by bearings which are immersed in reservoirs of oil that are cooled by heat exchangers. The cooling medium for these heat exchangers is provided by the component cooling system. A failure in either of the motor bearings (upper or lower) will cause the motor and pump shaft to experience excessive vibration. This shaft vibration is assumed to be severe enough to cause a failure in all three pump shaft seals and in the thermal barrier labyrinth seal.

2.3.7.1.3 Summary of RCP Seals

In summary, the major assumptions used to develop a model for a Reactor Coolant Pump loss-of-coolant accident are listed below:

1) Any uncontrolled loss-of-coolant from the RCS through the pumps constitutes a RC pump LOCA,
2) the thermal barrier heat exchanger will only fail due to a random failure since the tubes were designed for high pressure and temperature,
3) rupture in the thermal barrier heat exchanger will allow sufficient flow to pass out the pump to constitute a RCS pump LOCA,
4) the thermal barrier heat exchanger will not provide sufficient cooling to prevent reactor coolant escaping the RCS from flashing to steam,
5) loss of seal water injection will cause a failure in all the pump seals and the pump lower radial bearing,
6) failure in seal water injection can also result in a leak path out the pump,
7) random failure of the pump lower radial bearing will cause excessive shaft vibration and a subsequent failure in the shaft seals and the thermal barrier labyrinth seal,
8) failure of either motor bearing (upper or lower) will cause excessive pump shaft vibration and a subsequent failure of the thermal barrier labyrinth seal and the shaft seals,
9) the No. 3 shaft seal is a vapor seal only and will not hold the seal water injection pressure or the reactor coolant system pressure,
10) failure of the thermal barrier labyrinth seal and leak path out the pump will cause a larger size LOCA, and
11) the No. 2 seal leak-off system will not block a RC pump LOCA due to the low pressure piping which cannot hold RCS pressure.

2.3.7.2 Chemical and Volume Control System

The Chemical and Volume Control System performs many functions. The function of interest is the provision of high pressure reactor coolant pump seal water injection. Therefore, the failure of the CVCS to provide adequate injection flow and pressure to the RC pumps seal area was modeled.

The portion of the CVCS associated with the RC pumps seal water injection consists of: the three positive displacement charging pumps, a source of injection water, the seal injection filters and the piping from the charging pumps discharge to the RC pumps.

The primary water source for the charging pumps is the volume control tank. However, the CVCS is so configured that the charging pumps can take suction from a number of sources including: the refueling water storage tank, the primary water storage tank, the chemical mixing tank and the boric acid tanks. These water sources connect to the charging pump suction headers at different points. Therefore, this header was modeled as a crosstie allowing for the various sources to reach each pump inlet. The piping from the volume control tank was included in the model. The other water sources were modeled as water source nodes to the pumps suction header and their associated piping was not included in the model.

During normal plant operation, one charging pump supplies the flow necessary for the seal water injection and the other feed and bleed operations needed for RCS chemical and volume control. The normally running pump is usually automatically controlled by the pressurizer level control system. The other two pumps must be manually started and controlled if they are needed for additional flow to the RCS. Charging pumps 30, 32 and 33 are powered from the 480 V buses 5a, 3a and 6a, respectively, and cooled by water from the component cooling system.

The unit models for the charging pumps were developed for the control circuitry that closes the main ac circuit breaker that connects the power source to the pump motors. These pump models assume No. 30 is normally running and fails to continue to run. The other two pumps either fail to start or once started, fail to continue to run. For the normally running pump, loss of dc control power will not trip it off line, however, dc control power is needed to start a pump that is not running. Charging pump 32 and 33 receive dc control power from distribution panels 33 and 32, respectively.

The discharge of each charging pump divides into two paths. One path connects to the RCS charging lines, the other path is the seal water injection line. These is also a recirculation line back to the volume control tank on each pump discharge. The RCS charging lines and the recirculation lines were modeled as degradation nodes to the seal water injection line since faults in the piping may reduce the pressure needed by the seals.

All three seal water injection lines join a single pipe that goes to the seal injection filters. The seal injection filters consist of two filters and a valved bypass line. Each filter has isolation valves, one on its inlet and one on its discharge. All values on the seal injection filter assembly are manually operated. Normally, one filter is in use. All three filter lines can supply sufficient flow to the seal area. Therefore, all three paths must fail for loss of seal water injection.

The discharge of the seal injection filter assembly flows to a header that feeds the RC pumps inlet lines.

Each RC pump inlet line contains a needle valve for adjusting seal water flow, and an isolation valve before passing into the containment building. Inside containment, each line has three check valves and three valved vent lines before joining the RC pump seal inlet flange.

2.3.8 Component Cooling Digraphs

2.3.8.1 Introduction

The Component Cooling system is designed as two trains. Each train cools redundant equipment and the pumps and heat exchangers can be used to route flow through either of the trains. Figure B.8 in Appendix B provides the component cooling system schematic.

2.3.8.2 Crossties

The interchangeability between pumps, headers, and heat exchangers in the Component Cooling System leads to three crossties in the component cooling model. The first crosstie is located at the input to the Component Cooling Water Pumps (CCWPs) (two inputs and one output). The second crosstie exists at the discharge side of the CCWPs (three inputs and two outputs). The last crosstie consists of the output of the Component Cooling Heat Exchangers (two inputs and two outputs).

2.3.8.3 Flow Paths

The two outputs of the CCHXRs and the two inputs to the CCWPs make up the two trains provide cooling for various items of equipment. Each train consists of nested "loops" which can be isolated in the event of a pipe rupture. Examples of this looping effect is shown in Figs. B.8.1 - B.8.3. Notice that the arrows represent propagation of failure to the equipment and are shown pointing into each sink. This is necessary to prevent a failure from propagating back through the crossties and causing the failure (in the digraph) of every other component in the model. Because of these loops any failure on the path is a singleton to its associated sink, that is, all nodes on the path to a sink (except those located in a crosstie) are singletons.

The system failure criterion for the CCWPs is defined as failure of all three pumps since the crosstie allows any one pump to pressurize both trains.

2.3.8.4 Components

Cooling to the SIPs is accomplished whether the CCWPs are running or not. There is a mini shaft pump on each SI pump which provides cooling water flow in the event that the CCWPs are not running.

Two of the SIPs are cooled by train 32 and the third SIP is cooled by train 31. This insures that sufficient cooling would be provided for the minimal number of SIPs for a small LOCA given one cooling train operational. If train 32 fails and there is a medium LOCA, a supplemental flow of cooling would be needed in order to provide SIP cooling until the point where Residual Heat Removal pumps (RHRPs) can become effective.

There are two Residual Heat Exchangers and two Residual Heat Removal Pumps - one of each is cooled by each component cooling train. Since only one of each is necessary for core cooling during low pressure recirculation, loss of one train will not prevent long-term cooling.

The two Recirculation Pumps are cooled during the injection phase by Component Cooling Booster Pumps (two for each RECP) (also called Auxiliary Component Cooling Pumps). These CCBPs are actuated by the SI signal and dedicated to the RECPs to protect them from the hostile containment atmosphere. One CCBP per RECP is sufficient, leaving the other as back-up in case of active component failure.

The injection to recirculation switch-over sequence shuts the CCBPs down and brings on the main CCWPs. (They were stripped off in the case of loss of offsite power.) The CCWPs are not needed for RHXR cooling and will cool the RECPs as well.

The cooling water for all four Reactor Coolant Pumps (upper and lower bearings and thermal barrier) is provided by component cooling train 32. It is for this reason that if a problem occurs in train 32 which can not be remedied in two minutes, the reactor and the RCPs are tripped.

The three Changing Pumps (CP) oil coolers (two per pump) are also cooled by train 32 and are in the nested loop downstream of SIPs 32 and 33. Downstream of the CPs are the Seal Water Heat Exchanger (SWHXR) and Non-Regenerative Heat Exchanger (NRHXR), which are in the same loop.

2.3.9 Service Water System Digraph

2.3.9.1 Introduction

The digraph of the Service Water System (SWS) consists of two parts: 1) One-to-one mappings of the hardware from P&IDs to a flowpath model; and 2) flowrate failure criteria. The P&ID mappings capture all of the possible cooling flowpaths to the following support system hardware including:

1) Diesel generators;
2) Component cooling heat exchangers;
3) Instrument air system;
4) Boiler feed pump lube oil coolers; and
5) Closed cooling system.

The flowrate failure criteria consists of the different number of pumps needed to adequately remove the heat generated by the support systems during various accident modes of operation (see associated P&IDs and digraphs in B.9 of Appendix B.)

2.3.9.2 Flow Path Model

By mapping from the P&IDs to a digraph, openness of all possible flowpaths from the Hudson River to hardware and back to the river can be captured. "Openness" can be defined in terms of the normal alignment of the valves in the system and what is needed to open alternate paths if a normal path should not be available. This includes detailed modeling of the service water pump electronics to accurately capture dependencies which facilitate the successful flowpath through the pump. It also includes inputs from operators who manually open a closed valve to create a new flowpath. Thus, implicit in the flowpath model are initial conditions relating to the state of the flow permitting components at T_0.

2.3.9.3 Initial Conditions

As described above, the valves in the SWS are manually aligned to be consistent with the selection of which three main pumps are to cool "essential" hardware and which three cool "non-essential" hardware in the event of an accident. The essential pumps can turn on automatically; the others cannot. The model must therefore reflect the selection of the pumps. At Indian Point-3 pumps 31 - 33 are almost always selected for essential cooling. The model allows for the selection by the mode select switch of either group of pumps. This choice is fixed at T_0. The remaining six pumps require beneficial operator intervention to be used and thus have corresponding inputs on the digraph. During normal plant operation, any pump(s) may be operating. For the sake of this analysis, it will be assumed that, as a worst case, the pumps selected as essential are off at T_0 and therefore require actuation in the event of an accident.

Checkoff list COL-RW-2 is used to guide operators in the manual alignment of valves. This alignment constrains the pumps selected as essential to only cool essential hardware and the non-essential pumps to only cool non-essential hardware. Thus, valves between non-essential pumps and essential hardware (and vice-versa) are manually closed. To open these paths requires operator input and thus every valve which the checkoff list says is shut has an input from an operator node in the digraph.

2.3.9.4 Flowpath Modeling Assumptions

Based on Inidan Point-3 operator discussions, certain assumptions were made in the course of modeling the flowpaths. They primarily concern exclusion of dependencies due to large time delays between failure of a component and propagation of the effect of that failure.

Water drawn by the main pumps passes through "traveling screens" which filter out water borne debris. There is a screen dedicated to each of the three redundant paths from the river through the intake structure to the pump well. These screens are flushed clean by water supplied by the service water pumps. This flushing requirement was excluded from the model, therefore, flowpath failures due to clogging of the three redundant paths AND failure to flush them out are not in the model. After water has passed through the service water pumps it passes through "automatic strainers". These perform the same function as the traveling screens and filter out particles over 1/8" in diameter. The requirement for flushing these was also excluded. After passing through the strainers, the water flows through some lengths of outdoor piping. This piping is heat traced to keep the contents from freezing. Blockage due to failure of any or all heat tracing during an accident was excluded.

2.3.9.5 Flowrate Failure Criteria

The amount of waste heat generated by the plant varies with plant accident mode. Consequently, the total flowrate of river water that has to be pumped through the service water system to adequately remove that waste heat also varies. The necessity for a different number of pumps to be working during different plant modes is captured in a group of models called the Flowrate Failure Criteria. The information used to create these models is from the FSAR, Sectin 9.6.1 and Table. 9.6-1, Plant System Description 24.0, Technical Specification, page 3.3-18, and operator discussions. The plant accident modes are "Non-LOCA" and "LOCA" for the system combinations chosen for this analysis. The flow rate requirements are shown in Figure 2-6.

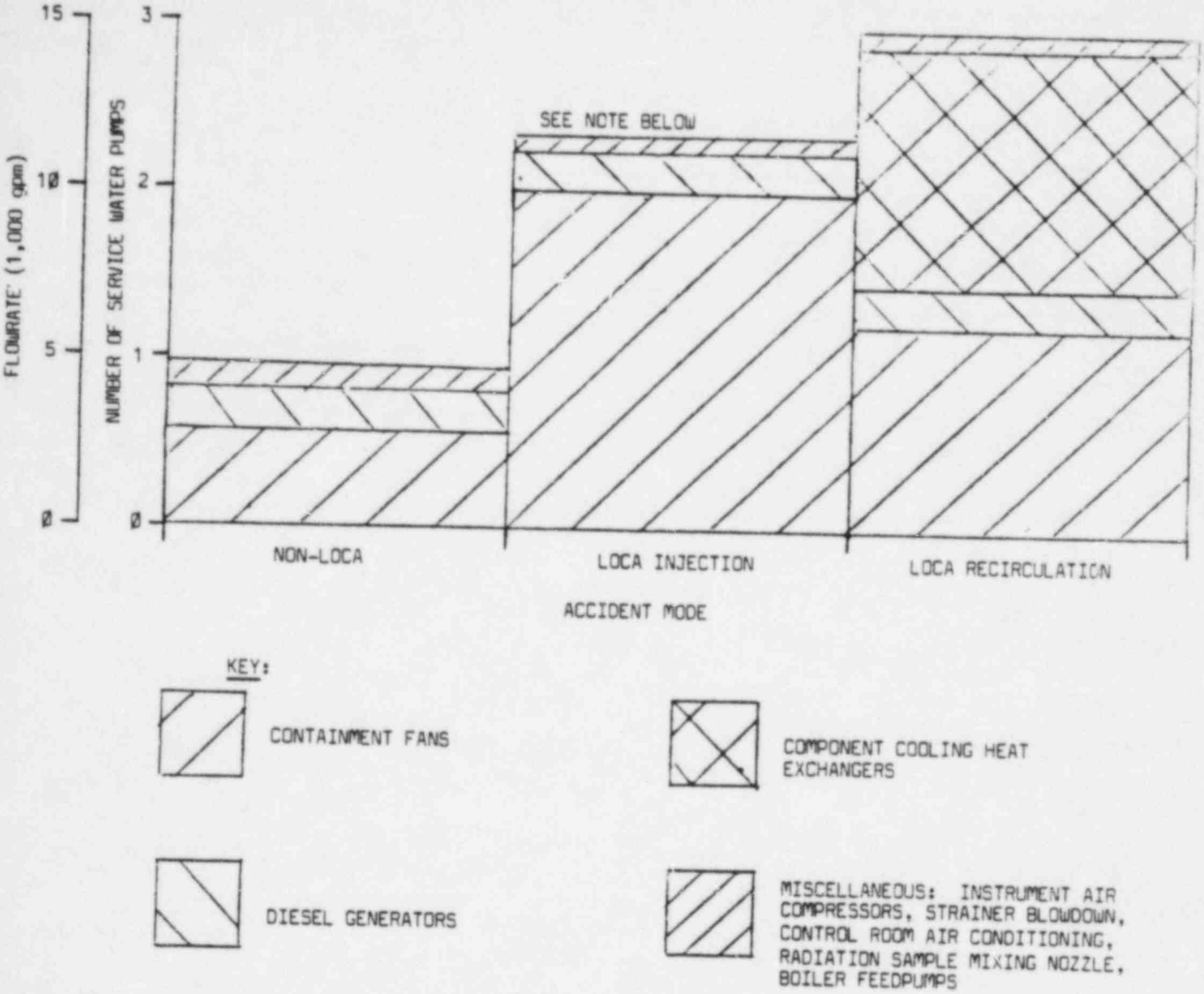
2.3.9.5.1 Non-LOCA Accident Mode (System Combinations 5,6)

The first plant accident mode, non-LOCA, applies to system combinations 5 and 6 which involve the main and auxiliary feedwater systems being called upon to remove heat from the reactor coolant system when there is no simultaneous LOCA. The service water system flowrate requirements can be met by a single pump (5,000 gpm). The hardware requiring heat removal includes the boiler feed pump lube oil coolers, containment fans, diesel generators, closed cooling system, and miscellaneous equipment. The model decribing the flowrate requirement takes into account that only the six main service water pumps can cool the boiler feed pump lube oil coolers and the closed cooling system. All nine pumps can, however, cool the other hardware. This difference is due to the three backup pumps being downstream of check valves which isolate them from the flowpaths to the boiler feed pump lube oil coolers and the closed cooling system. Since only one pump is required for the system to succeed, the flowrate failure criteria is already captured by the path model and any path from the river to the hardware passes through only one pump since no pumps are in series.

Since the closed cooling system is considered non-essential, the three main pumps aligned with it are automatically turned off on receipt of a safety injection signal. Thus, strictly speaking, the hardware, such as the condensate pump motor bearings, cooled by the closed cooling system would necessarily overheat. Since this would not occur immediately, the requirement of heat removal from the closed cooling system to the rest of the SWS isn't modeled for cases representing immediate response to an accident.

2.3.9.5.2 LOCA Accident Mode

The LOCA accident mode is divided into two phases: injection and recirculation. For the purposes of modeling service water flowrate failure criteria, injection phase pertains to the plant response immediately after a LOCA, regardless of whether the system combination includes the high or low pressure safety injection systems. System Combinations 1 - 4, 7, 8, and 10 fall into this category. LOCA recirculation mode is for long-term response and is modeled in System Combination 9.



NOTE: ALTHOUGH THE TOTAL REQUIRED FLOWRATE FOR LOCA INJECTION INDICATES THE NEED FOR MORE THAN TWO PUMPS, FSAR P. 9.6-3 SAYS TWO ARE ADEQUATE. THIS WAS CONFIRMED IN OPERATOR DISCUSSION.

FIGURE 2-6 TOTAL SERVICE WATER REQUIREMENTS @ 75°F AS FUNCTION OF PLANT ACCIDENT MODE (FROM FSAR TABLE 9-6-1 AND OPERATOR DISCUSSIONS)

2.3.9.5.3 Injection Phase (System Combinations 1 -4, 7, 8, 10)

Immediately after a LOCA, the primary heat sources that have to be cooled by the SWS are the containment fan units and the diesel generators. While the containment fans are not modeled in any system combination, requirements for their cooling are included in the SWS failure criteria since they are an essential load with a flowrate requirement of 10,000 gpm as listed in FSAR Table 9.6.-1. That requirement is based at keeping containment temperature at or below 120°F. The three diesel generators together require a flowrate of 1,200 gpm. Other hardware requirements are less than 1,000 gpm. Cooling of the turbine lube oil and seal oil are excluded since the turbines are not used to mitigate the accident. The total required flowrate of approximately 12,000 gpm indicates the need of at least three of the 5,000 gpm capacity service water pumps, however, Technical Specification page 3.3-18 and operator discussion agree that two pumps would be adequate.

2.3.9.5.4 Recirculation Phase

Flowrate requirements for recirculation phase are 7,000 gpm for heat removal from the component cooling heat exchangers. In this phase, residual heat is transferred from the core to the component cooling system by the residual heat exchangers. This heat is then transferred to the SWS via the component cooling heat exchangers. Flow requirements to the containment fans is 6,400 gpm and the diesel generators require 1,200 gpm. With miscellaneous additional requirements, the FSAR Table 9.6-1 and operators agree that three service water pumps are required. Since the recirculation phase is entered long after the accident begins, and since it requires manual intervention to initiate, credit is given for operators to turn on those pumps that were automatically tripped before, thus greatly reducing the likelihood of inadequate flow.

2.3.9.6 Results of Service Water System Modeling

The Service Water System appears as a support system in every system combination. Its effect on the integrity of the reactor coolant system depends upon which support systems it can act through, as well as whether beneficial human intervention is allowed. However, given that its function is heat removal, primary consideration has to be given to how long it would take for a failure in the SWS to propagate to the hardware it is cooling. For instance, the time before a failure to cool the component cooling heat exchangers causes problems is much longer than when cooling to the diesel generators stops. A significant dependency was found between the SWS and the diesel generators owing to the fact that the diesels have an immediate cooling requirement.

The Indian Point-3 Nuclear Plant derives its automatic emergency onsite high voltage power from three diesel generators. The DGs must be cooled in order to keep from failing due to overheating. The cooling is accomplished by transferring heat to the Service Water System (SWS) which is designed to circulate river water through DG heat exchangers when the DGs are in use. Loss of this cooling will result in failure of the DGs to generate power due either to protective shut off or damage due to overheating. In either event, a generator will cease to produce power within a few minutes of loss of heat removal.

To ensure heat removal from the DGs during an accident, they are aligned with a set of three main service water pumps designed to turn on automatically. These pumps are preselected for cooling "essential" hardware in the event of an emergency (see Section 2.2.12). The other set of three main SWPs is selected to cool "non-essential" hardware by default since a two-position mode select switch is used to enable the pumps. The non-essential pumps are tripped on SI signals and the flowpaths to the essential hardware are isolated from those to the non-essential hardware. Thus, even though under normal plant operation pumps from both groups are pumping through both trains, the DGs can only be cooled by a single train. Furthermore, under normal plant operation, water is kept from flowing through the DG heat exchangers by two normally closed valves in parallel on a common downstream path. On SI or high DG oil or water temperature they are de-energized and open.

The single trained cooling flowpath and the normal absence of flow through the DG heat exchangers presents the following noteworthy vulnerabilities:

1. Failure of DGs to Generate Power Due to a Misaligned Switch

   As mentioned above, the essential SWP train is aligned to enable DG cooling immediately after an accident whereas the non-essential SWP train is aligned such that it cannot cool the DGs immediately after the accident. Having so configured the SWS, improper selection of which pumps are essential and non-essential would result in a failure of the generators to be cooled immediately after the accident. This selection is made using the "mode selector switch" on the right hand safequards panel in the control room (System Description 24.0, Section 3.2.B). Detection of this error before an accident rests primarily on the accurate implementation of the SWS check-off list (COL-RW-2) and subsequent inspections of valve positions and/or flow instrumentation. The latter requires correlating the inspections with the state of the mode selector switch to expose the error.

2. Failure of DGs to Generate Power Due to Misaligned Valves

Each SWP train has two butterfly valves in series, either of which if closed and undetected would mean failure of DGs to be cooled immediately after an accident, should that train have been selected as essential. If SWPs 31-33 are selected as essential, then the valves are SWN-98 and SWN-30. If SWPs 34-36 are selected as essential, then the valves are SWN-99 and SWN-29. Misalignment of any of the valves could result from inaccurate application of the check-off list or of a maintenance or testing error. However, the means of detecting misalignment of SWN-98 or 99 is very different from that of SWN-29 or 30.

A misalignment in the first set is fairly easily detected since there is normally flow through each valve and just downstream of each valve is a pressure meter which is connected to an indicator light and annunciator in the central control room. Therefore, during normal plant operation a misalignment would be indicated quickly and automatically. Misalignment of either of the other valves (SWN-29, 30), however, is neither automatically nor quickly detected. After the intial procedure of following the check-off list, inspection of the valve position consists of monitoring a local pressure gauge every 8 hours. The location of the pressure tap is shown in Figure 2-7 which is a copy of a section of the main SWS P&ID 9321-F-27223-21. There is no indication of the tap on the original P&ID and its presence was derived from an operator. Also noted are butterfly valves 29 and 30. If SWNs 31-33 are selected as essential, then SWN-30 is normally open as are SWNs-62A, C, and E which lie just upstream of each diesel heat exchanger pair. SWNs 29, 62B, D, and F would be correspondingly closed. Detection of SWN-30 being inadvertently closed is currently accomplished by monitoring the local pressure gauge and noting a drop in pressure. Should the valve be closed long enough for the pressure to drop below a threshold, an alarm sounds in the central control room.

2.3.10 Pressure Operated Relief Valve Digraphs

2.3.10.1 Introduction

The pressure operated relief valve and the safety valves at Indian Point 3 are part of the Overpressure Pressure Protection System (OPS). The Overpressure Protection System prevents the reactor vessel from exceeding the Technical Specifications pressure-temperature limits. This is accomplished through the use of the pilot operated relief valves (PORVs), the safety valves, and a pressure-temperature logic system that arms and disarms the OPS, and automatically opens the PORVs. (See Figure B.10 in Appendix B).

The two PORVs (PCV-455C and PCV-456) are set to open automatically at 2335 psig. The pressurizer pressure instrumentation and control system also initiates a reactor trip at 2365 psig. Finally, the three safety valves (PCV-464, PCV-466, and PCV-468) open automatically at 2485 psig (the reactor coolant system design pressure). At reactor coolant pressures lower than normal operating conditions, the pressurizer instrumentation and control system unblocks the safety injection bistable at 1880 psig, trips the reactor at 1820 psig, and initiates low pressure safety injection at 1720 psig.

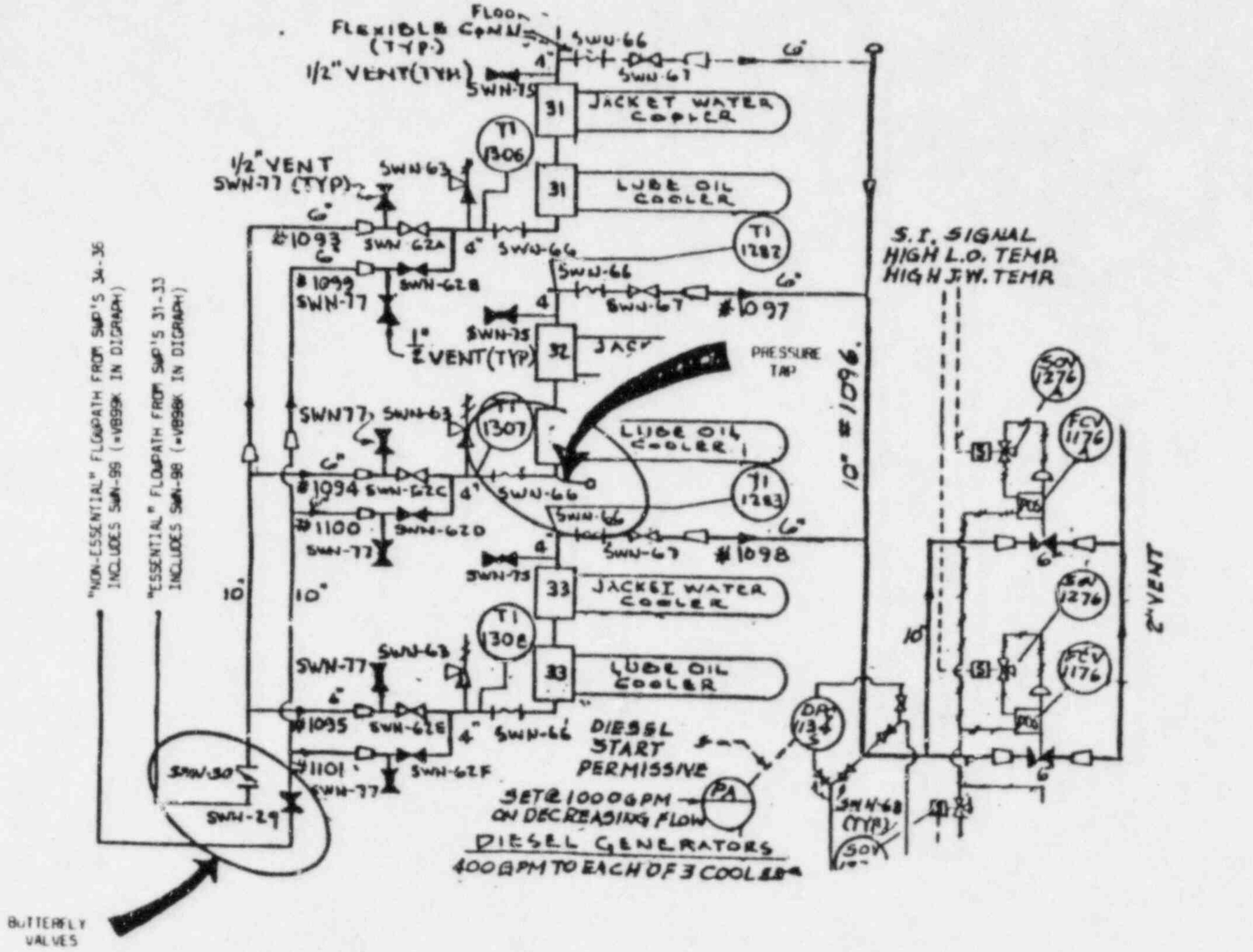


FIGURE 2-7 FLOWPATHS TO DIESEL GENERATOR HEAT EXCHANGERS CORRESPONDING TO SELECTION OF SWP'S 31-33 AS "ESSENTIAL" ⋈ = NORMALLY CLOSED (FROM U.E. AND C. DWG. NO. 9321-F-27223-21 AND CHECK-OFF LIST COL-RW-2)

The three safety valves (PCV-464, PCV-466, and PCV-468) and the two PORVs (PCV-455C and PCV-456) discharge their steam through discharge piping that connects to the pressurizer relief tank (PRT). Block valves (MOV-535 and MOV-536) located upstream of the PORVs serve to isolate the PORVs should they fail to reclose after opening. Loop seal drain lines located at the low point of the loop seal upstream of the safety valves, drain condensate before the safety valves are tested. Normally, a water seal is maintained below each safety valve by the loop seal to inhibit leakage. A valve on each loop seal drain line (574A, 574B and 574C) and a valve, 526, on the combined drain line, maintains primary pressure boundary integrity. Three smaller (3/4 in.) lines, two sampling lines and a waste disposal line, must be valved off to maintain primary pressure boundary integrity. A failure by this system is considered to be any breach of the primary pressure boundary integrity by valves associated with the pressurizer.

2.3.10.2 Pilot Operated Relief Valve (PORV) Unit Model

The two Pilot Operated Relief Valves (PCV-455C and PCV-456) used at Indian Point 3 are Copes-Vulcan 3 in. class 1500 model D-100-160 valves An ASCO #HT8316C15 3-way solenoid operated valve controls the flow of nitrogen (N2) gas to the PORV diaphragm located on the top of the PORV. Flow of N2 gas to the PORV diaphragm located on the top of the PORV. Flow of N2 gas into the PORV diaphragm pressurizes the diaphragm which expands, raising the valve body frame and valve stem upward. As the valve stem moves up, it lifts the valve plug, allowing steam out the discharge piping. The upward movement of the valve body frame also compresses a spring which, when the diaphragm is depressurized, provides a closing force on the valve stem and valve plug. The PORVs fail close with loss of nitrogen supply, provided that the N2 supply line is vented. The PORVs are normally set to open at 2335 psig. A failure in the PORV will be failure to reclose.

2.3.10.3 Safety Valve Unit Model

The three Safety Valves (PCV-464, PCV-466, and PCV-468) used at Indian Point 3 are Crosby Valve & Gauge series HB-BP-86 3 in. spring loaded, enclosed pop type valves with back pressure compensation. They are set for the system design pressure of 2485 psig. These valves constitute a failure when they fail open.

2.3.10.4 Instrument Nitrogen (N2) Supply System

The instrument nitrogen (N2) supply system supplies nitrogen gas from the nuclear equipment nitrogen system to the diaphragm of the two PORVs (PCV-455C and PCV-456). A failure by this system is considered to be the failure to vent the nitrogen gas from the diaphragms of either PORV via the 3-way solenoid operated valve or by the nitrogen supply line.

2.3.11 Instrument Air System Digraphs

2.3.11.1 Introduction

The Instrument Air System digraph encompasses all of the equipment contained in the Control Building, as well as selected parts of the Containment Building, Turbine Building, and Auxiliary Feedwater Pumphouse. Development of the Station Air and Administration Building Air interfaces to Instrument Air was considered outside the scope of the modeling effort and has not been included. Electrical interfaces have been modeled for components such as compressors and dryers which do not fail to a safe position on the loss of electrical power (see associated P&IDs and digraphs in B.11 of Appendix B).

2.3.11.2 Instrument Air Compressors

The two Instrument Air Compressors are located in the same room. Consequently, they are subject to common location failures. Excessive dust or smoke could clog the intake filters. The atmospheric suction (ATMSUCT) node models this interaction. Fire, flooding, and steam could also affect both compressors, as well as the operator's ability to locally initiate corrective action.

Since the compressors are identical, the electrical circuitry was unit modeled. A given compressor, its V-belts, and its motor were all modeled as one node (IAC) since a failure of any of them would prevent the compression of air. Based on the Auxiliary Feedwater nitrogen bottle regulator pressure, failure of the Instrument Air System is assumed to occur whenever the air pressure delivered to a component is less than 50 psig. Thus, failure of the unloader solenoid (SOV 1198/1199) to vent results in compressor failure, since the compressor will not load until system pressure falls below 30 psig. Compressor failure will also occur if the flow of Service Water to a compressor or an aftercooler is not sufficient to prevent a high temperature compressor trip. One compressor will pressurize the system to well over 90 psig.

2.3.11.3 Emergency Tie to Station Air

The Instrument Air System is connected to the Station Air System just upstream of IA-30. The node STATIONAIR is the boundary between the two systems.

Air must flow from STATIONAIR through one set of prefilters and a normally shut isolation valve (PCV1142) in order for the emergency tie to be effective. The operation of the prefilters is similar to that of the other parallel filter sets (described below) in the IA System. PCV1142 opens when PCS1169 senses a low air pressure condition through IA-28 or whenever power is lost to SOV1142. The Station Air System will adequately pressurize the IA System even if no IA compressors are running.

The Station Air System also supplies emergency makeup to the IA Weld Channel Pressurization System. This path was modeled up through valve IA-55, though none of the other systems in the present study uses air from this branch of the IA System.

2.3.11.4 Parallel Filter Sets

Parallel filter sets are located throughout the Instrument Air System. The hardware consists of two interlocked filter selector valves, the filters themselves, a differential pressure gauge, and two gauge isolation root valves.

Though the filter selector valves are mechanically interlocked, they have also been modeled as independently operable "Y" (inlet) and "Z" (outlet) selector valves. Each selector valve was further subdivided into "A" and "B" paths. Thus, it is possible for air to flow through neither, both, or only one filter path. Air must flow through at least one filter path to pressurize the downstream piping.

The pressure drop across the filter is proportional to the flow through the filter. Thus, the operator must place the backup ("A") set of filters on service when the gauge reads high. In order for the gauge to indicate correctly, both root valves must be open and there must not be any breaks or blocks in the gauge piping. The LINK node propagates a gauge line block into the gauge and a gauge line break into the gauge root junction. Note, however, that a full scale break model, which would propagate failure upstream as well as downstream, has not been attempted for this system.

2.3.11.5 Refrigerant Dryers

Two refrigerant dryers are installed downstream of the station air emergency tie to dehumidify the air. A single dryer has sufficient capacity to supply the needs of the IA System. A dryer which is not running is assumed to pass no flow.

PCDS1131 senses the pressure drop across the dryers. It energizes SOV1542 on high pressure (low flow) to open PCV1542 by applying air pressure to the top of its diaphragm. This path bypasses the dryers and provides an adequate flow rate. The dryers may also be bypassed by an operator (OPR1542 or OPR65) who manually opens PCDS1131 or the equalizing valve (IA-65) respectively.

2.3.11.6 Emergency Tie to Administration Building Air

The Instrument Air System is connected to the Administration Building Air System just upstream of IA-36 in the Turbine Building. The node ADMINAIR is the boundary between the two systems.

ADMINAIR is tied into the Conventional Plant IA Loop by manually (OPR36) opening the isolation valve (VGA36). This makeup air ties into the nuclear service IA header at IA-4 after passing through an orifice. The Administrtion Building Air System's capacity is sufficient to pressurize the IA System without the assistance of the IA or SA compressors.

2.3.11.7 Regenerative Desiccant Dryers

A regenerative desiccant dryer consists of a four-way selector valve and two desiccant beds. Bidirectional flow through the desiccant beds is incorporated by way of dummy nodes which denote the component and direction of airflow. The selector valve was modeled as four independent valves ("AA", "AB", "BA", "BB"), where the first letter refers to the desiccant bed on service and the second letter refers to the inlet ("A") or purge ("B") path.

Heat tracing (HTRC) in each desiccant bed is used to regenerate the desiccant. A desiccant bed which cannot be dried is assumed to fail due to line freeze up. This condition could occur if the purge path to the atmospheric exhaust (ATMEXH) was blocked or if the heat tracing failed.

2.3.11.8 Nonregenerative Desiccant Dryers

A pressure switch senses the discharge pressure of the regenerative desiccant dryer through a normally open valve. On low pressure or loss of power, it will trip open the nonregenerative desiccant dryer isolation valve by venting its diaphragm through the solenoid operated valve.

2.3.11.9 Results

The Instrument Air System digraph was analyzed for singletons and doubletons to the FCV 261A diaphragm. This valve is important in regulating the flow of seal injection water to the reactor coolant pumps. The results indicate that all but one of the singletons are due to the single line nature of the air piping downstream of IA-4 which services the Containment Building. The majority of doubletons appear as combinations of regenerative and nonregenerative desiccant dryer components. This result illustrates the backup protection afforded to the regenerative dryer by the nonregenerative dryer.

A singleton failure of interest involves the desiccant dryer after filter set selector valve (IA-12). The valve could be positioned such that neither filter is lined up to pass air flow. This type of failure could be attributed to a faulty mechanical interlock which would allow the inlet valve (IA-12Y) to be aligned to one filter while the discharge valve (IA-12Z) is aligned to the other. Failure could also occur due to blockage inside one of these valves, regardless of its position.

The doubletons which result from the simultaneous failure of components in the desiccant dryers can be better understood by discussing the regnerative and nonregenerative components separately. Since air normally flows through the regenerative beds, the regenerative piping will be considered first.

A loss of the heat tracing in either regenerative desiccant bed (HTRC1206 or HTRC1207) or a loss of their power supply (MCC34) could cause an ice plug to form as the moist air expands into the downstream piping and freeze. Electrical power is assumed to be lost in a fire, flood, or steam leak casualty. Thus, these events contribute to the same type of blockage, though one could argue that the heat from a fire or steam rupture would tend to thaw the pipes and prevent freezing. Failure of the four way valve (4V1105) to periodically change position could also result in freezing since the on service bed would not properly regenerate. Blockage, due to the entry of foreign material, can occur in the check valves, fittings, beds, purge lines, valves, and pipes which compose the regenerative desiccant dryer. A blocked purge path prevents warm air from circulating through the off service desiccant bed, thus yielding another case of pipe freezing when the bed is restored to service.

The nonregenerative desiccant dryer is also susceptible to blockage. It will fail if SOV 1143 does not reposition to vent the PCV 1143 diaphragm. The node NRDD1143 (nonregenerative desiccant dryer) encompasses all desiccant failure modes including blockage, depletion, and absence.

Several potential failures of the Instrument Air System are attributable to components other than the desiccant dryers. Blockage of flow will occur, regardless of selector valve position, if both after filters (F12A and F12B) are clogged. If F12B (normally on service) is clogged, a steam rupture or fire in the same room would make it difficult or impossible for an operator to swap filters.

A blockage in the line just upstream (J7) or just downstream (J10) of the refrigerant dryers, combined with a loss of the Administration Building Air System, effectively blocks all sources of air to the nuclear services header which enters Containment. A blockage on each side of the T fitting (J59) into the Containment Building Instrument Air Loop could act to cause the same effect.

2.3.12 Lube Oil System Digraph

2.3.12.1 Introduction

The Lube Oil System (see Fig. B.12 of Appendix B) is a complicated crosstie network of pumps and vented tanks. Since the tanks are not pressurized, it is not sufficient to model only the connectivity of the system. Direct flow is not allowed between two vented tanks. A vented tank's contents may only flow to the suction of a pump. The discharge of a pump, however, may flow to either the suction of another pump or a vented tank.

In situations where either unpressurized or pressurized oil situations may occur in the same line at different times, two dummy paths flowing in the same direction may be necessary. An example of this condition is the discharge through check valve 46B on the digraph (this valve is unlabeled on the P&ID). The dummy 'A' path may be pressurized or unpressurized while the 'B' path must always be pressurized for flow to occur. Notice that the 'A' path from J46A supplies the Oil Storage Tank Transfer and Cleanup Pump while the 'B' path eventually connects to the fill lines of the Clean and Dirty Oil Storage Tanks.

2.3.12.2 Boiler Feed Pump Oil Console

The Boiler Feed Pump Oil Console is the hub of the Lube Oil System. All of the oil which is used to lubricate and control the Boiler Feed Pumps must pass through this tank.

The physical ability of the tank to pass and store oil is represented by BFPOC. The console's oil level (OILBFP) is determined by its initial inventory (OILBFPOC) and the net rate of addition from other sources (PATHBFPOC). Since oil is recirculated through the console, OILBFPOC and PATHBFPOC provide redundant supplies of oil to the Boiler Feed Pumps.

2.3.12.3 Sources of Oil

A large fraction of the digraph is devoted to pumping oil to PATHBFPOC. The dashed lines on the digraph represent flow into the oil storage tanks (COST and XDOST) and the main turbine-generator oil reservoir (TLOR). For the purposes of this model, these tanks were assumed to contain a much larger volume of oil than the BFP Oil Console. Thus, it was unnecessary to consider the inflow to these tanks.

Oil may also be added to the system through the truck fill (TRK) connection. A fully loaded oil tanker is assumed to be readily available. The tanker's capacity is much larger than that of the BFP Oil Console.

2.3.12.4 Main Lube Oil Pumps

The section of the digraph between the Boiler Feed Pumps and the BFP oil console is based upon the feedwater system test (System Description No. 21) test. The valve numbering sequence for this section was arbitrarily started from 100. The solenoid operated dump valves (LO-105A/B/C) are designed for testing purposes but are included to model the effects of inadvertent actuation. The power supplies of the two ac and one dc Main Oil Pumps were arbitrarily selected.

The two oil cooler selector valves (LO-111Y/Z) are assumed to be mechanically interlocked so that operation of one valve will cause the other valve to align to the same cooler. Each oil cooler (BFPLOHX) is capable of removing the entire system head load while providing full flow to the feed pumps. Loss of Service Water heat removal capability to the on service cooler will cause BFP bearing failure.

2.3.12.5 System Success Criteria

Successful operation of the Lube Oil System is obtained when control and lubricating oil is able to flow to both Boiler Feed Pumps. All blank flanges are assumed to be in their normal configuration. The swing connection between LO-1 and LO-3 is modeled as a T-junction (i.e., oil may simultaneously flow from each valve into the downstream piping). Relief valves LO-8 and LO-30 provide an alternate flow path when the normal path is blocked. Breaks of up to 1/2 inch are assumed not to affect the flow of oil.

2.4 System Combinations and Their Minimal Cut Set Results

The system modeling efforts described above yielded individual system digraphs. The next task was the combination and analysis of the systems in combinations as discussed in Section 2.1 and summarized in Table 2-4. For each specified combination of systems (i.e., accident sequence or event tree scenario) the systems involved must be merged to provide a system combination digraph. The process involves the modification of each system digraph to account for common boundary nodes and interfacing for the propagation of failures across the relevant system boundaries. The resulting system combination models are frequently very large (8-10 thousand nodes) and difficult to process. Problems encountered at this level of analysis include the computational difficulty of considering increasingly higher levels of combinations, and inter system cycles that are much more difficult to detect and correct than those at the system level.

In this section, each system combination (see Table 2-4) is described along with , and the results in terms of singleton and doubleton minimal cut sets. The detailed results discussed below will be presented in the matrix format shown below. 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 in the following sections represent the fully expanded cut sets.

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

(a) Doubleton Matrix

A*B
A*D

(b) Cut Sets

The discussion of the doubleton cut set matrices is in terms of submatrices, or "blocks." Notice that the matrices containing the results are symmetric and that the upper left (submatrix block (1.1) is letter "A", and represents a frontline system. Then each "row" is sequentially lettered (e.g. second "row" B,C up to the diagonal, then the third "row" is lettered D, E, F and so on. In the complete version of this report, the full singleton lists and doubleton matrices are given in Volume 1-B which is referred to as the enclosures. In order to make this volume of the report more readable, we have included the relevant portions of the enclosure volume at the end of each of the system combination subsections.

In some cases, the doubleton matrices were too large to be included.

2.4.1 Medium LOCA and Loss of Low Pressure Injection (S_1D_i)

2.4.1.1 Introduction

In this system combination, we have searched for singleton and doubleton failures that would cause a loss of Low Pressure Injection during a given, but unspecified, medium (2"-6" pipe rupture) LOCA. Figure 2-8 shows that core melt could potentially result from this system combination scenario. Supporting the low pressure injection system are the safety injection actuation system, the electrical system, the Component Cooling system, Instrument Air system and the Service Water system. Notice that the bi-directional relationship between several support systems establishes intersystem cycles.

In July 1984, the competing team from Brookhaven National Laboratory identified a safety violation at Indian Point-3 which could occur during a medium LOCA. They discovered that a failure of Battery 32 in conjunction with the nonfailure of offsite power would result in the failure of the RHR pumps to start. Our original results did not show this singleton.

On review of the DMA model we discovered several electrical load shedding errors. In particular we had not included the following load shedding steps:

1. The Safety Injection signal causes the following breakers to trip:

52/2AT5A	as per IP-3 Electrical System
52/3AT6A	Description p. 65A

2. The breakers UT1 - UT4 which connect the main generator to the electrical system are tripped. The unit auxiliary transformer is also turned off representing the tripping of the main generator.

3. Motor Control Centers, MCC-39 and MCC-37 are stripped from their buses. This results in Battery Chargers 31 and 32 becoming deenergized. Battery Charger 33 is left energized.

The reanalysis of System Combination One (SC1) did not directly show battery 32 as a singleton. The reason for this omission is the lack of the NOT operation in the present DMA methodology. Battery 32 is a singleton only if there is voltage on 480v bus 2A. Since DMA models the components of the system in their failed condition, the non-failure of the bus did not show the battery as a singleton. Battery 32 is seen as a doubleton with the interlock (ITLBKREG1P) which responds (indirectly) to the presence of voltage on bus 2A. Careful evaluation of this doubleton shows that unless there is a failure which will cause a Bus 2A voltage failure, Battery 32 is a singleton.

In order to identify the doubletons which should be checked in detail, it is necessary to flag components whose "success" acts as a system failure. Thus any doubleton containing a failure node and a success node should be investigated further. In the DMA model for SC1 the prefixes UV (undervoltage), UV^1 (failure to detect undervoltage) and ITL

Figure 2-8

SYSTEM COMBINATION #1

S1 LOCA with Low Pressure Injection

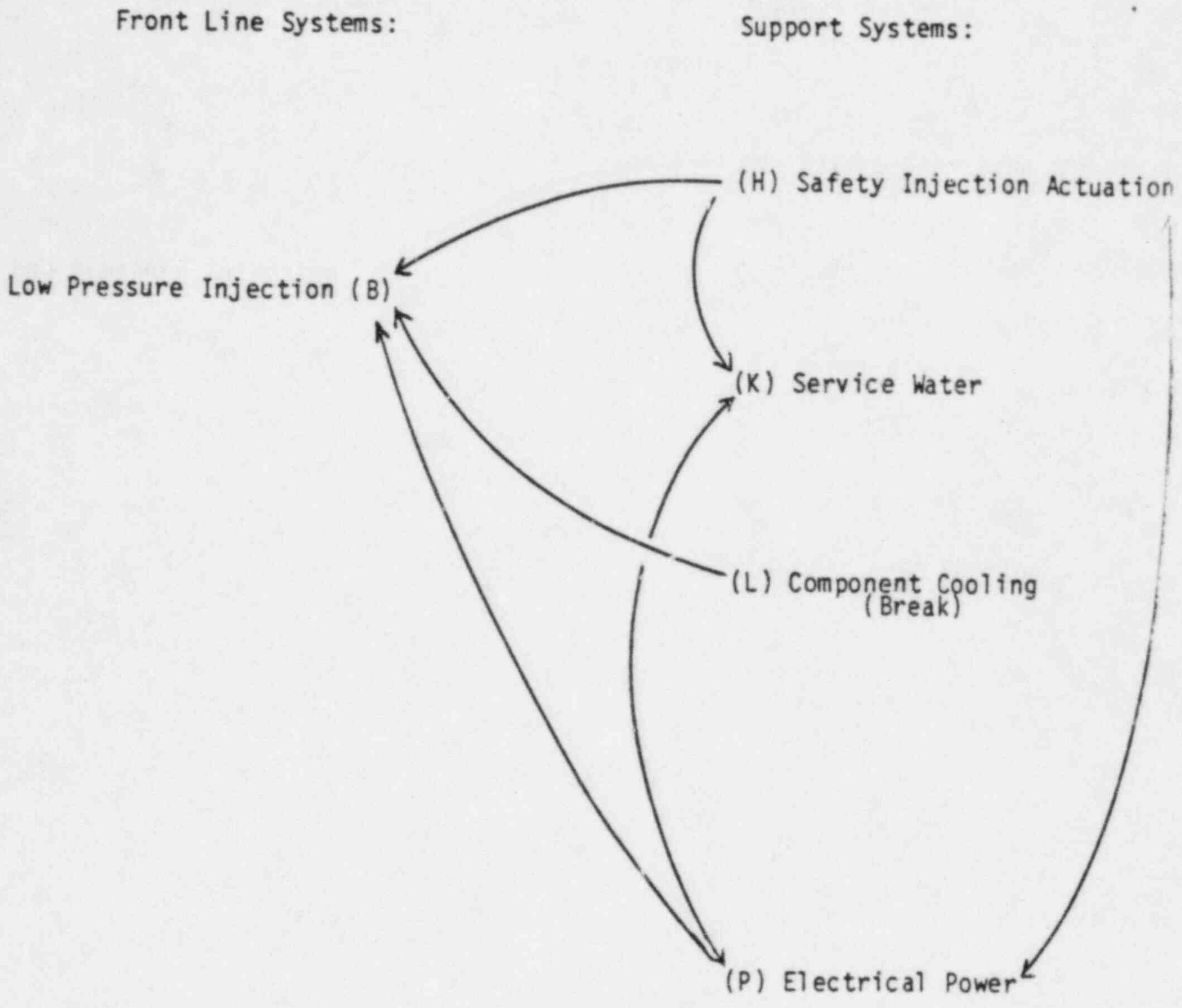
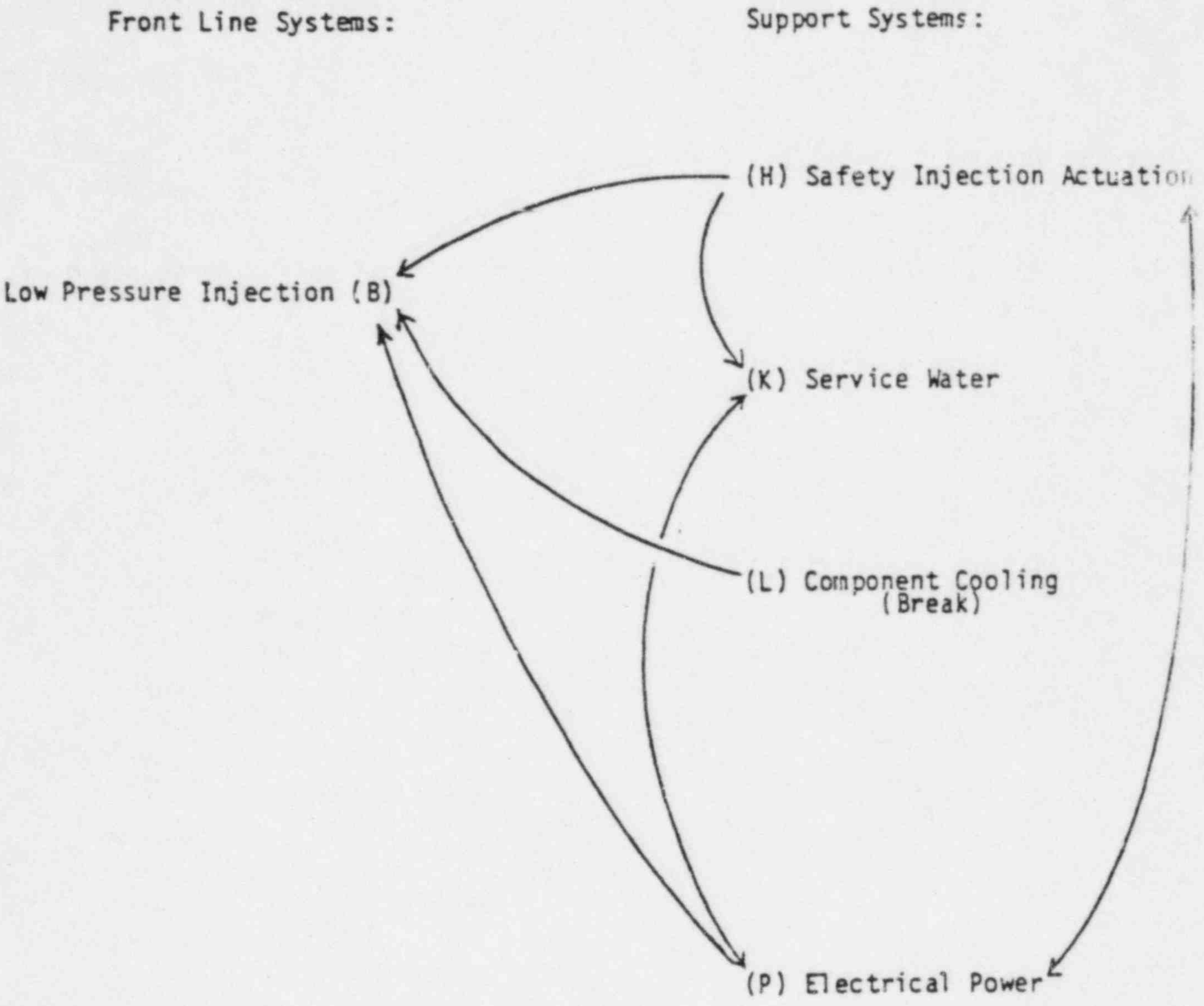


Figure 2-8

SYSTEM COMBINATION #1

S1 LOCA with Low Pressure Injection


Front Line Systems:
Support Systems:
(H) Safety Injection Actuation
Low Pressure Injection (B)
(K) Service Water
(L) Component Cooling (Break)
(P) Electrical Power

2.4.1.3 Results for the Front-Line System Acting Alone: Case I

The Low Pressure Injection System (LPIS) is the front-line system for this sequence. For Case I, we consider all support systems to work with probability equal to ONE. Several components within the system have been identified as singleton failures which cause a loss of low pressure injection ability (see Enclosure 1, Case I).

The Refueling Water Storage Tank is the only source of injection water and, therefore, it and its associated piping and valves are singletons (node 24). The tank must be full of borated water prior to the start of the accident. (This requirement is reflected in the time transition node TTRWSTH2O). The RWST isolation valve (VGA846) must be open and the path to the RHR pump suction motor operated stop valve (MOV882) must be clear of blockage. The RHR pump suction check valve (VC881) must pass flow to the RHR pump common suction junction (J735B) (see Figure B.1.2.A in Appendix B).

The path from the common RHR pump discharge junction (JRHR) to the Residual Heat Loop isolation valve (MOV744) must be free of flow restrictions. MOV744 must be open and the RHR containment check valve (VC741) must open to permit flow to reach the Residual Heat Loop inlet junction (J745B).

The Residual Heat Loop contains the piping downstream of J745B which connects to the Residual Heat Exchangers (RHXs). It is bounded by junction between MOV1869A and MOV1869B (J1869), the Containment Spray Isolation Valves (MOV889A and MOV889B), and crosstie junctions (J899A and J899B) downstream of the loop discharge stop valves (MOV899A and MOV899B) (see Figure B.1.1.A).

The Residual Heat Loop is susceptible to catastrophic pipe breaks which sever all of the low pressure injection paths to the core. A failure (BRC745AJ745B) which causes the piping between the two RHXR inlet junctions (J745A and J745B) to break off at both ends would prevent flow from reaching the heat exchangers. The probability of such a catastrophic failure is remote; however, low pressure injection still fails even if the pipe breaks only at J745B. A similar situation exists at the outlets of the RHXs (J889 and J1869B), though this break (BRC889J1869B) must be double ended to completely isolate the downstream low pressure injection system.

The crosstie downstream of MOV899A and MOV899B on the Residual Heat Loop outlet merits special mention. Failure of low pressure injection will occur if either junction (J899A or J899B) ruptures. This failure (BRC899BJ899A) is more serious than the two previously discussed because the piping connecting the two junctions contains no isolation valves. The Low Pressure Injection System is designed with parallel flowpaths throughout a majority of its length. A doubleton failure occurs where two events are capable of simultaneously blocking both piping trains. These interactions are shown in block "A" of the doubleton matrix.

* A copy of the material in this enclosure has been included at the end of this section.

At least one of the two Residual Heat Removal Pump trains must be supplying water to the downstream common junction (JRHR). The operational path must have its inlet (VGA735A or VGA735B), check (VC738A or VC738B), and outlet (VGA739A or VGA739B) valves open while the corresponding pump (RHRP31 or RHRP32) is running.

A minimum of one Residual Heat Exchanger must be able to supply water to a downstream crosstie junction (J889 or J1869B). Note that the path through RHXR31 will be isolated if either of the motor operated stop valves (MOV745A or MOV745B) is shut.

The Residual Heat Loop (RHL) must be able to discharge to the injection leg header junctions (J838Q or J838R). Thus, at least one of the RHL discharge legs must be able to pass flow. Therefore, at least one set of valves (HCV638/MOV747/MOV899B or HCV640/MOV746/MOV899A) must be open.

In order for the LPI System to perform successfully flow from the injection leg header junctions must reach the core through at least one injection leg. This requirement will not be fulfilled if both injection header leg junctions (J838Q and J838R) are simultaneously blocked. A failure of only one of these junctions in coincidence with a block in the opposite crosstie junction (J899A or J899B) would prevent flow from reaching the core too. A similar condition could also arise if both crosstie junctions (J899A and J899B) were to become fouled.

2.4.1.4 Results for the Front-Line and Support Systems Acting Together: Case II

Additional singletons and doubletons are generated when the scope of the analysis is expanded to include hardware failures of the support systems. The Safety Injection Actuation, Electrical, and Component Cooling Systems directly support the Low Pressure Injection System. The Service Water System supplies cooling water from the Hudson River to the emergency diesel generators. During a loss of offsite electrical power, these generators power the RHR pumps. Thus, the Service Water System indirectly supports the LPIS (see Enclosure 1.2).

All of the additional singletons we identified are due to the Component Cooling System. The system is required to be filled when the RHR pumps are operating. The water contained in the system piping provides a heat sink for the RHR Pump Seal Heat Exchangers (PSHXR1871B and PSHXR1871D).

Three catastrophic breaks were identified in the Component Cooling System. System water inventory will be lost if the Component Cooling Pump inlet piping header between J760A and J760C is severed at both junctions. This break is denoted by BRC760CJ760A on the digraph. Similar failures (BRC762CJ760A and BRC765BJ765A) also occur at the CCP outlet piping header (J762A to J762C) and the Component Cooling Heat Exchanger outlet piping header (J765A to J765B), respectively. Actually, a break anywhere in the Component Cooling System without operator isolation action will drain the piping. This effect is not evident in our results because the CCS model was developed for the recirculation phase where flow is required to cool the various components.

The doubleton matrix has been divided into blocks corresponding to the contribution from each system. First notice that the matrix is symmetric and lettered sequentially starting from the upper left corner with the letter "A". Blocks "D", "E", "F", "I", and "R" contain no doubletons. Block "A" was discussed in the previous section. Blocks "J", "O", "S", and "U" are doubletons internal to an individual support system. They will be lightly touched upon in this section. A discussion of these systems is included in Section 2.2 and the models for these systems were discussed in Section 2.3. Blocks "B", "C", "H", "L", and "Q" involve the Component Cooling System. Based on previous discussion these blocks contain no doubletons since all CCS breaks are singletons.

All other blocks represent intersystem contributions. The joint contributions from the LPI and Safety Injection Actuation Systems are contained in Blocks "G" and "P". These failures arise because none of the RHR pumps are able to supply flow to the common discharge header junction (JRHR). One RHR pump path fails because of electrical or mechanical problems. The other path fails because its pump does not receive the Safety Injection Actuation Signal. Loss of the dc distribution panel (PNLDIS34) removes the source of power necessary to energize the SI logic relays. Failure of a Channel 2 logic gate (LG1OF2SIA2B) to indicate an abnormal condition also prevents the master relay (RSI2) from changing state. The auxiliary relay (RSI21X) will fail to close the Safety Injection Actuation Signal starting contact (RL3-16A) of No. 32 RHR pump if the output of RSI2 or another Channel 2 logic gate (LG2OF2SIA2B) is not in the actuation state.

Failure of a Channel 1 meter relay (RSI1) to change state during an abnormal condition prevents the auxiliary relay (RSI11XZ) from closing the Safety Injection Signal starting contact (RL3-13A) of No. 31 RHR pump.

The contributions from the Low Pressure Injection and Electrical Systems are contained in Block "K". As expected, one node of many doubleton pairs consisted of a failure of an RHR pump 480V ac bus or dc control power supply. The other nodes of these pairs represent failure of the opposite RHR pump path due to mechanical reasons. Bus failure can arise from a loss of power (BUSn), an undervoltage condition (UVBUSn), or a short circuit to ground (BUSn/) where "n" is the bus number (3A or 6A). The remaining doubletons indirectly interact with the LPI system. These doubletons appear because a loss of some dc power supplies propagates failure to the SIAS, which in turn affects the RHR pumps.

Block "M" contains the Service Water and Electrical System doubletons. All of the pairs in this block result from a simultaneous loss of offsite power and diesel generators. Offsite power can be lost by a failure of either the offsite power grid (SOURCE1) or the onsite Station Auxiliary Transformer (STAUXXFMR). In this block the emergency generators are lost because of a failure of Service Water cooling to the diesel engines. A discussion of the Service Water System is included in Sections 2.2.12 and 2.3.9.

Blocks "J", "S", and "U" are composed of doubletons internal to the Safety Injection Actuation System. Many of these doubletons represent a simultaneous failure of both SIAS channels. Since RHR pump No. 32 starts on receipt of a Channel 2 SI signal and RHR pump 31 starts on receipt of either a Channel 1 or 2 signal, failure of both SIAS channels prevent both pumps from starting automatically. A pump will also not start if an undervoltage condition is sensed on its bus. Combinations of undervoltage conditions (RL27-...) and failures of SI relays (RL3-1...) can prevent both pumps from starting. Refer to Sections 2.2.7, 2.3.1, and 2.3.2 for a complete description of the system.

Blocks "N" and "T" contain the Electrical and Safety Injection Actuation Systems doubletons. All of these failures propagate so as to prevent both RHR pumps from starting. Three basic types of failures were identified, any one of which could be one half of a doubleton pair.

The first category is based on the ability a RHR pump to obtain electrical power from its bus. Category 2 relates to the availability of the dc supplies which power the SIAS circuitry. The operation of the SIAS components downstream of the dc power supplies forms the basis of the third category.

The Category 1 failures were previously decribed in the Block "K" section. A more complete description of the second and third categories can be found in Sections 2.2.7, 2.3.1, and 2.3.2.

Block "O" is composed of doubletons internal to the Electrical System. Most of these doubletons consist of combinations of the Category 1 and Category 2 failures described previously. The remaining doubletons consist of a loss of offsite power (SOURCE1) or the Station Auxiliary Transformer (STAAUXXFMR) combined with a failure of any of the following:

Bus Tie Breaker 3A-6A interlock (ITLBKR3AT6A).
Bus Tie Breaker 2A-5A interlock (ITLBKR2AT5A).
Compressed air in the diesel generator receiver (TTRCVR31).

Failure of the bus tie breaker 3A-6A interlock prevents the diesel generators from powering the RHR pumps (see Section 3.1 for a further discussion of this significant systems interaction).

Compressed air is required to start the diesel generators.

2.4.1.5 Results for the Front-Line and Support Systems Acting Together with Common Location Vulnerabilities

Additional singletons and doubletons are generated when the scope of the analysis is expanded to include the effects of common component location. Three singletons and three doubletons were found to be significant (see Enclosure 1, Case III).

The RHR pumps share a common room; consequently, they are susceptible to fire (LFRHR), steam (LSRHR), or flooding (LWRHR) failures. Possible location effects were also identified in the 888 room and the Residual Heat Exchanger portion of the Containment Building (see Figures B.1.1C and B.1.2C). The motor operated valves in these areas, however, are normally correctly aligned and do not require repositioning. The controllers which operate these motors are located in the switchboards, not at the motor. Thus, accidental operation due to steam shorted contacts is also impossible.

The other two singletons consist of the electrical locations LOCD and LOCS. LODC includes the 15 foot elevation of the Control Building where BUS 3A and BUS 6A (the RHR pump power supplies) share a common location. The Central Control Room (LOCS) houses both PNLDIS32 and PNLDIS33, the RHR pump motor controller supplies.

At the 33 foot elevation of the Control Building is a cable spreading area (LOCR) which contains the dc controller power supply for RHR Pump No. 32. Thus, this location forms a doubleton with RHR Pump No. 31.

The two remaining locations (LOCA and LOCC) represent the 6900V switchgear and the Station Auxiliary Transformer. They form doubletons with the Service Water System because of the cooling of the emergency diesel generators by the SW pumps.

2.4.1.6 Results for the Front-Line and Support Systems with Common Location Vulnerabilities and Operator Action

In this section the effects of operator action, both failure of the operator action to perform a right action (OPR) and operator performing a wrong action (OPW), were analyzed. Only the differences between the previous sections and this section will be discussed (see Enclosure 1, Case IV).

Several incorrect operator valve manipulations were identified as singletons. These actions are the shutting of the RWST isolation (OPW846), the RHR pump suction isolation (OPW882), and the RHR pump discharge isolation (OPW744) valves. However, Indian Point-3 has taken safeguards with these valves. Deliberate effort is required to reposition these valves since VGA846 is normally locked open and the motor operated valves (MOV744 and MOV882) are de-energized open at their motor control centers.

In Case I, II, and III, no operator action was allowed during the accident; in Case IV, the operator takes actions that make him operate as a "backup system".

One of the singletons previously identified is reduced to a doubleton because of the redundancy provided by the operator. Blockage in the pipe reducer (PPR1810) can be bypassed by the operator (OPRA898) who opens the bypass valve (VGA898).

An OPW node appears for each component that may be incorrectly operated by manual intervention. The effect of these nodes is identical to that described for the component itself.

The number of doubletons identified in the RHR pump starting circuitry and SIAS circuitry is reduced because of the redundancy provided by the operator (OPRSWMRHRP31C and OPRSWMRHRP32C) who manually starts the pumps. The effect of the operators is quite dramatic when one compares the doubleton matrix for the automatic case with that of the manual case. Notice that the number of doubletons involving the Safety Injection Actuation System has been drastically reduced.

All of the singletons caused by breaks in the Component Cooling System have been degraded to doubletons because of the actions taken by the operators to isolate these leaks. The operator may also refill the system if an excessive volume of water was lost through a break.

The doubletons identified in the electrical system which involve the Station Auxiliary Transformer, the diesel generator air receiver, and the bus tie breaker interlocks have been elminated because of the redundancy provided by the operator.

2.4.1.7 Effect of Model Corrections.

The reanalysis of System Combination 1 which included the corrections given earlier showed no singletons than those already presented. Approximately 350 new doubletons were found including doubletons related to the infamous Battery 32. New doubletons were also found with Battery 31. These included:

BATTERY31 * PNLDIS34P, etc.	Distribution Panel 34
BATTERY31 * LG20F2SIA2BH, etc.	SI Actuation Logic Components
BATTERY31 * RSI21XZ	SI Actuation Logic Components
BATTERY31 * PWRPNL32P	Not Real since PWRPNL32P is a singleton
BATTERY31 * BATTERY32/P	Short in Battery 32
BATTERY31 * FUSEPNL32/P	Short in Fuse Panel
BATTERY31 * PWPPNL32/P	Short on Power Panel
BATTERY31 * BKRDPNL34/P	Short in Distribution Panel Breaker
BATTERY31 * PNLDIS34/P	Short in Distribution Panel

As stated above, we did not detect directly the singleton effect of the loss of BATTERY 32 due to the lack of a "NOT" gate in the DMA methodology. In the DMA doubleton matrix for the revised model, BATTERY32 is seen as a doubleton with ITLBKREG1. The IP-3 electrical system specification (p 65B) states that the breaker BKR2AT3A will not close unless the following conditions are satisfied:

1) Undervoltage on bus 3A
b) Tie Breaker 3AT6A opened
c) Normal bus feed breaker 52/3A is opened
d) Diesel generator 31 breaker (BKREGOO is closed supplying bus 2A
e) No faults exist on bus 3A or 5A.

The diesel generator breaker is controlled in our model by a component called ITLBKREG1 (Interlock breaker EG1). Diesel 31 will not load onto its bus if the bus is powered. The node DUMBUS2A represents the no voltage state of the bus. Thus, any direct connection between DUMBUS2A and ITLBKREG1 will nodel the wrong condition. If a "NOT" gate is put between DUMBUS2A and BKREG1 and BKREG1 is connected to BKR2AT3A, an analysis of the digraph would show the not condition and hence BATTERY32 as a singleton. We could partially address this problem by identifying any switch or interlock which depends on the success of another node by a special symbol and then investigating each of the doubletons which contain variables using this special symbol.

In the digraph following prefixes have special meaning:
UV - Undervoltage Condition
UV' - Failure to detect undervoltage condition
ITL - Interlock
In the doubleton matrix for System Combination One, all components which are doubletons with the following variables were investigated:

ITLBKREG1
ITLUV'BUS3AP
ITLBFBUS3AP
ITLBKR3AP
ITLBKR3AT6AP
ITLBFBUS5AP
ITLBKR2AT5AP
UVBUS2AP
UVBUS3AP
UVBUS6AP

The component ITLBKREG1 is the interlock which prevents the BKREG1 bus tie breaker from closing. This breaker is in turn controlled by BKREG1 which connects the diesel generator 31 to BUS 2A. BKREG1 will remain open (in our model in the failed state) if there is voltage on bus 2A. Thus, any components which are doubletons with ITLBKREG1 are actually singletons.

The other suspect variables will now be discussed.

ITLUV"BUS3AP, ITLBFBUS3AP, ITLBKR3AP

This component is a doubleton with

UVBUS6AP	-Undervoltage Sensor
TIMELONG8P	-Special Condition Node
BATTERY32/P	
FUSEPNL32/P	Short Circuit
PWRPNL32/P	

ITLBKR3AT6AP

This component is a doubleton with

STAUXXFMR	Loss of Offsite Power
BKR5AT6P	
BUS6P	
BATTERY32	Discussed Earlier
TTBATTERY32	Special Condition Node
LOCCP	Location

Since Battery 32 is a "singleton", this component is not relevant.

ITLBFBUS5AP

This component is an interlock on the bus feed breaker (52/5A) for Bus 5A. This breaker is tripped by any of the following conditions:

a) Undervoltage on associated Bus (5A)
b) Manual Trip Button at Breaker
c) Trip Switch in CCR
d) Trip Switch in Diesel Building
e) Overcurrent

None of these are "success' conditions as discussed above, so doubletons involving this component are true doubletons.

UVBUS(2,3,6)A

These components are the physical devices which sense undervoltage on their associated buses.

ITLBK2AT5AP

This component reads the state of BKR2AT5AP which must be open for BKREG1 and BKREG3 to close. The breaker BKR2AT5AP is normally open so that doubletons including this component are true doubletons.

Comparison of Quantitative Results (Quantitative results are discussed in detail in Section 4.1

The singletons found in the analysis of the upgraded model of System Combination One are identical to those discussed earlier except for Battery 32 related components. The addition of these components does not significantly change the quantitative results. The new model does contain significantly more doubletons than before. The new components which give rise to these added doubletons are listed below in Table 2-10. A comparison of the quantitative results from the earlier model and the upgraded model can be found in Table 2-11. The third column in Table 2-11 represents the effects of adding in the singletons which arise from the Battery 32 singleton. There are six singletons which are related to the Battery 32 failure. These are:

BATTERY32P
FUSEPNL32P
PWRPNL32/P
FUSEPNL32/P Short Circuits
BATTERY32/P
PNLDIS34/P

Table 2-10 New Components in System Combination One.

```
 BATTERY31/P    WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND DURING ACCIDENT
@       BATTERY SHORTED TO GROUND DURING ACCIDENT
 BATTERY32/P    WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND DURING ACCIDENT
@       BATTERY SHORTED TO GOUND DURING ACCIDENT
 BATTERY32      BAT000  2  8.350E-05-8.350E-08
@       BATTERY FAILS PRIOR TO OR DURING ACCIDENT
@       COMPUTED BY 2000HRS (INSPECTION PERIOD)/2 *8.35E-08/HOUR
@       REFERENCE IP PSS 1.6-164 AND TABLE 1.6.1-4
 BATTERY31      BAT000  2  8.350E-05-8.350E-08
@       BATTERY FAILS PRIOR TO OR DURING ACCIDENT
@       COMPUTED BY 2000HRS (INSPECTION PERIOD)/2 *8.35E-08/HOUR
@       REFERENCE IP PSS 1.6-164 AND TABLE 1.6.1-4
 FUSEPML31/P    WIR000   1 -7.520E-06
@       SHORT CIRCUIT TO GROUND DURING ACCIDENT
 FUSELPNL32/P  WIR000          1 -7.520E-06
@       SHORT CIRTUIT TO GROUND DURING ACCIDENT
 BKRDPNL31P     BKR213   1 -0.267E-05
@       BREAKER INADVERTENTLY OPENS
 BKRDPNL34P     BKR213   1 -0.267E-05
@       BREAKER INADVERTENTLY OPENS
 BKRST6P        BKR120   2  1.330E-03-0.267E-05
@       BREAKER FAILS TO CLOSE AND INADVERTENTLY OPENS
 FUSEPNL31P     FUS100   1 -8.320E-07
@       FUSE PREMATURELY OPENS
 FUSEPNL32P     FUS100   1 -8.320E-07
@       FUSE PREMATURELY OPENS   IP3 PSS TABLE 1.6.1-4  ITEM 36
 LG10F2SIA2AH  SAR110   1 -2.430E-07
 LG10F2SIA2BH  SAR110   1 -2.430E-07
 LG20F2SIA2BH  SAR110   1 -2.430E-07
 R86ST6P        SAR110   1 -2.430E-07
 RLSI2A1I       SAR110   1 -2.430E-07
 RLSI6A1I       SAR110   1 -2.430E-07
 ITLBFBLUS3AP  SAR111   1 -2.430E-07
@       ELECTRICAL INTERLOCK FAILURE RELAY FAIL TO OPERATE
@       SIMILAR TO IP3 PSS ITEM 38
 ITLBFBUS5AP    SAR111   1 -2.430E-07
@       ELECTRICAL INTERLOCK FAILURE RELAY FAIL TO OERATE
@       SIMILAR TO IP3PSS ITEM 38
 ITLBKR3AP      SAR111   1 -2.430E-07
@       ELECTRICAL INTERLOCK FAILURE RELAY FAIL TO OPERATE
@       SIMILAR TO IP3 PSS ITEM 38
 ITLBKREG1P    SAR111   1 -2.430E-07
@       ELECTRICAL INTERLOCK FAILURE RELAY FAIL TO OPERATE
@       SIMILAR TO IP3 PSS ITEM 38
 BKR2AT3AP     BKR120   2  1.330E-03-0.267E-05
@       BREAKER FAILS TO CLOSE AND INADVERTENTLY OPENS
```

Table 2-11 Comparison of Old and Revised Model for System Combination One

REVISED MODEL	OLD MODEL	REVISED MODEL	WITH BATTERY32 AS SINGLETON
Number of Singletons	17	17	22
Singleton Probability	8.05E-4	8.05E-4	9.00E-4
Number of Doubletons	2105	2465	-
Doubleton Probability	3.51E-6	3.79E-6	-
Total Failure Probability	8.08E-4	8.08E-4	9.00E-4

Fully Automatic Operation

Note that the singletons related to BATTERY32 cause only a 12% change in the failure probability Thus, from a probabilistic reliability point of view, the Battery 32 singleton is not significant. It does, however, violate the single failure criteria.

Effect of PASNY Fix to BATTERY32 Singleton

After the Battery 32 singleton was discovered, the Indian Point 3 personnel in conjunction with Westinghouse made a change which shorted contact 52A/EG1 in the 480 volt ac switchgear. The implementation of this short in the digraph is the indentation of the following line in the adjacency input. (Appendix C)

```
ITLBKREGOP, AXFRBKR2AT3AP,1
```

This change removes the connection between the BKREG1 interlock and the crosstie breaker 2AT3AP. The DMA model was rerun with this change with the quantitative results shown in Table 2-12.

	REVISED MODEL WITH BATTERY 32 AS SINGLETON	MODEL WITH PASNY PATCH
Number of Singletons	22	17
Singleton Probability	9.00E-4	8.05E-4
Number of Doubletons	-	2640
Doubleton Probability	-	3.79E-6
Total Failure Probability	9.00E-4	8.08E-4

Table 2-12 Quantitative Effect of PASNY Battery 32 Patch

As can be seen from this table, the patch doesn't significantly affect the overall failure probability (and unavailability). This effect points out the danger in relying strictly on quantitative results as a measure of safety.

ENCLOSURE 1

A COMPLETE COPY OF THIS
ENCLOSURE CAN BE FOUND
IN VOLUME 1-B

ENCLOSURE 1

SYSTEM COMBINATION 1

MEDIUM LOCA WITH LOW PRESSURE INJECTION

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

```
            SINGLETONS

      2      LPI-MLOCAD
      5      J735BD
      5      J898D
      5      J1863D
      5      MOV882D
      5      VC881D
      5      PPI735D
      5      J735AD
      6      PPR1810D
     10      J111XD
     10      JRHRD
     10      J740AD
     10      J636D
     10      J883D
     10      MOV744D
     10      VC741D
     10      J110XD
     24      J1810D
     25      J290AD
     25      J200D
     25      PPI846D
     25      HTRC846ZD
     25      VGA846D
     25      HTRC846YD
     25      PPR846D
     25      RWST1D
     26      TTRWSTH20D
     51      BRC899BJ899AB
     66      BRC745AJ745BD
     68      BRC889J1869BD
     70      J745BD
```

```
FILE IDENTIFICATION:
  REACH PAIR:   I=    1    J=    2
  DATE:  8/13/84
  ANSWER.POS FILE IS: DRO:SC1810MC3.POS
  OUTPUT.DAT FILE IS: DRO:SC1810MOT.TRP
  VARIAB.DAT FILE IS: DRO:SC1727MVB.DAT
  RENUMSRT.DAT FILE IS: DRO:SC1727MRT.DAT
  SIGMA PI FILE NAME IS: DRO:SC1810MSI.C3
```

MEDIUM LOCA WITH LOW PRESSURE INJECTION

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

DOUBLETONS

```
       1 3 3 4 4 4 4 5 5 5 6 6
     9 1 0 9 0 7 8 9 2 7 9 7 9

 9   - * - - - - - - - - - - *
11   * - - - - - - - - - - * -
30   - - - * * - - - - - - - -
31   - - - * * - - - - - - - -
35   - - - * * - - - - - - - -
39   - - * - - - - - - - - - -
40   - - * - - - - - - - - - -
44   - - * - - - - - - - - - -
47   - - - - - - * * - - - - -
48   - - - - - * - - - * - - -
49   - - - - - * - - - * * - *
52   - - - - - - - - - * * - *
57   - - - - - - * * * - - * -
59   - - - - - - - * * - - * -
67   - * - - - - - - - * * - *
69   * - - - - - - * * - - * -
```

MEDIUM LOCA WITH LOW PRESSURE INJECTION

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

VARIABLE LIST FOR SC1 CASE I DOUBLETON MATRIX

9	J745AD
9	RHXR32Z
9	MOV745BD
9	MOV745AD
11	VGA742D
11	RHXR31Z
30	VGA735BD
30	J1867BD
30	J101XD
30	CON182252/RHR2I
30	RHRP32Z
30	J1866DD
30	VC738BD
30	J107D
30	VGA739BD
30	J830BL
30	J6278AL
30	J6278BL
30	J6278CL
30	JA502L
30	J017BL
30	J601BL
30	J602BL
30	J602CL
30	J1871AL
30	VGL736BL
30	J736BL
30	PPR736BL
30	PSHXR1871BL
30	PPR750DL
30	J750DL
30	PPI1871AL
30	VGL1871AL
30	J1871BL
30	PPI1871BL
30	PPR1871BL
30	VGL1871BL
30	VC750DL
30	ORFC645BL
30	FIC645L
30	ORFC645AL
30	VGL737BL
30	JA501AL
30	JA501L
39	J740BD
39	VGA735AD
39	J1867AD
39	J103XD
39	CON172152/RHR1I
39	RHRP31Z
39	J1866BD
39	VC738AD
39	J104D
39	VGA739AD
39	PPI739AD
39	JA14AL
39	JA14L
39	J830AL
39	JTIC627L
39	J627AL
39	J017AL
39	J602AL
39	J601AL
39	J601CL
39	J601DL
39	J1871CL
39	VGL736AL
39	J736AL
39	PPR736AL
39	PSHXR1871DL
39	PPR750EL
39	J750EL
39	VGL1871DL
39	J1871DL
39	PPI1871DL
39	PPR1871DL
39	VGL1871CL
39	VC750EL
39	ORFC646BL
39	FIC646L
39	ORFC646AL
39	VGL737AL
39	J627BL
40	CON91352/RHR1I
47	J838QB
47	J639B
47	J638B
48	J838RB
48	J641AB
48	J641B
48	J640B
49	J899AB
52	MOV899AB
52	MOV746B
52	J733AB
52	HCV640B
52	J889AB
57	J899BB
59	MOV899BB
59	MOV747B
59	J733BB
59	HCV638B
59	J889BB
67	J889D
69	J1869BD
83	VGA760AL
84	J1805L
85	PPR1805L
87	J760AL
88	BRC760AJ760BL
95	BRC760CJ760BL
98	VGA760CL
100	J760CL
102	JA57L
103	ORFC760CL
104	CCWP33L
108	JA55L
109	ORFC760AL
110	CCWP31L
111	ORFCCCW33L
112	VC761CL
113	JA3L
114	VGA762CL
116	J763BL
116	VGA759BL
116	JA8L
116	CCHXRS32Z
116	VGA765BL
116	J764BL
118	J762CL
119	BRC762CJ762BL
128	BRC762AJ762BL
129	ORFCCCW31L
130	VC761AL
131	JA1L
132	VGA762AL
133	J763AL
133	VGA759AL
133	JA7L
133	CCHXRS31Z
133	JA10L
133	VGA765AL
133	J764AL
133	PPI765AL
135	J762AL
142	J765BL
146	J765AL
213	J1190K
213	J98AK
213	J1093BK
213	J1093AK
213	J1093DK
213	VB30K
213	J1095K
214	VC98K
214	HTRC409K
214	J4K
214	J106BK
214	J409K
214	J1221K
214	HTRC98K
214	VB98K
227	RIVHUDSONK
228	STRCTRINTKK
234	SWPWELL1K
236	TRASH1K
238	J131K
242	J133K
243	J132BK
260	CHNLDSK
260	CHNLDS3K
260	J95AK
260	J95BK
260	J95CK
260	J95DK
267	J95FK
267	J1096AK
270	J1096BK
275	J1094K
289	COL-RW-2K

ENCLOSURE I

SYSTEM COMBINATION 1

MEDIUM LOCA WITH LOW PRESSURE INJECTION

COMBINED CASE II & CASE III RESULTS

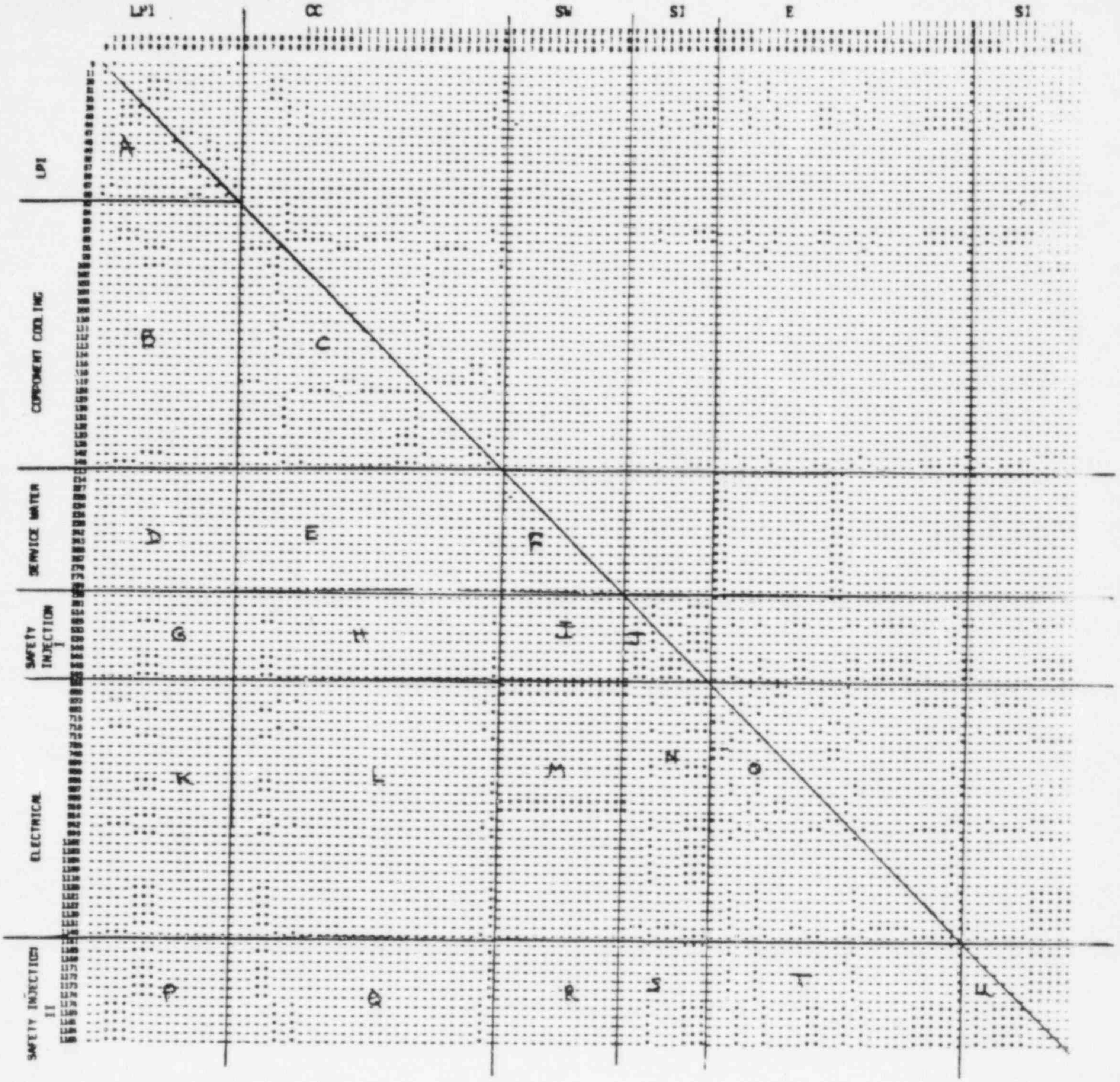
CASE II FULLY AUTOMATIC FRONT-LINE AND SUPPORT SYSTEMS

CASE II FULLY AUTOMATIC FRONT-LINE, SUPPORT SYSTEMS, AND LOCATIONS

SINGLETONS

```
                                2      LPI-MLOCAD
                                5      J7358D
                                5      J898D
                                5      J1863D
                                5      MOV882D
                                5      VC881D
                                5      PPI735D
                                5      J735AD
                                6      PPR1810D
                               10      J111XD
                               10      JRHRD
                               10      J740AD
                               10      J636D
                               10      J883D
                               10      MOV744D
                               10      VC741D
                           *   10      LF888D
                           *   10      LS888D
                           *   10      LW888D
                               10      J110XD
                               24      J1810D
                               25      J290AD
                               25      J200D
                               25      PPI846D
                               25      HTRC846ZD
                               25      VGA846D
                               25      HTRC846YD
                               25      PPR846D
                               25      RWST1D
                               26      TTRWSTH20D
                           *   27      LFRHRD
                           *   28      LSRHRD
                           *   29      LWRHRD
                               51      BRC899BJ899AB
                           *   54      LFRHXRB
                           *   55      LSRHXRB
                           *   56      LWRHXRB
                               66      BRC745AJ745BD
                               68      BRC889J1869BD
                               70      J745BD
                               89      BRC760CJ760AL
                              120      BRC762CJ762AL
                              143      BRC765BJ765AL
                           *  911      LOCDP                   LOCATIONS
                           *  915      LOCSP                   (CASE III)
* INDICATES LOCATION         1159      TESTELECP

                                    FILE IDENTIFICATION:
                                      REACH PAIR:   I=   1   J=   2
                                      DATE:  8/13/84
                                      ANSWER.POS FILE IS: DRO:SC1810MC3.POS
                                      OUTPUT.DAT FILE IS: DRO:SC1810MOT.TRP
                                      VARIAB.DAT FILE IS: DRO:SC1727MVB.DAT
                                      REMUMSRT.DAT FILE IS: DRO:SC1727MRT.DAT
                                      SIGMA PI FILE NAME IS: DRO:SC1810MSI.C3
```



SI LOCA WITH LOW PRESSURE INJECTION
CASE II & III
DOUBLETONS

MEDIUM LOCA WITH LOW PRESSURE INJECTION

CASE II & CASE III (CONTINUED)

VARIABLE LIST FOR SC1 CASE II & III DOUBLETON MATRIX

9	J745AD
9	RHXR32Z
9	MOV745BD
9	MOV745AD
11	VGA742D
11	RHXR31Z
30	VGA735BD
30	J1867BD
30	J101XD
30	CON182252/RHR2I
30	BS17RHRP320P
30	RHRP32Z
30	J1866DD
30	SEMOTSRHRP320P
30	SWMOA11RHRP32P
30	VC738BD
30	J107D
30	VGA739BD
30	J830BL
30	J627BAL
30	J627BBL
30	J627BCL
30	JA502L
30	J017BL
30	J601BL
30	J602BL
30	J602CL
30	J1871AL
30	VGL736BL
30	J736BL
30	PPR736BL
30	PSHXR1871BL
30	PPR750DL
30	J750DL
30	PPI1871AL
30	VGL1871AL
30	J1871BL
30	PPI1871BL
30	PPR1871BL
30	VGL1871BL
30	VC750DL
30	ORFC645BL
30	FIC645L
30	ORFC645AL
30	VGL737BL
30	JA501AL
30	JA501L
31	CON91352/RHR2I
31	CON2RHRP320P
31	RL27-6AX2I
35	PWRPNL32P
35	BKRDPNL34P
39	J740BD
39	VGA735AD
39	J1867AD
39	J103XD
39	CON172152/RHR1I
39	BS17RHRP310P
39	RHRP31Z
39	J1866BD
39	SEMOTSRHRP310P
39	SWMOA11RHRP31P
39	VC738AD
39	J104D

39	VGA739AD
39	PPI739AD
39	JA14AL
39	JA14L
39	J830AL
39	JTIC627L
39	J627AL
39	J017AL
39	J602AL
39	J601AL
39	J601CL
39	J601DL
39	J1871CL
39	VGL736AL
39	J736AL
39	PPR736AL
39	PSHXR1871DL
39	PPR750EL
39	J750EL
39	VGL1871DL
39	J1871DL
39	PPI1871DL
39	PPR1871DL
39	VGL1871CL
39	VC750EL
39	ORFC646BL
39	FIC646L
39	ORFC646AL
39	VGL737AL
39	J627BL
40	CON91352/RHR1I
40	CON2RHRP310P
44	PWRPNL33P
47	J838QB
47	J639B
47	J638B
48	J838RB
48	J641AB
48	J641B
48	J640B
49	J899AB
52	MOV899AB
52	MOV746B
52	J733AB
52	HCV640B
52	J889AB
57	J899BB
59	MOV899BB
59	MOV747B
59	J733BB
59	HCV638B
59	J889BB
67	J889D
69	J1869BD
83	VGA760AL
84	J1805L
85	PPR1805L
87	J760AL
88	BRC760AJ760BL
95	BRC760CJ760BL
98	VGA760CL
100	J760CL
102	JA57L
103	ORFC760CL
104	CCWP33L

108	JA55L
109	ORFC760AL
110	CCWP31L
111	ORFCCCW33L
112	VC761CL
113	JA3L
114	VGA762CL
116	J763BL
116	VGA759BL
116	JA8L
116	CCHXRS32Z
116	VGA765BL
116	J764BL
118	J762CL
119	BRC762CJ762BL
128	BRC762AJ762BL
129	ORFCCCW31L
130	VC761AL
131	JA1L
132	VGA762AL
133	J763AL
133	VGA759AL
133	JA7L
133	CCHXRS31Z
133	JA10L
133	VGA765AL
133	J764AL
133	PPI765AL
135	J762AL
142	J765BL
146	J765AL
213	J1190K
213	J98AK
213	J1093BK
213	J1093AK
213	J1093DK
213	VB30K
213	J1095K
214	VC98K
214	HTRC409K
214	J4K
214	J106BK
214	J409K
214	J122IK
214	HTRC98K
214	VB98K
227	RIVHUDSONK
228	STRCTRINTKK
234	SWPWELL1K
236	TRASH1K
238	J131K
242	J133K
243	J132BK
260	CHNLDSK
260	CHNLDS3K
260	J95AK
260	J95BK
260	J95CK
260	J95DK
267	J95FK
267	J1096AK
270	J1096BK
275	J1094K
289	COL-RW-2K
290	SW123456P

301	PWRPNL31P
514	PNLDIS31P
514	BKRDPNL31P
525	PNLDIS34P
533	LG2OF2SIA2AH
539	LG1OF2SIA2AH
539	RSI1H
540	RSI11XZ
545	LG2OF2SIA2BH
548	LG1OF2SIA2BH
548	RSI2H
549	RSI21XZ
558	STAUXXFMRP
600	SOURCE1P
690	BUS3AP
693	BUS6AP
715	ITLBKR3AT6AP
718	UVBUS3AP
719	UVBUS6AP
728	ITLBKR2AT5AP
900	BATTERY31P
900	FUSEPNL31P
900	LOCOP
907	BATTERY32P
907	FUSEPNL32P
907	LOCQP
909	LOCAP
910	LOCCP
914	LOCRP
942	BUS3A/P
949	BUS6A/P
1102	BATTERY31/P
1103	FUSEPNL31/P
1104	PWRPNL31/P
1109	BKRDPNL31/P
1110	PNLDIS31/P
1120	BATTERY32/P
1121	FUSEPNL32/P
1122	PWRPNL32/P
1130	BKRDPNL34/P
1131	PNLDIS34/P
1140	PWRPNL33/P
1161	CON2024SI11XI
1168	CON913SI21XI
1169	CON2024SI21XI
1171	RL3-16AI
1171	CON91327-6AX3I
1172	RL27-6AX1I
1172	CON3927-6AX1I
1173	RL27-6AX4I
1173	CON3927-6AX4I
1174	RL27-6AX3I
1176	RL3-13AI
1176	CON2627-3AX3I
1180	RL27-3AX1I
1180	CON3527-3AX1I
1181	RL27-3AX4I
1181	CON3527-3AX4I
1184	RL27-3AX2I
1185	RL27-3AX3I

ENCLOSURE 1

SYSTEM COMBINATION 1

MEDIUM LOCA WITH LOW PRESSURE INJECTION

CASE IVA & IVB - MANUALLY ASSISTED

CASE IVA - MANUALLY ASSISTED, FAILURE BY OMISSION

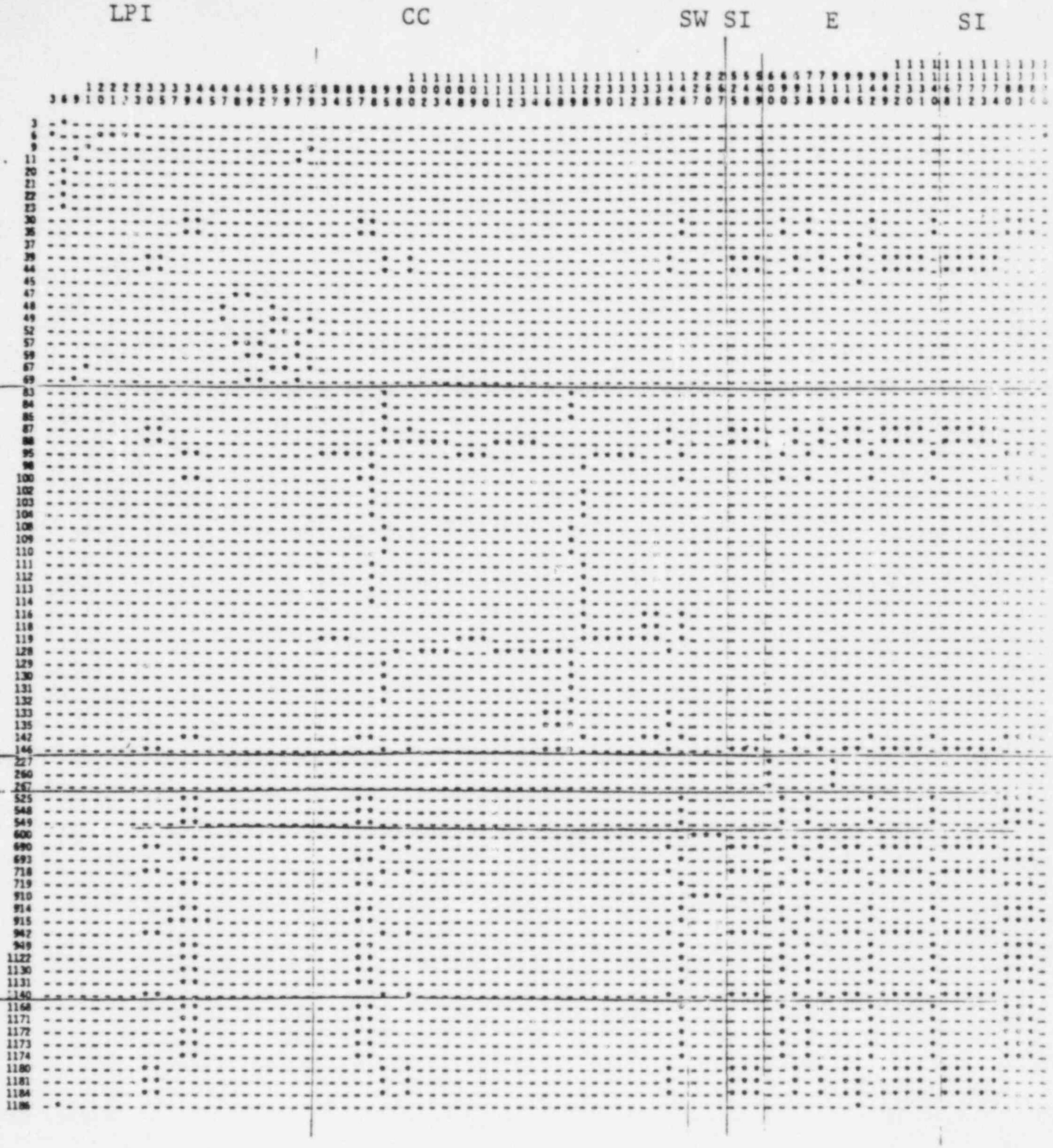
CASE IVB - MANUALLY ASSISTED, FAILURE BY OMISSION AND FAILURE BY COMMISSION

```
                 SINGLETONS

      2      LPI-MLOCAD
      5      J735BD
      5      J898D
      5      J1863D
      5      MOV882D
      5      OPW882D
      5      VC881D
      5      PPI735D
      5      J735AD
     10      J111XD
     10      JRHRD
     10      J740AD
     10      J636D
     10      J883D
     10      MOV744D
     10      OPW744D
     10      VC741D
    *10      LF888D
    *10      LS888D
    *10      LW888D
     10      J110XD
     24      J1810D
     25      J290AD
     25      J200D
     25      PPI846D
     25      HTRC846ZD
     25      OPW846D
     25      VGA846D
     25      HTRC846YD
     25      PPR846D
     25      RWST1D
     26      TTRWSTH2OD
    *27      LFRHRD
    *28      LSRHRD
    *29      LWRHRD
     51      BRC899BJ899AB
    *54      LFRHXRB
    *55      LSRHXRB
    *56      LWRHXRB
     66      BRC745AJ745BD
     68      BRC889J1869BD
     70      J745BD
     89      BRC760CJ760AL
    120      BRC762CJ762AL
    143      BRC765BJ765AL
   *911      LOCDP
   1159      TESTELECP

* INDICATES LOCATION

             FILE IDENTIFICATION:
               REACH PAIR:   I=    1    J=    2
               DATE:  8/ 3/84
               ANSWER.POS FILE IS: DR0:SC1727MC4.POS
               OUTPUT.DAT FILE IS: DR1:[220,1]SC1727MOT.DAT
               VARIAB.DAT FILE IS: DR1:[220,1]SC1727MVB.DAT
               RENUMSRT.DAT FILE IS: DR1:[220,1]SC1727MRT.DAT
               SIGMA PI FILE NAME IS: DR0:SC1727MSI.C4
```



DOUBLETONS

MEDIUM LOCA WITH LOW PRESSURE INJECTION

CASE IVA & IVB - MANUALLY ASSISTED (CONTINUED)

CASE IVA & IVB - MANUALLY ASSISTED

CASE IVA & IVB - MANUALLY ASSISTED

VARIABLE LIST FOR SC1 CASE IVA & IVB DOUBLETON MATRIX

3	J18290
3	J887AD
3	OPW887AD
3	MOV887AD
3	OPW887BD
3	MOV887BD
3	J203AD
3	OPRA898D
3	VGA898D
3	OPW898D
3	J204D
6	PPR1810D
9	J745AD
9	RHXR32Z
9	OPW745BD
9	MOV745BD
9	OPW745AD
9	MOV745AD
11	VGA742D
11	OPW742D
11	RHXR31Z
* 20	LFSIPD
* 21	LWSIPD
* 22	LSSIPD
23	J203D
23	VC847D
23	MOV1810D
23	OPW1810D
30	VGA735BD
30	J1867BD
30	OPW735BD
30	J101XD
30	CON182252/RHR2I
30	BS17RHRP320P
30	RHRP32Z
30	J1866DD
30	OPWRHRP32D
30	SENOTSRHRP320P
30	SWMOA11RHRP32P
30	VC738BD
30	J107D
30	VGA739BD
30	OPW739BD
30	OPWRHRP32E
30	J830BL
30	J627BAL
30	J627BBL
30	J627BCL
30	JA502L
30	J017BL
30	J601BL
30	J602BL
30	J602CL
30	J1871AL
30	VGL736BL
30	OPW736BL
30	J736BL
30	PPR736BL
30	PSHXR1871BL
30	PPR750DL
30	J750DL
30	PPI1871AL
30	VGL1871AL
30	OPW1871AL
30	J1871BL
30	PPI1871BL
30	PPR1871BL
30	VGL1871BL
30	OPW1871BL
30	VC750DL
30	ORFC645BL
30	FIC645L
30	ORFC645AL
30	VGL737BL
30	OPW737BL
30	JA501AL
30	JA501L
35	PWRPNL32P
35	BKRDPNL34P
37	SWRS3P
39	J740BD
39	OPW735AD
39	VGA735AD
39	J1867AD
39	J103XD
39	CON172152/RHR1I
39	BS17RHRP310P
39	RHRP31Z
39	J1866BD
39	OPWRHRP31D
39	SENOTSRHRP310P
39	SWMOA11KHRP31P
39	VC738AD
39	J104D
39	VGA739AD
39	OPW739AD
39	PPI739AD
39	JA14AL
39	JA14L
39	J830AL
39	JTIC627L
39	J627AL
39	J017AL
39	J602AL
39	J601AL
39	J601CL
39	J601DL
39	J1871CL
39	VGL736AL
39	OPW736AL
39	J736AL
39	PPR736AL
39	PSHXR1871DL
39	PPR750EL
39	J750EL
39	VGL1871DL
39	OPW1871DL
39	J1871DL
39	PPI1871DL
39	PPR1871DL
39	VGL1871CL
39	OPW1871CL
39	VC750EL
39	ORFC646BL
39	FIC646L
39	ORFC646AL
39	VGL737AL
39	OPW737AL
39	J627BL
44	PWRPNL33P
45	OPRSWMRHRP31CP
47	J838QB
47	J639B
47	J638B
48	J838RB
48	J641AB
48	J641B
48	J640B
49	J899AB
52	MOV899AB
52	MOV746B
52	J733AB
52	HCV640B
52	J889AB
57	J899BB
59	MOV899BB
59	MOV747B
59	J733BB
59	HCV638B
59	J889BB
67	J889D
69	J1869BD
83	VGA760AL
83	OPW760AL
84	J1805L
85	PPR1805L
87	J760AL
88	BRC760AJ760BL
95	BRC760CJ760BL
98	OPW760CL
98	VGA760CL
100	J760CL
102	JA57L
103	ORFC760CL
104	CCWP33L
108	JA55L
109	ORFC760AL
110	CCWP31L
111	ORFCCCW33L
112	VC761CL
113	JA3L
114	VGA762CL
114	OPW762CL
116	J763BL
116	VGA759BL
116	OPW759BL
116	JA8L
116	CCHXRS32Z
116	VGA765BL
116	OPW765BL
116	J764BL
118	J762CL
119	BRC762CJ762BL
128	BRC762AJ762BL
129	ORFCCCW31L
130	VC761AL
131	JA1L
132	VGA762AL
132	OPW762AL
133	J763AL
133	VGA759AL
133	OPW759AL
133	JA7L
133	CCHXRS31Z
133	JA10L
133	VGA765AL
133	OPW765AL
133	J764AL
133	PPI765AL
135	J762AL
142	J765BL
146	J765AL
227	RIVHUDSONK
260	CHNLDSK
260	CHNLDS3K
260	J95AK
260	J95BK
260	J95CK
260	J95DK
267	J95FK
267	J1096AK
525	PNLDIS34P
548	LG1OF2SIA2BH
548	RSI2H
549	RSI21XZ
600	SOURCE1P
690	BUS3AP
693	BUS6AP
718	UVBUS3AP
719	UVBUS6AP
* 910	LOCCP
* 914	LOCRP
915	LOCSP
942	BUS3A/P
949	BUS6A/P
1122	PWRPNL32/P
1130	BKRDPNL34/P
1131	PNLDIS34/P
1140	PWRPNL33/P
1168	CON913SI21XI
1171	RL3-16AI
1171	CON91327-6AX3I
1172	RL27-6AX1I
1172	CON3927-6AX1I
1173	RL27-6AX4I
1173	CON3927-6AX4I
1174	RL27-6AX3I
1180	RL27-3AX1I
1180	CON3527-3AX1I
1181	RL27-3AX4I
1181	CON3527-3AX4I
1184	RL27-3AX2I
1186	TRIPMASTER

* INDICATES LOCATION

2.4.2 Medium LOCA and Loss of High Pressure Injection

2.4.2.1 Introduction

Figure 2 shows that core melt could potentially result from a loss of High Pressure Injection during a given, but unspecified, medium (2"-6" pipe rupture) LOCA. In this system combination we have looked for singleton and doubleton failures that could cause failure of the High Pressure Injection system during a medium LOCA. The High Pressure Injection system has the following support systems: the Safety Injection Actuation system, the Electrical system, the Component Cooling system, and the Service Water system. Figure 2.9 shows the connectivity of these systems.

2.4.2.2. Failure Criteria of Individual Systems

High Pressure Injection
For the smaller range of medium LOCAs two out of three high head injection pumps may be required to deliver sufficient flow to the reactor coolant system. The charging pumps are not considered.

Support Systems
Electrical System
The electrical block and break models are included in this system combination in the same manner as all of the other combinations. Electrical systems are needed for Safety Injection Actuation, motor operated valve actuation, and for pump operation.

Component Cooling System
In this system combination, a Component Cooling System failure represents failure due to a pipe break. The assumption is made that, although the safety injection pumps do not need component cooling water circulated by the component cooling pumps, water must be available in the pipes to act as a heat sink and be circulated via the mini-pumps attached to the safety injection pump shafts. For this reason, a block in component cooling which keeps the component cooling pumps from functioning would not necessarily result in overheating of the SIPs.

Service Water System
The Service Water System is needed in this system combination for support of the diesel generators only. Since heat removal from the residual heat exchangers is not necessary for the component cooling system operation, the SWS is not needed.

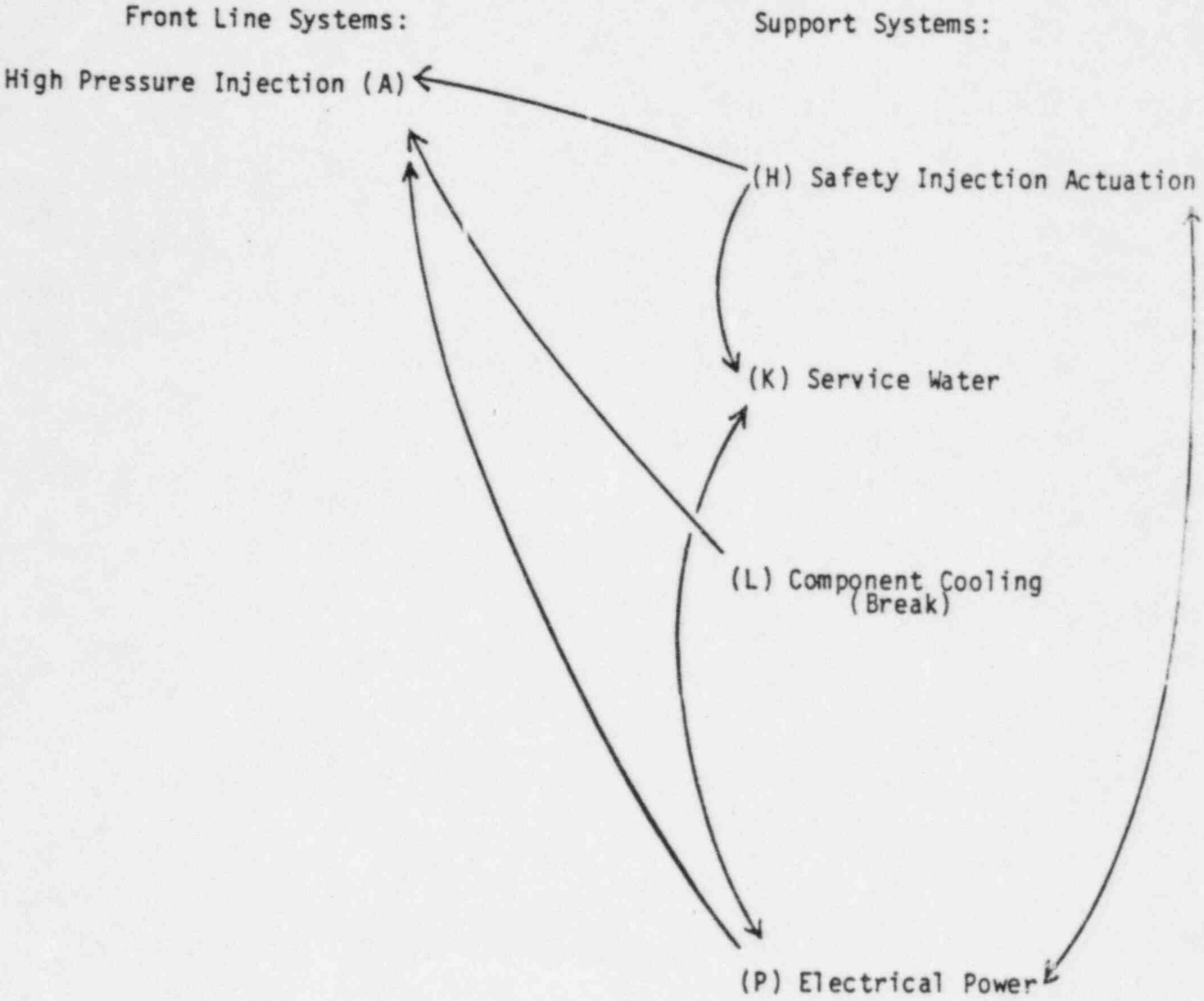
Safety Injection Actuation
The Safety Injection Actuation system is required in the automatic mode in order to start the Safety Injection System. (In the manual case there are redundant operators to initiate SI).

The digraphs for the above systems are located in Appendix B and the alpha input lists are in Appendix C.

Figure 2-9

SYSTEM COMBINATION #2

S1 LOCA with High Pressure Injection



2.4.2.3 Results for the Front-Line Systems Act Alone: Case I

All singleton variables contained in node number 328 relate to the RWST and the piping from it to the first junction where flow can go in one of two directions (see Enclosure 2, Case I). TTRWSTH20D is a node which represents filling of the RWST at some time prior to the accident. RWST1D represents the RWST in an available state. PPR846D is the pipe reducing element just outside the RWST. Immediately after the pipe reducing element is some heat tracing named HTRC846YD which preceeds the gate valve VGA846D. This valve is locked open. Following the valve is more heat tracing (HTRC846ZD) and a pipe increasing element (PPI846D). A vent is the next item in the flow path which connects to the pipe junction (J200D), followed by another junction (J290D) which leads to the charging pumps (see Figures B.1.1.A and B.1.2.A).

In addition to the above nodes, other singletons to the front-line system include J1810D (the junction which splits the piping between the SIPs and the RHRs), MOV1810D, VC847D, J203D (all in line to the header prior to the SIPs).

The next node in line to the SIPs is the junction (J203AD) which connects the input pipe to the header.

J1829D is a singleton in this system combination since 2 SIPs are needed for a medium LOCA. If there is a block at J1829D, flow can only get to SIP31 which is insufficient.

BRC852BJ852AA represents the low probability event of a double-ended pipe break on the output header of the SIPs. A break of this type would not be mitigatable without shutting down high pressure safety injection.

HPI-MLOCA is the terminal node for this system combination. This node represents the core and its need for cooling.

The front-line doubletons can be found by referring to the first block in the upper left hand corner of the doubleton matrix (see Enclosure 1.1).

Rows 38, 41, and 42 each represent one SIP and the pattern that depicts the fact that any two pumps are sufficient.

Looking next at Row #235 displays the redundancy of a two train system. Since the reactor is assumed to be scrammed at the start of the accident, the Boron Injection Tank (BIT) is not needed. For this reason, either the path without the BIT (condensed node number 235) or the BIT path which includes node numbers 173, 177, 241, 249, and 267 form doubletons.

The next group of interest involves a square including rows and columns number 286 through 322. This cluster of nodes again represents the three SIPs and the need for at least two of them functioning. These nodes are on the length of pipe from the pumps to the output header of the SIPs.

* Copies of the materials included in Enclosure 2 can be found at the end of this section

Row 334 is the junction from the SIP intake header to SIP31. This junction is a doubleton with any other node which keeps flow from either of the other two pumps.

2.4.2.4 Results for the Front-Line and Support Systems Acting Together: Case II

The singletons added due to support systems' failures include only those from the component cooling break model as well as an electrical model test node.

The nodes condensed into #371 (J830BL, J627BAL, J627BBL, J787L, VGL787, FIC634BL, JA59L, J749EL) are all on a direct line from the output of the secondary component cooling side of SIP32 and SIP33 to the component cooling pump intake header. A break in this line would drain the component cooling piping rendering it useless as a heat sink for the SIPs. Since the scenario includes a medium LOCA, the one intact pump SIP31 is not sufficient and would eventually be void of water also (assuming no mitigation). The two trains are designed so that they can be isolated in the event of a break in one train but this requires operation action.

The above description applies to all the piping leading to the safety injection pumps as well. These nodes include #430 (JA502L, J601BL, J602BL, J602CL, J765B1) and #441 (J602DL, J756CL, J749BL).

In addition to the above component cooling nodes, there are four break nodes which are included as worst case, double-ended pipe breaks on the input and output headers of the component cooling pumps as well as the output header of the component cooling heat exchangers. A break of this nature would not be mitigatable. These nodes are BRC760CJCJ760AL, BRC762CJCJ720AL, BRC765CJCJ765AL, and BRC760CJCJ760BL.

The last node (TESTELECP) is a test node in the electrical system which is included for checking results only. It represents failure of the entire electrical system.

Referring to the doubleton matrix in Enclosure 2, Case II, it is easy to see that the vast majority of doubletons revolve around the safety injection pumps and the associated piping with each pump. In order to see this, note the columns which contain the SIP nodes (38, 41, 42, and 272 through 322). Following these columns down through the support systems yields nearly all of the doubletons.

The matrix blocks have been labeled with letters "A" through "U".

The doubletons located in the blocks on the diagonals ("A", "C", "F", "J", "U") represent doubletons within a system. For instance, a star in the second block "C" on the diagonal would indicate two failures required within the component cooling break model.

Block "A" is discussed in this section as front-line system alone.

The doubletons in block "B" represent a break in one train of the component cooling system along with the failure of a component which takes out one of the pumps that is on the other component cooling train.

Since the service water system is not required for component cooling heat removal, no doubletons are located in blocks "D" or "E". Also, there are no doubletons in block "F" means that there are no two failures within the SWS which could result in failure of the diesel generators to lead to core melt.

Block "G" doubletons arise because of failures in a relay that disables safety injection actuation to one pump along with another failure in the safety injection piping which yields another pump failure.

Doubletons which arise because of failures in safety injection actuation relays (the same as block "G") and breaks in component cooling which result in failure of another SIP can be found in block "H".

Failures in safety injection actuation result from loss of a dc distribution panel (PNLDIS31 or PNLDIS34) which is responsible for providing the source of power necessary to energize the logic relay (RSI1 and RSI2).

Block "I" has no doubletons for the same reason discussed above for blocks "D" and "E".

Block "J" doubletons result from the above two distribution panels failing or the above two logic relays failing together, resulting in the failure of safety injection actuation. Either of these yields simultaneous loss of both SIAS channels.

The next block ("K") as well as block "L" include doubletons due to loss of power to the SIPs. These failures result in two out of three pump failures in the same way that the safety injection actuation blocks were described. The difference is in the way the pumps fail (not actuated vs. no electrical power).

Block "M" is the only block which contains joint contributions which include the Service Water system. If the Service Water system fails to cool the diesel engines, then the emergency generators will fail. The doubletons result from loss of offsite power and simultaneous loss of the diesel generators.

Block "N" involves the doubletons resulting from failures in one channel of SIAS and the electrical system failing in such a mode that takes out the other channel.

THe SICON blocks represent failures in the connections from the safety injection actuation system to the equipment vital to the SIPs. These connections represent failure of the contacts or failure to propagate the SI signal from the above referenced relays. The same equipment referred to in block "G" and "H" is responsible for the other half of the doubleton pair in blocks "P" and "Q" respectively.

Block "R" is empty because of the same reasons for the Service Water system discussed above.

Block "S" shows doubleton pairs with connections from SICON combining with the opposite logic relay in SIAS.

The doubletons in block "T" are similar to the ones in block "N" except that the failures are represented by the connections rather than the relays themselves.

Block "U" is simply the connections from one channel in SICON with the connections from the other channel.

2.4.2.5 Front-Line Support Systems and Location Vulnerabilities: Case III

The addition of location considerations adds six new nodes to the singleton list. THese six nodes represent four different locations in the plant.

LFSIPD, LWSIPD, LSSIPD represent fire, flood, steam vulnerabilities (respectively) in the Safety Injection Pump Room. This room contains all three SIPs as well as much of the piping and valves related to SIP functions.

LOCDP is the Control Building at 15 feet elevation. This location is common to buses 2, 3, 5 and 6 which, if failed, would result in the loss of all three SIPs.

The Control Building is also covered by LOCRP (33 feet elevation). This is the cable-spreading area. PWRPNL #31, 32, and 34 are all affected by this location, which will also cause the SIPs to fail.

LOCSP is the location of the Control Room. This location is a singleton because the dc distribution panels are located there, and they are needed to close the starting circuit relays to the pumps.

Location doubleton contributions because of the Boron Injection Tank room add five more rows of doubletons. These rows contain only the single node #235 which represents the path to the core which bypass the BIT. If something should block this path and a problem occurs in the BIT room, it is possible to lose both paths to the core.

LFBIT, LWBIT, and LSBIT represent fire, flood and steam problems in the BIT room. LF1835, and LS1835 represent fire and steam problems in the room with valves 1835A and B. There is a direct connection on the floor back to the BIT room which means that both rooms are susceptible to the same flooding conditions.

LOCAP and LOCCP are locations which act in the same manner. The locations are responsible for the failure of the station aux transformer which is the backup offsite supply of power. The Service Water system provides cooling to the diesel generators which are the onsite supply of power. These are redundant sources.

LOCHP is the name of the common location for Motor Control Centers 36A and 36B. MCC36A and 36B provide redundant power to all of the valves in the Safety Injection system. Loss of both trains as well as a loss of the path which bypasses the BIT would result in core melt since flow could not pass through the BIT because the isolation valves would be closed.

2.4.2.6 Front-Line, Support Systems, Location Vulnerabilities, and Operation Action: Case IV

Operator action usually means that redundancy is introduced because of alternate paths and component actuation as a result of the operator acting as backup. Therefore, the number of singletons is normally reduced. However, allowing the operator to act means allowing him to have incorrect action as well as correct action. This introduces OPWs (operator doing the wrong thing) into the singleton list (see Enclosure 2, Case IV).

In system combination 2, the singletons which were removed due to operator redundancy fell into two groups. The first group included J1829D, J203AD, J203D, VC847D, and MOV1810D. These nodes are no longer singletons because flow can be routed through VGA898 or, if necessary, through the RHR pumps and back through MOV888A and B to the SIPs.

The second group eliminated a location (LOCSP) which depicts the Control Room. The distribution panels are located there and are needed to close the starting circuit relays to the SIPs. In this case, the operator can close these relays manually providing redundant operation.

There are two added OPW singletons which include the closing of valve VGA846D. This valve is the gate valve on the pipe from the RWST and is locked open.

The second OPW is located in the component cooling break model. This OPW (OPW787) represents the extremely low probability event of an operator facilitating a break in this system. This particular break is located on the return line from the SIPs (on the train which contains two SIPs).

Since there are now three paths to the SIPs, the singletons in the automatic case (MOV1810, VC847, and J203) are now reduced to tripletons.

An operator action that hinders rather than helps the system results from the fact that an operator can turn the SIPs off using switch 6 (SWRS6P) from the change over to recirculation phase if the SIAS is not present. These doubletons are shown on block "G". The SIAS could be terminated because of hardware error or an operator could turn it off.

The blocks representing SICON are basically unchanged from case 3 since an operator is not redundant to any of this hardware. The doubletons represent the failure of connection from safety injection actuation affecting one pump with the failure of another pump or its associated hardware.

The doubleton matrix has been reduced substantially due to increased redundancy in all blocks except the component cooling break model and the electrical system. This is because there are no alternate ways for an operator to reroute flow in the CCS or the EPS. In addition, there is no operator mitigation action modeled in the CCS Break model.

The major change in the doubleton matrix involves the addition of two alternate methods of getting RWST water to the SIPs. The first method utilizes VGA898 - a valve at the junction just past the junction to MOV1810. An operator can pen this valve and allow the delivery of water to the SIPs in the event that the normal path is blocked.

The other path which bypasses both MOV1810 and VGA898 involves routing flow from the RWST to the RHR pumps, to the residual heat exchangers, and back to the SIPs via MOV888A and B. (An operator must open these valves.)

Summary

There were no safety violations found in this system combination.

Since the combinations chosen for injection assume that the reactor is scrammed, there is no requirement for Boron Injection. This yields a high pressure safety injection system which is much more redundant and robust than an accident sequence involving the need for Boron would provide. This is the reason that the valves which isolate the Boron Injection Tank are not more visible as cutsets than they are. The path which bypasses the BIT provides all that is necessary to supply the core with sufficient coolant in these system combinations.

ENCLOSURE 2

SYSTEM COMBINATION 2

MEDIUM LOCA WITH HIGH PRESSURE INJECTION

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

SINGLETONS

271	BRC852BJ852AA
317	J1829D
324	J203AD
327	J1810D
328	J290AD
328	J200D
328	PPI846D
328	MOV1810D
328	VC847D
328	HTRC846ZD
328	VGA846D
328	HTRC846YD
328	PPR846D
328	RWST1D
329	TTRWSTH20D

```
FILE IDENTIFICATION
  REACH PAIR:   I=    1     J=   43
  DATE:  6/12/84
  ANSWER.POS FILE IS: DR1:[220,1]SC2607MC3.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC2607MOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC2607MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC2607MRT.DAT
  SIGMA PI FILE NAME IS: DR1:SC2607MSI.C3
```

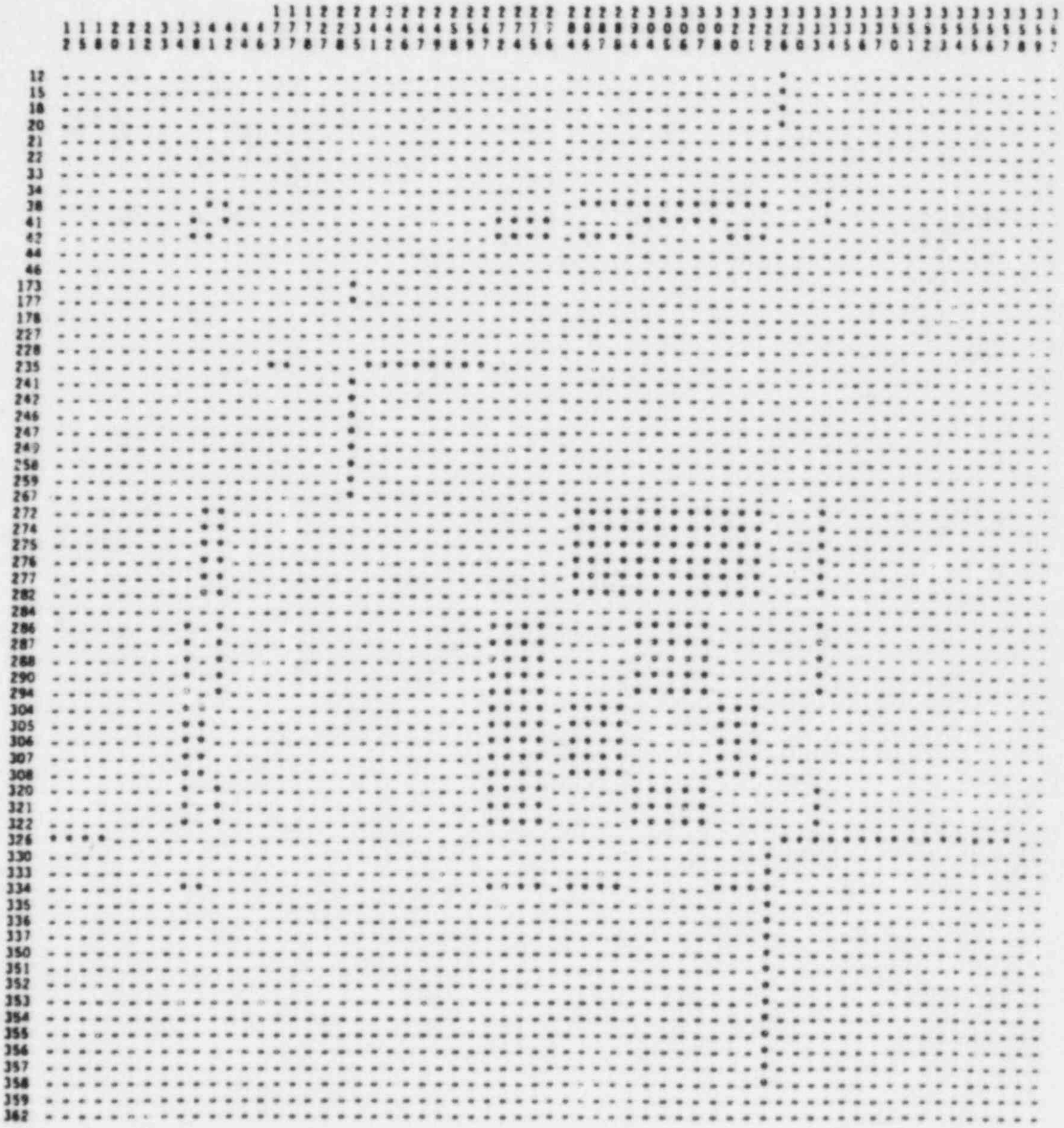
ENCLOSURE 2

SYSTEM COMBINATION 2

MEDIUM LOCA WITH HIGH PRESSURE INJECTION

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

DOUBLETONS



MEDIUM LOCA WITH HIGH PRESSURE INJECTION

CASE I (CONTINUED)

VARIABLE LIST FOR SC2 CASE I DOUBLETON MATRIX

12	PPR1810D
15	J735BD
15	J1863D
15	MOV882D
15	VC881D
15	PPI735D
15	J735AD
18	J888AD
18	J133D
18	J1869AD
18	J115D
18	J114D
20	J111XD
20	JRHRD
20	J740AD
20	J636D
20	J883D
20	MOV744D
20	VC741D
20	J110XD
21	VC857AA
21	J857GA
21	VC857GA
21	J856AA
21	MOV856AA
21	FE926A
22	J857AB
22	PATH897AD
22	VC897AB
22	J112BB
33	VC857UA
33	J857WA
33	VC857WA
33	J856KA
33	MOV856KA
33	FE982A
33	PPR982A
34	J857UB
34	PATH897DD
34	VC897DB
34	J139B
38	SIP33Z
38	ORFCR33A
38	VGA848BA
38	J1819CA
38	J947A
38	PPR947A
41	SIP32Z
41	ORFCR32A
41	J1819BA
42	SIP31Z
42	ORFCR31A
42	VGA848AA
44	CLL4BR1D
46	CLL1BR1D
173	J926AA
177	J983A
177	J858BA
177	J117A
177	J117BA
177	HTRC117A
177	J117AA

178	J982A
227	J980A
228	J926BA
235	J981A
235	J858AA
235	J1837A
235	J116A
235	J853AA
235	J852AA
235	J853CA
235	ORFC853A
241	J1835BA
241	J1821A
241	HTRC1821A
241	J1823AA
241	J1842A
241	PPR1842A
241	BIT1A
241	J1843A
241	J1847A
241	J1848A
241	HTRC1822A
241	J1822A
241	HTRC1848AA
241	HTRC1848BA
241	HTRC106A
241	J106AA
241	J106BA
* 242	LF1835A
* 246	LWBITA
* 247	LS1835A
249	J1844A
249	ORFC916AA
249	FI916A
249	ORFC916BA
249	J916A
249	HTRC916A
249	VC1849A
249	VGL1846A
249	J1846A
* 258	LFBITA
* 259	LSBITA
267	J1852BA
267	J103A
267	J853BA
267	J852BA
272	PPI1850BA
274	MOV1902BA
275	MOV1901BA
276	VC849BA
277	JSIP33A
286	J851BA
287	J851AA
288	JSIP32A
304	PPI1850AA
305	MOV1902AA
306	MOV1901AA
307	VC849AA
308	JSIP31A
320	J887AD
321	MOV887AD
322	MOV887BD
326	J203D
326	VC847D
326	MOV1810D
330	J898D

333	PP203D
334	J1819AD
335	LFRHRD
* 336	LSRHRD
* 337	LWRHRD
* 350	LF888D
* 351	LS888D
* 352	LW888D
* 353	LFRECD
* 354	LSRECD
* 355	LWRECD
356	BRC745AJ745BD
357	BRC889J1869BD
358	J745BD
359	J897AD
362	J897DD
406	CCHXRS32Z
423	CCHXRS31Z
442	BWCL54AZ
445	BWCL54BZ
447	SIPC31Z
449	OCLSIP31Z
453	BWCL55AZ
456	BWCL55BZ
458	SIPC32Z
460	OCLSIP32Z
466	BWCL56AZ
469	BWCL56BZ
471	SIPC33Z
473	OCLSIP33Z
869	RSI11XZ
879	RSI21XZ

* INDICATES LOCATION

ENCLOSURE 2

SYSTEM COMBINATION 2

MEDIUM LOCA WITH HIGH PRESSURE INJECTION

CASE II FULLY AUTOMATIC FRONT-LINE AND SUPPORT SYSTEMS

CASE III FULLY AUTOMATIC FRONT-LINE, SUPPORT SYSTEMS, AND LOCATIONS

SINGLETONS

```
*   37      LFSIPD
*   39      LWSIPD
*   40      LSSIPD
    43      HPI-MLOCAD
   271      BRC852BJ852AA
   317      J1829D
   324      J203AD
   327      J1810D
   328      J290AD
   328      J200D
   328      PPI846D
   328      HTRC846ZD
   328      VGA846D
   328      HTRC846YD
   328      PPR846D
   328      RWST1D

   371      J830BL
   371      J627BAL
   371      J627BBL
   371      J627BCL
   378      BRC760CJ760AL
   384      BRC760CJ760BL
   389      J760CL
   391      PPR627BCL
   391      J787L
   391      VGL787L
   391      FIC634BL
   391      JA59L
   391      J749EL
   410      BRC762CJ762AL
   430      JA502L
   430      J017BL
   430      J601BL
   430      J602BL
   430      J602CL
   433      J765BL
   434      BRC765BJ765AL
   441      J602DL
   441      J756CL
   441      J749BL
* 1241      LOCDP
* 1244      LOCRP
* 1245      LOCSP
  1489      TESTELECP

                        * INDICATES LOCATION

    FILE IDENTIFICATION:
      REACH PAIR:   I=    1    J=   43
      DATE:  6/12/84
      ANSWER.POS FILE IS: DR1:[220,1]SC2607MC3.POS
      OUTPUT.DAT FILE IS: DR1:[220,1]SC2607MOT.TRP
      VARIAB.DAT FILE IS: DR1:[220,1]SC2607MVB.DAT
      RENUMSRT.DAT FILE IS: DR1:[220,1]SC2607MRT.DAT
      SIGMA PI FILE NAME IS: DR1:SC2607MSI.C3
```

MEDIUM LOCA WITH HIGH PRESSURE INJECTION

COMBINED CASE II & CASE III (CONTINUED)

DOUBLETONS

MATRIX TOO LARGE TO INCLUDE - SEE VOLUME I-B - ENCLOSURES

MEDIUM LOCA WITH HIGH PRESSURE INJECTION

CASE II & III (CONTINUED)

VARIABLE LIST FOR SC2 CASE II & III DOUBLETON MATRIX

12	PPR1810D
15	J735BD
15	J1863D
15	MOV882D
15	VC881D
15	PP1735D
15	J735AD
18	J888AD
18	J133D
18	J1869AD
18	J115D
18	J114D
20	J111XD
20	JRHRD
20	J740AD
20	J636D
20	J883D
20	MOV744D
20	VC741D
20	J110XD
21	VC857AA
21	J857GA
21	VC857GA
21	J856AA
21	MOV856AA
21	FE926A
22	J857AB
22	PATH897AD
22	VC897AB
22	J112BB
33	VC857UA
33	J857WA
33	VC857WA
33	J856KA
33	MOV856KA
33	FE982A
33	PPR982A
34	J857UB
34	PATH897DD
34	VC897DB
34	J139B
38	SIP33Z
38	CON192352/SI3I
38	BS14SIP330P
38	SENOTSSIP330P
38	SWMOA11SIP33P
38	ORFCR33A
38	VGA848BA
38	J1819CA
38	J947A
38	PPR947A
41	SIP32Z
41	CON182252/SI2I
41	BS14SIP320P
41	SENOTSSIP320P
41	SWMOA11SIP32P
41	ORFCR32A
41	J1819BA
42	SIP31Z
42	CON182252/SI1I
42	BS14SIP310P
42	SENOTSSIP310P
42	SWMOA11SIP31P
42	ORFCR31A
42	VGA848AA
44	CLL4BR1D
46	CLL1BR1D
173	J926AA
177	J983A
177	J858BA
177	J117A
177	J117BA
177	HTRC117A
177	J117AA
178	J982A
227	J980A
228	J926BA
235	J981A
235	J858AA
235	J1837A
235	J116A
235	J853AA
235	J852AA
235	J853CA
235	ORFC853A
241	J1835BA
241	J1821A
241	HTRC1821A
241	J1823AA
241	J1842A
241	PPR1842A
241	BIT1A
241	J1843A
241	J1847A
241	J1848A
241	HTRC1822A
241	J1822A
241	HTRC1848AA
241	HTRC1848BA
241	HTRC106A
241	J106AA
241	J106BA
* 242	LF1835A
* 246	LWBITA
* 247	LS1835A
249	J1844A
249	ORFC916AA
249	FI916A
249	ORFC916BA
249	J916A
249	HTRC916A
249	VC1849A
249	VGL1846A
249	J1846A
* 258	LFBITA
* 259	LSBITA
267	J1852BA
267	J103A
267	J853BA
267	J852BA
272	PP1850BA
274	MOV1902BA
275	MOV1901BA
276	VC849BA
277	JSIP33A
278	CON4852/SI3I
278	CON2SIP330P
282	PWRPNL32P
282	BKRDPNL34P
284	SWRS6P
286	J851BA
287	J851AA
288	JSIP32A
290	CON2652/SI2I
290	CON2SIP320P
294	PWRPNL33P
304	PP1850AA
305	MOV1902AA
306	MOV1901AA
307	VC849AA
308	JSIP31A
309	CON3752/SI1I
309	RL3-15AI
309	CON91327-5AX2I
310	CON2SIP310P
314	PWRPNL31P
320	J887AD
321	MOV887AD
322	MOV887BD
326	J203D
326	VC847D
326	MOV1810D
330	J898D
333	PP203D
334	J1819AD
* 335	LFRHRD
* 336	LSRHRD
* 337	LWRHRD
* 350	LF888D
* 351	LS888D
* 352	LW888D
* 353	LFRECD
* 354	LSRECD
* 355	LWRECD
356	BRC745AJ745BD
357	BRC889J1869BD
358	J745BD
359	J897AD
362	J897DD
369	JA14AL
369	JA14L
369	J830AL
369	JTIC627L
369	J627AL
370	PPR627AL
370	J749DL
370	J750AAL
370	VGL749DL
370	FIC634AL
370	JA58L
370	VC750AL
372	VGA760AL
373	J1805L
374	PPR1805L
376	J760AL
377	BRC760AJ750BL
382	J760BL
387	VGA760CL
388	PPR760CL
390	VGA766BL
392	JA57L
393	ORFC760CL
394	CCWP33L
398	JA55L
399	ORFC760AL

* INDICATES LOCATION

MEDIUM LOCA WITH HIGH PRESSURE INJECTION

CASE II & III (CONTINUED)

VARIABLE LIST FOR SC2 CASE II & III DOUBLETON MATRIX

400	CCWP31L
401	ORFCCCW33L
402	VC761CL
403	JA3L
404	VGA762CL
406	J763BL
406	VGA759BL
406	JA8L
406	CCHXRS32Z
406	VGA765BL
406	J764BL
408	J762CL
409	BRC762CJ762BL
418	BRC762AJ762BL
419	ORFCCCW31L
420	VC761AL
421	JA1L
422	VGA762AL
423	J763AL
423	VGA759AL
423	JA7L
423	CCHXRS31Z
423	JA10L
423	VGA765AL
423	J764AL
423	PPI765AL
425	J762AL
435	PPR765BL
436	VGA766DL
437	J017AL
437	J602AL
437	J601AL
437	J601CL
437	J601DL
438	J765AL
439	VGA766CL
440	J601EL
440	J749AL
440	VGL749AL
440	PMP54L
440	J54AL
442	BWCL54AZ
443	J750ADL
444	J54BL
445	BWCL54BZ
446	J54CL
447	SIPC31Z
448	J54DL
449	OCLSIP31Z
450	J750ACL
451	J750ABL
452	VGL749BL
452	PMP55L
452	J55AL
453	BWCL55AZ
454	J750BDL
455	J55BL
456	BWCL55BZ
457	J55CL
458	SIPC32Z
459	J55DL
460	OCLSIP32Z
461	J750BCL
462	J750BBL
463	J750BAL
463	VGL749EL
463	VC750BL
464	PPR749FL
464	VGL749FL
464	VC750CL
464	J750CAL
465	PPR749CL
465	VGL749CL
465	PMP56L
465	J56AL
466	BWCL56AZ
467	J750CDL
468	J56BL
469	BWCL56BZ
470	J56CL
471	SIPC33Z
472	J56DL
473	OCLSIP33Z
474	J750CCL
475	J750CBL
541	J1190K
541	J98AK
541	J1093BK
541	J1093AK
541	J1093DK
541	VB30K
541	J1095K
542	VC98K
542	HTRC409K
542	J4K
542	J106BK
542	J409K
542	J1221K
542	HTRC98K
542	VB98K
556	RIVHUDSONK
557	STRCTRINTKK
563	SWPWELL1K
565	TRASH1K
567	J131K
571	J133K
572	J132BK
589	CHNLDSK
589	CHNLDS3K
589	J95AK
589	J95BK
589	J95CK
589	J95DK
596	J95FK
596	J1096AK
599	J1096BK
604	J1094K
618	COL-RW-2K
619	SW123456P
842	PNLDIS31P
842	BKRDPNL31P
853	PNLDIS34P
861	LG2OF2SIA2AH
867	LG1OF2SIA2AH
868	RSI1H
869	RSI11XZ
874	LG2OF2SIA2BH
877	LG1OF2SIA2BH
878	RSI2H
879	RSI21XZ
888	STAUXXFMRP
930	SOURCEIP
1009	BUS5AP
1014	BUS2AP
1023	BUS6AP
1046	UVBUS5AP
1047	UVBUS2AP
1049	UVBUS6AP
1058	ITLBKR2AT5AP
* 1239	LOCAP
* 1240	LOCCP
* 1242	LOCHP
1252	BUS5A/P
1262	BUS2A/P
1279	BUS6A/P
1434	PWRPNL31/P
1439	BKRDPNL31/P
1440	PNLDIS31/P
1452	PWRPNL32/P
1460	BKRDPNL34/P
1461	PNLDIS34/P
1470	PWRPNL33/P
1490	CON913SI11XI
1491	CON2024SI11XI
1493	RLSI5A1I
1494	RL27-5AX1I
1494	CON3527-5AX1I
1495	RL27-5AX4I
1495	CON3527-5AX4I
1496	RL27-5AX2I
1497	RL27-5AX3I
1499	CON913SI21XI
1500	CON2024SI21XI
1502	RL3-16AI
1502	CON91327-6AX2I
1503	RL27-6AX1I
1503	CON3927-6AX1I
1504	RL27-6AX4I
1504	CON3927-6AX4I
1505	RL27-6AX2I
1508	RL3-12AI
1508	CON2627-2AX3I
1512	RL27-2AX1I
1512	CON3527-2AX1I
1513	RL27-2AX4I
1513	CON3527-2AX4I
1516	RL27-2AX2I
1517	RL27-2AX3I

* INDICATES LOCATION

```
FILE IDENTIFICATION:
  REACH PAIR:   I=    1    J=   43
  DATE:  6/12/84
  ANSWER.POS FILE IS: DR1:[220,1]SC2607M:3.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC2607M:T.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC2607M:B.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC26C'MRT.DAT
  SIGMA PI FILE NAME IS: DR1:SC2607MSI.C3
```

ENCLOSURE 2

SYSTEM COMBINATION 2

MEDIUM LOCA WITH HIGH PRESSURE INJECTION

CASE IVA & IVB - MANUALLY ASSISTED

CASE IVA - MANUALLY ASSISTED, FAILURE BY OMISSION

CASE IVB - MANUALLY ASSISTED, FAILURE BY OMISSION AND FAILURE BY COMMISSION

SINGLETONS

```
 *   37      LFSIPD
 *   39      LWSIPD
 *   40      LSSIPD
     43      HPI-MLOCAD
    271      BRC852BJ852AA
    327      J1810D
    328      J290AD
    328      J200D
    328      PPI846D
    328      HTRC846ZD
    328      OPW846D
    328      VGA846D
    328      HTRC846YD
    328      PPR846D
    328      RWST1D

    371      J830BL
    371      J627BAL
    371      J627BBL
    371      J627BCL
    378      BRC760CJ760AL
    384      BRC760CJ760BL
    389      J760CL
    391      PPR627BCL
    391      J787L
    391      VGL787L
    391      OPW787L
    391      FIC634BL
    391      JA59L
    391      J749EL
    410      BRC762CJ762AL
    430      JA502L
    430      J017BL
    430      J601BL
    430      J602BL
    430      J602CL
    433      J765BL
    434      BRC765BJ765AL
    441      J602DL
    441      J756CL
    441      J749BL
 * 1241      LOCDP
 * 1244      LOCRP
   1489      TESTELECP

                               * INDICATES LOCATION
      FILE IDENTIFICATION:
        REACH PAIR:   I=    1    J=   43
        DATE:  6/13/84
        ANSWER.POS FILE IS: DR1:[220,1]SC2607MC4.POS
        OUTPUT.DAT FILE IS: DR1:[220,1]SC2607MOT.DAT
        VARIAB.DAT FILE IS: DR1:[220,1]SC2607MVB.DAT
        RENUMSRT.DAT FILE IS: DR1:[220,1]SC2607MRT.DAT
        SIGMA PI FILE NAME IS: DR1:SC2607MSI.C4
```

MEDIUM LOCA WITH HIGH PRESSURE INJECTION

CASE IVA & IVB

VARIABLE LIST FOR SC2 CASE IVA & IVB DOUBLETON MATRIX

12	PPR1810D
38	SIP33Z
38	CON192352/SI3I
38	BS14SIP330P
38	OPWSIP33A
38	SENOTSSIP330P
38	SWMOA11SIP33P
38	ORFCR33A
38	VGA848BA
38	OPW848BA
38	J1819CA
38	J947A
38	PPR947A
41	SIP32Z
41	CON182252/SI2I
41	BS14SIP320P
41	SENOTSSIP320P
41	SWMOA11SIP32P
41	ORFCR32A
41	J1819BA
42	SIP31Z
42	CON182252/SI1I
42	BS14SIP310P
42	OPWSIP31A
42	SENOTSSIP310P
42	SWMOA11SIP31P
42	ORFCR31A
42	VGA848AA
42	OPW848AA
173	J926AA
177	J983A
177	J858BA
177	J117A
177	J117BA
177	HTRC117A
177	J117AA
235	J981A
235	J858AA
235	J1837A
235	J116A
235	J853AA
235	J852AA
235	J853CA
235	ORFC853A
241	J1835BA
241	J1821A
241	HTRC1821A
241	J1823AA
241	J1842A
241	PPR1842A
241	BIT1A
241	J1843A
241	J1847A
241	J1848A
241	HTRC1822A
241	J1822A
241	HTRC1848AA
241	HTRC1848BA
241	HTRC106A
241	J106AA
241	J106BA
* 242	LF1835A

* INDICATES LOCATION

* 246	LWBITA
* 247	LS1835A
267	J1852BA
267	J103A
267	J853BA
267	J852BA
272	PPI1850BA
274	OPW1902BA
274	MOV1902BA
275	MOV1901BA
275	OPW1901BA
276	VC849BA
277	JSIP33A
282	PWRPNL32P
282	RKRDPNL34P
284	SWRS6P
286	J851BA
287	J851AA
288	JSIP32A
294	PWRPNL33P
304	PPI1850AA
305	OPW1902AA
305	MOV1902AA
306	MOV1901AA
306	OPW1901AA
307	VC849AA
308	JSIP31A
314	PWRPNL31P
317	J1829D
320	J887AD
324	J203AD
326	J203D
326	VC847D
326	MOV1810D
326	OPW1810D
330	J898D
331	OPRA898D
331	VGA898D
331	OPW898D
332	J204D
334	J1819AD
369	JA14AL
369	JA14L
369	J830AL
369	JTIC627L
369	J627AL
370	PPR627AL
370	J749DL
370	J750AAL
370	VGL749DL
370	OPW749DL
370	FIC634AL
370	JA58L
370	VC750AL.
372	VGA760AL
372	OPW760AL
373	J1805L
374	PPR1805L
376	J760AL
377	BRC760AJ760BL
382	J760BL
387	OPW760CL
387	VGA760CL
388	PPR760CL
390	VGA766BL
390	OPW766BL

392	JA57L
393	ORFC760CL
394	CCWP33L
398	JA55L
399	ORFC760AL
400	CCWP31L
401	ORFCCCW33L
402	VC761CL
403	JA3L
404	VGA762CL
404	OPW762CL
406	J763BL
406	VGA759BL
406	OPW759BL
406	JA8L
406	CCHXRS32Z
406	VGA765BL
406	OPW765BL
406	J764BL
408	J762CL
409	BRC762CJ762BL
418	BRC762AJ762BL
419	ORFCCCW31L
420	VC761AL
421	JA1L
422	VGA762AL
422	OPW762AL
423	J763AL
423	VGA759AL
423	OPW759AL
423	JA7L
423	CCHXRS31Z
423	JA10L
423	VGA765AL
423	OPW765AL
423	J764AL
423	PPI765AL
425	J762AL
435	PPR765BL
436	VGA766DL
436	OPW766DL
437	J017AL
437	J602AL
437	J601AL
437	J601CL
437	J601DL
438	J765AL
439	VGA766CL
439	OPW766CL
440	J601EL
440	J749AL
440	VGL749AL
440	OPW749AL
440	PMP54L
440	J54AL
442	BWCL54AZ
443	J750ADL
444	J54BL
445	BWCL54BZ
446	J54CL
447	SIPC31Z
448	J54DL
449	OCLSIP31Z
450	J750ACL
451	J750ABL
452	VGL749BL

MEDIUM LOCA WITH HIGH PRESSURE INJECTION

CASE IVA & IVB

VARIABLE LIST FOR SC2 CASE IVA & IVB DOUBLETON MATRIX

	452	OPW749BL
	452	PMP55L
	452	J55AL
	453	BWCL55AZ
	454	J750BDL
	455	J55BL
	456	BWCL55BZ
	457	J55CL
	458	SIPC32Z
	459	J55DL
	460	OCLSIP32Z
	461	J750BCL
	462	J750BBL
	463	J750BAL
	463	VGL749EL
	463	OPW749EL
	463	VC750BL
	464	PPR749FL
	464	VGL749FL
	464	OPW749FL
	464	VC750CL
	464	J750CAL
	465	PPR749CL
	465	VGL749CL
	465	OPW749CL
	465	PMP56L
	465	J56AL
	466	BWCL56AZ
	467	J750CDL
	468	J56BL
	469	BWCL56BZ
	470	J56CL
	471	SIPC33Z
	472	J56DL
	473	OCLSIP33Z
	474	J750CCL
	475	J750CBL
	556	RIVHUDSONK
	589	CHNLDSK
	589	CHNLDS3K
	589	J95AK
	589	J95BK
	589	J95CK
	589	J95DK
	596	J95FK
	596	J1096AK
	599	J1096BK
	842	PNLDIS31P
	842	BKRDPNL31P
	867	LG1OF2SIA2AH
	868	RSI1H
	869	RSI11XZ
	930	SOURCE1P
	1009	BUS5AP
	1014	BUS2AP
	1023	BUS6AP
	1046	UVBUS5AP
	1047	UVBUS2AP
	1049	UVBUS6AP
*	1240	LOCCP
*	1245	LOCSP
	1252	BUS5A/P
	1262	BUS2A/P
	1279	BUS6A/P
	1434	PWRPNL31/P
	1439	BKRDPNL31/P
	1440	PNLDIS31/P
	1452	PWRPNL32/P
	1460	BKRDPNL34/P
	1470	PWRPNL33/P
	1490	CON913SI11XI
	1493	RLSISA1I
	1494	RL27-5AX1I
	1494	CON3527-5AX1I
	1495	RL27-5AX4I
	1495	CON3527-5AX4I
	1497	RL27-5AX3I
	1503	RL27-6AX1I
	1503	CON3927-6AX1I
	1504	RL27-6AX4I
	1504	CON3527-6AX4I
	1505	RL27-6AX2I
	1512	RL27-2AX1I
	1512	CON3527-2AX1I
	1513	RL27-2AX4I
	1513	CON3527-2AX4I
	1516	RL27-2AX2I
	1521	TRIPMASTER

* INDICATES LOCATION

MATRIX TOO LARGE TO INCLUDE
SEE VOLUME 1-B - ENCLOSURES

2.4.3 PORV LOCA and Loss of High Pressure Injection

2.4.3.1 Introduction

Figure 2-10 illustrates how a core melt could occur if the High Pressure Injection system should fail during a specific small LOCA (PORV open). In this system combination, we seek Singleton and Doubleton failures that will simultaneously fail the HPI system and prevent the closure (or isolation) of a PORV (which has been opened due to a transient). Safety Injection Actuation, Electrical, Component Cooling, Instrument Air, Nitrogen Control, and Service Water, collectively support the Pressure Operated Relief Valves and the HPI. Figure 2-10 describes the connectivity of those various systems into one global model.

2.4.3.2 Failure Criteria of Individual Systems

High Pressure Injection System

For a small LOCA, one out of three high head injection pumps is required to deliver sufficient flow to the reactor coolant systems. The charging pumps are not considered.

PORV

All PORV and safety relief valves must be able to close or be isolated.

Support Systems

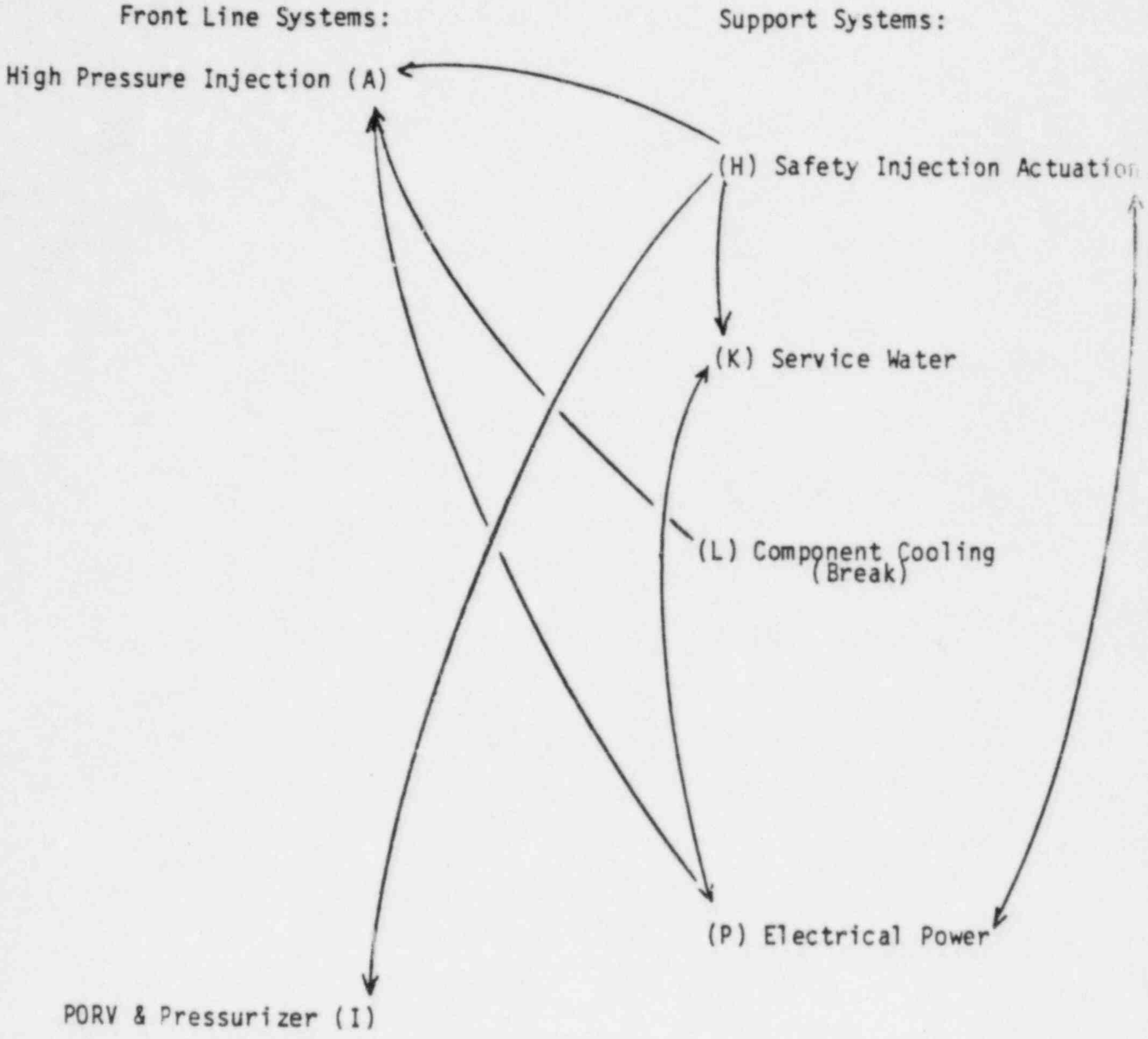
The support systems in System Combination 3 are identical to those in System Combination 2 and System Combination 4.

The digraphs for these systems can be found in Appendix B and the input lists are in Appendix C.

Figure 2-10

SYSTEM COMBINATION # 3

PORV Induced S2 LOCA with High Pressure Injection



2.4.3.3 Results for Front-Line Alone: Case I

We identified no singletons in this system combination. The PORV model shared no common vulnerability with the injection system. This means that the singletons for each Frontline system model acting alone will become doubletons with each other to the systems acting together (see Enclosure 3, Case I).

In the PORV model there are 3 groups which are doubletons with everything else. These are the three safety valves (PCV464, 466, 468) and their associated stems and springs, and each PORV (PCV455C, and PCV456). Failure of any of these along with the failure of the RWST and its piping to the first header (node numbers 327, 328, and 329) or the output header of the SIPs (270) would lead to core melt.

2.4.3.4 Front-Line with Support Systems and Location: Cases II and III

There were no singletons (see Enclosure 3, Cases II and III).

In addition to the HPI doubletons listed for Case I, CCS break and EPS systems contribute components to act with the PORV model valves to cause core melt. These nodes include three header breaks in Component Cooling (the same three as in System Combination 2) and two electrical locations (LOCDP and LOCSP). Descriptions of these nodes can be found in System Combination 2, Case 3 results.

The TESTELEC node is test node in the electrical systems and is used for processing checks only.

2.4.3.5 Front-Line with Support Systems, Location Vulnerability, and Operation Action: Case IV

The only redundancy provided by the operators is the ability to close the block valves. (The block valves isolate to the PORVs.) This means that the rows of doubletons attributed to the inability to close the PORVs are now removed except for the doubleton which includes LOCDP. This location can simultaneously affect both MCC36A and B resulting in block valve failure (see Enclosure 3, Case IV).

Summary

There were no safety violations found in this System Combination. With no singletons and such a small doubleton matrix, the results are very easy to view. It is very clear that the doubleton matrix is the list of singletons for each system (PORV and HPI) together.

ENCLOSURE 3

SYSTEM COMBINATION 3

PORV INDUCED LOCA WITH HIGH PRESSURE INJECTION

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

NO SINGLETONS

DOUBLETONS

```
                1 1 1 2 3 3 3
                0 0 0 7 2 2 2
        2 4 6 8 1 2 3 0 7 8 9

    2   - * * * - - - - - - -
    4   * - - - * * * * * * *
    6   * - - - * * * * * * *
    8   * - - - * * * * * * *
  101   - * * * - - - - - - -
  102   - * * * - - - - - - -
  103   - * * * - - - - - - -
  270   - * * * - - - - - - -
  327   - * * * - - - - - - -
  328   - * * * - - - - - - -
  329   - * * * - - - - - - -
```

```
FILE IDENTIFICATION:
  REACH PAIR:   I=    1    J=    3
  DATE:  6/11/84
  ANSWER.POS FILE IS: DR1:[220,1]SC3605MC3.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC3605MOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC3605MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC3605MRT.DAT
  SIGMA PI FILE NAME IS: DR1:SC3605MSI.C3
```

PORV INDUCED LOCA WITH HIGH PRESSURE INJECTION

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

VARIABLE LIST FOR SC3 CASE I DOUBLETON MATRIX

2	HPI-SLOCAD
4	PRIBREACHI
4	PCV464I
4	PCV466I
4	PCV468I
4	VSPNG464I
4	VSTEM464I
4	VSPNG466I
4	VSTEM466I
4	VSPNG468I
4	VSTEM468I
6	PCV455CI
6	SOV455CI
6	VDPHM455CI
6	VSTEM455CI
6	VSPNG455CI
8	PCV456I
8	SOV456I
8	VDPHM456I
8	VSTEM456I
8	VSPNG456I
* 101	LFSIPD
* 102	LWSIPD
* 103	LSSIPD
270	BRC852BJ852AA
327	J181OD
328	J290AD
328	J200D
328	PPI846D
328	HTRC846ZD
328	VGA846D
328	HTRC846YD
328	PPR846D
328	RWST1D

* INDICATES LOCATION

ENCLOSURE 3

SYSTEM COMBINATION 3

PORV INDUCED LOCA WITH HIGH PRESSURE INJECTION

COMBINED CASE II & CASE III RESULTS

CASE II FULLY AUTOMATIC FRONT-LINE AND SUPPORT SYSTEMS

CASE III FULLY AUTOMATIC FRONT-LINE, SUPPORT SYSTEMS, AND LOCATIONS

NO SINGLETONS

DOUBLETONS

```
                                  1 1 1
              1 1 1 2 3 3 3 3 4 4 2 2 5
              0 0 0 7 2 2 2 7 0 2 4 5 0
      2 4 6 8 1 2 3 0 7 8 9 6 2 6 7 1 2

   2  - * * * - - - - - - - - - - - - -
   4  * - - - * * * * * * * * * * * * *
   6  * - - - * * * * * * * * * * * * *
   8  * - - - * * * * * * * * * * * * *
 101  - * * * - - - - - - - - - - - - -
 102  - * * * - - - - - - - - - - - - -
 103  - * * * - - - - - - - - - - - - -
 270  - * * * - - - - - - - - - - - - -
 327  - * * * - - - - - - - - - - - - -
 328  - * * * - - - - - - - - - - - - -
 329  - * * * - - - - - - - - - - - - -
 376  - * * * - - - - - - - - - - - - -
 402  - * * * - - - - - - - - - - - - -
 426  - * * * - - - - - - - - - - - - -
1247  - * * * - - - - - - - - - - - - -
1251  - * * * - - - - - - - - - - - - -
1502  - * * * - - - - - - - - - - - - -
```

```
FILE IDENTIFICATION:
  REACH PAIR:   I=    1    J=    3
  DATE:  6/11/84
  ANSWER.POS FILE IS: DR1:[220,1]SC3605MC3.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC3605MOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC3605MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC3605MRT.DAT
  SIGMA PI FILE NAME IS: DR1:SC3605MSI.C3
```

PORV INDUCED LOCA WITH HIGH PRESSURE INJECTION

CASE II & CASE III (CONTINUED)

VARIABLE LIST FOR SC3 CASE II & III DOUBLETON MATRIX

2	HPI-SLOCAD
4	PRIBREACHI
4	PCV464I
4	PCV466I
4	PCV468I
4	VSPNG464I
4	VSTEM464I
4	VSPNG466I
4	VSTEM466I
4	VSPNG468I
4	VSTEM468I
6	PCV455CI
6	SOV455CI
6	VDPHM455CI
6	VSTEM455CI
6	VSPNG455CI
8	PCV456I
8	SOV456I
8	VDPHM456I
8	VSTEM456I
8	VSPNG456I
* 101	LFSIPD
* 102	LWSIPD
* 103	LSSIPD
270	BRC852BJ852AA
327	J1810D
328	J290AD
328	J200D
328	PRI846D
328	HTRC846ZD
328	VGA846D
328	HTRC846YD
328	PPR846D
328	RWST1D
376	BRC760CJ760AL
402	BRC762CJ762AL
426	BRC765BJ765AL
* 1247	LOCDP
* 1251	LOCSP
1502	TESTELECP

* INDICATES LOCATION

ENCLOSURE 3

SYSTEM COMBINATION 3

PORV INDUCED LOCA WITH HIGH PRESSURE INJECTION

CASE IVA & IVB - MANUALLY ASSISTED

CASE IVA - MANUALLY ASSISTED, FAILURE BY OMISSION

CASE IVB - MANUALLY ASSISTED, FAILURE BY OMISSION AND FAILURE BY COMMISSION

NO SINGLETONS

DOUBLETONS

```
                                  1 1
              1 1 1 2 3 3 3 3 4 4 2 5
              0 0 0 7 2 2 2 7 0 2 4 0
      2 4 6 8 1 2 3 0 7 8 9 6 2 6 7 2

   2  - * - - - - - - - - - - - - - -
   4  * - - - * * * * * * * * * * * *
   6  - - - - - - - - - - - - - - * *
   8  - - - - - - - - - - - - - - * *
 101  - * - - - - - - - - - - - - - -
 102  - * - - - - - - - - - - - - - -
 103  - * - - - - - - - - - - - - - -
 270  - * - - - - - - - - - - - - - -
 327  - * - - - - - - - - - - - - - -
 328  - * - - - - - - - - - - - - - -
 329  - * - - - - - - - - - - - - - -
 376  - * - - - - - - - - - - - - - -
 402  - * - - - - - - - - - - - - - -
 426  - * - - - - - - - - - - - - - -
1247  - * * * - - - - - - - - - - - -
1502  - * * * - - - - - - - - - - - -
```

```
FILE IDENTIFICATION:
  REACH PAIR:   I=    1    J=    3
  DATE:  6/11/84
  ANSWER.POS FILE IS: DR1:[220,1]SC3605MC4.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC3605MOT.DAT
  VARIAB.DAT FILE IS: DR1:[220,1]SC3605MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC3605MRT.DAT
  SIGMA PI FILE NAME IS: DR1:SC3605MSI.C4
```

PORV INDUCED LOCA WITH HIGH PRESSURE INJECTION

CASE IVA & IVB

VARIABLE LIST FOR SC3 CASE IVA & IVB DOUBLETON MATRIX

2	HPI-SLOCAD
4	PRIBREACHI
4	PCV464I
4	PCV466I
4	PCV468I
4	VSPNG464I
4	VSTEM464I
4	VSPNG466I
4	VSTEM466I
4	VSPNG468I
4	VSTEM468I
6	PCV455CI
6	SOV455CI
6	VDPHM455CI
6	VSTEM455CI
6	VSPNG455CI
8	PCV456I
8	SOV456I
8	VDPHM456I
8	VSTEM456I
8	VSPNG456I
* 101	LFSIPD
* 102	LWSIPD
* 103	LSSIPD
270	BRC852BJ852AA
327	J1810D
328	J290AD
328	J200D
328	PPI846D
328	HTRC846ZD
328	OPW846D
328	VGA846D
328	HTRC846YD
328	PPR846D
328	RWST1D
329	TTRWSTH20D
376	BRC760CJ760AL
402	BRC762CJ762AL
426	BRC765BJ765AL
* 1247	LOCDP
1502	TESTELECP

* INDICATES LOCATION

FILE IDENTIFICATION:
REACH PAIR: I= 1 J= 3
DATE: 6/11/84
ANSWER.POS FILE IS: DR1:[220,1]SC3605MC4.POS
OUTPUT.DAT FILE IS: DR1:[220,1]SC3605MOT.DAT
VARIAB.DAT FILE IS: DR1:[220,1]SC3605MVB.DAT
RENUMSRT.DAT FILE IS: DR1:[220,1]SC3605MRT.DAT
SIGMA PI FILE NAME IS: DR1:SC3605MSI.C4

2.4.4 RCP Seal LOCA and Loss of High Pressure Injection

2.4.4.1 Introduction

Loss of High Pressure Injection during an RCP Seal LOCA could potentially result in a core melt condition. Figure 2-11 shows the relationship between the front-line and support systems for this system combination. The support systems include the Chemical and Volume Control system, Electrical system, Instrument Air system, Component Cooling system, Safety Injection Actuation system, and the Service Water system.

In order to accomplish this analysis, two plant operating modes were analyzed, each with its own model. The first mode is normal automatic plant operation. From that model, singletons and doubletons are found which result in the failure of the RCP seals, thus initiating a LOCA. The second operating mode is the plant's automatic response to the LOCA. From that model, singletons and doubletons are found which keep the safety injection system from succeeding. Thus, failure sets common to the models represent failure(s) that both cause the LOCA AND keep the safety injection system from responding. Such significant failure sets exist and are discussed below.

The two plant operating modes have different dependencies because of the effect of the safety injection actuation system (SIAS).

Model for Normal Plant Operation

The model for normal plant operation does not incorporate the failures which would propagate from the digraphs for safety injection actuation. This was accomplished by setting all of the outputs from SIAs to true, which effectively prevents upstream failures from propagating into the rest of the model.

Model for Plant Responding to a LOCA

The digraph model for the time period after the occurence of the LOCA is the same as for the earlier injection cases

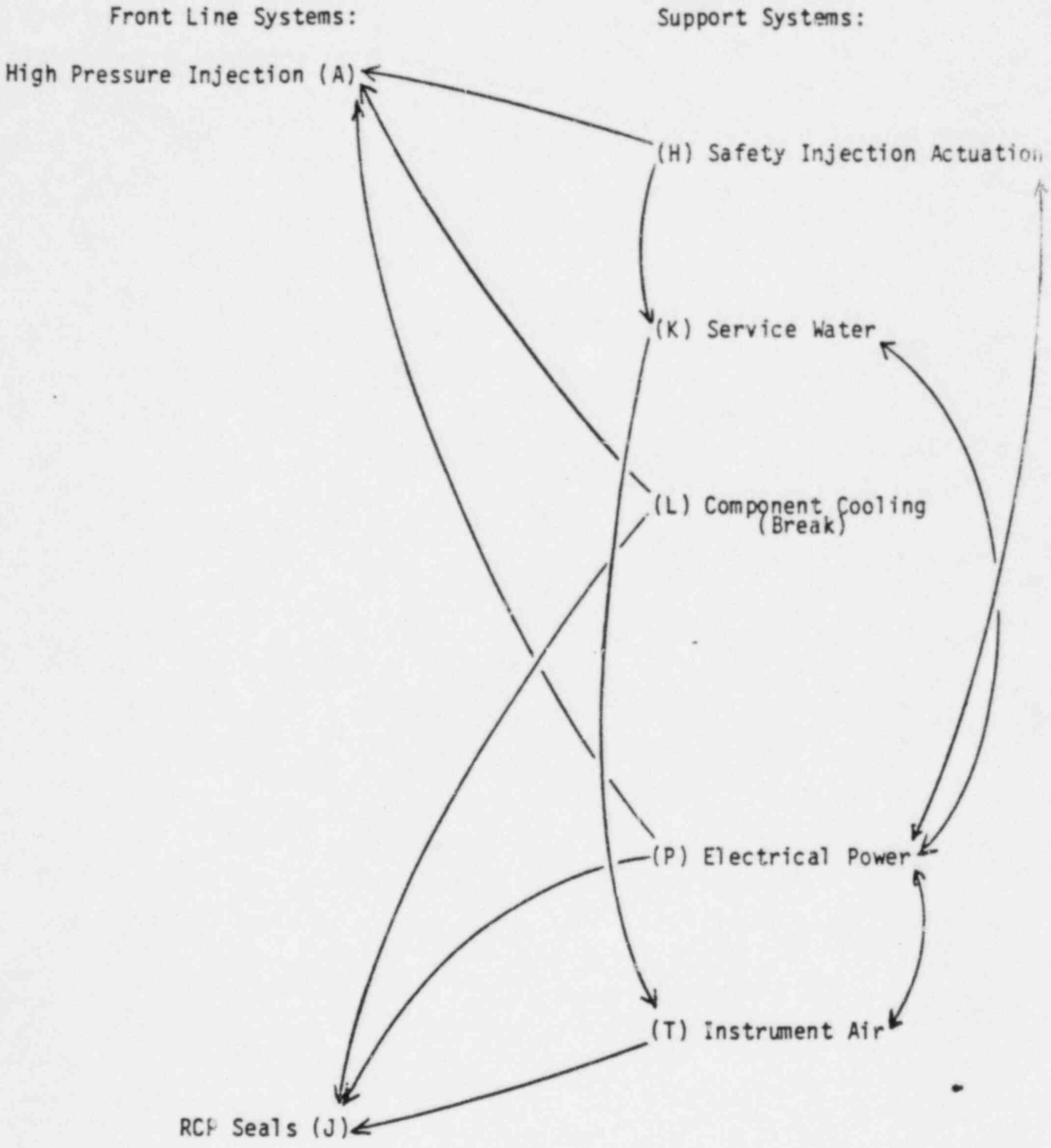
Search for Failure Sets Common to the Two Modes

Failure sets common to three phases can only occur in common systems. The only systems which are used in both operating modes are the electric power system (EPS) and the service water system (SWS). The EPS supports the RCP seals via two paths: 1) 480 V ac power to the charging pumps which inject flow through the seals against RCS pressure; and 2) 480 V ac power to the component cooling pumps which circulate water to keep the seals cool. The EPS also supports the safety injection system by supplying 480 V ac and 129 V dc power to the injection pumps as well as power to the automatic safeguards actuation system. The SWS supports the EPS by supplying cooling water to the diesel generators. The diesel generators are the only source of onsite 480 V ac power if offsite power is lost. Single components exist in the EPS and SWS which can cause the diesel generators to fail. Thus, should one of those components fail and not be detected before a loss of offsite power, that failure will cause a LOCA through all four RCS seals AND prevent the safety injection system from responding when offsite power is lost.

Figure 2-11

SYSTEM COMBINATION #4

RCP Seals Induced S2 LOCA with High Pressure Injection



2.4.4.2 Failure Criteria for Individual Systems

RCP Seals - Prior to LOCA
Leakage from RCP Seals constitutes a LOCA.

High Pressure Injection
For a small LOCA, one out of three high head injection pumps is required to deliver sufficient flow to the reactor coolant system. The charging pumps are not considered.

Support Systems - Prior To and After LOCA
The support systems in System Combination 4 are identical to those in System Combinations 2 and 3.

The digraphs for these systems can be found in Appendix B and the alpha input lists are in Appendix C.

2.4.4.3 Results for the Front-Line Systems Acting Alone: Case I

There are no front-line singletons in this system combination which could cause a seal LOCA and also cause the Safety Injection System to fail. (See Enclosure 4.)

There are no front-line doubletons in this system combination. This means that there are no two components in either the SIS or the seal model, which could lead to a seal LOCA and yield a loss of the Safety Injection System.

2.4.4.4 Front-Line and Support Systems: Case II

Singletons:
The only support systems singletons that occur are three break nodes from the Component Cooling System. These nodes are discussed in System Combination 2, Case 2.

Doubletons:
Figures 2-11a and 2-11b are the doubleton arrays for automatic normal plant operation and automatic plant response to a large LOCA, respectively. Figure 2-11a shows the doubletons which cause seal failure during normal automatic plant operation and Figure 2-11b shows the doubletons which cause failure of the automatic low pressure injection system.

The three blocked off areas in each array are those in which there are doubletons between support systems which are used in both plant operating modes. These systems are the EPS and the SWS. In both figures, the upper left triangles are doubletons of the EPS with itself, the upper right rectangle are doubletons of the EPS with the SWS, and the lower right triangle are doubletons of the SWS with itself of which there are none in either mode. The doubletons in the areas were compared. The row corresponding to doubletons involving loss of offsite power (SOURCE1P) is highlighted in the figure. Within the rectangles of both arrays and in the highlighted row is a circled node corresponding to a butterfly valve in the SWS. In the upper left triangle of both arrays and in the

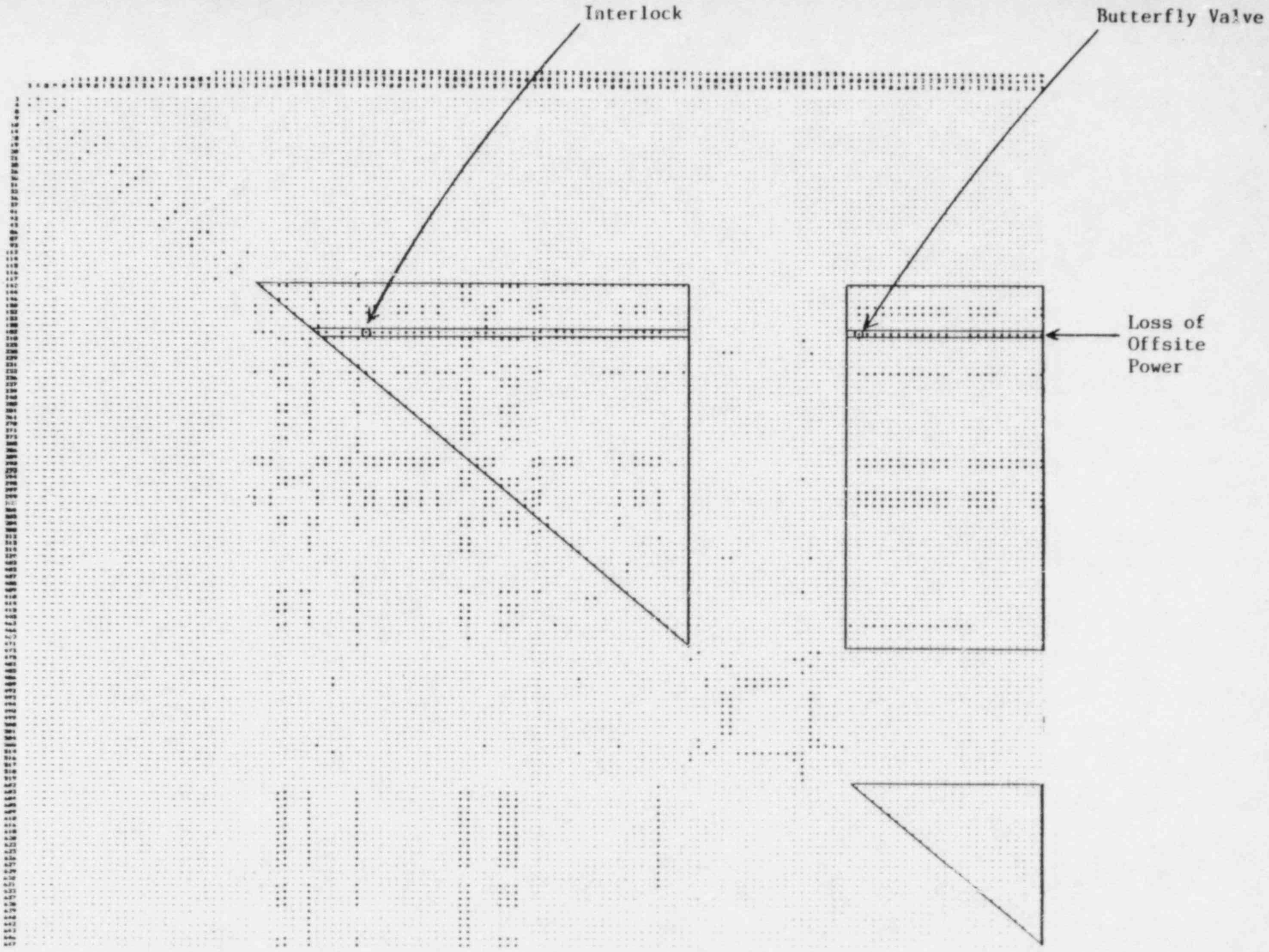


Figure 2-11a Doubleton Array for Seal Failure During Normal Automatic Plant Operation. Upper left triangle is EPS*EPS, upper right rectangle is EPS*SWS, lower right triangle is SWS*SWS.

```
   3    SEALLAB31J      146   GENDSL33OP      289   LOCAP
   4    PATHLSW31J      146   GENDSL33P       290   LOCCP
   4    PATH1BP31J      146   BKREG3P         293   LOCNP
   4    ORFCBD31J       146   ITLUV'BUS5AP    294   LOCRP
   8    HXRTBT31J       146   AXFRBKREG3P     295   LOCSP
   9    PATHHXR31J      146   ITLVDG33P       297   BKRSS5/P
  10    CAVINJ31J       146   ITLFDG33P       299   XFMRSS5/P
  14    SEALLAB32J      146   ITLBKR5AP       300   BKR5A/P
  15    PATHLSW32J      146   STAIR33P        301   BKR5A:P
  15    PATH1BP32J      146   OILXFR33P       303   GENDSL33/P
  15    ORFCBD32J       146   STSVW33P        304   BKREG3/P
  19    HXRTBT32J       146   XCTR33P         305   BKREG3:P
  20    PATHHXR32J      146   TKD33P          312   BUS2A/P
  21    CAVINJ32J       146   VDF18CP         313   GENDSL31/P
  25    SEALLAB33J      146   FLTRA33P        314   BKREG1/P
  26    PATHLSW33J      146   PBSTR33P        329   BUS6A/P
  26    PATH1BP33J      146   FLTRB33P        402   BKRMCC39/P
  26    ORFCBD33J       146   JKTHX33P        403   MCC39/P
  30    HXRTBT33J       146   OILCLR33P       407   BATTERY31/P
  31    PATHHXR33J      146   LOCKP           408   FUSEPNL31/P
  32    CAVINJ33J       150   BKRSS5P         409   PWRPNL31/P
  36    SEALLAB34J      150   XFMRSS5P        410   BKRMCC39:P
  37    PATHLSW34J      150   BKR5AP          414   BKRDPNL31/P
  37    PATH1BP34J      150   R86SS5P         415   PNLDIS31/P
  37    ORFCBD34J       150   OIBUS5AP        445   PWRPNL33/P
  41    HXRTBT34J       152   BUS5P           463   TIMELONG
  42    PATHHXR34J      153   STAUXXFMRP      466   TIMELONG7P
  43    CAVINJ34J       155   BKRST5P         469   TIMELONG14P
  86    VGA248J         155   R86ST5P         471   TIMELONG16P
  87    JPPCH6J         182   SOURCE1P        473   CCHXRS32Z
  93    JPPCH5J         218   PWRPNL31P       473   J763BL
  93    JPPCH4J         225   BUS2AP          473   VGA759BL
 113    SWRLR31J        228   BUS6AP          473   JA8L
 114    SWMCTO31J       229   PWRPNL33P       473   VGA765BL
 115    SWRLL31J        231   ITLBFBUS5AP     473   J764BL
 116    SWLOY31J        232   UVBUS5AP        475   CCHXRS31Z
 117    SWMTO31J        236   ITLBKR2AT5AP    475   CCHXRP32Z
 142    BEFOREDIESE     237   PNLDIS31P       475   J763AL
 144    GENDSL31OP      237   BKRDPNL31P      475   VGA759AL
 144    GENDSL31P       239   RCVR31P         475   JA7L
 144    BKREG1P         240   TTRCVR31P       475   CCHXRP31Z
 144    ITLUV'BUS2/     250   RCVR33P         475   PPR765BL
 144    AXFRBKREG1P     251   TTRCVR33P       475   VGA766DL
 144    ITLVDG31P       761   LCV1209BP       475   JA10L
 144    ITLFDG31P       261   AUTOLCV1209BP   475   VGA765AL
 144    ITLBFBUS2AP     261   TTTKD31P        475   J764AL
 144    ITLBKR2AP       270   LCV1207BP       475   PPI765AL
 144    STAIR31P        270   AUTOLCV1207BP   475   J765AL
 144    OILXFR31P       270   TTTKD33P        475   VGA766CL
 144    STSVW31P        271   UV'BUS2AP       483   CCWP33L
 144    XCTR31P         273   UV'BUS5AP       483   XDD6ACCP33AP
 144    TKD31P          285   TTBATTERY31P    483   CONMCCP33ACP
 144    VDF18AP         286   BATTERY31P      483   MOLDCCP33AP
 144    FLTRA31P        286   FUSEPNL31P      483   XDDACCP33P
 144    PBSTR31P        286   LOCOP           483   XDD6ACCP33BP
 144    FLTRB31P                              483   CONMCCP33BCP
 144    JKTHX31P                              483   MOLDCCP33BP
 144    OILCLR31P                             483   XDDBCCP33P
                                              483   XDD6ACCP33CP
                                              483   CONMCCP33CCP
                                              483   MOLDCCP33CP
                                              483   XDDCCCP33P
```

Figure 2-11a (cont.). Variable Name List (page 1 of 2)

485	VGA760AL
485	J1805L
485	PPR1805L
485	JA55L
485	ORFC760AL
485	CCWP31L
485	ORFCCCW31L
485	VC761AL
485	JA1L
485	VGA762AL
485	XDD5ACCP31AP
485	CONMCCP31ACP
485	BKRCCP31P
485	MOLDCCP31AP
485	XDDACCP31P
485	XDD5ACCP31BP
485	CONMCCP31BCP
485	MOLDCCP31BP
485	XDDBCCP31P
485	XDD5ACCP31CP
485	CONMCCP31CCP
485	MOLDCCP31CP
485	XDDCCCP31P
485	JELE1CCP31P
485	RLCCP31P
485	CONTDCCP31OP
485	SWMCA12CCP31P
485	XDDCCP31BP
485	JELE21DCCP31P
485	JELE18CCP31P
485	JELE15CCP31P
485	JELE15ACCP31P
485	JELE14CCP31P
485	JELE13CCP31P
485	T13CCP31P
485	XDD13CCP31P
485	CON13CCP31OP
485	RLOTSACCP31OP
485	XDD14CCP31P
485	XDD3CCP31P
485	CCOILCCP31P
485	CONCCP31DOP
485	JELE3CCP31P
485	XDD4CCP31P
485	JELE4CCP31P
485	FUSECCP31NP
485	JELE12CCP31P
485	JELE16CCP31P
485	JELE5CCP31P
485	JELE28CCP31P
485	JELE86CCP31P
485	TNCCP31P
485	SENOTSCCP31OP
485	CONOTSCCP31ACP
485	CONOTSCCP31BCP
485	CONOTSACCP31CP
485	BS8HCCP31OP
485	SWMOA 1CCP31P
486	BRC760AJ760BL
489	J760BL
489	PPR760CL
489	VGA766BL
492	VGA760CL
493	JA57L
494	ORFC760CL
498	ORFCCCW33L
499	VC761CL
500	JA3L
501	VGA762CL
504	J762CL
505	BRC762CJ762BL
514	BRC762AJ762BL
516	J762AL
517	FUSECCP31PP
517	JELE1BCCP31P
517	T1CCP31P
517	JELE1ACCP31P
518	XDDCCP31AP
518	JELEA12CCP31P
519	JELEA1CCP31P
519	JELEH12CCP31P
519	JELE11CCP31P
519	JELEE12CCP31P
519	JELEE1CCP31P
519	JELEXCCP31P
519	JELEA11CCP31P
519	JELEC12CCP31P
519	SWMCC12CCP31P
519	XDDCCP31JP
519	T15DCCP31P
519	JELE20CCP31P
602	J1191K
602	J97CK
602	J97AK
602	J97BK
602	PPR24INK
602	VB32K
602	PPR411K
603	J1190K
603	J98AK
603	J1093BK
603	J1093AK
603	J1093DK
603	VB30K
603	J1095K
604	VC98K
604	HTRC409K
604	J4K
604	J106BK
604	J409K
604	J1221K
604	HTRC98K
604	VB98K
605	VC99K
605	J135BK
605	J135AK
605	HTRC408K
605	J5K
605	J106AK
605	J1220K
605	J1222K
605	HTRC99K
605	VB99K
609	RIVHUDSON
610	STRCTRINTK
616	SWPWELL1K
618	TRASH1K
620	J131K
622	J133K
623	J132BK
626	J136K
627	J134K
629	JDEGRK
629	J410K
629	J1237K
629	J390K
629	J263K
629	J1271K
630	J411AK
631	CHNLDSK
631	CHNLDS3K
631	J95AK
633	J95BK
633	J95CK
633	J95DK
637	JKTTEMPK
638	J95FK
638	J1096AK
639	J1096BK
640	J1096CK
640	WCL31K
640	PPR1281K
640	VGA1281K
640	CFLX1281K
640	J1281K
642	J1094K
643	PPR1094AK
643	PPR1306K
643	J1306AK
643	VGA62AK
643	J1306CK
643	J1306DK
643	J1306EK
643	CFLX1306K
643	OCL31K
646	PPR1095K
646	J1095AK
646	VGA62EK
646	J1308AK
646	J1308BK
646	J1308CK
646	CFLX1308K
646	OCL33K
647	WCL33K
647	PPR1098K
647	VGA1098K
647	CFLX1283K
647	J1283K
647	J1283AK

Figure 2-11a (cont.). Variable Name List (page 2 of 2)

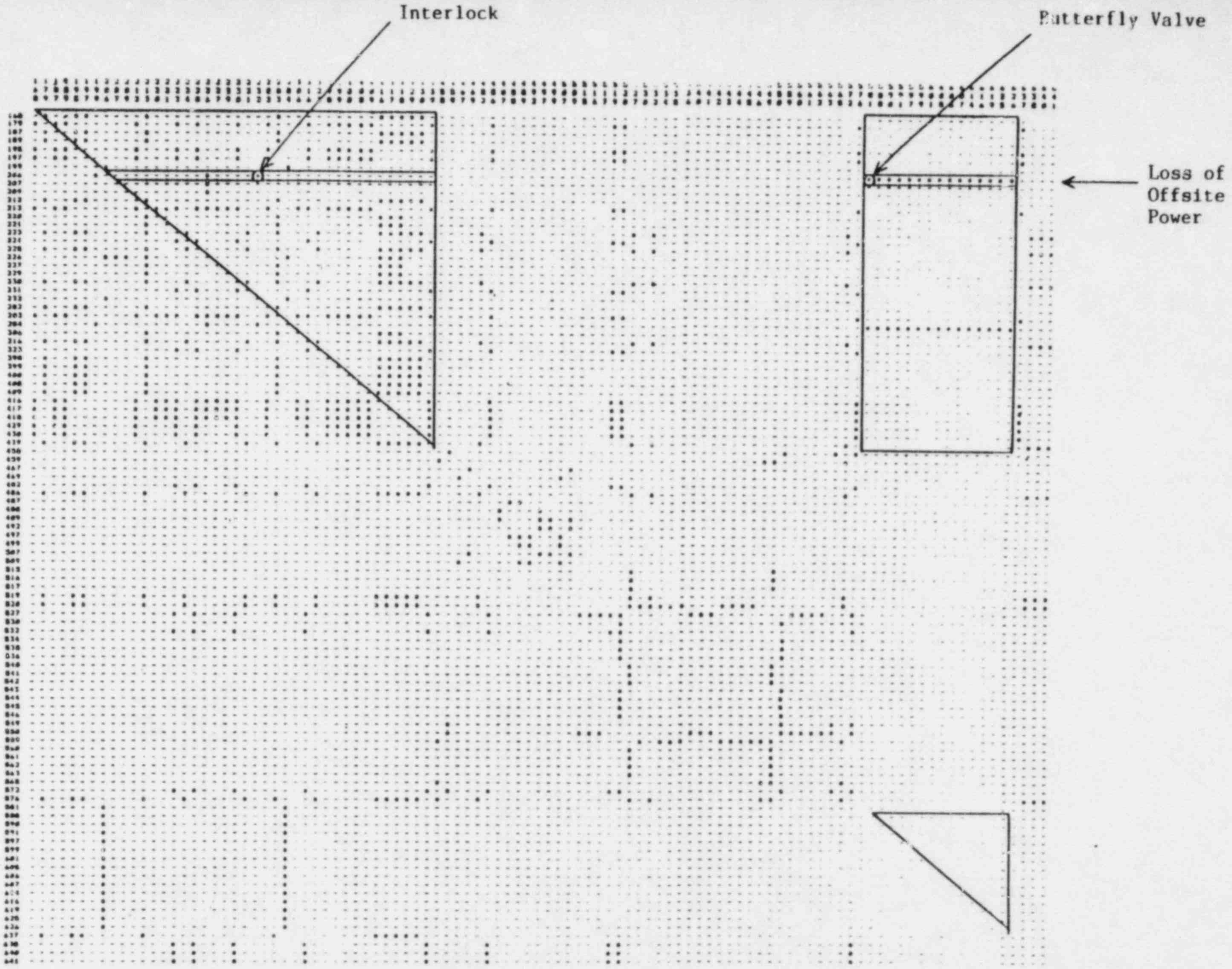


Figure 2-11b Doubleton Array for Automatic Low Pressure Injection. Upper left triangle is EPS*EPS, upper right rectangle is EPS*SWS, lower right triangle is SWS*SWS.

168	PNLDIS31P
168	BKRDPNL31P
179	PNLDIS34P
179	BKRDPNL34P
187	LG2OF2SIA2AH
187	LG1OF2SIA2AH
187	RSI1H
189	RSI11XZ
195	LG2OF2SIA2BH
195	LG1OF2SIA2BH
195	RSI2H
197	RSI21XZ
199	BEFOREDIESEL
2Ø6	STAUXXFMRP
2Ø6	SOURCE1P
2Ø6	LOCAP
2Ø7	BKRST6P
2Ø7	RB6ST6P
2Ø9	BUS6P
212	PWRPNL31P
212	BATTERY31P
212	FUSEPNL31P
212	LOCOP
213	PWRPNL32P
213	BATTERY32P
213	FUSEPNL32P
213	LOCOP
22Ø	BUS2AP
221	BKR2AT3AP
221	ITLUV'BUS3AP
221	AXFRBKR2AT3AP
221	ITLBFBUS3AP
221	ITLBKR3AP
223	BUS3AP
224	BUS6AP
225	PWRPNL33P
226	ITLBKR3AT6AP
227	ITLBFBUS5AP
229	UVBUS2AP
23Ø	UVBUS3AP
231	UVBUS6AP
232	ITLBKR2AT5AP
282	TTBATTERY31P
282	TIMELONG7P
283	TTBATTERY32P
283	TIMELONG8P
284	LOCCP
3Ø6	BUS2A/P
316	BUS3A/P
323	BUS6A/P
398	BATTERY31/P
399	FUSEPNL31/P
4ØØ	PWRPNL31/P
4Ø8	BKRDPNL31/P
4Ø9	PNLDIS31/P
416	BATTERY32/P
417	FUSEPNL32/P
418	PWRPNL32/P
429	BKRDPNL34/P
43Ø	PNLDIS34/P
439	PWRPNL33/P
458	TIMELONG3K
458	CCHXRS32Z
458	J763BL
458	VGA759BL
458	JA8L
458	VGA765BL
458	J764BL
459	TIMELONG4K
459	CCHXRS31Z
459	J763AL
459	VGA759AL
459	JA7L
459	JA1ØL
459	VGA765AL
459	J764AL
459	PPI765AL
467	J745AD
467	RHXR32Z
467	MOV745BD
467	MOV745AD
469	VGA742D
469	RHXR31Z
482	VGA733BD
482	J1867BD
482	J1Ø1XD
482	CON182252/RHR2I
482	BS17RHRP32OP
482	RHRP32Z
482	J1866DD
482	XDD3ARHRP32AP
482	CONMRHRP32ACP
482	BKRRHRP32P
482	MOLDRHRP32AP
482	XDDARHRP32P
482	XDD3ARHRP32BP
482	CONMRHRP32BCP
482	MOLDRHRP32BP
482	XDDBRHRP32P
482	XDD3ARHRP32CP
482	CONMRHRP32CCP
482	MOLDRHRP32CP
482	XDDCRHRP32P
482	FUSERHRP32PP
482	JELE1BRHRP32P
482	T1RHRP32P
482	JELE1ARHRP32P
482	JELE1RHRP32P
482	CONRHRP32TDOP
482	RLRHRP32P
482	XDD1ARHRP32P
482	JELEA1RHRP32P
482	JELE19ARHRP32P
482	T13RHRP32P
482	XDD13RHRP32P
482	CON13RHRP32OP
482	RLOTSARHRP32OP
482	XDD14RHRP32P
482	XDD3RHRP32P
482	CCOILRHRP32P
482	CONRHRP32DOP
482	JELE3RHRP32P
482	XDD4RHRP32P
482	JELE4RHRP32P
482	FUSERHRP32NP
482	JELEH12RHRP32P
482	JELE11RHRP32P
482	JELE12RHRP32P
482	JELEE12RHRP32P
482	JELEE1RHRP32P
482	JELEKRHRP32P
482	JELE16RHRP32P
482	JELE5RHRP32P
482	JELEA11RHRP32P
482	SWMCA12RHRP32P
482	XDDRHRP32BP
482	T32CRHRP32P
482	CON2RHRP32OP
482	TNRHRP32P
482	SENOTSRHRP32O
482	CONOTSRHRP32ACP
482	CONOTSRHRP32BCP
482	CONOTSARHRP32C
482	CON2652/RHR2I
482	CON6RHRP32P
482	SWMOA11RHRP32P
482	VC738BD
482	J1Ø7D
482	VGA739BD
482	J83ØBL
482	J627BAL
482	J627BBL
482	J627BCL
482	JA5Ø2L
482	JØ17BL
482	J6Ø1BL
482	J6Ø2BL
482	J6Ø2CL
482	J1871AL
482	VGL736BL
482	J736BL
482	PPR736BL
482	PSHXR1871BL
482	PPR75ØDL
482	J75ØDL
482	PPI1871AL
482	VGL1871AL
482	J1871BL
482	PPI1871BL
482	PPR1871BL
482	VGL1871BL
482	VC75ØDL
482	ORFC645BL
482	FIC645L
482	ORFC645AL
482	VGL737BL
482	JA5Ø1AL
482	JA5Ø1L
482	RLSI6A1I
486	J74ØBD
486	VGA735AD
486	J1867AD
486	J1Ø3XD
486	CON91352/RHR1I
486	CON2RHRP31OP
486	RHRP31Z
486	J1866BD
486	XDD3ARHRP31AP
486	CONMRHRP31ACP
486	BKRRHRP31P
486	MOLDRHRP31AP
486	XDDARHRP31P
486	XDD3ARHRP31BP
486	CONMRHRP31BCP

Figure 2-11b (cont.). Variable Name List (page 1 of 2)

486	CONMRHRP31BCP
486	MOLDRHRP31BP
486	XDDBRHRP31P
486	XDD3ARHRP31CP
486	CONMRHRP31CCP
486	MOLDRHRP31CP
486	XDDCRHRP31P
486	FUSERHRP31PP
486	JELE1BRHRP31P
486	T1RHRP31P
486	JELE1ARHRP31P
486	JELE1RHRP31P
486	CONRHRP31TDOP
486	RLRHRP31P
486	XDD1ARHRP31P
486	JELEA1RHRP31P
486	JELE19ARHRP31P
486	T13RHRP31P
486	XDD13RHRP31P
486	CON13RHRP31OP
486	RLOTSARHRP31OP
486	XDD14RHRP31P
486	XDD3RHRP31P
486	CCOILRHRP31P
486	CONRHRP31DOP
486	JELE3RHRP31P
486	XDD4RHRP31P
486	JELE4RHRP31P
486	FUSERHRP31NP
486	JELEH12RHRP31P
486	JELE11RHRP31P
486	JELE12RHRP31P
486	JELEE12RHRP31P
486	JELEE1RHRP31P
486	JELEKRHRP31P
486	JELE16RHRP31P
486	JELE5RHRP31P
486	JELEA11RHRP31P
486	SWMCA12RHRP31P
486	XDDRHRP31BP
486	T32CRHRP31P
486	TNRHRP31P
486	SENOTSRHRP31OP
486	CONOTSRHRP31ACP
486	CONOTSRHRP31BCP
486	CONOTSARHRP31CP
486	BS17RHRP31OP
486	CON2652/RHR1I
486	CON6RHRP31P
486	SWMOA11RHRP31P
486	VC738AD
486	J1Ø4D
486	VGA739AD
486	PPI739AD
486	JA14AL
486	JA14L
486	J83ØAL
486	JTIC627L
486	J627AL
486	JØ17AL
486	J6Ø2AL
486	J6Ø1AL
486	J6Ø1CL
486	J6Ø1DL
486	J1871CL
486	VGL736AL
486	J736AL
486	PPR736AL
486	PSHXR1871DL
486	PPR75ØEL
486	J75ØEL
486	VGL1871DL
486	J1871DL
486	PPI1871DL
486	PPR1871DL
486	VGL1871CL
486	VC75ØEL
486	ORFC646BL
486	FIC646L
486	ORFC646AL
486	VGL737AL
486	J627BL
486	RLSI2A1I
486	RL3-13AI
486	CON2627-3AX3I
486	RL27-3AX1I
486	CON3527-3AX1I
486	RL27-3AX4I
486	CON3527-3AX4I
486	RL27-3AX3I
487	J838QB
487	J639B
487	J638B
488	J838RB
488	J641AB
488	J641B
488	J64ØB
489	J899AB
492	MOV899AB
492	MOV746B
492	J733AB
492	HCV64ØB
492	J889AB
497	J899BB
499	MOV899BB
499	MOV747B
499	J733BB
499	HCV638B
499	J889BB
5Ø7	J889D
5Ø9	J1869BD
515	VGA76ØAL
516	J18Ø5L
517	PPR18Ø5L
519	J76ØAL
52Ø	BRC76ØAJ76ØBL
527	BRC76ØCJ76ØBL
53Ø	VGA76ØCL
532	J76ØCL
534	JA57L
535	ORFC76ØCL
536	CCWP33L
54Ø	JA55L
541	ORFC76ØAL
542	CCWP31L
543	ORFCCCW33L
544	VC761CL
545	JA3L
546	VGA762CL
549	J762CL
55Ø	BRC762CJ762BL
559	BRC762AJ762BL
56Ø	ORFCCCW31L
561	VC761AL
562	JA1L
563	VGA762AL
565	J762AL
572	J765BL
576	J765AL
581	J119ØK
581	J98AK
581	J1Ø93BK
581	J1Ø93AK
581	J1Ø93DK
581	VB3ØK
581	J1Ø95K
588	VC98K
588	HTRC4Ø9K
588	J4K
588	J1Ø6BK
588	J4Ø9K
588	J1221K
588	HTRC98K
588	VB98K
59Ø	RIVHUDSONK
591	STRCTRINTKK
597	SWPWELL1K
599	TRASH1K
6Ø1	J131K
6Ø5	J133K
6Ø6	J132BK
6Ø7	CHNLDSK
6Ø7	CHNLDS3K
6Ø7	J95AK
6Ø7	J95BK
6Ø7	J95CK
6Ø7	J95DK
614	J95FK
614	J1Ø96AK
616	J1Ø96BK
619	J1Ø94K
625	COL-RW-2K
625	T1COL1K
626	SW123456P
637	CON2Ø24SI11XI
638	CON913SI21XI
64Ø	RL3-16AI
64Ø	CON91327-6AX3I
641	RL27-6AX1I
641	CON3927-6AX1I
641	RL27-6AX4I
641	CON3927-6AX4I
641	RL27-6AX3I

Figure 2-11b (cont.). Variable Name List (page 2 of 2)

SOURCE1P row is an electrical interlock in the EPS. Thus, those doubletons both cause the accident and prevent mitigation.

Butterfly Valve Closure

In the SWS, there are many single items whose failure would cause a stoppage of cooling water to all three diesel generators (DGs). Such a failure would have the major effect of causing the DGs to fail due to overheating about 10 minutes after they were started.* There is no automatic trip for this condition and the DGs would likely by severely damaged and not recoverable.

There are two cooling paths from the Hudson River through the service water pumps and to the DGs. However, just one train is pre-selected and aligned for "Essential" cooling functions (such as for the DGs). The other train is pre-selected and aligned for other "Non-Essential" loads (see Section 2.2.12). Thus, the DGs are actually only cooled by a single train. The DGs do not have cooling water flowing through their heat exchangers during normal plant operation. This keeps them from becoming too cold. However, that normal lack of flow makes it more difficult to monitor the availability of a cooling flow path. Normally, the cooling path from the river to the heat exchangers is open and the discharge side is closed by two air operated valves (energized shut) on parallel paths. On the inlet side are three valves, any of which could block all cooling flow to the DGs if they were to be shut. Two of the valves are adjacent to each other in a part of SWS where water is normally flowing to other loads. If the train pressurized by pumps 31-33 is selected as Essential, these valves are butterfly valve SWN-98 and check valve SWN-100. If the train pressurized by pumps 34-36 is selected as Essential, the valves are butterfly valve SWN-99 and check valve SWN-100 (the two check valves are both labelled SWN-100). Regardless which train is selected, the two adjacent valves are well monitored by downstream placement of pressure meters. Should one of the valves be shut, the meters would immediately generate an alarm since the normal flow of water would be interrupted and sensed at that time.

Closer to the DGs, where water is not normally flowing, there is a butterfly valve on each train that can block all flow to the DG heat exchangers. If pumps 31-33 are Essential, the valve is SWN-30. If pumps 34-36 are Essential, the valve is SWN-29. The state of the butterfly valve is not monitored directly and is administratively controlled. Its state is checked at the beginning of each 8-hour shift by noting the reading on an analog pressure gauge two rooms away in the DG32 room. The pressure sensed is on the inlet side of the DG32 heat exchangers. That pressure should be the same for the heat exchangers of the other two DGs since there are open paths between them. Should the butterfly valve be closed (such as by error of omission during a switch of the trains from Essential to Non-Essential or by error of commission after the re-alignment) the gauge would be sensing the pressure of the volume trapped between that valve and the normally closed parallel valves on the discharge side. Thus, the only way the misalignment could be noticed is for the pressure in that volume to decay and for the trend to be

* Per operator reference to a study performed for EBASCO by diesel manufacturer, Alco.

noticed. Should the pressure decay to a low enough level, an alarm sounds in the CCR. Even if the valves were visually inspected, their state could not be deduced as is evidenced in the photograph of the butterfly valves on each of the two cooling trains (Figure 2-11c). One valve should be open and one should be closed. The valve against the wall is SWN-29 and the other is SWN-30. At the time the photograph was taken, March 20, 1984, the plant was at full power and the train selected as Essential was pressurized by pumps 31-33. Thus, SWN-30 should have been open and SWN-29 should have been closed.

In the event that the valve that should have been opened was closed and offsite power was lost, the following sequence of events would most likely transpire. Immediately upon loss of offsite power, the main generator would be tripped and the diesel generators would start. Once either the diesel lube oil or jacket water temperature was high enough, the two air operated valves on the discharge side of the heat exchangers would automatically open, but no cooling flow would be established due to closure of the inlet butterfly valve. There are both local and remote indicators of diesel generator overheat, but there is no automatic high temperature trip. About 10 minutes after loss of offsite power, the diesels would overheat and fail, probably irreversibly. There would then be no 480 volt power in the plant. The charging pumps would stop. Component cooling of the labyrinth seal heat exchangers would also cease. Thus, RCS primary coolant at core pressure and temperature would be free to flow out through all four reactor coolant pump (RCP) seals, unopposed by the charging system and not cooled by the CCS. The coolant would immediately turn to steam in the seals, most likely causing damage. About 480 gallons per minute would flow out each RCP seal, making the total rate of coolant loss 1920 gpm. A large LOCA would have been initiated. Without 480 volt power, no injection systems would be able to start and the RCS pressure and coolant level would continue to fall. While the passive low pressure accumulators would inject, there would be no containment heat removal since the fans and sprayers would not be functioning. There would also be no recirculation, of course.

The operators would have on the order of 30 minutes after the diesels irreversibly failed (40 minutes after loss of offsite power) to find another power supply before the fuel rods would be uncovered. A gas turbine generator exists near the Indian Point-1 plant which could be used to run the safety injection system since it could be connected to the Unit 3 grid. That generator, however, is only controlled from Unit 1 and it is not known how long it would take to manually start it and for it to produce sufficient voltage. It was also learned that not all operators know about the other generator. In the event the gas turbine generator was brought up in time or if offsite power was restored, it would then be possible to control the Unit 3 accident. Needless to say, the rapid development of this major accident would place a great burden on the operators.

Interlock Subcomponent Open Circuit

Another hardware item in the electrical system may disable the function of the diesel generators. Its failure causes a significant degradation of service water cooling to the diesel generators and may lead to a scenario similar to that caused by the butterfly valve closure. The capability of the safety injection system is also significantly reduced.

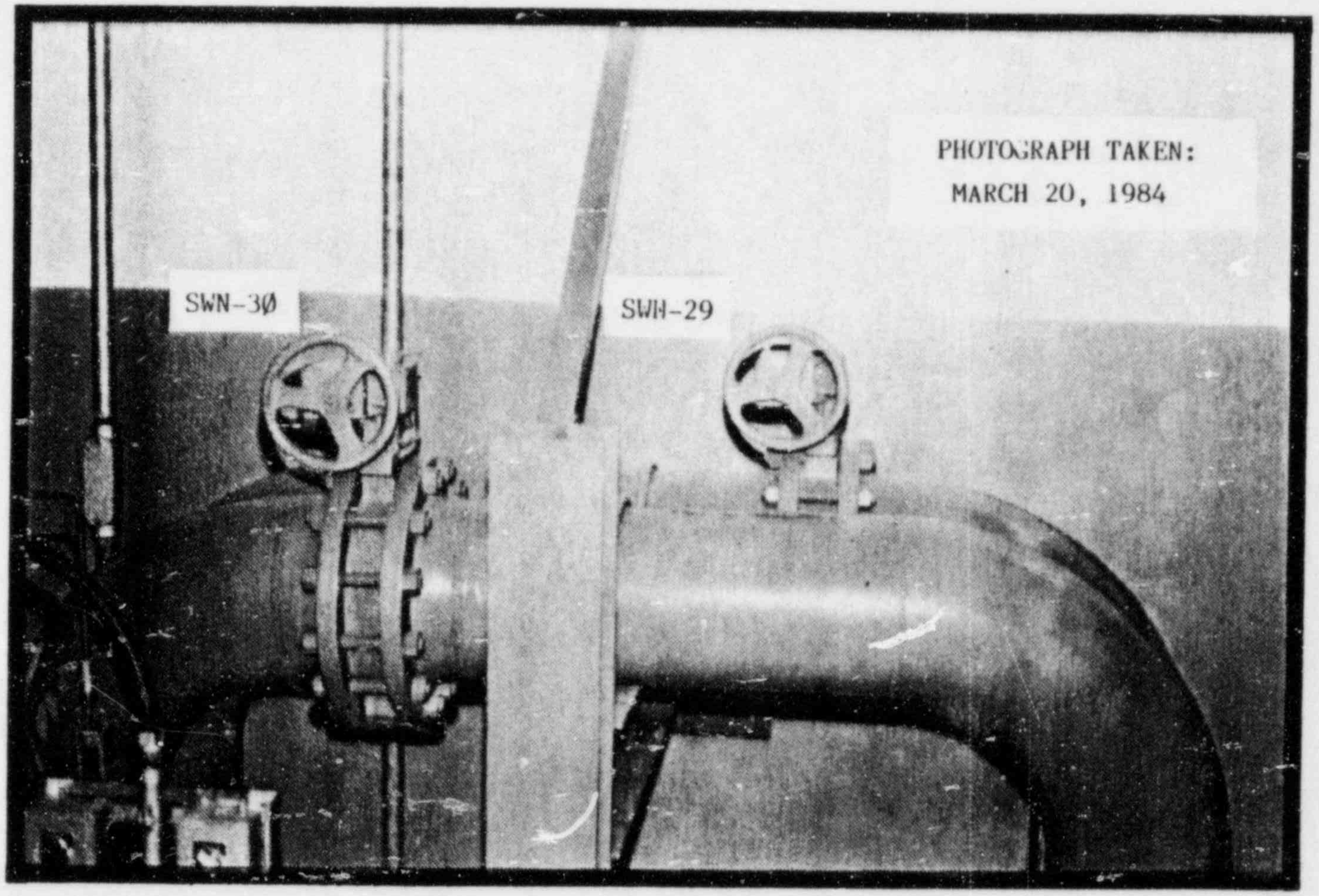


Figure 2-11c Service Water System Butterfly Valves on Cooling Paths to All Three Diesel Generators. Per procedure, one valve should be open and one should be closed.

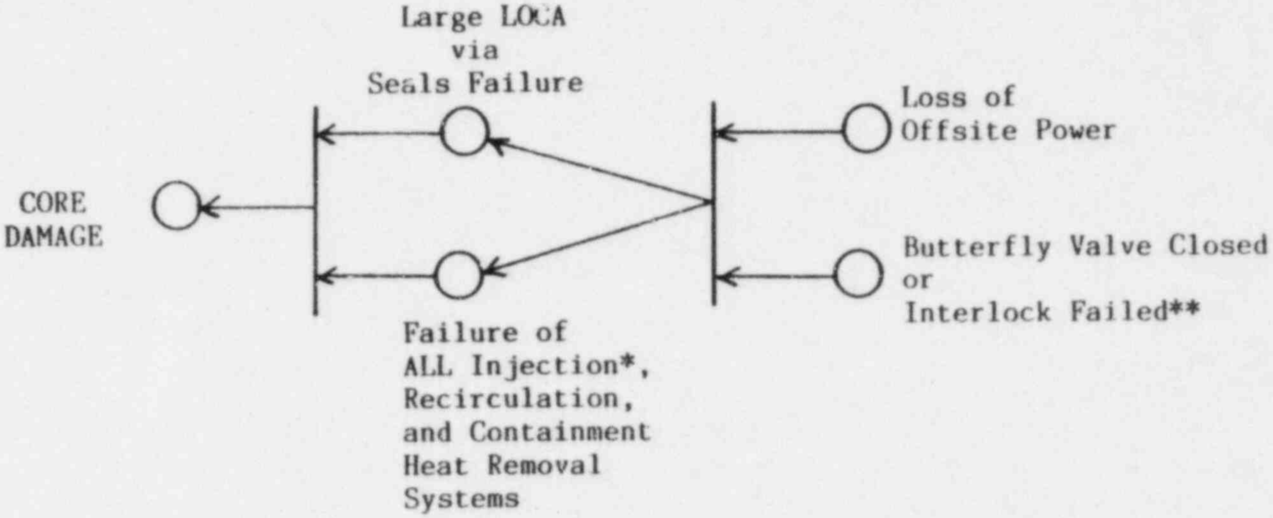
The hardware failure is a subcomponent of electrical interlock 2AT5A. Based on available information, an open circuit between two contacts in the closing circuit could keep three 480 V ac buses from being automatically energized on loss of offsite power. The interlock is connected to auto closing mechanisms which load DG31 and DG33 onto 480 V ac buses 2A and 5A, respectively. On loss of offsite power, the DGs are started. To load them onto the buses, the interlock must change state. Should the connection in the interlock be broken, buses 2A or 5A would not be energized. Loss of power to bus 5A would cut power to the dedicated charging pump 31, thus causing the large LOCA. Bus 3A is powered by bus 2A so it would also be not loaded.

The effect of the three dead buses is to cut power to essential service water pumps 31 and 32, which would leave one essential pump, number 33, to supply flow to all heat sinks cooled by the service water system. All three essential pumps are automatically actuated in the event of a LOCA. From FSAR Table 9.6-1 and page 9.6-3, two service water pumps are needed to supply the cooling in response to a LOCA. This was confirmed by operator discussion. At least 11,000 gallons per minute need to be pumped and a single pump is rated at about 5,000 gpm. Of the total flow required, 10,000 gpm is needed to remove heat from the containment fan units and 1,200 gpm is needed to cool the diesels. A hydrodynamic analysis would be required to determine how much water would flow through the diesels if only one pump were functioning. If that flowrate is inadequate for diesel cooling, the operators would have more time to act than in the case of the closed valve. If they noticed the problem in time, the diesels could be loaded onto their buses manually, thus guaranteeing sufficient service water system heat removal.

The three dead buses also leave only one of the three high pressure safety injection pumps and one of the two residual heat removal pumps available. A medium LOCA requires two high pressure safety injection pumps, but the failure of all four seals initiates a large LOCA. The core would depressurize fast enough so that the only available RHR pump would probably suffice.

Conclusion

Figure 2-11d shows how the doubletons described above can lead to core damage. The failures of the butterfly valve and interlock demonstrate how a large and detailed logic model can yield non-intuitive safety significant systems interactions. The valve is a substantial piece of hardware, perhaps heretofore considered obscure only because it is in the interior of a support system which supports another support system. But since the breadth of the global model embraced all components from the reactor coolant pump seals to the Hudson River, its essential role as contributor to a major uncontrollable accident was exposed. Similarly, the interlock subcomponent failure that could contribute to a major accident points to the value of modeling the system in depth. The presence of the interlock in failure sets in both modes of plant operation served to guide the analyst into the workings of the device.



*except low pressure accumulators

**may require hydrodynamic analysis to assess effect

Figure 2-11d Doubleton Failures Leading to Core Damage

2.4.4.5. Front-Line with Support Systems and Location: Case III

The only location singleton, which propagates through the model, is LOCDP, which is the 15' elevation of the Control Room. This location provides a vulnerability to Buses 2, 3, 5, and 6, which would simultaneously yield a failure in the Charging Pumps (leading to the seal LOCA) and the Safety Injection Pumps (resulting in failure to inject).

Rows 220, 221, and 222 are location nodes describing fire, flood, and steam vulnerabilities to the Safety Injection Pump Room which could lead to loss of Safety Injection. These nodes are doubletons with all of the nodes responsible for a seal LOCA.

The next location doubleton involves the loss of offsite power due to LOCAP and LOCCP with Service Water failures which result in the loss of onsite power.

The last two location doubletons involves LOCRP and LOCSP which are responsible for the failure of the power panels (and distribution panels). Losing the power panels will result in the loss of the three SIPs (they won't start) and the distribution panels which will cause 2 of the charging pumps to fail to start. The third charging pump is already running so it will continue to run. Therefore, this node is a doubleton with all nodes propagating failure to the third charging pump in order to cause the seal LOCA.

2.4.4.6 Front-Line, Support, Location Vulnerability and Operator Action: Case IV

There is no change in the singletons from Case 3 to Case 4.

As in previous System Combinations, the doubleton matrix is reduced in Case 4. The major sections which provide the reductions are in the support systems. The starting circuity for the charging pumps is no longer a singleton to a seal LOCA because an operator can attempt to restart the pumps.

Another set of doubletons which are removed from the matrix are the Safety Injection Actuation doubletons because an operator can start all necessary equipment manually.

The set of doubletons in the Electrical System which exist because of failures propagating to both the Unit Auxiliary Transformer and the Station Auxiliary Transformer are removed because the operator can start the gas turbines.

ENCLOSURE 4

SYSTEM COMBINATION 4

RCP SEALS INDUCED S2 LOCA WITH HIGH PRESSURE INJECTION

NO SINGLETONS

DOUBLETONS

```
                                              1 1 1 1 1 2 2 2 2 3 3 4 4 4 4 4 4 4 4 4 5
              1 1 1 2 2 2 3 3 3 4 4 4 4 8 9 9 0 0 2 3 3 1 2 2 2 6 9 2 3 3 3 3 5 5 5 5 6
    2 4 7 8 9 3 8 9 0 4 9 0 1 5 0 1 2 6 9 2 6 2 8 8 8 9 9 0 1 2 1 7 9 0 1 2 3 1 2 3 8 9

  2 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
  4 * - * * * * * * * * * * * * * * * * * * * * - - * - - - - - - - - - - - - - - - - -
  7 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
  8 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
  9 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 13 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 18 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 19 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 20 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 24 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 29 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 30 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 31 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 35 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 40 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 41 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 42 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 46 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 89 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 92 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
 96 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
102 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
108 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
128 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
138 - * - - - - - - - - - - - - - - - - - - - - - - - - - * * * - * - - - - - * * * - -
139 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
219 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
220 * - * * * * * * * * * * * * * * * * * * * * - - * - - - - - - - - - - - - - - - - -
221 * - * * * * * * * * * * * * * * * * * * * * - - * - - - - - - - - - - - - - - - - -
222 * - * * * * * * * * * * * * * * * * * * * * - - * - - - - - - - - - - - - - - - - -
361 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
397 * - * * * * * * * * * * * * * * * * * * * * - - * - - - - - - - - - - - - - - - - -
429 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
430 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
431 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
432 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
433 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
451 * - * * * * * * * * * * * * * * * * * * * * - - * - - - - - - - - - - - - - - - - -
452 * - * * * * * * * * * * * * * * * * * * * * - - * - - - - - - - - - - - - - - - - -
453 * - * * * * * * * * * * * * * * * * * * * * - - * - - - - - - - - - - - - - - - - -
458 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

```
FILE IDENTIFICATION
  REACH PAIR:   I=    1    J=    3
  DATE:  7/19/84
  ANSWER.POS FILE IS: DRO:SC4CRAYC3.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC4CRAYOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC4622MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC4622MRT.DAT
  SIGMA PI FILE NAME IS: DRO:SC4CRAYSI.C3
```

RCP SEALS INDUCED S2 LOCA WITH HIGH PRESSURE INJECTION

CASE I (CONTINUED)

VARIABLE LIST FOR SC4 CASE I DOUBLETON MATRIX

2	RCSLOCA
4	HPI-SLOCAD
7	BRGPLR31J
8	BRGMU31J
8	BOC31AZ
9	BRGML31J
9	BOC31BZ
13	PATHSWI31J
13	JPPP312J
13	VC251AJ
13	VC251JJ
13	JPPP311J
13	VC251EJ
13	VGL250AJ
13	PPI31J
13	VGA241AJ
13	PPR31J
13	ORFCFE144J
18	BRGPLR32J
19	BRGMU32J
19	BOC32AZ
20	BRGML32J
20	BOC32BZ
24	PATHSWI32J
24	JPPP322J
24	VC251BJ
24	VC251KJ
24	JPPP321J
24	VC251FJ
24	VGL250BJ
24	PPI32J
24	VGA241BJ
24	PPR32J
24	ORFCFE143J
29	BRGPLR33J
30	BRGMU33J
30	BOC33AZ
31	BRGML33J
31	BOC33BZ
35	PATHSWI33J
35	JPPP332J
35	VC251CJ
35	VC251LJ
35	JPPP331J
35	VC251GJ
35	VGL250CJ
35	PPI33J
35	VGA241CJ
35	PPR33J
35	ORFCFE116J
40	BRGPLR34J
41	BRGMU34J
41	BOC34AZ
42	BRGML34J
42	BOC34BZ
46	PATHSWI34J
46	JPPP342J
46	VC251DJ
46	VC251MJ
46	JPPP341J
46	VC251HJ
46	VGL250DJ
46	PPI34J
46	VGA241DJ
46	PPR34J
46	ORFCFE115J
89	JPPI32J
92	JPPI33J
96	JPPI34J
102	JPPCH3J
102	JPPCH2J
108	PPIP31J
108	VGL232J
108	VC8101J
108	JPPCP331J
108	JPPCP231J
108	JPP1J
108	PUMPCRG21J
108	JPPCP131J
108	VBUT278J
108	OTSC1J
108	SIGLOPT31J
108	CPOC31AZ
108	CPOC31BZ
108	JCP31L
108	J833AL
108	VGL833AL
108	VGL757AL
128	JPPCHI31J
138	AUTOCTZ
139	SWRLR31J
219	SIP31Z
219	ORFCR31A
219	VGA848AA
* 220	LFSIPD
* 221	LWSIPD
* 222	LSSIPD
361	J981A
361	J858AA
361	J1837A
361	J116A
361	J853AA
361	J852AA
361	J853CA
361	ORFC853A
397	BRC852BJ852AA
429	PPI850AA
430	MOV1902AA
431	MOV1901AA
432	VC849AA
433	JSIP31A
451	J1810D
452	J290AD
452	J200D
452	PPI846D
452	HTRC846ZD
452	VGA846D
452	HTRC846YD
452	PPR846D
452	RWST1D
458	J1819AD

* INDICATES LOCATION

ENCLOSURE 4

SYSTEM COMBINATION 4

RCP SEALS INDUCED S2 LOCA WITH HIGH PRESSURE INJECTION

COMBINED CASE II & CASE III RESULTS

CASE II FULLY AUTOMATIC FRONT-LINE AND SUPPORT SYSTEMS

CASE III FULLY AUTOMATIC FRONT-LINE, SUPPORT SYSTEMS, AND LOCATIONS

SINGLETONS

3	RCS	
1481	LOCDP	LOCATION (CASE III)

```
FILE IDENTIFICATTION
  REACH PAIR:   I=    1    J=    3
  DATE:  7/19/84
  ANSWER.POS FILE IS: DRO:SC4CRAYC3.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC4CRAYOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC4622MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC4622MRT.DAT
  SIGMA PI FILE NAME IS: DRO:SC4CRAYSI.C3
```

RCP SEALS INDUCED S2 LOCA WITH HIGH PRESSURE INJECTION

CASE II & III (CONTINUED)

VARIABLE LIST FOR SC4 CASE II & III DOUBLETON MATRIX

2	RCSLOCA
4	HPI-SLOCAD
7	BRGPLR31J
8	BRGMU31J
8	BOC31AZ
8	VGL775AL
8	JA46L
8	ORFC772ABL
8	VGA772AL
8	ORFC772AAL
9	BRGML31J
9	BOC31BZ
9	VGL776AL
9	ORFC612AL
9	FI612L
9	ORFC612BL
9	JA22L
9	ORFC773ABL
9	VGA773AL
9	ORFC773AAL
13	PATHSWI31J
13	JPPP312J
13	VC251AJ
13	VC251JJ
13	JPPP311J
13	VC251EJ
13	VGL250AJ
13	PPI31J
13	VGA241AJ
13	PPR31J
13	ORFCFE144J
18	BRGPLR32J
19	BRGMU32J
19	BOC32AZ
19	VGL775BL
19	JA51L
19	ORFC772BBL
19	VGA772BL
19	ORFC772BAL
20	BRGML32J
20	BOC32BZ
20	VGL776BL
20	ORFC615AL
20	FI615L
20	ORFC615BL
20	JA34L
20	ORFC773BBL
20	VGA773BL
20	ORFC773BAL
24	PATHSWI32J
24	JPPP322J

MATRIX TOO LARGE TO INCLUDE

SEE VOLUME I-B - ENCLOSURES

24	VC251BJ
24	VC251KJ
24	JPPP321J
24	VC251FJ
24	VGL250BJ
24	PPI32J
24	VGA241BJ
24	PPR32J
24	ORFCFE143J
29	BRGPLR33J
30	BRGMU33J
30	BOC33AZ
30	VGL775CL
30	JA54L
30	ORFC772CBL
30	VGA772CL
30	ORFC772CAL
31	BRGML33J
31	BOC33BZ
31	VGL776CL
31	ORFC618AL
31	FI618L
31	ORFC618BL
31	JA35L
31	ORFC773CBL
31	VGA773CL
31	ORFC773CAL
35	PATHSWI33J
35	JPPP332J
35	VC251CJ
35	VC251LJ
35	JPPP331J
35	VC251GJ
35	VGL250CJ
35	PPI33J
35	VGA241CJ
35	PPR33J
35	ORFCFE116J
40	BRGPLR34J
41	BRGMU34J
41	BOC34AZ
41	VGL775DL
41	JA47L
41	ORFC772DBL
41	VGA772DL
41	ORFC772DAL
42	BRGML34J
42	BOC34BZ
42	VGL776DL
42	ORFC621AL
42	FI621L
42	ORFC621BL
42	JA36L
42	ORFC773DBL
42	VGA773DL
42	ORFC773DAL
46	PATHSWI34J
46	JPPP342J
46	VC251DJ
46	VC251MJ

46	JPPP341J
46	VC251HJ
46	VGL250DJ
46	PPI34J
46	VGA241DJ
46	PPR34J
46	ORFCFE115J
84	PWRPNL31P
89	JPPI32J
92	JPPI33J
96	JPPI34J
102	JPPCH3J
102	JPPCH2J
108	PPIP31J
108	VGL232J
108	VC8101J
108	JPPCP331J
108	JPPCP231J
108	JPP1J
108	PUMPCRG31J
108	JPPCP131J
108	VBUT278J
108	OTSC1J
108	SIGLOPT31J
108	CPOC31AZ
108	CPOC31BZ
108	JCP31L
108	J833AL
108	VGL833AL
108	VGL757AL
128	JPPCHI31J
138	AUTOCTZ
139	SWRLR31J
219	SIP31Z
219	CON182252/SI1I
219	BS14SIP31OP
219	SENOTSSIP31OP
219	SWMOA11SIP31P
219	ORFCR31A
219	VGA848AA
220	LFSIPD
221	LWSIPD
222	LSSIPD
361	J981A
361	J858AA
361	J1837A
361	J116A
361	J853AA
361	J852AA
361	J853CA
361	ORFC853A
397	BRC852BJ852AA
429	PPI850AA
430	MOV1902AA
431	MOV1901AA
432	VC849AA
433	JSIP31A
434	CON3752/SI1I
434	RL3-15AI

435	CON2SIP310P
451	J1810D
452	J290AD
452	J200D
452	PPI846D
452	HTRC846ZD
452	VGA846D
452	HTRC846YD
452	PPR846D
452	RWST1D
453	TTRWSTH20D
458	J1819AD
569	JA14AL
569	JA14L
569	J830AL
569	JTIC627L
569	J627AL
570	PPR627AL
570	J749DL
570	J750AAL
570	VGL749DL
570	FIC634AL
570	JA58L
570	VC750AL
571	J830BL
571	J6273AL
571	J627BBL
571	J627BCL
572	VGA760AL
573	J1805L
574	PPR1805L
576	J760AL
577	BRC760AJ760BL
584	BRC760CJ760BL
587	VGA760CL
589	J760CL
591	PPR627BCL
591	J787L
593	JA57L
594	ORFC760CL
595	CCWP33L
599	JA55L
600	ORFC760AL
601	CCWP31L
602	ORFCCCW33L
603	VC761CL
604	JA3L
605	VGA762CL
607	J763BL
607	VGA759BL
607	JA8L
607	CCHXRS32Z
607	VGA765BL
607	J764BL
609	J762CL
610	BRC762CJ762BL
619	BRC762AJ762BL
620	ORFCCCW31L
621	VC761AL

623	VGA762AL
624	J763AL
624	VGA759AL
624	JA7L
624	CCHXRS31Z
624	JA10L
624	VGA765AL
624	J764AL
624	PPI765AL
626	J762AL
631	JA502L
631	J017BL
631	J601BL
631	J602BL
631	J602CL
634	J765BL
638	J017AL
638	J602AL
638	J601AL
638	J601CL
638	J601DL
639	J765AL
641	J601EL
641	J749AL
641	VGL749AL
641	PMP54L
641	J54AL
642	J602DL
643	J756CL
644	PPR602DL
644	JGFFDBL
644	J602EL
644	J769L
644	MOV769L
644	MOV797L
644	VC770L
644	JA33L
644	J734AL
644	JA33AL
645	BWCL54AZ
646	J750ADL
647	J54BL
648	BWCL54BZ
649	J54CL
650	SIPC31Z
651	J54DL
652	OCLSIP31Z
653	J750ACL
654	J750ABL
680	JA501AL
680	JA501L
681	PPRA501AL
681	JGFFDAL
681	JA501BL
681	JA501CL
682	JA501DL
682	MOV786L
682	MOV784L
682	J782L
682	JA20L

682	J734BL
682	JA21L
682	JA21AL
685	VGL734AL
686	PPRA21AL
686	J780CL
687	VGA780DL
687	J622L
687	J775DL
688	PPR730CL
688	VGA780CL
688	J619L
688	J775CL
689	JA21BL
690	VGA780BL
690	J616L
690	J775BL
691	PPRA21BL
691	VGA780AL
691	J613L
691	J775AL
692	PPRA33AL
692	J771CL
693	VGA771DL
693	J772DL
694	J773DL
695	PPR771CL
695	VGA771CL
695	J772CL
696	J773CL
697	J771AL
698	VGA771BL
698	J772BL
699	J773BL
700	PPR771AL
700	VGA771AL
700	J772AL
701	J773AL
703	J756AL
703	VGA756AL
703	J701AL
703	J757AL
771	J1190K
771	J98AK
771	J1093BK
771	J1093AK
772	VC98K
772	HTRC409K
772	J4K
772	J106BK
772	J409K
772	J1221K
772	HTRC98K
772	VB98K
786	RIVHUDSONK
787	STRCTRINTKK
793	SWPWELL1K
795	TRASH1K
797	J131K
801	J133K
802	J132BK
819	CHNLDSK
819	CHNLDS3K
819	J95AK
819	J95BK
821	J95CK
821	J95DK
827	J95FK
827	J1096AK
830	J1096BK
845	J1093DK
845	VB30K
845	J1095K
846	J1094K
860	COL-RW-2K
860	TTCOL1K
861	SW123456P
1084	PNLDIS31P
1084	BKRDPNL31P
1103	LG20F2SIA2AH
1109	LG10F2SIA2AH
1110	RSI1H
1111	RSI11XZ
1127	BKRSS5P
1127	XFMRSS5P
1127	BKR5AP
1127	R86SS5P
1127	OIBUS5AP
1129	BUS5P
1130	STAUXXFMRP
1172	SOURCE1P
1251	BUS5AP
1288	UVBUS5AP
1300	ITLBKR2AT5AP
1319	TTRCVR31P
1479	LOCAP
1480	LOCCP
1484	LOCRP
1485	LOCSP
1487	BKRSS5/P
1489	XFMRSS5/P
1490	BKR5A/P
1492	BUS5A/P
1674	PWRPNL31/P
1679	BKRDPNL31/P
1680	PNLDIS31/P
1730	CON913SI11XI
1734	RL27-5AX1I
1734	CON3527-5AX1I
1735	RL27-5AX4I
1735	CON3527-5AX4I
1736	RL27-5AX2I
1737	RL27-5AX3I

ENCLOSURE 4

SYSTEM COMBINATION 4

RCP SEALS INDUCED S2 LOCA WITH HIGH PRESSURE INJECTION

CASE IVA & IVB - MANUALLY ASSISTED

CASE IVA - MANUALLY ASSISTED, FAILURE BY COMMISSION

CASE IVB - MANUALLY ASSISTED, FAILURE BY OMMISSION AND FAILURE BY COMMISSION

SINGLETONS

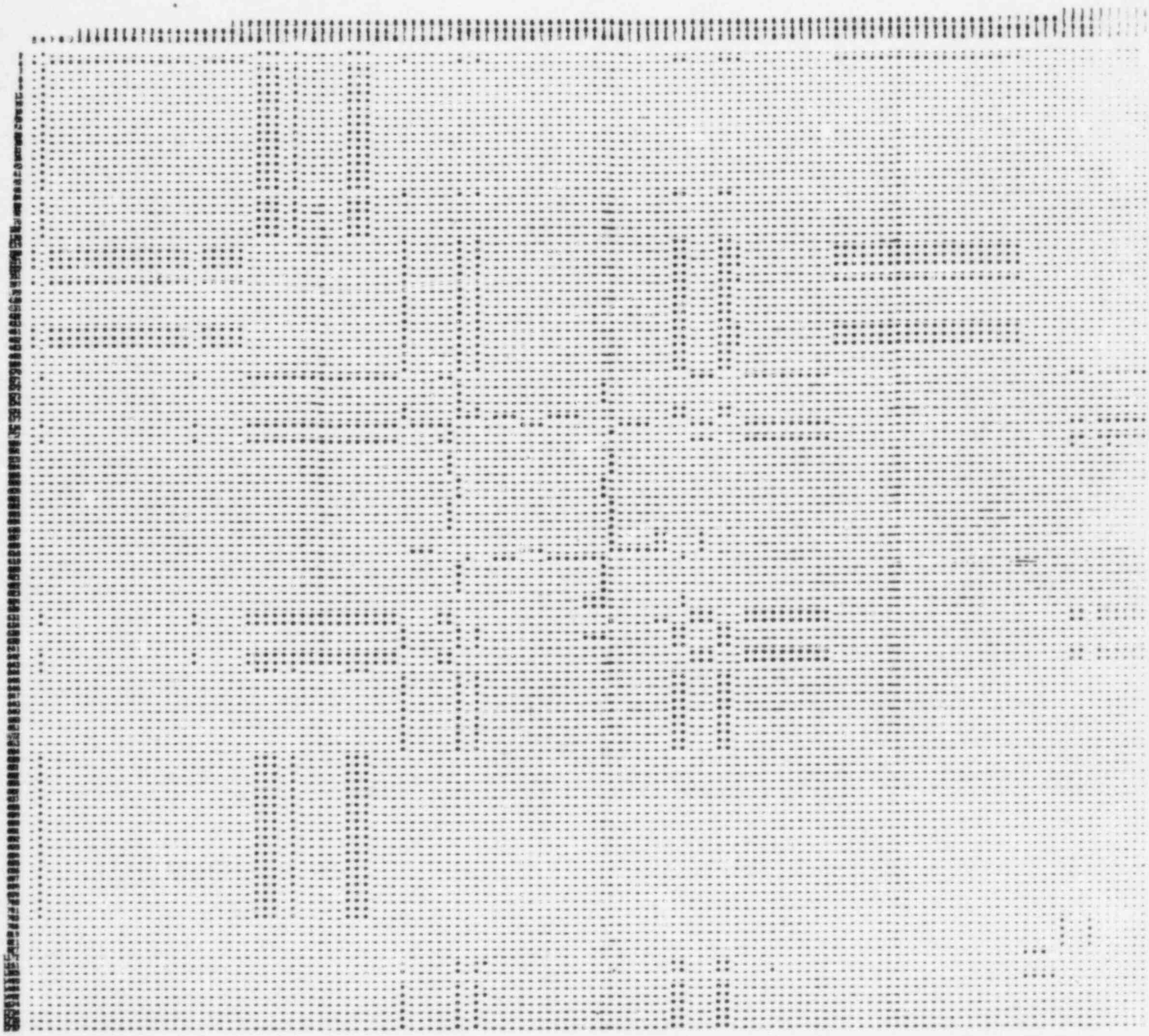
3	RCS
578	BRC760CJ760AL
611	BRC762CJ762AL
635	BRC765BJ765AL
1481	LOCDP
1729	TESTELECP

```
FILE IDENTIFICATION
  REACH PAIR:  I=    1    J=    3
  DATE:  7/20/84
  ANSWER.POS FILE IS: DR1:SC4CRAYC4.POS
  OUTPUT.DAT FILE IS: DR1:SC4CRAYOT.DAT
  VARIAB.DAT FILE IS: DR1:SC4622MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:SC4622MRT.DAT
  SIGMA PI FILE NAME IS: DR1:SC4CRAYSI.C4
```

RCP SEALS INDUCED S2 LOCA WITH HIGH PRESSURE INJECTION

CASE IVA * IVB - MANUALLY ASSISTED

DOUBLETONS



RCP SEALS INDUCED S2 LOCA WITH HIGH PRESSURE INJECTION

CASE IVA & IVB

VARIABLE LIST FOR SC4 CASE IVA & IVB DOUBLETON MATRIX

```
FILE IDENTIFICATION
  REACH PAIR:   I=    1    J=    3
  DATE:  7/20/84
  ANSWER.POS FILE IS: DR1:SC4CRAYC4.POS
  OUTPUT.DAT FILE IS: DR1:SC4CRAYOT.DAT
  VARIAB.DAT FILE IS: DR1:SC4622MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:SC4622MRT.DAT
  SIGMA PI FILE NAME IS: DR1:SC4CRAYSI.C4
```

2	RCSLOCA
4	HPI-SLOCAD
7	BRGPLR31J
8	BRGMU31J
8	BOC31AZ
8	VGL775AL
8	OPW775AL
8	JA46L
8	ORFC772ABL
8	VGA772AL
8	OPW772AL
8	ORFC772AAL
9	BRGML31J
9	BOC31BZ
9	VGL776AL
9	OPW776AL
9	ORFC612AL
9	FI612L
9	ORFC612BL
9	JA22L
9	ORFC773ABL
9	VGA773AL
9	OPW773AL
9	ORFC773AAL
13	PATHSWI31J
13	JPPP312J
13	VC251AJ
13	VC251JJ
13	JPPP311J
13	VC251EJ
13	VGL250AJ
13	PPI31J
13	VGA241AJ
13	PPR31J
13	ORFCFE144J
13	OPW250AJ
13	OPW241AJ
18	BRGPLR32J
19	BRGMU32J
19	BOC32AZ
19	VGL775BL
19	OPW775BL
19	JA51L
19	ORFC772BBL
19	VGA772BL
19	OPW772BL
19	ORFC772BAL
20	BRGML32J
20	BOC32BZ
20	VGL776BL
20	OPW776BL
20	ORFC615AL
20	FI615L
20	ORFC615BL
20	JA34L
20	ORFC773BBL

20	VGA773BL
20	OPW773BL
20	ORFC773BAL
24	PATHSWI32J
24	JPPP322J
24	VC251BJ
24	VC251KJ
24	JPPP321J
24	VC251FJ
24	VGL250BJ
24	PPI32J
24	VGA241BJ
24	PPR32J
24	ORFCFE143J
24	OPW250BJ
24	OPW241BJ
29	BRGPLR33J
30	BRGMU33J
30	BOC33AZ
30	VGL775CL
30	OPW775CL
30	JA54L
30	ORFC772CBL
30	VGA772CL
30	OPW772CL
30	ORFC772CAL
31	BRGML33J
31	BOC33BZ
31	VGL776CL
31	OPW776CL
31	ORFC618AL
31	FI618L
31	ORFC618BL
31	JA35L
31	ORFC773CBL
31	VGA773CL
31	OPW773CL
31	ORFC773CAL
35	PATHSWI33J
35	JPPP332J
35	VC251CJ
35	VC251LJ
35	JPPP331J
35	VC251GJ
35	VGL250CJ
35	PPI33J
35	VGA241CJ
35	PPR33J
35	ORFCFE116J
35	OPW250CJ
35	OPW241CJ
40	BRGPLR34J
41	BRGMU34J
41	BOC34AZ
41	VGL775DL
41	OPW775DL
41	JA47L
41	ORFC772DBL

41	VGA772DL
41	OPW772DL
41	ORFC772DAL
42	BRGML34J
42	BOC34BZ
42	VGL776DL
42	OPW776DL
42	ORFC621AL
42	FI621L
42	ORFC621BL
42	JA36L
42	ORFC773DBL
42	VGA773DL
42	OPW773DL
42	ORFC773DAL
46	PATHSWI34J
46	JPPP342J
46	VC251DJ
46	VC251MJ
46	JPPP341J
46	VC251HJ
46	VGL250DJ
46	PPI34J
46	VGA241DJ
46	PPR34J
46	ORFCFE115J
46	OPW250DJ
46	OPW241DJ
84	PWRPNL31P
89	JPPI32J
92	JPPI33J
96	JPPI34J
102	JPPCH3J
102	JPPCH2J
138	AUTOCTZ
219	SIP31Z
219	CON182252/SI1I
219	BS14SIP31OP
219	OPWSIP31A
219	SENOTSSIP31OP
219	SWMOA11SIP31P
219	ORFCR31A
219	VGA848AA
219	OPW848AA
220	LFSIPD
221	LWSIPD
222	LSSIPD
361	J981A
361	J858AA
361	J1837A
361	J116A
361	J853AA
361	J852AA
361	J853CA
361	ORFC853A
397	BRC852BJ852AA
429	PPI850AA
430	OPW1902AA

430	MOV1902AA
431	MOV1901AA
431	OPW1901AA
432	VC849AA
433	JSIP31A
451	J1810D
452	J290AD
452	J200D
452	PPI846D
452	HTRC846ZD
452	OPW846D
452	VGA846D
452	HTRC846YD
452	PPR846D
452	RWST1D
453	TTRWSTH20D
458	J1819AD
569	JA14AL
569	JA14L
569	J830AL
569	JTIC627L
569	J627AL
570	PPR627AL
570	J749DL
570	J750AAL
570	VGL749DL
570	OPW749DL
570	FIC634AL
570	JA58L
570	VC750AL
571	J830BL
571	J627BAL
571	J627BBL
571	J627BCL
572	VGA760AL
572	OPW760AL
573	J1805L
574	PPR1805L
576	J760AL
577	BRC760AJ760BL
584	BRC760CJ760BL
587	OPW760CL
587	VGA760CL
589	J760CL
591	PPR627BCL
591	J787L
593	JA57L
594	ORFC760CL
595	CCWP33L
599	JA55L
600	ORFC760AL
601	CCWP31L
602	ORFCCCW33L
603	VC761CL
604	JA3L
605	VGA762CL
605	OPW762CL
607	J763BL

607	VGA759BL
607	OPW759BL
607	JA8L
607	CCHXRS32Z
607	VGA765BL
607	OPW765BL
607	J764BL
609	J762CL
610	BRC762CJ762BL
619	BRC762AJ762BL
620	ORFCCCW31L
621	VC761AL
622	JA1L
623	VGA762AL
623	OPW762AL
624	J763AL
624	VGA759AL
624	OPW759AL
624	JA7L
624	CCHXRS31Z
624	JA10L
624	VGA765AL
624	OPW765AL
624	J764AL
624	PPI765AL
626	J762AL
631	JA502L
631	J017BL
631	J601BL
631	J602BL
631	J602CL
634	J765BL
638	J017AL
638	J602AL
638	J601AL
638	J601CL
638	J601DL
639	J765AL
641	J601EL
641	J749AL
641	VGL749AL
641	OPW749AL
641	PMP54L
641	J54AL
642	J602DL
643	J756CL
644	PPR602DL
644	JGFFDBL
644	J602EL
644	J769L
644	MOV769L
644	OPW769L
644	MOV797L
644	OPW797L
644	VC770L
644	JA33L
644	J734AL
644	JA33AL

645	BWCL54AZ
646	J750ADL
647	J54BL
648	BWCL54BZ
649	J54CL
650	SIPC31Z
651	J54DL
652	OCLSIP31Z
653	J750ACL
654	J750ABL
680	JA501AL
680	JA501L
681	PPRA501AL
681	JGFFDAL
681	JA501BL
681	JA501CL
682	JA501DL
682	MOV786L
682	OPW786L
682	MOV784L
682	OPW784L
682	J782L
682	JA20L
682	J734BL
682	JA21L
682	JA21AL
685	VGL734AL
685	OPW734AL
686	PPRA21AL
686	J780CL
687	VGA780DL
687	OPW780DL
687	J622L
687	J775DL
688	PPR780CL
688	VGA780CL
688	OPW780CL
688	J619L
688	J775CL
689	JA21BL
690	VGA780BL
690	OPW780BL
690	J616L
690	J775BL
691	PPRA21BL
691	VGA780AL
691	OPW780AL
691	J613L
691	J775AL
692	PPRA33AL
692	J771CL
693	VGA771DL
693	OPW771DL
693	J772DL
694	J773DL
695	PPR771CL
695	VGA771CL
695	OPW771CL
695	J772CL
696	J773CL
697	J771AL
698	VGA771BL
698	OPW771BL
698	J772BL
699	J773BL
700	PPR771AL
700	VGA771AL
700	OPW771AL
700	J772AL
701	J773AL
703	J756AL
703	VGA756AL
703	OPW756AL
703	J701AL
703	J757AL
786	RIVHUDSONK
819	CHNLDSK
819	CHNLDS3K
819	J95AK
819	J95BK
821	J95CK
821	J95DK
827	J95FK
827	J1096AK
1172	SOURCE1P
1251	BUS5AP
1288	UVBUS5AP
1480	LOCCP
1484	LOCRP
1492	BUS5A/P
1674	PWRPNL31/P
1734	RL27-5AX1I
1734	CON3527-5AX1I
1735	RL27-5AX4I
1735	CON3527-5AX4I
1737	RL27-5AX3I

2.4.5 Turbine Trip and Loss of Feedwater

2.4.5.1 Introduction

In this system combination, we searched for singleton and doubleton failures that would result in the loss of all feedwater given a turbine trip had occurred (for an unknown reason). The model size was over nine-thousand nodes. Figure 2-12 contains the support systems for Feedwater. They are; Safety Injection Actuation, Feedwater Isolation and Actuation, Control Oil, Electric, Instrument Air, and Service Water.

System Combinations 5 - 8 are qualitatively different from the other system combinations because of the longer time frames involved and the greater degree of operator involvement.

2.4.5.2 Failure Criteria of Individual Systems

The normal progress of this transient is reactor trip, turbine trip resulting from reactor trip, main feedwater trip, and then auxiliary feedwater actuation resulting from low-low steam generator level. This is followed by the operator taking control of the AFWS and secondary cooling.

Main Feedwater

Main feedwtaer is required during normal operation but is tripped off when the turbine trips. The entire main feedwater system and the main feedwater isolation system were modeled even though they were expected to immediately trip. By doing this, we were able to explore possible interactions between main and auxiliary feedwater. We found, however, that the main and auxiliary trains were independent.

Auxiliary Feedwater

The Auxiliary Feedwater system success depends on the start of one motor-driven or turbine-driven pump, in response to an automatic signal or operator action. The low-low steam generator level signal starts the automatic signal.

Secondary cooling is achieved by removing heat from the steam generator. This is done automatically or manually by opening a relief valve associated with a steam generator receiving auxiliary feedwater. Heat can also be removed by safeties, steam dumps to the main condenser if the MSIVs are not closed, or blowdown. Only the steam reliefs and safeties are modeled for secondary cooling since they are adequate.

Heat removal from the primary system can be provided by one steam generator. Given these conditions, the reactor core will be cooled by forced flow or by single or two-phase natural circulation to the steam generator.

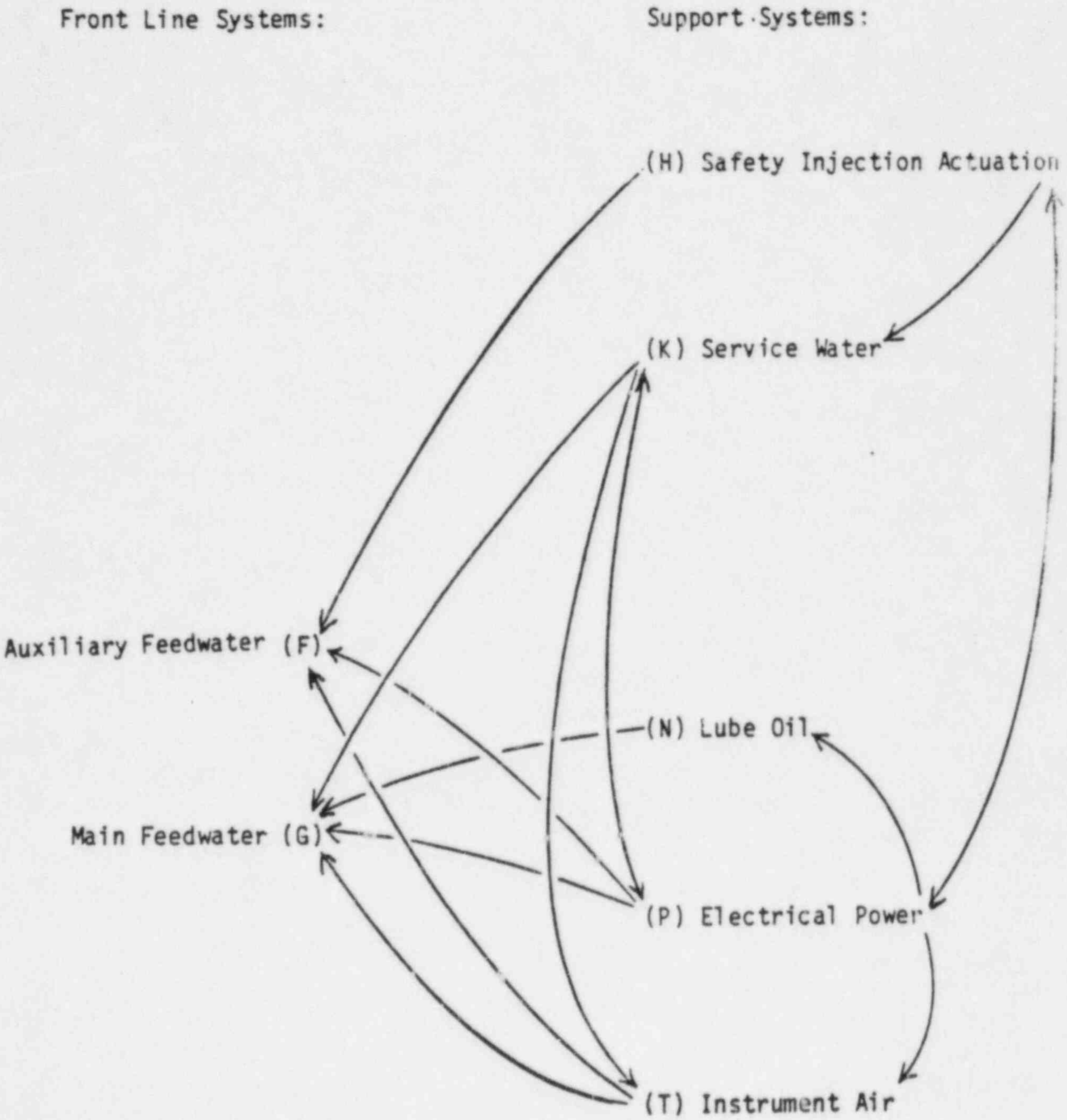
2.4.5.3 Results for Front-Line Systems: Case I

Enclosure 5 contains the results for system combination #5. In Case I, the front-line systems were considered in isolation (e.g., no support systems failures allowed) with no operation action allowed. The results

Figure 2-12

SYSTEM COMBINATION #5

Turbine Trip with Main and Auxiliary Feedwater



consisted of four singletons associated with the condensate storage tank (TANKCSTF), its header (HDR1072X1073F), and its valves (VGA69F and VBUT6F). The fact that no doubletons occurred is a demonstration of the robustness of the front-line trains when no support system failures are considered (e.g., probability of a support system failure is zero).

2.4.5.4 Results for Front-Line and Support Systems: Case II

In Case II, we consider the front-line and support systems working together (but without operator actions) and look for singleton or doubleton hardware failures that will fail them. The results for this case are the same as Case I. There were only five singletons (associated with the condensate storage tank) and there were no doubletons (other than those associated with test nodes which were used for quality assurance of the computer codes and models). These results show a qualitative robustness of the auxiliary feedwater system for this system combination.

2.4.5.5 Results for Front-Line and Support Systems with Location Vulnerabilities: Case III

In addition to the hardware failures for Cases I and III, there were four location vulnerabilities that were identified as singletons (LOC001, AFW pump room, LOC002, piping between AFW pump room and SGS, LOC003, Steam Generation in Containment Building, LOC004, area around condensate storage tank), and one location vulnerability (LOCDP, 480 V bus area) that recurred in the doubleton matrix. Location vulnerabilities did not imply initiating events or failures that cause a fire, flood, etc. They only indicate that should a fire, etc., occur and not be mitigated, that the entire location could be lost with failures of multiple trains.

It is interesting to note that should a fire or other external event occur in LOCDP, both AFW electric-driven pumps would be lost and the doubleton matrix shows what failures (nodes 307-401) could eliminate the AFW turbine driven pump (TURBPUMP32F, node 310).

2.4.5.6 Results for Front-Line and Support Systems with Location Vulnerabilities and Operator Actions: Case IV

In this case, we consider hardware failures, location vulnerabilities and operator actions. Operator actions include operators starting pumps, opening valves, bypassing failed components, actuating signals, and operators shutting valves, stopping pumps and turning off signals. The operator can cause failures by either failing to take a correct action (failure by omission) or by taking an incorrect action (failure by commission).

In this system combination, allowing the operator to act, allows him to open VGA49F and bring on the city water supply. As a result, the singletons associated with the condensate storage tank now become doubletons with failures associated with city water (H2OCITYF). This greatly improves system reliability. We identified two wrong operator actions in the doubleton matrix; OPWAF2TG, operator inadvertently trips

AF2TG which fails the AFW turbine driven pump, and OPRVGA49F, operator fails to oper VGA49F which fails the city water supply.

The probability results for Case IV show a dramatic improvement over earlier cases as a result of operator actions. Clearly for this system combination, the operator will contribute significantly to improving reliability.

ENCLOSURE 5

SYSTEM COMBINATION 5

TURBINE TRIP AND LOSS OF FEEDWATER

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

SINGLETONS

3	LOSSFEEDWATER
314	HDR1072X1073F
314	VGA64F
314	VBUT6F
314	TANKCSTF
* 314	LOC004

* INDICATES LOCATION

NO DOUBLETONS

```
FILE IDENTIFICATION
  REACH PAIR:   I=    1    J=    3
  DATE:  7/31/84
  ANSWER.POS FILE IS: DR0:SC5CRAYC3.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC5CRAYOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC5717MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC5717MRT.DAT
  SIGMA PI FILE NAME IS: DR0:SC5CRAYSI.C3
```

ENCLOSURE 5

SYSTEM COMBINATION 5

TURBINE TRIP AND LOSS OF FEEDWATER

COMBINED CASE II AND CASE III RESULTS

CASE II FULLY AUTOMATIC FRONT-LINE AND SUPPORT SYSTEMS

CASE III FULLY AUTOMATIC FRONTLINE, SUPPORT SYSTEMS, AND LOCATIONS

SINGLETONS

3	LOSSFEEDWATER	
314	HDR1072X1073F	
314	VGA64F	
314	VBUT6F	
314	TANKCSTF	
314	LOC004	LOCATIONS (CASE III)
409	LOC001	
410	LOC002	
411	LOC003	

DOUBLETONS

LOCATION (CASE III)

	2	4	307	310	316	331	332	333	334	335	400	401	869	1124	1445	1446	1761
2	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
307	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
310	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
316	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
331	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
332	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
333	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
334	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
335	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
400	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
401	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
LOCATION (CASE III) → 869	-	-	*	*	*	*	*	*	*	*	*	*	-	-	*	*	-
1124	-	-	*	*	*	*	*	*	*	*	*	*	-	-	*	*	-
1445	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
1446	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*
1761	-	-	*	*	*	*	*	*	*	*	*	*	-	-	*	*	-

TURBINE TRIP AND LOSS OF FEEDWATER

CASE II & III (CONTINUED)

VARIABLE LIST FOR SC5 CASE II & III DOUBLETON MATRIX

2	SG1
4	SG2
307	VC31F
310	PUMP32F
310	TURBPUMP32F
310	PCV1139F
310	SOV20-1AF
310	PPPUMPX1031F
310	VGL121F
310	VC122F
310	VGA125F
310	PP1080G
310	HDR123X124F
310	PP1030F
310	VTRIPTURBSTMF
310	TRIPOVERSPEEDF
310	HCV1118F
310	VGA54F
310	PCV1310BF
310	PCV1310AF
310	MAINSTEAMF
310	VGL124AF
310	VGL124F
310	PPTURBX1031AF
310	PPTURBX1031BF
310	LG3AF2G
310	LG2AF2G
310	LG1AF2G
310	LGB3AF2G
310	LGB2AF2G
310	LGB1AF2G
310	LGNOTAF2G
310	SWMAF2TG
316	VGA30F
316	VC29F
331	SW1-1T/ABFP2F
332	SOV20-2AF
333	SWL33-3F
334	SW1-2T/ABFP2F
335	SOV20-3AF
400	HDR1014F
400	HDR1005X1014F
401	HC1118F
* 869	LOCDP
1124	TESTELECP
1445	J1276BT
1446	J405T
1761	SCENE4

* INDICATES LOCATION

```
FILE IDENTIFICATION
 REACH PAIR:   I=    1    J=    3
 DATE:  7/31/84
 ANSWER.POS FILE IS: DRO:SC5CRAYC3.POS
 OUTPUT.DAT FILE IS: DR1:[220,1]SC5CRAYOT.TRP
 VARIAB.DAT FILE IS: DR1:[220,1]SC5717MVB.DAT
 RENUMSPT.DAT FILE IS: DR1:[220,1]SC5717MRT.DAT
 SIGMA PI FILE NAME IS: DRO:SC5CRAYSI.C3
```

ENCLOSURE 5

SYSTEM COMBINATION 5

TURBINE TRIP AND LOSS OF FEEDWATER

CASE IVA & IVB - MANUALLY ASSISTED, FAILURE BY OMMISSION

CASE IVA - MANUALLY ASSISTED, FAILURE BY OMMISSION

CASE IVB - MANUALLY ASSISTED, FAILURE BY OMMISSION AND FAILURE BY COMMISSION

SINGLETONS

	3	LOSSFEEDWATER
*	409	LOCO01
*	410	LOCO02
*	411	LOCO03

* INDICATES LOCATION

DOUBLETONS

CASE IVB FAILURE (OPERATOR ERROR) → 310

	2	4	307	310	313	314	317	400	869	1124	1780
2	-	*	-	-	-	-	-	-	-	-	-
4	*	-	-	-	-	-	-	-	-	-	-
307	-	-	-	-	-	-	-	-	*	*	-
310	-	-	-	-	-	-	-	-	*	*	-
313	-	-	-	-	-	*	-	-	-	-	-
314	-	-	-	-	*	-	*	-	-	-	*
317	-	-	-	-	-	*	-	-	-	-	-
400	-	-	-	-	-	-	-	-	*	*	-
869	-	-	*	*	-	-	-	*	-	-	-
1124	-	-	*	*	-	-	-	*	-	-	-

CASE IVB FAILURE (OPERATOR ERROR) → 310

TURBINE TRIP AND LOSS OF FEEDWATER

CASE IVA AND IVB

VARIABLE LIST FOR SC5 CASE IVA & IVB DOUBLETON MATRIX

2	SG1	310	PPTURBX1031BF
4	SG2	310	LG3AF2G
307	VC31F	310	LG2AF2G
310	PUMP32F	310	LG1AF2G
310	TURBPUMP32F	310	LGB3AF2G
310	PCV1139F	310	LGB2AF2G
310	SOV20-1AF	310	LGB1AF2G
310	PPPUMPX1031F	310	LGNOTAF2G
310	VGL121F	310	SWMAF2TG
310	VC122F	310	OPWAF2TG
310	VGA125F	313	HDR1076X1075F
310	PP1080G	314	HDR1072X1073F
310	HDR123X124F	314	VGA64F
310	PP1030F	314	VBUT6F
310	VTRIPTURBSTMF	314	TANKCSTF
310	TRIPOVERSPEEDF	* 314	LOC004
310	HCV1118F	317	VGA49F
310	VGA54F	317	H2OCITYF
310	PCV1310BF	317	OPRVGA49F
310	PCV1310AF	400	HDR1014F
310	MAINSTEAMF	400	HDR1005X1014F
310	VGL124AF	* 869	LOCDP
310	VGL124F	1124	TESTELECP
310	PPTURBX1031AF	1780	TRIPMASTER

* INDICATES LOCATION

```
FILE IDENTIFICATION
  REACH PAIR:  I=    1    J=    3
  DATE:  7/31/84
  ANSWER.POS FILE IS: DR0:SC5CRAYC4.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC5CRAYOT.DAT
  VARIAB.DAT FILE IS: DR1:[220,1]SC5717MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC5717MRT.DAT
  SIGMA PI FILE NAME IS: DR0:SC5CRAYSI.C4
```

2.4.6 Loss of Offsite Power and Loss of Feedwater

2.4.6.1 Introduction

In this system combination we have searched for singleton and doubleton failures that would cause loss of all feedwater given a Loss of Offsite Power (for an unknown reason). Figure 2-13 illustrates this case. The support systems are: Safety Injection Actuation, Feedwater Isolation and Actuation, Control Oil, Electric, Instrument Air, and Service Water.

2.4.6.2 Failure Criteria of Individual Systems

The failure (or success) criteria for the individual systems is given below: (See Section 2.2 for general system description and Appendix B for the associated P&IDs and digraphs.)

Main Feedwater
The normal progress of these transients is reactor trip, turbine trip resulting from reactor trip, main feedwater isolation and auxiliary feedwater actuation resulting from low-low steam generator level. This is followed by the operator taking control of the AFWS and secondary cooling.

Auxiliary Feedwater
The Auxiliary Feedwater system success depends on the start of one motor-driven or turbine-driven pump, in response to an automatic signal or operator action. The low-low steam generator level signal starts the automatic signal.

Secondary cooling is achieved by removing heat from the steam generator. This is done by automatically or manually opening a relief valve associated with a steam generator receiving auxiliary feedwater. Heat can also be removed by safeties, steam dumps to the main condenser if the MSIVs are not closed, or blowdown. Only the steam reliefs and safeties are modeled for secondary cooling since they are adequate.

Safety Injection Actuation System
It is assumed that whatever gave rise to the need for the feedwater systems also created the need for a safety injection signal. This system succeeds by sending actuation signals to many components such as pumps and valves which must change state to succeed.

Instrument Air System
The instrument air system succeeds by providing pressurized gas to air operated valves that must change state.

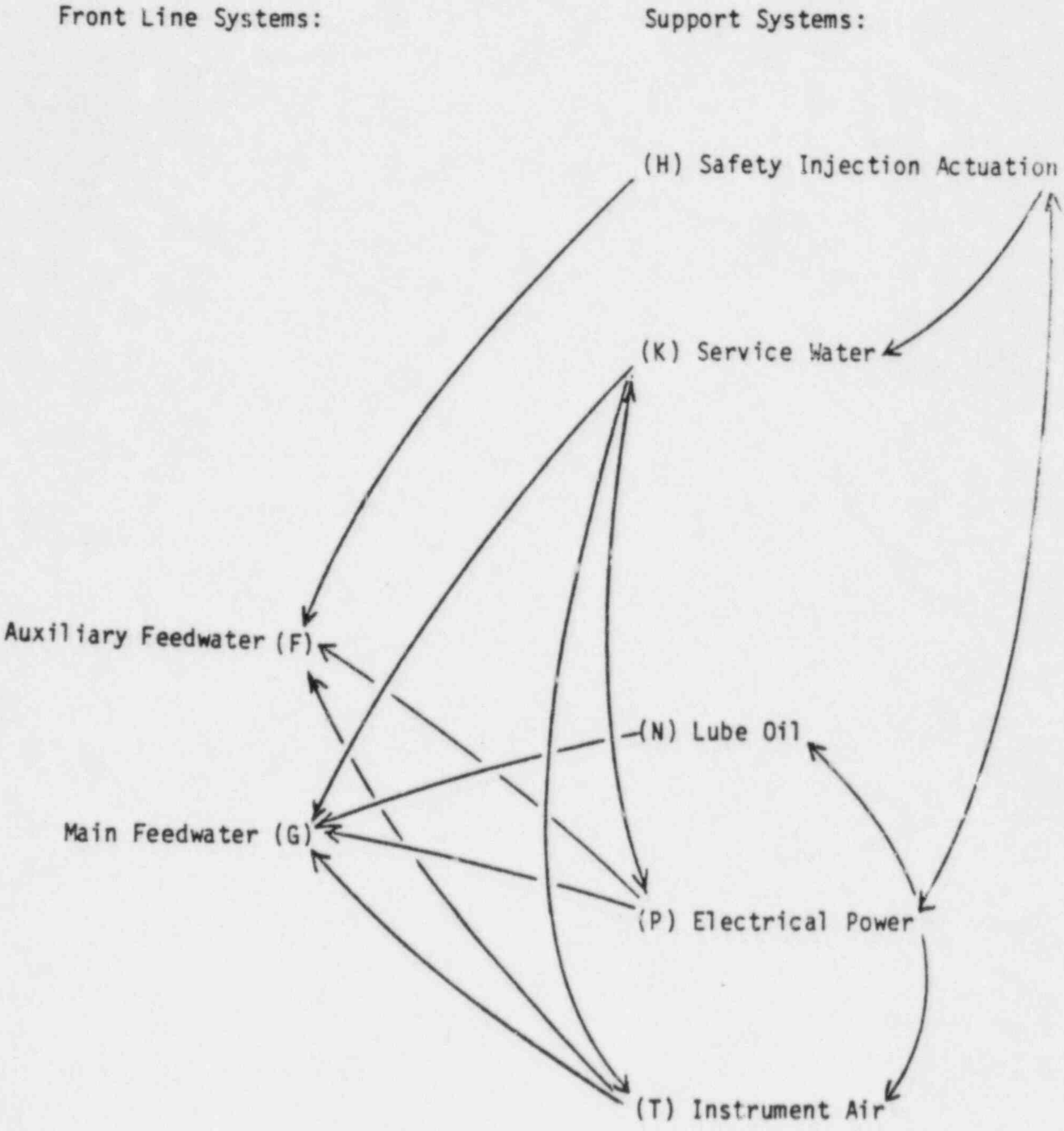
Service Water System
The service water system succeeds by cooling the instrument air compressors and the diesel generators.

Electric Power System
The electric power system succeeds by supplying the necessary high and low voltage ac and dc power needed by various components throughout the global system. For this system combination, the EPS is called upon to

Figure 2-13

SYSTEM COMBINATION #6

Loss of Offsite Power with Main and Auxiliary Feedwater



generate power from its diesel generators and, in some cases, its gas turbine generator.

2.4.6.3 Results for the Front-Line System Acting Alone: Case I

The four hardware singleton failures for this case are associated with the normal source of feedwater, the condensate storage tank. These four items are: HDR1072X1073F, a piping header to all three AFW pumps; VGA54F, a normally open gate valve; VBUT6F, a normally open butterfly valve; and TANKCSTF, the condensate storage tank.

2.4.6.4 Results for the Front-Line and Support Systems Acting Together: Case II

Once the support systems are considered with the front-line system, failures in the Service Water System (SWS), Electrical Power System (EPS), and Instrument Air System (IAS) can cause a system combination failure. No new singleton failures occur but many new doubletons arise that cause the failure of all three aux feed pumps. As shown in Enclosure 6, the support system doubletons are pairings of the following two groups of singletons: (A) those that cause both motor driven aux feed pumps to fail, and (B) those that cause the steam driven aux feed pump to fail.

The items in groups A and B are components whose failures result in the cutting of the power supplies to the respective pumps. For instance, the two motor driven pumps depend exclusively on two of the three diesel generators for their power. This arises from the constraints that no offsite power is available and that no operator action is allowed to bring on the gas turbines.

Group A contains items which cause at least two diesels to fail to generate power. Another group A failure keeps power generated by the diesels from reaching the pumps.

The steam driven pump, on the other hand, can fail from group B. There are valves on the path from MAINSTEAMF to the pump that require instrument air to remain open.

Group A: Singletons to Both Motor Driven Aux Feed Pumps

With no offsite power available and no operator intervention for this case, the plant receives its ac power from the three diesel generators. Thus, any hardware which could cause them to fail would also cause both motor driven aux feed pumps to fail. All of the hardware failures in group A arise from the dependence of the diesels on the SWS for cooling. As described in Section 2.2.12, the SWS draws cooling water from the Hudson River (RIVHUDSONK) and circulates it through various support system heat exchangers to effect heat removal. Under normal plant operation, there is no flow through the diesel generator exchangers. Air operated valves on the downstream side of them are energized closed and open automatically upon receipt of high diesel temperature or safety injection signal. Service water pumps can then move water through the cooling circuit, provided the rest of the circuit is open and the right set of pumps turns on. Without cooling flow, the diesels would fail in about 10 minutes, based on a rough estimate done for EBASCO by the diesel manufacturer, Alco.

Group A is comprised of piping junctions and other passive hardware and structures which, if they were to be blocked, would keep the diesel cooling circuit from being completed. There are also two butterfly valves (VB98K and VB30K) which are normally open but would cause a total blockage of cooling flow if they were inadvertently closed. These valves are in line with service water pumps 31-33 which are assumed to have been selected as "Essential". (See Section 2.3.9). If pumps 34-36 had been selected, there are other corresponding valves.)

Also in group A are items associated with assuring that the right set of SW pumps turns on in the event that diesel cooling is needed. A checkoff list (COL-RW-2K) and a mode select switch (SW123455P) are implemented to enable pumps 31-33 to turn on instead of pumps 34-36. Should a mistake be made in the checkoff list or if the switch is misaligned, the needed pumps would be shut off and the pumps which are not in line with the diesels would be turned on. A special node with no physical meaning, TTCOL1K, flags the fact that there is a lapse of time between the implementation of the checkoff list and the time of the accident. A third valve, VC98K, is a check valve just upstream of VB98K. Should it stick shut, it would prevent cooling to the diesels. These failure modes are detailed further in Section 2.3.9.

An additional group A failure, ITLBKR3AT6AP, is an electrical interlock in the EPS. A failure in this component could keep power generated by the diesels from reaching the motor driven aux feed pumps. One feed pump is powered by BUS6A and the other by BUS3A. The interlock connects to both of these buses and a short in the interlock mechanism could cause both buses to fail. This failure is discussed in more detail in Section 3.2.

Group B: Singletons to the Steam Driven Aux Feed Pump

The support system contribution to the failure of the steam driven aux feed pump arises from the need of two isolation valves in series to be open to permit steam to flow from MAINSTEAMF to the pump turbine. The air operated valves (PCV1310AF, PCV1310BF) normally are open but require instrument air to stay open. The pressurized air supply to the valves can come from either the instrument air compressors or from any of three standy bottles of pressurized nitrogen gas. The first supply could be unavailable, due to many of the group A failures. Those failures cause the loss of all three diesel generators, resulting in the failure of the motor driven feed pumps and the instrument air compressors. Failures of any but the following three items in group A result in the total loss of diesel generated power: electrical interlock ITLBKR3AT6AP and piping junctions J1096BK and J1094K. Each of the three items cause diesel generators 31 and 32 to be ineffective, disabling both electric aux feed pumps. This leaves diesel generator 33 to supply power to the IAS to enable the redundant supply to the nitrogen bottles.

Also captured in the model is the dependence of the IAS on the SWS for air compressor cooling. Many of the items in group A act to cause loss of the IAS not only due to diesel overheating, but also due to compressor overheating. Two of the three valves, VC98K and VB98K, that can cause loss of diesel function are also on a common cooling path to the IAS and can thus render it inoperative. The time delay associated with heating up the IAS cooling system is unknown but estimated by operators to be short term (on the order of 10 minutes. See Section 2.1.10). Upon failure of the compressors, any pressure that may have been stored in the IAS would rapidly decay. Thus, given almost any group A failure, the ONLY way for the one remaining aux feed pump to succeed is for the backup bottes of nitrogen to supply the needed pressure. The bottles do not require any support system to supply the pressure. An independent regulating valve on the path from each bottle opens to align the bottle with the IAS when the IAS pressure has dropped below 100 psi. Thus, the failures which can keep the gas from reaching the steam valve are all three regulating valves sticking shut or either of the two piping junctions in the IAS, J1276BT and J405T, being blocked or broken. J1276BT is the common junction of all three paths from the bottles and J405T is the junction of the nitrogen bottle and instrument air compressor supplies of pressure.

2.4.6.5 Results for the Front-Line and Support Systems Acting Together with Common Location Vulnerabilities

When common location information is considered, four singletons and numerous doubletons are added to the list of failure sets.

The four singletons are LOC001, 2, 3, 4. LOC001 is the location shared by all four steam generators. Failure of hardware in this location would obviously result in system failure. LOC002 is the space between containment and the AFW pump room. In this location is the piping and check valves for all four feedwater connections to the four steam generators. LOC003 is the AFW pump room which, with all three pumps and required pipes and valving, would also obviously cause system failure should its contents fail to operate. The last singleton location is LOC004, the location of the condensate storage tank, whose failure to supply feedwater due to a location coupled initiator would cause system failure.

The doubletons added by inclusion of location data are all based on the effects of the failure of hardware in LOCDP, the EPS 480 V switchgear area. In this shared location are the buses which supply power to the motor operated feedwater pumps and the instrument air compressors. How failure of this hardware impacts the aux feedwater system was discussed above.

There were no damaging initiators found in the locations included in the model. Presence of a location in a failure set doesn't imply that all of its hardware had to fail for the "location failure" to be made manifest. It reveals that combinations of hardware failures exist in that location which can contribute to system failure the same as does the single location node. The combinations can be extracted should the nature of the impact of the common location be of interest.

2.4.6.6 Results for the Front-Line and Support System with Common Location Vulnerabilities and Operator Action

When beneficial (OPR-) and detrimental (OPW-) operator actions are integrated into the system model, the number of singletons and doubletons are reduced significantly. In this system combination, ability of operators to act is restricted to the long term time frame which is on the order of 100 minutes or later (see Section 2.1.10).

Positive human intervention permits enabling of alternate paths around failed hardware. Because of this ability, all vulnerabilities posed by the SWS are gone. Many SWS based failures were founded on the effective single-trained configuration of that system in automatic mode (see Section 2.3.9). But since that system is a switchyard of pumps and valves, many alternate paths can be created to greatly increase the robustness of the entire global model.

The four singletons resulting from dependence on the condensate storage tank water supply also disappear. This is because of the ability of an operator to supply feedwater from city water. Thus, the four condensate storage tank singletons are now doubletons with city water (H2OCITY) and the beneficial operator action (OPRVGA49F) to open the valve (VGA49F) to the redundant supply (see Figure 2-X). Three location singletons remain, LOC001, 2, 3, which is to be expected since within them is the hardware vital to system success, as described in the previous section.

With the onsite electric supply not nearly as vulnerable as before, the only contributions of it to system failure are LOCDP (the shared location of the buses which supply power to the electric aux feed pumps) and the fictitious node TESTELECP which represents loss of all onsite power.

In this long term time frame, actions by operators are required to maintain onsite power generation. This is because the diesel generator short term fuel supply is depleted and filling of the day tanks requires operator intervention. The gas turbine generator can be used as a backup but it requires operator action to start. The requirement for some operator actions shows up in the doubleton matrix with the presence of the TRIPMASTER node. This node represents all beneficial human actions. It can be seen to be a doubleton with all of the hardware that disables the utility of the steam driven aux feed pump. This hardware includes valves and piping just upstream and downstream of it and the piping junctions from the nitrogen backup pressurized gas supply (group B hardware from Section 2.4.6.4). That pump alone can supply sufficient feedwater to the steam generators and it requires no electric power to run. Thus, the loss of onsite power generation due to operator inaction (TRIPMASTER=TRUE), while causing the two motor driven pumps to fail, will not by itself result in system combination failure.

Also captured in the model are detrimental operator actions or acts of commission. These are actions which can occur after the accident has begun and are, thus, considered distinct from erroneous maintenance, testing, or other operator action which make a component unavailable before the accident. Three actions show up in the doubleton matrix. All three are associated with making the steam driven pump ineffective. OPWAF2TG is an operator manually tripping the steam driven pump. Two other actions, OPWSWI-1TF and OPWSWI-2TF, are operator actions which close PCV1130F, a pressure control valve that is used to regulate the steam into the pump. With this valve shut, the supply of steam to the pump would be cut off.

ENCLOSURE 6

SYSTEM COMBINATION 6

TURBINE TRIP AND LOSS OF FEEDWATER WITH LOSS OF OFFSITE POWER

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

SINGLETONS

3	LOSSFEEDWATER
314	HDR1072X1073F
314	VGA64F
314	VBUT6F
314	TANKCSTF
* 314	LOC004

* INDICATES LOCATION

NO DOUBLETONS

```
FILE IDENTIFICATION
  REACH PAIR:  I=    1    J=    3
  DATE:  8/ 1/84
  ANSWER.POS FILE IS: DRO:SC6CRAYC3.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC6CRAYOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC6719MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC6719MRT.DAT
  SIGMA PI FILE NAME IS: DRO:SC6CRAYSI.C3
```

ENCLOSURE 6

SYSTEM COMBINATION 6

TURBINE TRIP AND LOSS OF FEEDWATER WITH LOSS OF OFFSITE POWER

COMBINED CASE II AND CASE III RESULTS

CASE II FULLY AUTOMATIC FRONT-LINE AND SUPPORT SYSTEMS

CASE III FULLY AUTOMATIC FRONT-LINE, SUPPORT SYSTEMS, AND LOCATIONS

SINGLETONS

3	LOSSFEEDWATER	
314	HDR1072X1073F	
314	VGA64F	
314	VBUT6F	
314	TANKCSTF	
314	LOC004	LOCATIONS (CASE III)
409	LOC001	
410	LOC002	
411	LOC003	

LOCATION (CASE III)

DOUBLETONS

	2	4	307	310	316	331	332	333	334	335	400	401	651	682	869	1124	1143	1149	1162	1163	1169	1171	1173	1174	1178	1179	1191	1204	1205	1207	1215	1219	1232	1233	1298	1299	1441	1442	1757	1759
2	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
307	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
310	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
316	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
331	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
332	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
333	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
334	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
335	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
400	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
401	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
651	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-
682	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-
869	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1124	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1143	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1149	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1162	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1163	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1169	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1171	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1173	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1174	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1178	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1179	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1191	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1204	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1205	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1207	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1215	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1219	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-
1232	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1233	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	-	-
1298	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1299	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1441	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	*	-	*	*	-	-	*	*
1442	-	-	-	-	-	-	-	-	-	-	-	-	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	-	-	*	*
1757	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-
1759	-	-	*	*	*	*	*	*	*	*	*	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-

TURBINE TRIP AND LOSS OF FEEDWATER WITH LOSS OF OFFSITE POWER

CASE II & III (CONTINUED)

VARIABLE LIST FOR SC6 CASE II & CASE III DOUBLETON MATRIX

2	SG1	310	LGB1AF2G	1174	J4K
4	SG2	310	LGNOTAF2G	1174	J409K
307	VC31F	310	SWMAF2TG	1174	J106BK
310	PUMP32F	316	VGA30F	1178	J133K
310	TURBPUMP32F	316	VC29F	1179	J132BK
310	PCV1139F	331	SW1-1T/ABFP2F	1191	J1221K
310	SOV20-1AF	332	SOV20-2AF	1204	CHNLDSK
310	PPPUMPX1031F	333	SWL33-3F	1205	CHNLDS3K
310	VGL121F	334	SW1-2T/ABFP2F	1205	J95AK
310	VC122F	335	SOV20-3AF	1205	J95BK
310	VGA125F	400	HDR1014F	1207	J95CK
310	PP1080G	400	HDR1005X1014F	1207	J95DK
310	HDR123X124F	401	HC1118F	1215	J95FK
310	PP1030F	651	ITLBKR3AT6AP	1215	J1096AK
310	VTRIPTURBSTMF	682	TTRCVR31P	1219	J1096BK
310	TRIPOVERSPEEDF	* 869	LOCDP	1232	J1093DK
310	HCV1118F	1124	TESTELECP	1232	VB30K
310	VGA54F	1143	J1190K	1232	J1095K
310	PCV1310BF	1143	J98AK	1233	J1094K
310	PCV1310AF	1143	J1093BK	1298	COL-RW-2K
310	MAINSTEAMF	1143	J1093AK	1298	TTCOL1K
310	VGL124AF	1149	VC98K	1299	SW123456P
310	VGL124F	1149	HTRC98K	1441	J1276BT
310	PPTURBX1031AF	1149	VB98K	1442	J405T
310	PPTURBX1031BF	1162	RIVHUDSONK	1757	SCENE2
310	LG3AF2G	1163	STRCTRINTKK	1757	TIMELONG
310	LG2AF2G	1169	SWPWELL1K	1759	SCENE4
310	LG1AF2G	1171	TRASH1K		
310	LGB3AF2G	1173	J131K		
310	LGB2AF2G	1174	HTRC409K		

* INDICATES LOCATION

```
FILE IDENTIFICATION
  REACH PAIR:   I=    1    J=    3
  DATE:  8/ 1/84
  ANSWER.POS FILE IS: DR0:SC6CRAYC3.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC6CRAYOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC6719MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC6719MRT.DAT
  SIGMA PI FILE NAME IS: DR0:SC6CRAYSI.C3
```

ENCLOSURE 6

SYSTEM COMBINATION 6

TURBINE TRIP AND LOSS OF FEEDWATER WITH LOSS OF OFFSITE POWER

CASE IVA & IVB - MANUALLY ASSISTED

CASE IVA - MANUALLY ASSISTED, FAILURE BY OMMISSION

CASE IVB - MANUALLY ASSISTED, FAILURE BY OMISSION AND FAILURE BY COMMISS

SINGLETONS

	3	LOSSFEEDWATER
*	409	LOC001
*	410	LOC002
*	411	LOC003

* INDICATES LOCATION

DOUBLETONS

CASE IVB FAILURE (OPERATOR ERROR)

		2	4	307	310	313	314	316	317	331	332	333	334	335	336	337	400	401	869	1124	1441	1442	1756	1758
	2	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	4	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	307	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*	*
FAILURE →	310	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*	*
BY	313	-	-	-	-	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
OPERATOR	314	-	-	-	-	*	-	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	316	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	317	-	-	-	-	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	331	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	332	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	333	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	334	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	335	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	336	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	337	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	400	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*	-	-	*	*
	401	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	869	-	-	*	*	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-	-
	1124	-	-	*	*	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-	-
	1441	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	1442	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*	*
	1756	-	-	*	*	-	*	*	-	*	*	*	*	*	*	*	*	*	-	-	*	*	-	-
	1758	-	-	*	*	-	*	*	-	*	*	*	*	*	*	*	*	*	-	-	*	*	-	-

ENCLOSURE 6

SYSTEM COMBINATION 6

TURBINE TRIP AND LOSS OF FEEDWATER WITH LOSS OF OFFSITE POWER

2	SG1
4	SG2
307	VC31F
310	PUMP32F
310	TURBPUMP32F
310	PCV1139F
310	SOV20-1AF
310	PPPUMPX1031F
310	VGL121F
310	VC122F
310	VGA125F
310	PP1080G
310	HDR123X124F
310	PP1030F
310	VTRIPTURBSTMF
310	TRIPOVERSPEEDF
310	HCV1118F
310	VGA54F
310	PCV1310BF
310	PCV1310AF
310	MAINSTEAMF
310	VGL124AF
310	VGL124F
310	PPTURBX1031AF
310	PPTURBX1031BF
310	LG3AF2G
310	LG2AF2G
310	LG1AF2G
310	LGB3AF2G
310	LGB2AF2G
310	LGB1AF2G
310	LGNOTAF2G
310	SWMAF2TG
310	OPWAF2TG
313	HDR1076X1075F
314	HDR1072X1073F
314	VGA64F
314	VBUT6F
314	TANKCSTF
* 314	LOC004
316	VGA30F
316	VC29F
317	VGA49F
317	H2OCITYF
317	OPRVGA49F
331	SW1-1T/ABFP2F
332	SOV20-2AF
333	SWL33-3F
334	SW1-2T/ABFP2F
335	SOV20-3AF
336	OPWSW1-1TF
337	OPWSW1-2TF
400	HDR1014F
400	HDR1005X1014F
401	HC1118F
* 869	LOCDP
1124	TESTELECP
1441	J1276BT
1442	J405T
1756	SCENE1
1756	TRIPMASTER
1758	SCENE3

* INDICATES LOCATION

```
FILE IDENTIFICATION
  REACH PAIR:   I=    1    J=    3
  DATE:  8/ 1/84
  ANSWER.POS FILE IS: DRO:SC6CRAYC4.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SC6CRAYOT.DAT
  VARIAB.DAT FILE IS: DR1:[220,1]SC6719MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC6719MRT.DAT
  SIGMA PI FILE NAME IS: DRO:SC6CRAYSI.C4
```

2.4.7 RCP Seal LOCA and Loss of Feedwater

2.4.7.1 Introduction

In this system combination we have searched for singleton and doubleton failures that would result in the loss of all feedwater and an RCP Seal LOCA. Figure 2-14 contains the support systems For Feedwater. They are: Safety Injection Actuation, Feedwater Isolation and Actuation, Control Oil, Electric, Instrument Air, and Service Water, RCP Seals, Chemical and Volume Control, and Component Cooling.

2.4.7.2 Failure Criteria of Individual Systems

Main Feedwater

The normal progress of these transients is reactor trip, turbine trip resulting from reactor trip, main feedwater isolation and auxiliary feedwater actuation resulting from low-low steam generator level. This is followed by the operator taking control of the AFWS and secondary cooling.

Auxiliary Feedwater

The Auxiliary Feedwater system success depends on the start of one motor-driven or turbine-driven pump, in response to an automatic signal or operator action. The low-low steam generator level signal starts the automatic signal.

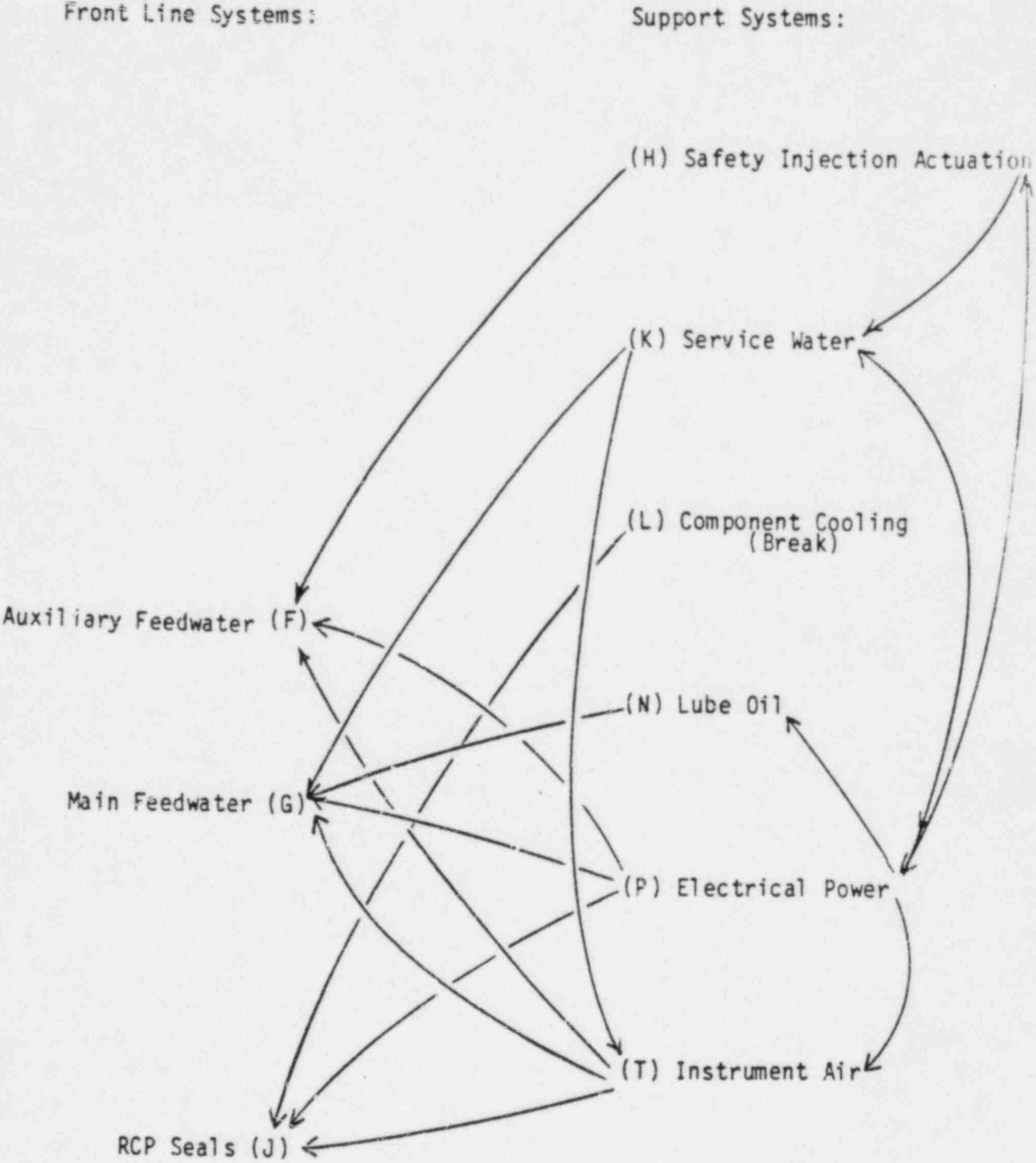
2.4.7.3 Results

See Enclosure 7 for the complete set of results and Section 4.7 for a discussion of components and probabilities.

Figure 2-14

SYSTEM COMBINATION #7

RCP Seals Induced S2 LOCA with Main and Auxiliary Feedwater



ENCLOSURE 7

SYSTEM COMBINATION 7

RCP SEAL LOCA WITH MAIN AND AUXILIARY FEEDWATER

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

NO SINGLETONS

DOUBLETONS

```
                                                                         1 1 2 2
                                               1 1 5 5 5 5 5 5 5 5 5 6 6 7 7 0 0
               1 1 . ! 2 2 3 3 3 4 4 4 4 8 9 9 0 3 5 6 6 6 8 8 8 8 8 5 5 4 4 6 6
     2 4 7 8 9 3 8 9 0 4 9 0 1 5 0 1 2 6 9 2 6 2 8 9 2 6 8 3 4 5 6 7 0 1 7 8 3 4

   2 - * * * * * * * * * * * * * * * * * * * * * * - - - - - - - - - - - - - * *
   4 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
   7 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
   8 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
   9 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  13 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  18 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  19 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  20 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  24 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  29 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  30 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  31 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  35 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  40 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  41 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  42 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  46 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  89 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  92 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
  96 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
 102 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
 138 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
 559 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
 562 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
 566 - * * * * * * * * * * * * * * * * * * * * * * - - - - - - - - - - - - - * *
 568 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
 583 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
 584 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
 585 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
 586 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
 587 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
 650 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
 651 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
1747 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
1748 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
2063 * - - - - - - - - - - - - - - - - - - - - - - - - * - - - - - - - - - - - -
2064 * - - - - - - - - - - - - - - - - - - - - - - * * * * * * * * * * * * * - -
```

```
FILE IDENTIFICATION
  REACH PAIR:   I=    1    J=    3
  DATE:  8/ 2/84
  ANSWER.POS FILE IS: DRO:SC7CRAYC3.POS
  OUTPUT.DAT FILE IS: DRO:SC7CRAYOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC7720MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC7720MRT.D
  SIGMA PI FILE NAME IS: DRO:SC7CRAYSI.C3
```

BREAK WITH MAIN AND AUXILIARY FEEDWATER

CASE I - FULLY AUTOMATIC - FRONT-LINE SYSTEMS ONLY

VARIABLE LIST FOR SC6 CASE I DOUBLETON MATRIX

2	LOSSFEEDWATER
4	RCSLOCA
7	BRGPLR31J
8	BRGMU31J
8	BOC31AZ
9	BRGML31J
9	BOC31BZ
13	PATHSWI31J
13	JPPP312J
13	VC251AJ
13	VC251JJ
13	JPPP311J
13	VC251EJ
13	VGL250AJ
13	PPI31J
13	VGA241AJ
13	PPR31J
13	ORFCFE144J
18	BRGPLR32J
19	BRGMU32J
19	BOC32AZ
20	BRGML32J
20	BOC32BZ
24	PATHSWI32J
24	JPPP322J
24	VC251BJ
24	VC251KJ
24	JPPP321J
24	VC251FJ
24	VGL250BJ
24	PPI32J
24	VGA241BJ
24	PPR32J
24	ORFCFE143J
29	BRGPLR33J
30	BRGMU33J
30	BOC33AZ
31	BRGML33J
31	BOC33BZ
35	PATHSWI33J
35	JPPP332J
35	VC251CJ
35	VC251LJ
35	JPPP331J
35	VC251GJ
35	VGL250CJ
35	PPI33J
35	VGA241CJ
35	PPR33J
35	ORFCFE116J
40	BRGPLR34J
41	BRGMU34J
41	BOC34AZ
42	BRGML34J
42	BOC34BZ
46	PATHSWI34J
46	JPPP342J
46	VC251DJ
46	VC251MJ
46	JPPP341J
46	VC251HJ
46	VGL250DJ
46	PPI34J
46	VGA241DJ
46	PPR34J
46	ORFCFE115J
89	JPPI32J
92	JPPI33J
96	JPPI34J
102	JPPCH3J
102	JPPCH2J
138	AUTOCTZ
559	VC31F
562	PUMP32F
562	TURBPUMP32F
562	PCV1139F
562	SOV20-1AF
562	PPPUMPX1031F
562	VGL121F
562	VC122F
562	VGA125F
562	PP1080G
562	HDR123X124F
562	PP1030F
562	VTRIPTURBSTMF
562	TRIPOVERSPEEDF
562	HCV1118F
562	VGA54F
562	PCV1310BF
562	PCV1310AF
552	MAINSTEAMF
562	VGL124AF
562	VGL124F
562	PPTURBX1031AF
562	PPTURBX1031BF
562	LG3AF2G
562	LG2AF2G
562	LG1AF2G
562	LGB3AF2G
562	LGB2AF2G
562	LGB1AF2G
562	LGNOTAF2G
562	SWMAF2TG
566	HDR1072X1073F
566	VGA64F
566	VBUT6F
566	TANKCSTF
568	VGA30F
568	VC29F
583	SW1-1T/ABFP2F
584	SOV20-2AF
585	SWL33-3F
586	SW1-2T/ABFP2F
587	SOV20-3AF
650	HDR1014F
650	HDR1005X1014F
651	HC1118F
1747	J1276BT
1748	J405T
2063	SCENE2
2063	TIMELONG
2064	SCENE4

ENCLOSURE 7

SYSTEM COMBINATION 7

BREAK WITH MAIN AND AUXILIARY FEEDWATER

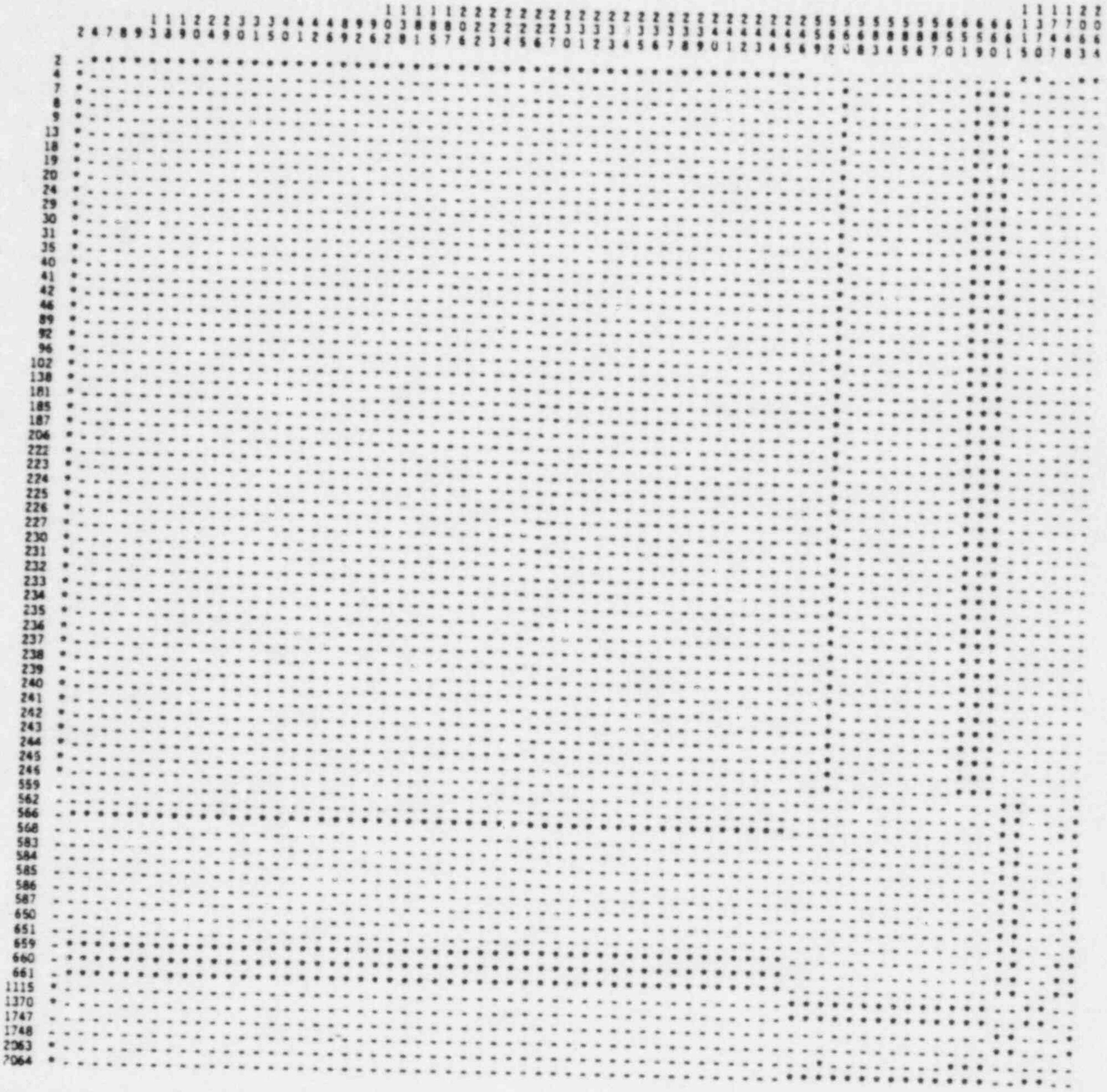
COMBINED CASE II & CASE III RESULTS

CASE II FULLY AUTOMATIC FRONT-LINE AND SUPPORT SYSTEMS

CASE III FULLY AUTOMATIC FRONT-LINE, SUPPORT SYSTEMS, AND LOCATIONS

NC SINGLETONS

```
FILE IDENTIFICATION
  DATE:  8/ 2/84
  ANSWER.POS FILE IS: DRO:SC7CRAYC3.POS
  OUTPUT.DAT FILE IS: DRO:SC7CRAYOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC7720MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC7720MRT.DAT
  SIGMA PI FILE NAME IS: DRO:SC7CRAYSI.C3
```



RCP SEALS INDUCED S2 LOCA WITH MAIN AND AUXILIARY FEEDWATER

CASE II & III

DOUBLETONS

BREAK WITH MAIN AND AUXILIARY FEEDWATER

CASE II & III (CONTINUED)

VARIABLE LIST FOR SC7 CASE II & III DOUBLETON MATRIX

2	TERMINAL
2	LOSSFEEDWATER
4	RCSLOCA
7	BRGPLR31J
8	BRGMU31J
8	BOC31AZ
6	VGL775AL
8	JA46L
8	ORFC772ABL
8	VGA772AL
8	ORFC772AAL
9	BRGML31J
9	BOC31BZ
9	VGL776AL
9	ORFC612AL
9	FI612L
9	ORFC612BL
9	JA22L
9	ORFC773ABL
9	VGA773AL
9	ORFC773AAL
13	PATHSWI31J
13	JPPP312J
13	VC251AJ
13	VC251JJ
13	JPPP311J
13	VC251EJ
13	VGL250AJ
13	PPI31J
13	VGA241AJ
13	PPR31J
13	ORFCFE144J
18	BRGPLR32J
19	BRGMU32J
19	BOC32AZ
19	VGL775BL
19	JA51L
19	ORFC772BBL
19	VGA772BL
19	ORFC772BAL
20	BRGML32J
20	BOC32BZ
20	VGL776BL
20	ORFC615AL
20	FI615L
20	ORFC615BL
20	JA34L
20	ORFC773BBL
20	VGA773BL
20	ORFC773BAL
24	PATHSWI32J
24	JPPP322J
24	VC251BJ
24	VC251KJ
24	JPPP321J
24	VC251FJ
24	VGL250BJ
24	PPI32J
24	VGA241BJ
24	PPP32J
24	ORFCFE143J
29	BRGPLR33J
30	BRGMU33J
30	BOC33AZ
30	VGL775CL
30	JA54L
30	ORFC772CBL
30	VGA772CL
30	ORFC772CAL
31	BRGML33J
31	BOC33BZ
31	VGL776CL
31	ORFC618AL
31	FI618L
31	ORFC618BL
31	JA35L
31	ORFC773CBL
31	VGA773CL
31	ORFC773CAL
35	PATHSWI33J
35	JPPP332J
35	VC251CJ
35	VC251LJ
35	JPPP331J
35	VC251GJ
35	VGL250CJ
35	PPI33J
35	VGA241CJ
35	PPR33J
35	ORFCFE116J
40	BRGPLR34J
41	BRGMU34J
41	BOC34AZ
41	VGL775DL
41	JA47L
41	ORFC772DBL
41	VGA772DL
41	ORFC772DAL
42	BRGML34J
42	BOC34BZ
42	VGL776DL
42	ORFC621AL
42	FI621L
42	ORFC621BL
42	JA36L
42	ORFC773DBL
42	VGA773DL
42	ORFC773DAL
46	PATHSWI34J
46	JPPP342J
46	VC251DJ
46	VC251MJ
46	JPPP341J
46	VC251HJ
46	VGL250DJ
46	PPI34J
46	VGA241DJ
46	PPR34J
46	ORFCFE115J
89	JPPI32J
92	JPPI33J
96	JPPI34J
102	JPPCH3J
102	JPPCH2J
138	AUTOCTZ
181	J830BL
181	J627BAL
181	J627BBL
181	J627BCL
181	J760CL
185	BRC760CJ760AL
187	BRC760CJ760BL
206	BRC762CJ762AL
222	J765BL
222	JA502L
222	J017BL
222	J601BL
222	J602BL
222	J602CL
222	J602DL
223	BRC765BJ765AL
224	J756CL
224	J756AL
224	VGA756AL
224	J701AL
224	J757AL
225	PPR602DL
225	JGFFDBL
225	J602EL
225	J769L
225	MOV769L
225	MOV797L
225	VC770L
225	JA33L
225	J734AL
225	JA33AL
226	JA501L
226	JA501AL
226	PPRA501AL
226	JGFFDAL
226	JA501BL
226	JA501CL
227	JA501DL
227	MOV786L
227	MOV784L
227	J782L
227	JA20L
227	J734BL
227	JA21L
227	JA21AL
230	VGL734AL
231	PPRA21AL
231	J780CL
232	VGA780DL
232	J622L
232	J775DL
233	PPR780CL
233	VGA780CL
233	J619L
233	J775CL
234	JA21BL
235	VGA780BL
235	J616L
235	J775BL
236	PPRA21BL
236	VGA780AL
235	J613L
236	J775AL
237	PPRA33AL
237	J771CL
238	VGA771DL
238	J772DL
239	J773DL
240	PPR771CL
240	VGA771CL
240	J772CL
241	J773CL
242	J771AL
243	VGA771BL
243	J772BL
244	J773BL
245	PPR771AL
245	VGA771AL
245	J772AL
246	J773AL
559	VC31F
562	PUMP32F
562	TURBPUMP32F
562	PCV1139F
562	SOV20-1AF
562	PPPUMPX1031F
562	VGL121F
562	VC122F
562	VGA125F
562	PP1080G
562	HDR123X124F
562	PP1030F
562	VTRIPTURBSTKF
562	TRIPOVERSPEEDF
562	HCV1118F
562	VGA54F
562	PCV1310BF
562	PCV1310AF
562	MAINSTEAMF
562	VGL124AF
562	VGL124F
562	PPTURBX1031AF
562	PPTURBX1031BF
562	LG3AF2G
562	LG2AF2G
562	LG1AF2G
562	LGB3AF2G
562	LGB2AF2G
562	LGB1AF2G
562	LGNOTAF2G
562	SWMAF2TG
566	HDR1072X1073F
566	VGA64F
566	VBUT6F
566	TANKCSTF
* 566	LOC004
568	VGA30F
568	VC29F
583	SW1-1T/ABFP2F
584	SOV20-2AF
585	SWL33-3F
586	SW1-2T/ABFP2F
587	SOV20-3AF
650	HDR1014F
650	HDR1005X1014F
651	HC1118F
* 659	LOC001
* 660	LOC002
* 661	LOC003
* 1115	LOCDP
1370	TESTELECP
1747	J1276BT
1748	J405T
2063	SCENE2
2063	TIMELONG
2064	SCENE4

* INDICATES LOCATION

FILE IDENTIFICATION
REACH PAIR: I= 1 J= 3
DATE: 8/ 2/84
ANSWER.POS FILE IS: DRO:SC7CRAYC3.POS
OUTPUT.DAT FILE IS: DRO:SC7CRAYOT.TRP
VARIAB.DAT FILE IS: DR1:[220,1]SC7720MV3.D
RENUMSRT.DAT FILE IS: DR1:[220,1]SC7720MRT
SIGMA PI FILE NAME IS: DRO:SC7CRAYSI.C3

ENCLOSURE 7

SYSTEM COMBINATION 7

BREAK WITH MAIN AND AUXILIARY FEEDWATER

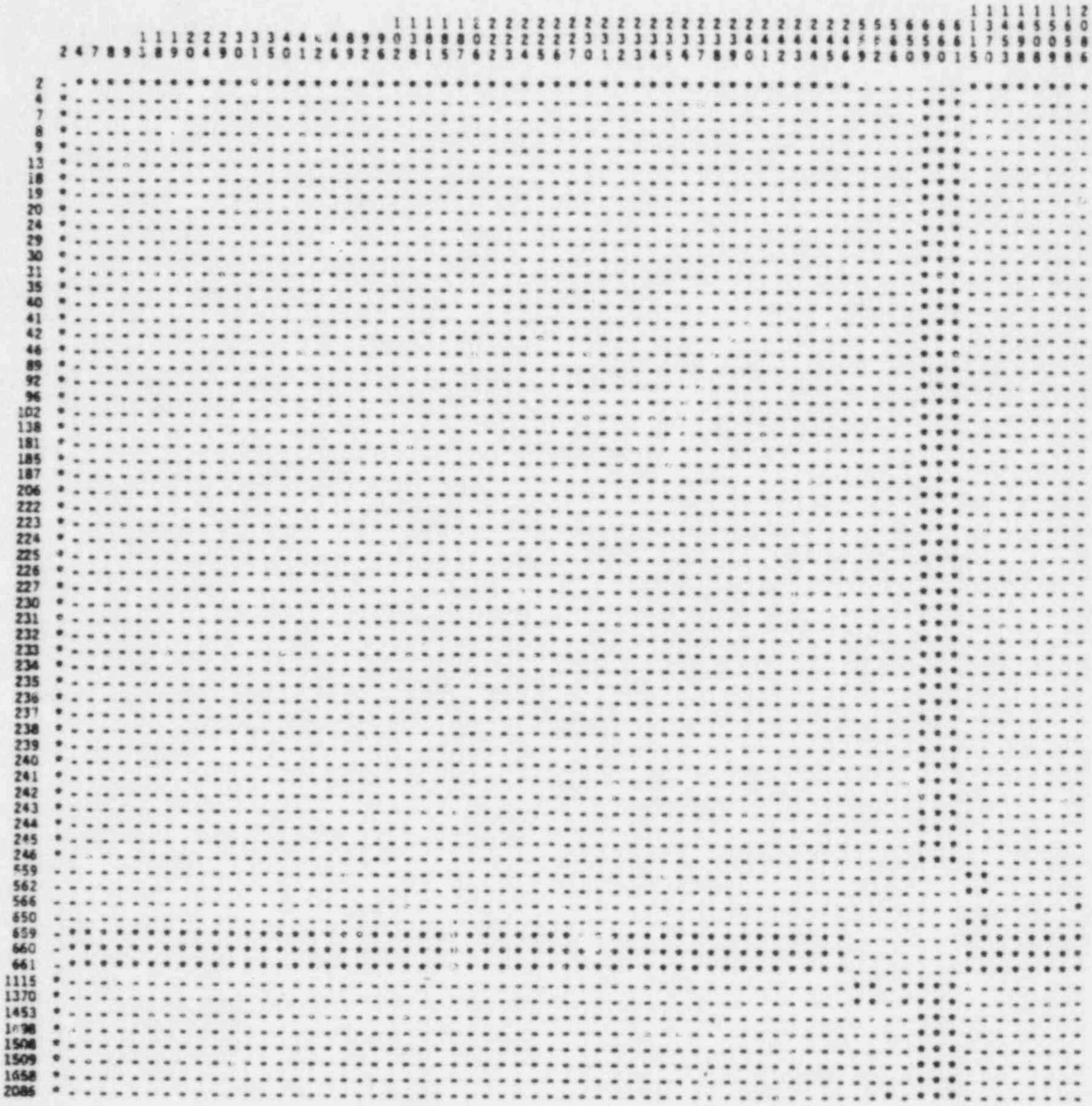
CASE IVA & IVB - MANUALLY ASSISTED

CASE IVA - MANUALLY ASSISTED, FAILURE BY OMISSION

CASE IVB - MANUALLY ASSISTED, FAILURE BY OMISSION AND FAILURE BY COMMISSION

NO SINGLETONS

```
FILE IDENTIFICATION
  REACH PAIR:   I=    1    J=    3
  DATE:  8/ 2/84
  ANSWER.POS FILE IS: DRO:SC7CRAYC4.POS
  OUTPUT.DAT FILE IS: DRO:SC7CRAYOT.DAT
  VARIAB.DAT FILE IS: DR1:[220,1]SC7720MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC7720MRT.DAT
  SIGMA PI FILE NAME IS: DRO:SC7CRAYSI.C4
```



RCP SEALS INDUCED S2 LOCA WITH MAIN AND AUXILIARY FEEDWATER

CASE IVA & IVB

DOUBLETONS

BREAK WITH MAIN AND AUXILIARY FEEDWATER

CASE IVA & IVB

VARIABLE LIST FOR SC7 CASE IVA & IVB DOUBLETON MATRIX

1	TERMINAL
2	LOSSFEEDWATER
4	RCSLOCA
7	BRGPLR31J
8	BRGMU31J
8	BOC31AZ
8	VGL775AL
8	OPW775AL
8	JA46L
8	ORFC772ABL
8	VGA772AL
8	OPW772AL
8	ORFC772AAL
9	BRGML31J
9	BOC31BZ
9	VGL776AL
9	OPW776AL
9	ORFC612AL
9	FI612L
9	ORFC612BL
9	JA22L
9	ORFC773ABL
9	VGA773AL
9	OPW773AL
9	ORFC773AAL
13	PATHSWI31J
13	JPPP312J
13	VC251AJ
13	VC251JJ
13	JPPP311J
13	VC251EJ
13	VGL250AJ
13	PPI31J
13	VGA241AJ
13	PPR31J
13	ORFCFE144J
13	OPW250AJ
13	OPW241AJ
18	BRGPLR32J
19	BRGMU32J
19	BOC32AZ
19	VGL775BL
19	OPW775BL
19	JA51L
19	ORFC772BBL
19	VGA772BL
19	OPW772BL
19	ORFC772BAL
20	BRGML32J
20	BOC32BZ
20	VGL776BL
20	OPW776BL
20	ORFC615AL
20	FI615L
20	ORFC615BL
20	JA34L
20	ORFC773BBL
20	VGA773BL
20	OPW773BL
20	ORFC773BAL
24	PATHSWI32J
24	JPPP322J
24	VC251BJ
24	VC251KJ
24	JPPP321J
24	VC251FJ
24	VGL250BJ
24	PPI32J
24	VGA241BJ
24	PPR32J
24	ORFCFE143J
24	OPW250BJ
24	OPW241BJ
29	BRGPLR33J
30	BRGMU33J
30	BOC33AZ
30	VGL775CL
30	OPW775CL
30	JA54L
30	ORFC772CBL
30	VGA772CL
30	OPW772CL
30	ORFC772CAL
31	BRGML33J
31	BOC33BZ
31	VGL776CL
31	OPW776CL
31	ORFC618AL
31	FI618L
31	ORFC618BL
31	JA35L
31	ORFC773CBL
31	VGA773CL
31	OPW773CL
31	ORFC773CAL
35	PATHSWI33J
35	JPPP332J
35	VC251CJ
35	VC251LJ
35	JPPP331J
35	VC251GJ
35	VGL250CJ
35	PPI33J
35	VGA241CJ
35	PPR33J
35	ORFCFE116J
35	OPW250CJ
35	OPW241CJ
40	BRGPLR34J
41	BRGMU34J
41	BOC34AZ
41	VGL775DL
41	OPW775DL
41	JA47L
41	ORFC772DBL
41	VGA772DL
41	OPW772DL
41	ORFC772DAL
42	BRGML34J
42	BOC34BZ
42	VGL776DL
42	OPW776DL
42	ORFC621AL
42	FI621L
42	ORFC621BL
42	JA36L
42	ORFC773DBL
42	VGA773DL
42	OPW773DL
42	ORFC773DAL
46	PATHSWI34J
46	JPPP342J
46	VC251DJ
46	VC251MJ
46	JPPP341J
46	VC251HJ
46	VGL250DJ
46	PPI34J
46	VGA241DJ
46	PPR34J
46	ORFCFE115J
46	OPW250DJ
46	OPW241DJ
89	JPPI32J
92	JPPI33J
96	JPPI34J
102	JPPCH3J
102	JPPCH2J
138	AUTOCTZ
181	J830BL
181	J627BAL
181	J627BBL
181	J627BCL
181	J760CL
185	BRC760CJ760AL
187	BRC760CJ760BL
206	BRC762CJ762AL
222	J765BL
222	JA502L
222	J017BL
222	J601BL
222	J602BL
222	J602CL
222	J602DL
223	BRC765BJ765AL
224	J756CL
224	J756AL
224	VGA756AL
224	OPW756AL
224	J701AL
224	J757AL
225	PPR602DL
225	JGFFDBL
225	J602EL
225	J769L
225	MOV769L
225	OPW769L
225	MOV797L
225	OPW797L
225	VC770L
225	JA33L
225	J734AL
225	JA33AL
226	JA501L
226	JA501AL
226	PPRA501AL
226	JGFFDAL
226	JA501BL
226	JA501CL
227	JA501DL
227	MOV786L
227	OPW786L
227	MOV784L
227	OPW784L
227	J782L

BREAK WITH MAIN AND AUXILIARY FEEDWATER

VARIABLE LIST FOR SC7 CASE IVA & IVB DOUBLETON MATRIX (CONTINUED)

227	JA20L
227	J734BL
227	JA21L
227	JA21AL
230	VGL734AL
230	OPW734AL
231	PPRA21AL
231	J720CL
232	VGA780DL
232	OPW780DL
232	J622L
232	J775DL
233	PPR780CL
233	VGA780CL
233	OPW780CL
233	J619L
233	J775CL
234	JA21BL
235	VGA780BL
235	OPW780BL
235	J616L
235	J775BL
236	PPRA21BL
236	VGA780AL
236	OPW780AL
236	J613L
236	J775AL
237	PPRA33AL
237	J771CL
238	VGA771DL
238	OPW771DL
238	J772DL
239	J773DL
240	PPR771CL
240	VGA771CL
240	OPW771CL
240	J772CL
241	J773CL
242	J771AL
243	VGA771BL
243	OPW771BL
243	J772BL
244	J773BL
245	PPR771AL
245	VGA771AL
245	OPW771AL
245	J772AL
246	J773AL
559	VC31F
562	PUMP32F
562	TURBPUMP32F
562	PCV1139F
562	SOV20-1AF
562	PPPUMPX1031F
562	VGL121F
562	VC122F
562	VGA125F
562	PP1080G
562	HDR123X124F
562	PP1030F
562	VTRIPTURBSTMF
562	TRIPOVERSPEEDF
562	HCV1118F
562	VGA54F
562	PCV1310BF
562	PCV1310AF
562	MAINSTEAMF
562	VGL124AF
562	VGL124F
562	PPTURBX1031AF
562	PPTURBX1031BF
562	LG3AF2G
562	LG2AF2G
562	LG1AF2G
562	LGB3AF2G
562	LGB2AF2G
562	LGB1AF2G
562	LGNOTAF2G
562	SWMAF2TG
562	OPWAF2TG
566	HDR1072X1073F
566	VGA64F
566	VBUT6F
566	TANKCSTF
* 566	LOC004
650	HDR1014F
650	HDR1005X1014F
* 659	LOC001
* 660	LOC002
* 661	LOC003
* 1115	LOCDP
1370	TESTELECP
1453	RIVHUDSONK
1498	JDEGRK
1498	J410K
1498	J1237K
1498	J390K
1498	J263K
1498	J1271K
1508	CHNLDSK
1509	CHNLDS3K
1509	J95AK
1658	SWSMASTER
2086	TRIPMASTER

* INDICATES LOCATION

2.4.8 PORV LOCA and Loss of Feedwater

2.4.8.1 Introduction

In this system combination we searched for singleton and doubleton failures that would result in the loss of all feedwater given a turbine trip had occurred (for an unknown reason) and failure to shut (or isolate) the PORV. Figure 2-15 contains the support systems. They are: Safety Injection Actuation, Feedwater Isolation and Actuation, Control Oil, Electric, Instrument Air, and Service Water.

2.4.8.2 Failure Criteria of Individual Systems

The failure (or success) criteria for the individual systems is given below: (See Section 2.2 for general system description and Appendix B for the associated P&IDs and digraphs.)

Main Feedwater

The normal progress of these transients is reactor trip, turbine trip resulting from reactor trip, main feedwater isolation and auxiliary feedwater actuation resulting from low-low steam generator level. This is followed by the operator taking control of the AFWS and secondary cooling.

Auxiliary Feedwater

The Auxiliary Feedwater system success depends on the start of one motor-driven or turbine-driven pump, in response to an automatic signal or operator action. The low-low steam generator level signal starts the automatic signal.

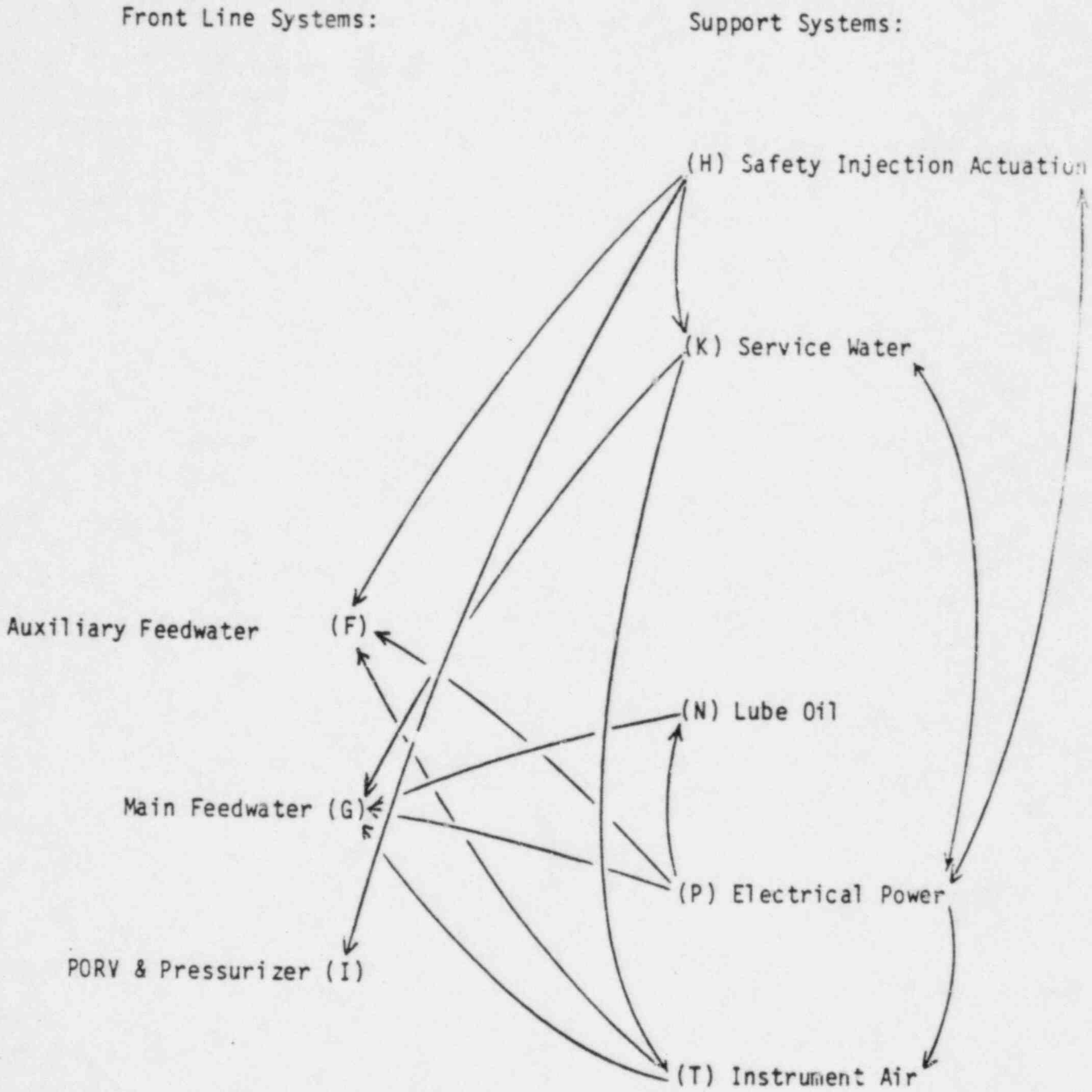
2.4.8.3 Results

See Enclosure 8 for the complete set of results and Section 4.8 for a discussion of components and probabilities.

Figure 2-15

SYSTEM COMBINATION #8

PORV Induced S2 LOCA with Main and Auxiliary Feedwater



ENCLOSURE 8

SYSTEM COMBINATION 8

PORV LOCA AND LOSS OF FEEDWATER

CASE I, II AND III - FULLY AUTOMATIC

NO SINGLETONS

DOUBLETONS

```
             3
             7
     2 4 7 8 3

  2  - * * * -
  4  * - - - *
  7  * - - - *
  8  * - - - *
373  - * * * -
```

```
FILE IDENTIFICATION
  REACH PAIR:   I=    1    J=    3
  DATE:  8/15/84
  ANSWER.POS FILE IS: DRO:SC8CRAYC3.POS
  OUTPUT.DAT FILE IS: DRO:SC8CRAYOT.TRP
  VARIAB.DAT FILE IS: DR1:[220,1]SC8722MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SC8722MRT.DAT
  SIGMA PI FILE NAME IS: DRO:SC87CRAYSI.C3
```

PORV LOCA WITH LOSS OF FEEDWATER

CASE I, II AND III - FULLY AUTOMATIC

VARIABLE LIST FOR SC8 CASE I, II AND III DOUBLETON MATRIX

2	TERMINAL
2	LOSSFEEDWATER
4	PRIBREACHI
4	PCV464I
4	PCV466I
4	PCV468I
4	VSPNG464I
4	VSTEM464I
4	VSPNG466I
4	VSTEM466I
4	VSPNG468I
4	VSTEM468I
6	PCV455CI
6	SOV455CI
6	VDPHM455CI
6	VSTEM455CI
6	VSPNG455CI
8	PCV456I
8	SOV456I
8	VDPHM456I
8	VSTEM456I
8	VSPNG456I
373	HDR1072X1073F
373	VGA64F
373	VBUT6F
373	TANKCSTF

SYSTEM COMBINATION # 8

CASE IV MANUAL

```
 ***unsuppressed singletons***
         3     rcs
1     ***doubletons***

the doubleton array has dimension     5

         2    4  468  469  47Ø
    2    -   *    -    -    -
    4    *    -    *    *    *
  468    -   *    -    -    -
  469    -   *    -    -    -
  47Ø    -   *    -    -    -
         2    4  468  469  47Ø

           -----------------------------
```

USE SAME VARIABLE LIST AS SC#8 AUTOMATIC

2.4.9 Large LOCA and Loss of Low Pressure Recirculation

2.4.9.1 Introduction

Figure 2-16 illustrates how a core melt could result if the Low Pressure Recirculation system should fail during a large LOCA. The singletons and doubletons in this System Combination are those which could prevent sufficient operation of the LPR system. The support systems consist of Electrical, Component Cooling, and Service Water.

2.4.9.2 Failure Criteria of Individual Systems

Low Pressure Recirculation System
For a large LOCA, either one out of two recirculation pumps (preferred) or one out of two RHR pumps are required to deliver sufficient flow to the RCS.

Electrical System
The electrical system is required to open the motor-operated valves and to run the pumps for Low Pressure Recirculation.

Component Cooling System
In addition to cooling the pumps during the recirculation mode, the CCW system is resposible for the heat removal of the recirculation water.

Service Water System
The Service Water system is used to remove heat from the diesels. In addition, the Service Water system removes heat from the Component Cooling system.

2.4.9.3 Results: Cases I, II, and III

There are no automatic runs in this System Combination since operators are required to initiate Low Pressure Recirculation.

2.4.9.4 Results of Front-Line with Support Location and Operator Intervention: Case IV

Nodes 23 (SOURCE) and 1001 (TESTELECP) are test nodes for the Component Cooling and Electrical systems respectively.

Node 2 (RHXRCOOLD) is a node which represents the lack of cooling to the Residual Heat Exchangers.

There are five "break nodes" which act as singletons to this System Combination. The first two (99-BRC899BJ899AB and 137-BRC889J1869BD), are breaks at the header by MOV899A/B and by the output of the RHXRs respectively.

The last three "break nodes" are at headers in the Component Cooling system (intake to CCW pumps, output of CCW pumps, and output of CCW Heat Exchangers).

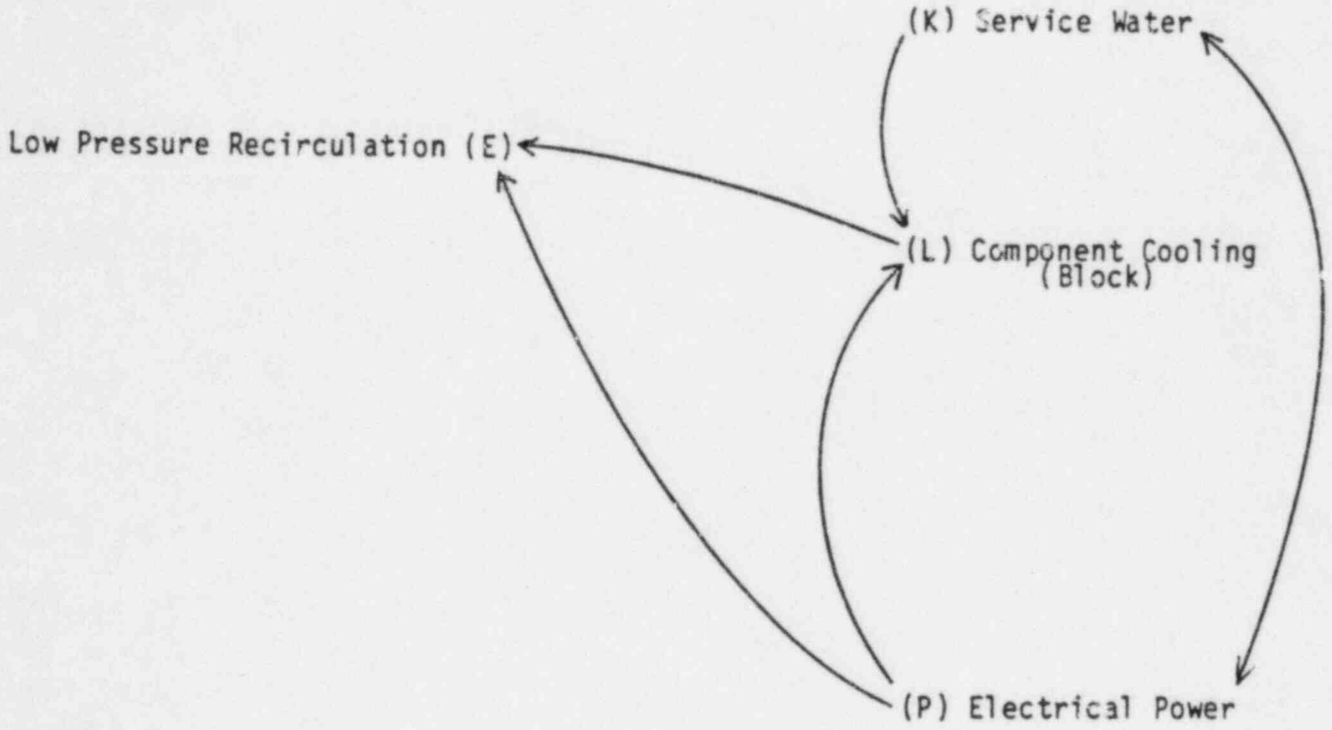
All five breaks represent double ended breaks on the outside of the isolation valves yielding unmitigatable output of water.

Figure 2-16

SYSTEM COMBINATION #9

Large LOCA with Low Pressure Recirculation

Front Line Systems: Support Systems:



Location nodes within the front-line LPR system include only fire, flood and steam vulnerabilities in the Residual Heat Exchanger Room represented by 102-LFRHXRB, 103-LSRHXRB, and 104-LWRHXRB.

The only other singleton location is 750-LOCDP which is the Control Room. Since this location could yield a failure of all of the buses, the recirculation pumps and Residual Heat Removal pump are also vulnerable.

Node 1360 (TRIPMASTER) is a master node which is connected to all operators in the model. Failure of this node means complete automatic operating.

The rest of the singletons are from the Service Water system and includes the piping from the output of the Component Cooling Heat Exchangers to the discharge channel in the Hudson River. If this piping should get blocked, there would be no method for removing heat from the Component Cooling Heat Exchangers.

SWSMASTER is a node connected to all operators in the Service Water system. With these operators disabled, it is not possible to get coolant to the Component Cooling HXRs from the normal operating node of SWS.

The doubletons in Block "A" (see Enclosure 9.4) represent front-line doubletons alone. These consist of two separate sections of double-trained flow. The first section exists because flow can come from either the recirculation sump (utilyzing the recirculation pumps) or the containment sump (with the RHR pumps).

The second section involves the two RHXRs leading to an output crosstie of two paths to the four injection legs. If both paths in either section are blocked, the recirculation system would fail to deliver flow to the core.

Block "B" provides an interesting column of doubletons between power panel 32 (PWRPNL32P) and the intake side of component cooling train. This doubleton exists because PWPPNL32P is required for both RHRP32 and RECP32 which are two of the four possible pumps used in low pressure recirculation. The other two pumps, RHRP31 and RECP31, are both vulnerable to the component cooling train failure. Therefore, loss of this section of pipe due to either a block, a break, or a loss of the water flow for any reason along with a loss of PWPPNL32 would result in the loss of all four pumps.

The doubleton failures within the Component Cooling system are found in Block "C". Since there are two trains in the Component Cooling system, the output matrix is grouped in lines representing these trains. Four of the columns represent component cooling break nodes. These nodes have the same meaning as in prior system combinations. The difference is that the rest of the nodes are block nodes instead of break nodes. The four break nodes are mitigatable in that they only fail two of the three pumps. The third pump can be isolated and used to feed its own train. The trains are redundant to each other because one piece of vital equipment is on one train while the other identical and redundant piece is on the other train. The doubletons involve a single failure of one train alaong with a single failure of the other.

In Block "D", there is a location doubleton stemming from LOCRP which is the Control Room and houses PWRPNLs #31, 32 and 34. Loss of the PWRPNLs would result in the loss of both recirculation pumps and RHR pump #32. Therefore, this node is a doubleton with all nodes which could propagate a failure to RHRP #31.

There is one other doubleton in Block "D" which is the result of losing the distribution panels due to LOCCP. Loss of these distribution panels would result in the loss of the starting of all pumps.

Block "E" shows several trains of doubletons representing the loss of component cooling trains with the loss of electrical buses 5 and 6. These buses power three of the four required pumps.

The doubletons in Block "F" are comprised entirely of the loss of two separate electrical locations. There are no two components in the electrical system that can be responsible for failure in this combination.

There are no doubletons in Block "G" which is the combination of Service Water and the front-line recirculation systems.

Service Water and Component Cooling is shown in Block "H" where doubletons exist because of the loss of SW flow to one Component Cooling Heat Exchanger (CCWHXR) along with the loss of CCW flow to the other CCWHXR.

Block "J" is composed of doubletons, both of which are in the Service Water model. These doubletons are those which cause a failure in both trains to the Component Cooling Heat Exchangers and, therefore, prevent the removal of heat from the Component Cooling Heat Exchanger to the Hudson River.

Summary

System Combination 9 is different from the other combinations. This is due partly to the fact that operators are required to initiate the system. There are no automatic cases for this combination.

Another main difference is that active heat removal is essential. In other combinations, the component cooling pumps may be shut down and the water in the pipes then acts as a heat sink. Now the recirculated water must be cooled before it is cycled back to the core in order to prevent core damage.

This system combination must also be considered to occur for a very long time. Injection scenarios last about 30 minutes depending on the size of the accident, whereas, the recirculation phase may last indefinitely.

The most noteworthy doubleton is the one which indicates that loss of component cooling train #31 and the loss of power panel #32 would result in the loss of all four low pressure recirculation pumps (two recirculation pumps and two residual heat removal pumps).

ENCLOSURE 9

SYSTEM COMBINATION 9

LOW PRESSURE RECIRCULATION IN RESPONSE TO LARGE LOCA

CASE IVA & IVB - MANUALLY ASSISTED

CASE IVA - MANUALLY ASSISTED, FAILURE BY OMISSION

CASE IVB - MANUALLY ASSISTED, FAILURE BY OMISSION AND FAILURE BY COMMISSION

SINGLETONS

2	LPR-LOCAD
2	RHXRCOOLD
23	SOURCE
99	BRC899BJ899AB
102	LFRHXRB
103	LSRHXRB
104	LWRHXRB
137	BRC889J1869BD
162	BRC760CJ760AL
193	BRC762CJ762AL
304	BRC765CJ765AL
753	LODP
1001	TESTELECP
1207	RIVHUDSONK
1243	JEGRK
1243	J1410K
1243	J1237K
1243	J390K
1243	J263K
1243	J1271K
1253	CHNLDSK
1253	CHNLDSK
1253	J95AK
1370	SWSMASTER
1370	TRIPMASTER

LOW PRESSURE RECIRCULATION IN RESPONSE TO LARGE LOCA

CASE IVA & IVB - MANUALLY ASSISTED

VARIABLE LIST FOR SC1 CASE IVA & IVB DOUBLETON MATRIX

55	BKR3AP
55	BKR3AP
55	BUS3AP
55	R86SS3P
55	OIBUS3AP
56	BKRSS6P
56	XFMRSS6P
56	BKRCAP
56	BUS6AP
56	R86SS6P
56	OIBUS6AP
57	VGA760AL
58	J1805L
59	PPR1805L
61	J760AL
C2	BRC760AJ760BL
69	BRC760CJ760BL
72	VGA760CL
74	J760CL
76	JA57L
77	ORFC760CL
78	CCWP33L
82	JA55L
83	ORFC760AL
84	CCWP31L
85	ORFCCCW33L
86	VC761CL
87	JA3L
88	VGA762CL
90	J763BL
90	\ A759BL
90	JA8L
90	CCHXRS32Z
90	VGA765BL
90	J764BL
93	BRC762CJ762BL
102	BRC762AJ762BL
103	ORFCCCW31L
104	VC761AL
105	JA1L
106	VGA762AL
107	J763AL
107	VGA759AL
107	JA7L
107	CCHXRS31Z
107	JA10L
107	VGA765AL
107	J764AL
107	PP1765AL
109	J762AL
116	J765BL
120	J765AL
287	PNLDIS31P
287	BKRDPNL31P
298	PNLDIS34P
306	LG20F2SIA2AH
306	LG10F2SIA2AH
306	RSI1H
306	RSI11XZ
312	LG20F2SIA2BH
312	LG10F2SIA2BH
312	RSI2H
312	RSI21XZ
322	BKRUT3ST6P
322	AXFRUT3ST6P
323	BUS3P
332	PWRPNL31P
332	BATTEKY31P
332	FUSEPNL31P
332	LOCOP
334	UVBUS3AP
335	UVBUS6AP
341	TTBATTERY31P
369	BKRSS3/P
371	XFMRSS3/P
372	BKR3A/P
374	BUS3A/P
376	BKRSS6/P
378	XFMRSS6/P
379	BKR6A/P
381	BUS6A/P
457	BATTERY31/P
458	FUSEPNL31/P
459	PWRPNL31/P
469	BKRDPNL31/P
4/0	PNLDIS31/P
483	CHARGER32/P
484	BKRCH320/P
485	BKRCH320:P
487	BKRDPNL32/P
488	BKRDPNL32:P
489	PNLDIS32/P
491	PNLDIS34/P
492	BKRDPNL34:P
500	PWRPNL33/P
518	CON2024SI11XI
519	CON91JSI21XI

MATRIX TOO LARGE TO INCLUDE

SEE VOLUME 1-B - ENCLOSURES

LOW PRESSURE RECIRCULATION IN RESPONSE TO LARGE LOCA

CASE IVA & IVB - MANUALLY ASSISTED

VARIABLE LIST FOR SC1 CASE IVA & IVB DOUBLETON MATRIX

6	J745AD
6	RHXR32Z
6	MOV745BD
6	MOV745AD
8	VGA742D
8	RHXR31Z
21	VGA735BD
21	J1867BD
21	J101XD
21	CON182252/RHR2I
21	BS17RHRP32OP
21	CON91352/RHR2I
21	CON2RHRP32OP
21	RHRP32Z
21	J1866DD
21	XDD3ARHRP32AP
21	CONMRHRP32ACP
21	BKRRHRP32P
21	MOLDRHRP32AP
21	XDDARHRP32P
21	XDD3ARHRP32BP
21	CONMRHRP32BCP
21	MOLDRHRP32BP
21	XDDBRHRP32P
21	XDD3ARHRP32CP
21	CONMRHRP32CCP
21	MOLDRHRP32CP
21	XDDCRHRP32P
21	FUSERHRP32PP
21	JELE1BRHRP32P
21	T1RHRP32P
21	JELE1ARHRP32P
21	JELE1RHRP32P
21	CONRHRP32TDOP
21	RLRHRP32P
21	XDD1ARHRP32P
21	JELEA1RHRP32P
21	JELE19ARHRP32P
21	T13RHRP32P
21	XDD13RHRP32P
21	CON13RHRP32OP
21	RLOTSARHRP32OP
21	XDD14RHRP32P
21	XDD3RHRP32P
21	CCOILRHRP32P
21	CONRHRP32DOP
21	JELE3RHRP32P
21	XDD4RHRP32P
21	JELE4RHRP32P
21	FUSERHRP32NP
21	JELEH12RHRP32P
21	JELE11RHRP32P
21	JELE12RHRP32P
21	JELEE12RHRP32P
21	JELEE1RHRP32P
21	JELEKRHRP32P
21	JELE16RHRP32P
21	JELE5RHRP32P
21	JELEA11RHRP32P
21	SWMCA12RHRP32P
21	XDDRHRP32BP
21	T32CRHRP32P
21	TNRHRP32P
21	SENOTSRHRP32OP
21	CONOTSRHRP32ACP
21	CONOTSRHRP32BCP
21	CONOTSARHRP32CP
21	CON5RHRP32P
21	SWMOA11RHRP32P
21	VC738BD
21	J107D
21	VGA739BD
21	J830BL
21	J627BAL
21	J627BBL
21	J627BCL
21	JA502L
21	J017BL
21	J601BL
21	J602BL
21	J602CL
21	J1871AL
21	VGL736BL
21	J736BL
21	PPR736BL
21	PSHXR1871BL
21	PPR750DL
21	J750DL
21	PPI1871AL
21	VGL1871AL
21	J1871BL
21	PPI1871BL
21	PPR1871BL
21	VGL1871BL
21	VC750DL
21	ORFC645BL
21	FIC645L
21	ORFC645AL
21	VGL737BL
21	JA501AL
21	JA501L
21	RL3-16AI
21	CON91327-6AX3I
21	RL27-6AX1I
21	CON3927-6AX1I
21	RL27-6AX4I
21	CON3927-6AX4I
21	RL27-6AX2I
21	RL27-6AX3I
25	J740BD
25	VGA735AD
25	J1867AD
25	J103XD
25	CON172152/RHR1I
25	BS17RHRP31OP
25	CON91352/RHR1I
25	CON2RHRP31OP
25	RHRP31Z
25	J1866BD
25	XDD3ARHRP31AP
25	CONMRHRP31ACP
25	BKRRHRP31P
25	MOLDRHRP31AP
25	XDDARHRP31P
25	XDD3ARHRP31BP
25	CONMRHRP31BCP
25	MOLDRHRP31BP
25	XDDBRHRP31P
25	XDD3ARHRP31CP
25	CONMRHRP31CCP
25	MOLDRHRP31CP
25	XDDCRHRP31P
25	FUSERHRP31PP
25	JELE1BRHRP31P
25	T1RHRP31P
25	JELE1ARHRP31P
25	JELE1RHRP31P
25	CONRHRP31TDOP
25	RLRHRP31P
25	XDD1ARHRP31P
25	JELEA1RHRP31P
25	JELE19ARHRP31P
25	T13RHRP31P
25	XDD13RHRP31P
25	CON13RHRP31OP
25	RLOTSARHRP31OP
25	XDD14RHRP31P
25	XDD3RHRP31P
25	CCOILRHRP31P
25	CONRHRP31DOP
25	JELE3RHRP31P
25	XDD4RHRP31P
25	JELE4RHRP31P
25	FUSERHRP31NP
25	JELEH12RHRP31P
25	JELE11RHRP31P
25	JELE12RHRP31P
25	JELEE12RHRP31P
25	JELEE1RHRP31P
25	JELEKRHRP31P
25	JELE16RHRP31P
25	JELE5RHRP31P
25	JELEA11RHRP31P
25	SWMCA12RHRP31P
25	XDDRHRP31BP
25	T32CRHRP31P
25	TNRHRP31P
25	SENOTSRHRP31OP
25	CONOTSRHRP31ACP
25	CONOTSRHRP31BCP
25	CONOTSARHRP31CP
25	CON6RHRP31P
25	SWMOA11RHRP31P
25	VC738AD
25	J104D
25	VGA739AD
25	PPI739AD
25	JA14AL
25	JA14L
25	J830AL
25	JTIC627L
25	J627AL
25	J017AL
25	J602AL
25	J601AL
25	J601CL
25	J601DL
25	J1871CL
25	VGL736AL
25	J736AL
25	PPR736AL
25	PSHXR1871DL
25	PPR750EL
25	J750EL
25	VGL1871DL
25	J1871DL
25	PPI1871DL
25	PPR1871DL
25	VGL1871CL
25	VC750EL
25	ORFC646BL
25	FIC646L
25	ORFC646AL
25	VGL737AL
25	J627BL
25	RL3-13AI
25	CON2627-3AX3I
25	RL27-3AX1I
25	CON3527-3AX1I
25	RL27-3AX4I
25	CON3527-3AX4I
25	RL27-3AX2I
25	RL27-3AX3I
26	PWRPNL33P
28	J838OB
28	J639B
28	J638B
29	J838RB
29	J641AB
29	J641B
29	J640B
30	J899AB
33	MOV899AB
33	MOV746B
33	J733AB
33	HCY640B
33	J889AB
38	J899BB
40	MOV899BB
40	MOV747B
40	J733BB
40	HCY638B
40	J899BB
48	J889D
50	J1869BD
55	BKRSS3P
55	XFMRSS3P

2.4.10 Medium LOCA and Loss of Injection $S_1U_iD_i$

2.4.10.1 Introduction

In this system combination, we have searched for singleton and doubleton failures that would cause a loss of all injection during a given, but unspecified, medium (2" to 6" pipe rupture) LOCA. Figure 2-17 shows that core melt could potentially result from this sytem combination scenario. The Residual Heat Removal (RHR) and Safety Injection (SI) Systems comprise the injection system for this system combination. Supporting the injection system are the Safety Injection Actuation system, the Electrical system, the Component Cooling system, and the Service Water system. Notice that the bidirectional relationship between several support systems establishes intersystem cycles.

2.4.10.2 Failure Criteria of Individual Systems

Residual Heat Removal and Safety Injection Systems

All medium LOCAs are conservatively judged to require the delivery of injection flow from one RHR pump or two SI pumps to the Reactor Coolant system. Flow from the SI pumps must reach the core through at least two unbroken high pressure injection legs.

Safety Injection Actuation System

A Safety Injection Actual Signal is required to start the RHR and SI pumps automatically. These pumps may also be started manually by an operator in the Central Control Room (CCR).

Electrical System

Electrical power is required to run the RHR and SI pumps. It is also required to open motor operated valves in the Safety Injection System. This power may be supplied from either offsite sources or the onsite emergency diesel generators. The pump control circuitry and the Safety Injection Actuation System (SIAS) are normally powered by rectified current from the above supplies. In the event of a loss of offsite electrical power, storage batteries provide backup power to the dc circuits and the diesel generator starting circuitry.

Component Cooling System

The Component Cooling System (CCS) is required to be filled and intact during all medium LOCAs. The system's water inventory provides a heat sink for the RHR Pump Seal Heat Exchangers and the Safety Injection Pumps. Note, however, that CCS flow is not required during this accident sequence.

Service Water System

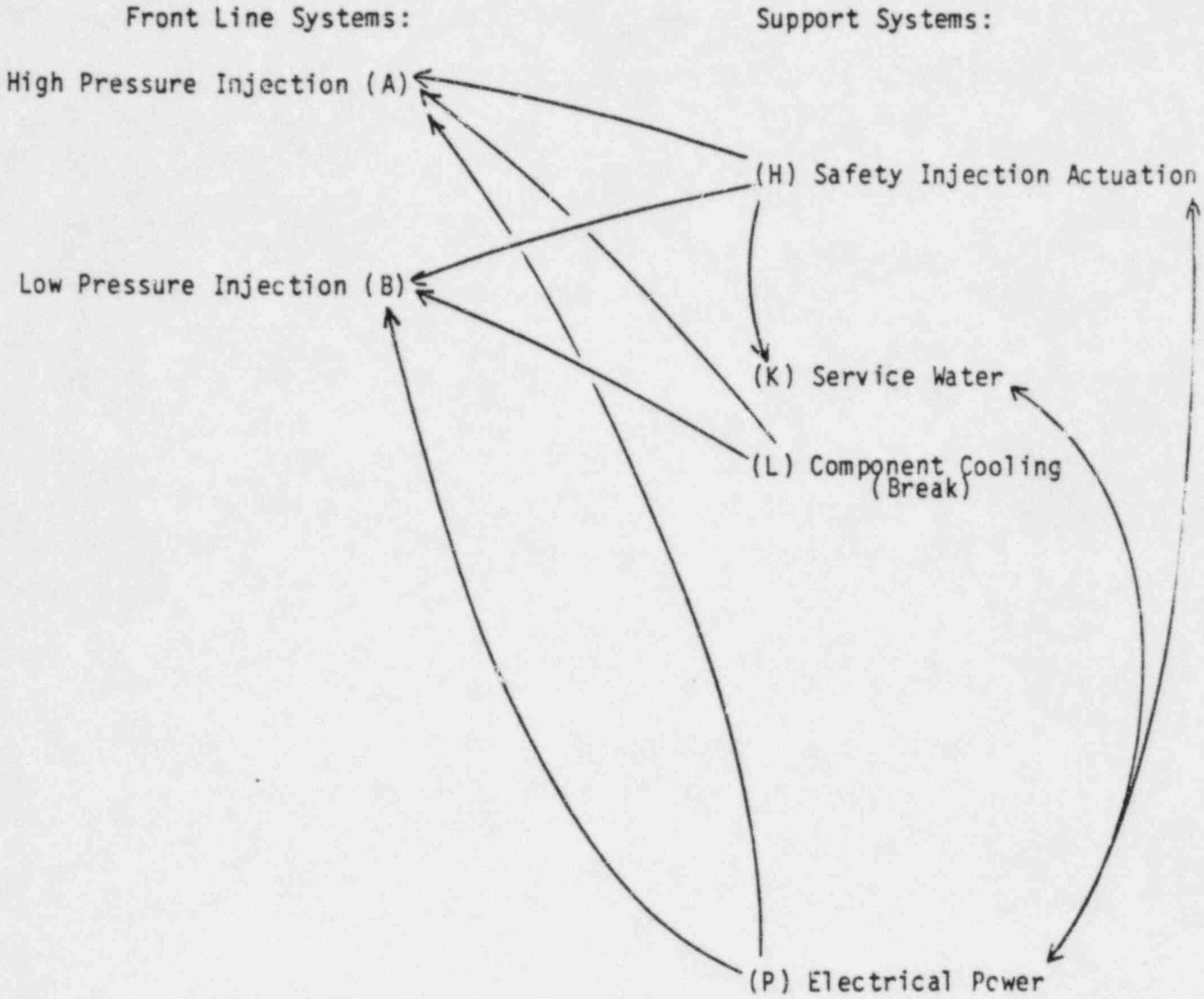
The Service Water System (SWS) is required when offsite electrical power is lost. The system circulates cooling water through the emergency diesel generators. Adequate cooling is provided by a minimum of one operating Service Water Pump.

The singleton and doubleton failures of the combined (low and high pressure) injection systems are listed in Enclosure 10. The front-line and support system digraphs are located in Appendix B. Piping and instrumentation diagrams (P&IDs) for each system are also found in this

Figure 2-17

SYSTEM COMBINATION # 10

S1 LOCA with High and Low Pressure Injection



appendix. Appendix C is a listing of the adjacency information contained in Appendix B. This listing is in a form suitable for computerized analysis using Digraph Matrix Analysis (DMA).

2.4.10.3 Results for the Front-Line System Acting Alone

As discussed previously, the Residual Heat Removal System (low pressure) and the Safety Injection System (high pressure) are the front-line systems for this sequence. A few components within these systems have been identified as singleton failures which cause a loss of injection ability.

The Refueling Water Storage Tank (RWST1) is the only source of injection water. The tank must be full of borated water prior to the start of the accident. This requirement is reflected in the time transition node TTRWSTH2O. The RWST isolation valve (VGA846) must be open and the path to the RHR/SI pump tee (J1810) must be clear of blockage.

The low and high pressure portions of the combined injection system are designed with parallel flowpaths throughout a majority of their lengths. A doubleton failure occurs where two events are capable of simultaneously blocking the high and low pressure paths. These interactions are shown in block "A" of the doubleton matrix.

Many of the doubletons were composed of junctions and reducers. While it is possible for a reducer or junction (tee) to become blocked, it is highly unlikely in this system because of the large diameter of the piping. Thus, doubletons containing these components will not be discussed for this system combination.

The motor operated RHR pump suction and discharge valves (MOV882 and MOV744) form doubletons with the SI pump combined suction isolation valve and check valve (MOV1810 and VC847). These are the only doubletons resulting from valve failure.

The remaining doubletons are due to catastrophic pipe breaks. The combination of a break or valve failure (MOV882, MOV744, MOV1810, or VC847) in both the RHR and SI systems results in a doubleton. The breaks include the SI pump discharge header between J852A and J852B (BRC852BJ852A) and the three (BRC745AJ745B, BRC889J1869B, and BRC899BJ899A) that were previously identified in the low pressure injection piping (see Section 2.4.1).

2.4.10.4 Results for the Front-Line and Support Systems Acting Together

Additional singletons and doubletons are generated when the scope of the analysis is expanded to include support systems. The Safety Injection Actuation, Electrical, and Component Cooling Systems directly support the RHR and SI systems. The Service Water System supplies cooling water from the Hudson River to the emergency diesel generators. During a loss of offsite electrical power, these generators power the RHR pumps, the SI pumps, and the SI motor operated valves. Thus, the Service Water System indirectly supports the injection systems.

All but one of the additional singletons are due to the Component Cooling System. System water inventory will be lost if the Component Cooling Pump inlet piping header between J760A and J760C is severed at both junctions. This break is denoted by BRC760CJ760A on the digraph. Similar failures (BRC762CJ760A and BRC765BJ765A) also occur at the CCP outlet piping header (J762A to J762C) and the Component Cooling Heat Exchanger outlet piping header (J765A to J765B), respectively. Actually, an unmitigated break anywhere in the Component Cooling System will drain the piping. This effect does not result in an extensive list of CCW components, because the CCS model was developed for the recirculation phase where flow is required to cool the various components as a scope limitation.

The doubleton matrix has been divided into blocks corresponding to the joint contributions of failures from each system. Blocks "D", "E", "F", "H", "I", "L", "P", "Q", "R", "S", and "U" contain no doubletons. Block "A" was discussed in the previous section. Blocks "J" and "O" are doubletons internal to an individual support system. They will be lightly touched upon in this section. A more thorough discussion of these systems is included in Sections 2.2 and 2.3. Blocks "B" and "C" involve the Component Cooling System. Based on previous discussion these blocks should contain no doubletons since all CCS breaks are singletons.

The joint contributions to failure between the injection systems and the SIAS are contained in Block "G". Loss of the dc distribution panel (PNLDIS34) removes the source of power necessary to energize the SI logic relays. Failure of a Channel 2 logic gate (LG1OF2SIA2B) to indicate an abnormal condition also prevents the master relay (RSI2) from changing state. The auxiliary relay (RSI21X) will fail to close the Safety Injection Actuation starting contacts of several pumps. When combined with a loss of dc control power from PWRPNL31, an insufficient number of pumps are available to meet the system success criteria.

The joint contributions from the injection systems and the Electrical system are contained in block "K". The one is similar to that described for Block "G", the only difference being the type of PNLDIS34 failure (short vice open circuit).

Block "M" contains doubletons that result from joint failures in the Service Water and Electrical system. All of the pairs in this block result from a simultaneous loss of offsite power and diesel generators. Offsite power can be lost by a failure of either the offsite power grid (SOURCE1) or the onsite Station Auxiliary Transformer (STAAUXXFMR). In this block the emergency generators are lost because of a failure of Service Water cooling to the diesel engines. A discussion of the Service Water System is included in Sections 2.2.12 and 2.3.9.

Block "J" is composed of doubletons internal to the Safety Injection Actuation System. These doubletons represent a simultaneous failure of both SIAS channels.

Blocks "N" and "T" contain the Electrical and Safety Injection Actuation Systems doubletons. These results are similar to those desribed in Blocks "G" and "K".

Block "O" is composed of doubletons internal to the Electrical System. These doubletons mainly consist of a loss of offsite power (SOURCE1) or the Station Auxiliary Transformer (STAAUXXFMR) combined with a failure of any of the following:

Bus Tie Breaker 2A-5A interlock (ITLBKR2AT5A)
Compressed air in the diesel generator receiver (TTRCVR31)

2.4.10.5 Results for the Front-Line and Support Systems Acting Together with Common Location Effects

Additional singletons and doubletons are generated when the scope of the analysis is expanded to include the effects of common component location. Two singletons and numerous doubletons were found to be significant.

The SI pumps share a common room; consequently, they are susceptible to electrical failures caused by fire (LFSIP), steam (LSSIP), or flooding (LWSIP). The RHR pumps also share their own room and have similar failure modes (LFRHR, LSRHR, and LWRHR). Any combination of location nodes which causes failure of both the low and high pressure pumps is a doubleton. Thus, there are nine doubleton pairs for common location in the injection systems. Possible location effects were also identified in the 888 room and the Residual Heat Exchanger portion of the Containment Building. All but four of the motor operated valves in these areas, however, are normally correctly aligned and do not require repositioning. The four valves which are required to change state are contained in tripleton and higher order cut sets. The controllers which operate all the valve motors are located in the switchboards, not at the motor. Thus, accidental operation due to steam shorted contacts is also impossible.

The two singletons consist of the electrical locations LOCD and LOCS. LOCD includes the 15 foot elevation of the Central Building where the 480V ac buses share a common location. The Central Control Room (LOCS) houses the dc distribution panels essential to power the pump motor controllers.

2.4.10.6 Results for the Front-Line and Support Systems with Common Location Effects and Operator Action

In this section the effects of operator action, both right (OPR) and wrong (OPW) taken during the accident are analyzed. Only the differences between the previous sections and this section will be discussed.

Only one incorrect operator valve manipulation was identified as a singleton, the shutting of the RWST isolation valve (OPW846). Deliberate effort is required to reposition this valve since VGS846 is normally locked open.

An OPW node appears for each component that may be incorrectly operated by manual intervention. The effect of these nodes is identical to that described for the component itself.

The number of doubletons identified in this system combination is greatly reduced because of the redundancy provided by the operator

(OPRSWMRHRP31C, OPRSWMRHR32C, OPRSWMSIP31C, OPRSWMSIP32C, and OPRSWMSIP33C) who manually start the RHR and SI pumps. The degree of redundancy is so great that the Safety Injection Actuation System does not appear in any of the singletons or doubletons.

All of the singletons caused by breaks in the Component Cooling System have been degraded to doubletons because of the actions taken by the operators to isolate these leaks. The operator may also refill the system if an excessive volume of water was lost through a break.

The doubletons identified in the electrical system which involve the Station Auxiliary Transformer, the diesel generator air receiver, and the bus tie breaker interlock have been eliminated because of the redundancy provided by the operator.

2.4.10.7 Summary

The digraph matrix analysis of the medium LOCA with loss of both Low Pressure and High Pressure Safety Injection has revealed no violations of applicable safety requirements.

ENCLOSURE 10

SYSTEM COMBINATION 10

MEDIUM LOCA WITH HIGH AND LOW PRESSURE INJECTION

SINGLETONS

38	MLOCAD
341	J1810D
342	J290AD
342	J200D
342	PPI846D
342	HTRC846ZD
342	VGA846D
342	HTRC846YD
342	PPR846D
342	RWST1D

DOUBLETONS

```
                            2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
        1 1 2 3 3 4 4 4 8 0 2 3 3 4 4 4 5 5 6 6 6 7 7 7 7 8 8 9
        2 5 3 7 9 0 2 3 5 8 8 1 8 0 4 9 0 1 4 5 6 1 4 5 6 6 8 0

 12     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
 15     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
 23     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
 37     - - - - * - - - - - - - - - - - - - - - - - - - - - - -
 39     - - - * - * * * - - - * * - - - - - - - - - - - - - - -
 40     * * * - * - - - - - - - - - * * * * * * * * * * * * * *
 42     * * * - * - - - - - - - - - * * * * * * * * * * * * * *
 43     * * * - * - - - - - - - - - * * * * * * * * * * * * * *
285     * * * - - - - - - - - - - - * * * * * * * * * * * * * *
308     - - - - - - - - - - - - - - - - - - - - - - - - - - - -
328     - - - - - - - - - - - - - - - - - - - - - - - - - - - -
331     - - - - * - - - - - - - - - - - - - - - - - - - - - - -
338     * * * - * - - - - - - - - - * * * * * * * - - - - * * *
340     * * * - - - - - - - - - - - * * * * * * * - - - - * * *
344     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
349     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
350     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
351     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
364     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
365     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
366     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
371     - - - - - * * * * - - - - - - - - - - - - - - - - - - -
374     - - - - - * * * * - - - - - - - - - - - - - - - - - - -
375     - - - - - * * * * - - - - - - - - - - - - - - - - - - -
376     - - - - - * * * * - - - - - - - - - - - - - - - - - - -
386     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
388     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
390     - - - - - * * * * - - - * * - - - - - - - - - - - - - -
```

```
FILE IDENTIFICATION
  REACH PAIR:    I= 1                    J= MLOCAD
  DATE:  6/20/84
  ANSWER.POS FILE IS: DR1:SCT615MC3.POS
  OUTPUT.DAT FILE IS: DR1:SCT615MOT.TRP
  VARIAB.DAT FILE IS: DR1:SCT615MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:SCT615MRT.DAT
  SIGMA PI FILE NAME IS: DR1:SCT615MSI.C3
```

MEDIUM LOCA WITH HIGH AND LOW PRESSURE INJECTION

CASE I (CONTINUED)

VARIABLE LIST FOR SC10 CASE I DOUBLETON MATRIX

12	PPR1810D
15	J735BD
15	J1863D
15	MOV882D
15	VC881D
15	PPI735D
15	J735AD
23	J111XD
23	JRHRD
23	J740AD
23	J636D
23	J883D
23	MOV744D
23	VC741D
23	J110XD
37	HPI-MLOCAD
39	LPI-MLOCAD
* 40	LFSIPD
* 42	LWSIPD
* 43	LSSIPD
285	BRC852BJ852AA
308	PWRPNL33P
328	PWRPNL31P
331	J1829D
338	J203AD
340	J203D
340	VC847D
340	MOV1810D
344	J898D
* 349	LFRHRD
* 350	LSRHRD
* 351	LWRHRD
* 364	LF888D
* 365	LS888D
* 366	LW888D
371	BRC899BJ899AB
* 374	LFRHXRB
* 375	LSRHXRB
* 376	LWRHXRB
386	BRC745AJ745BD
388	BRC889J1869BD
390	J745BD

* INDICATES LOCATION

ENCLOSURE 10

SYSTEM COMBINATION 10

MEDIUM LOCA WITH HIGH AND LOW PRESSURE INJECTION

COMBINED CASE II & CASE III RESULTS

CASE II FULLY AUTOMATIC FRONT-LINE AND SUPPORT SYSTEMS

CASE III FULLY AUTOMATIC FRONT-LINE, SUPPORT SYSTEMS, AND LOCATIONS

SINGLETONS

38	MLOCAD	
341	J1310D	
342	J290AD	
342	J200D	
342	PPI846D	
342	HTRC846ZD	
342	VGA846D	
342	HTRC846YD	
342	PPR846D	
342	RWST1D	
408	BRC760CJ760AL	
440	BRC762CJ762AL	
464	BRC765BJ765AL	
1271	LOCDP	LOCATIONS (CASE III)
1275	LOCSP	
1519	TESTELECP	- TEST NODE FOR MODEL

```
FILE IDENTIFICATION
  REACH PAIR:   I= 1                    J= MLOCAD
  DATE:  6/20/84
  ANSWER.POS FILE IS: DR1:SCT615MC3.POS
  OUTPUT.DAT FILE IS: DR1:SCT615MOT.TRP
  VARIAB.DAT FILE IS: DR1:SCT615MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:SCT615MRT.DAT
  SIGMA PI FILE NAME IS: DR1:SCT615MSI.C3
```

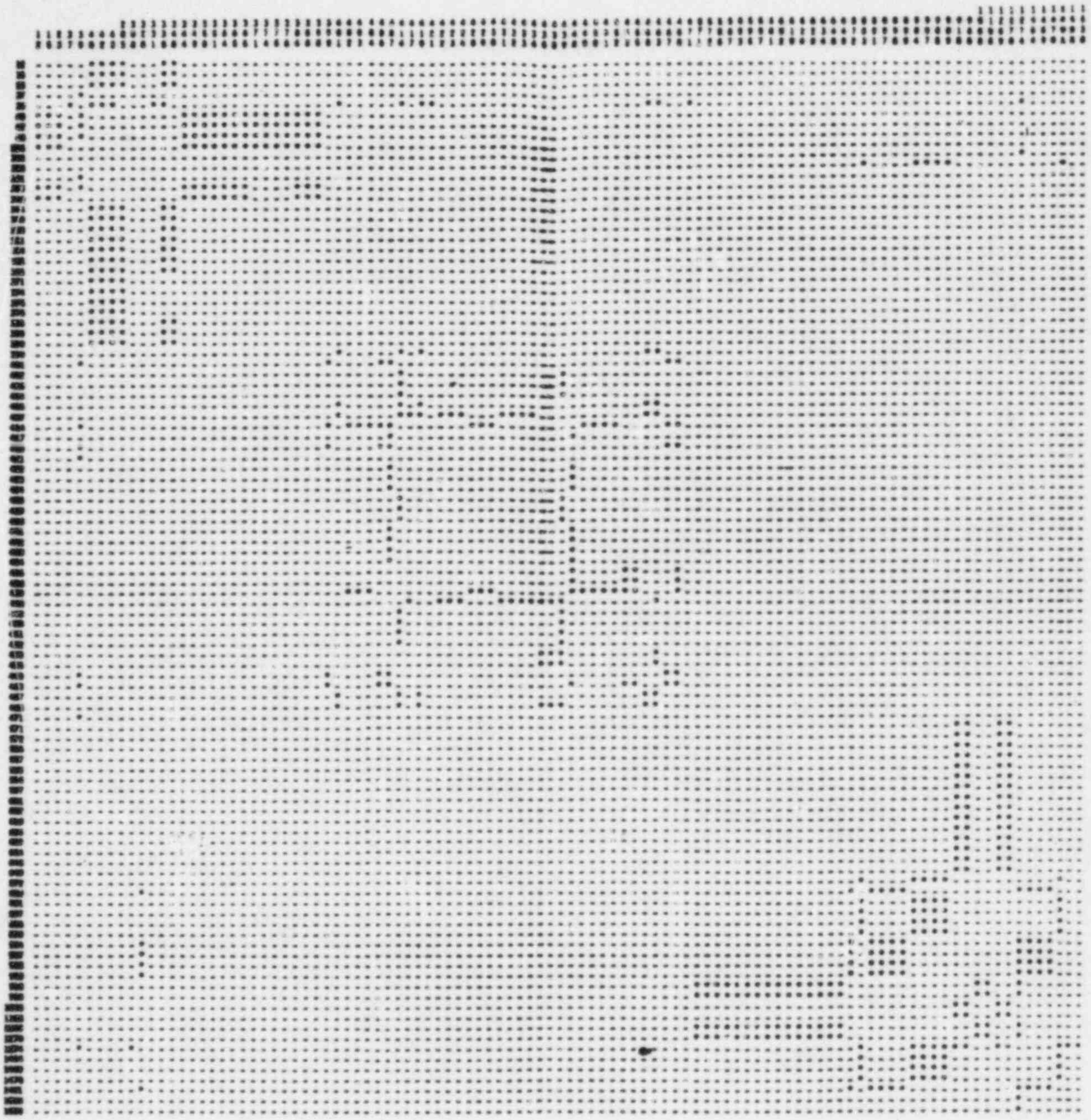
ENCLOSURE 10

SYSTEM COMBINATION 10

MEDIUM LOCA WITH HIGH AND LOW PRESSURE INJECTION

COMBINED CASE II & CASE III RESULTS

DOUBLETONS



ENCLOSURE 10

SYSTEM COMBINATION 10

MEDIUM LOCA WITH HIGH AND LOW PRESSURE INJECTION

CASE II & CASE III CONTINUED

VARIABLE LIST FOR SC10 CASE II & III DOUBLETON MATRIX

12	PPR1810D	401	J830BL	453	J764AL	629	J1096BK
15	J735BD	401	J627BAL	453	PPI765AL	634	J1094K
15	J1863D	401	J627BBL	455	J762AL	648	COL-RW-2K
15	MOV882D	401	J627BCL	460	JA502L	648	TTCOL1K
15	VC881D	402	VGA760AL	460	J017BL	649	SW123456P
15	PPI735D	403	J1805L	460	J601BL	872	PNLDIS31P
15	J735AD	404	PPR1805L	460	J602BL	872	BKRDPNL31P
23	J111XD	406	J760AL	460	J602CL	883	PNLDIS34P
23	JRHRD	407	BRC760AJ760BL	463	J765BL	891	LG2OF2S1A2AH
23	J740AD	414	BRC760CJ760BL	467	J017AL	897	LG1OF2S1A2AH
23	J636D	417	VGA760CL	467	J602AL	898	RSI1H
23	J883D	419	J760CL	467	J601AL	899	RSI11XZ
23	MOV744D	421	PPR627BCL	467	J601CL	904	LG2OF2S1A2BH
23	VC741D	421	J787L	467	J601DL	907	LG1OF2S1A2BH
23	J110XD	421	VGL787L	468	J765AL	908	RSI2H
37	HPI-MLOCAD	421	FIC634BL	471	J602DL	909	RSI21XZ
39	LPI-MLOCAD	421	JA59L	471	J756CL	918	STAUXXFMRP
* 40	LFSIPD	421	J749FL	471	J749BL	960	SOURCE3P
* 42	LWSIPD	422	JA57L	571	J1190K	1088	ITLBKR2AT5AP
* 43	LSSIPD	423	ORFC760CL	571	J98AK	1108	TTRCVR31P
285	BRC852BJ852AA	424	CCWP33L	571	J1093BK	* 1269	LOCAP
308	PWRPNL33P	428	JA55L	571	J1093AK	* 1270	LOCCP
328	PWRPNL31P	429	ORFC760AL	571	J1093DK	* 1274	LOCRP
331	J1829D	430	CCWP31L	571	VB30K	1464	PWRPNL31/P
338	J203AD	431	ORFCCCW33L	571	J1095K	1469	BKRDPNL31/P
340	J203D	432	VC761CL	572	VC98K	1470	PNLDIS31/P
340	VC847D	433	JA3L	572	HTRC409K	1491	PNLDIS34/P
340	MOV1810D	434	VGA762CL	572	J4K	1500	PWRPNL33/P
344	J898D	436	J763BL	572	J106BK	1530	CON2024S121X1
* 349	LFRHRD	436	VGA759BL	572	J409K		
* 350	LSRHRD	436	JA8L	572	J1221K		
* 351	LWRHRD	436	CCHXRS32Z	572	HTRC98K		
* 364	LF888D	436	VGA765BL	572	VB98K		
* 365	LS888D	436	J764BL	586	RIVHUDSONK		
* 366	LW888D	438	J762CL	587	STRCTRINTKK		
371	BRC899BJ899AB	439	BRC762CJ762BL	593	SWPWELL1K		
* 374	LFRHXRB	448	BRC762AJ762BL	595	TRASH1K		
* 375	LSRHXRB	449	ORFCCCW31L	597	J131K		
* 376	LWRHXRB	450	VC761AL	601	J133K		
386	BRC745AJ745BD	451	JA1L	602	J132BK		
388	BRC889J1869BD	452	VGA762AL	619	CHNLDSK		
390	J745BD	453	J763AL	619	CHNLDS3K		
399	JA14AL	453	VGA759AL	619	J95AK		
399	JA14L	453	JA7L	619	J95BK		
399	J830AL	453	CCHXRS31Z	619	J95CK		
399	JTIC627L	453	JA10L	619	J95DK		
399	J627AL	453	VGA765AL	626	J95FK		
				626	J1096AK		

* INDICATES LOCATION

FILE IDENTIFICATION
REACH PAIR: I= 1 J= MLOCAD
DATE: 6/20/84
ANSWER.POS FILE IS: DR1:SCT615MC3.POS
OUTPUT.DAT FILE IS: DR1:SCT615MOT.TRP
VARIAB.DAT FILE IS: DR1:SCT615MVB.DAT
RENUMSRT.DAT FILE IS: DR1:SCT615MRT.DAT
SIGMA PI FILE NAME IS: DR1:SCT615MSI.C3

ENCLOSURE 10

SYSTEM COMBINATION 10

MEDIUM LOCA WITH HIGH AND LOW PRESSURE INJECTION

CASE IVA & IVB - MANUALLY ASSISTED

CASE IVA - MANUALLY ASSISTED, FAILURE BY OMMISSION

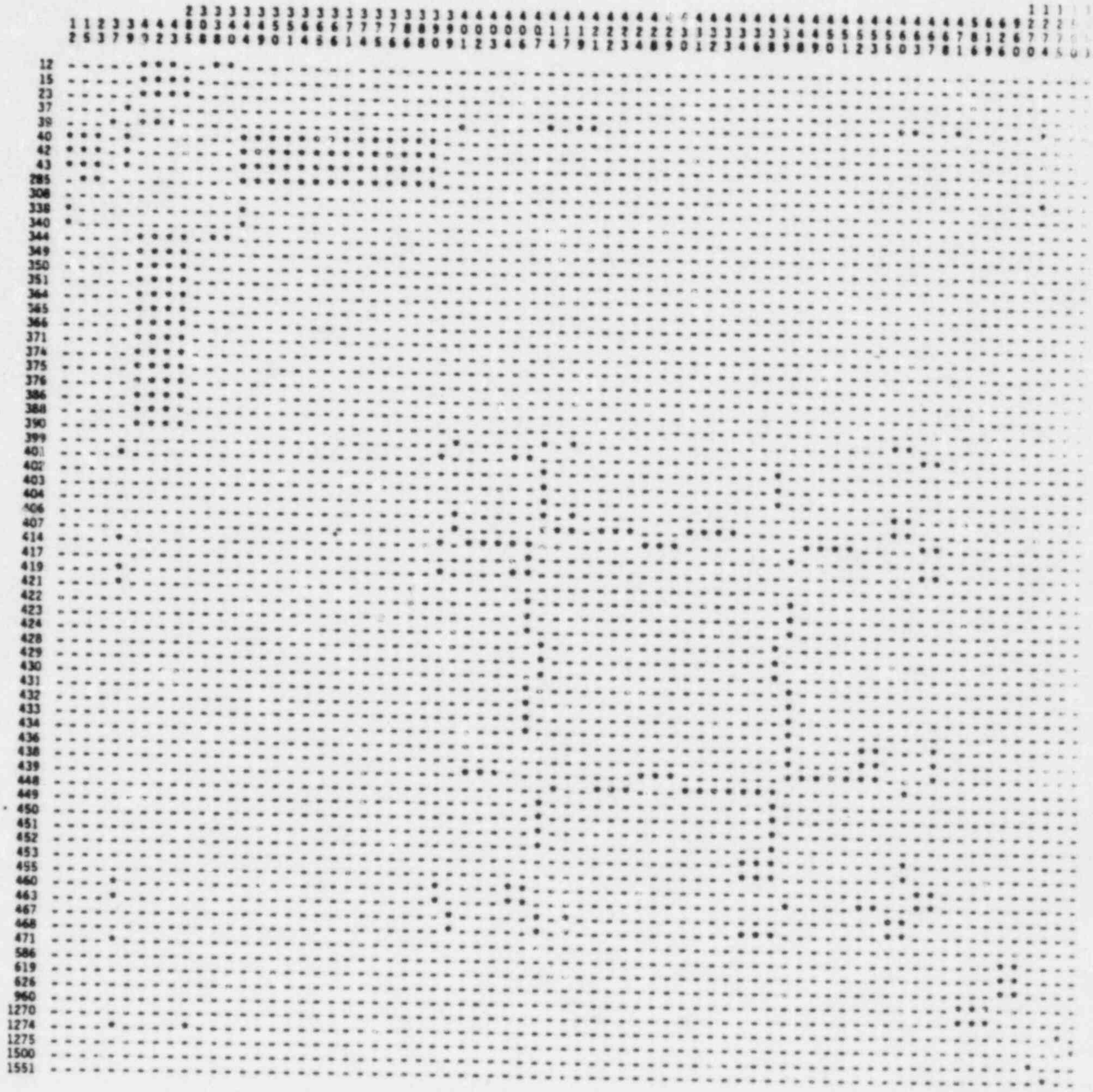
CASE IVB - MANUALLY ASSISTED, FAILURE BY OMMISSION AND FAILURE BY COMMISSION

SINGLETONS

38	MLOCAD
341	J1810D
342	J290AD
342	J200D
342	PPI846D
342	HTRC846ZD
342	OPW846D
342	VGA846D
342	HTRC846YD
342	PPR846D
342	RWST1D
343	TTRWSTH2OD
408	BRC760CJ760AL
440	BRC762CJ762AL
464	BRC765BJ765AL
* 1271	LOCDP
1519	TESTELECP

* INDICATES LOCATION

```
FILE IDENTIFICATION
  REACH PAIR:   I= 1                    J= MLOCAD
  DATE:  6/22/84
  ANSWER.POS FILE IS: DRO:SCT615MC4.POS
  OUTPUT.DAT FILE IS: DR1:[220,1]SCT615MOT.DAT
  VARIAB.DAT FILE IS: DR1:[220,1]SCT615MVB.DAT
  RENUMSRT.DAT FILE IS: DR1:[220,1]SCT615MRT.DAT
  SIGMA PI FILE NAME IS: DRO:SCT615MSI.C4
```



SI LOCA WITH HIGH AND LOW PRESSURE INJECTION Scrb

CASE IVA & IVB

DOUBLETONS

MEDIUM LOCA WITH HIGH AND LOW PRESSURE INJECTION

CASE IVA & IVB

VARIABLE LIST FOR SC10 CASE IVA & IVB DOUBLETON MATRIX

12	PPR1810D
15	J735BD
15	J1863D
15	MOV882D
15	OPW882D
15	VC881D
15	PPI735D
15	J735AD
23	J111XD
23	JRHRD
23	J740AD
23	J636D
23	J883D
23	MOV744D
23	OPW744D
23	VC741D
23	J110XD
37	HPI-MLOCAD
* 39	LPI-MLOCAD
* 40	LFSIPD
* 42	LWSIPD
* 43	LSSIPD
285	BRC852BJ852AA
308	PWRPNL33P
338	J203AD
340	J203D
340	VC847D
340	MOV1810D
340	OPW1810D
344	J852D
* 349	LFRHRD
* 350	LSRHRD
* 351	LWRHRD
* 364	LF888D
* 365	LS888D
366	LW888D
371	BRC899BJ899AB
* 374	LFRHXRB
* 375	LSRHXRB
*376	LWRHXRB
386	BRC745AJ745BD
388	BRC889J1869BD
390	J745BD
399	JA14AL
399	JA14L
399	J830AL
399	JTIC627L
399	J627AL
401	J830BL
401	J627BAL
401	J627BBL
401	J627BCL
402	VGA760AL
402	OPW760AL
403	J1805L
404	PPR1805L
406	J760AL
407	BRC760AJ760BL
414	BRC760CJ760BL
417	OPW760CL
417	VGA760CL
419	J760CL
421	PPR627BCL
421	J787L
421	VGL787L
421	OPW787L
421	FIC634BL
421	JA59L
421	J749EL
422	JA57L
423	ORFC760CL
424	CCWP23L
428	JA55L
429	ORFC760AL
430	CCWP31L
431	ORFCCCW33L
432	VC761CL
433	JA3L
434	VGA762CL
434	OPW762CL
436	J763BL
436	VGA759BL
436	OPW759BL
436	JA8L
436	CCHXRS32Z
436	VGA765BL
436	OPW765BL
436	J764BL
438	J762CL
439	BRC762CJ762BL
448	BRC762AJ762BL
449	ORFCCCW31L
450	VC761AL
451	JA1L
452	VGA762AL
452	OPW762AL
453	J763AL
453	VGA759AL
453	OPW759AL
453	JA7L
453	CCHXRS31Z
453	JA10L
453	VGA765AL
453	OPW765AL
453	J764AL
453	PPI765AL
455	J762AL
460	JA502L
460	J017BL
460	J601BL
460	J602BL
460	J602CL
463	J765BL
467	J017AL
467	J602AL
467	J601AL
467	J601CL
467	J601DL
468	J765AL
471	J602DL
471	J756CL
471	J749BL
586	RIVHUDSONK
619	CHNLDSK
619	CHNLDS3K
619	J95AK
619	J95BK
619	J95CK
619	J95DK
626	J95FK
526	J1096AK
960	SOURCE1P
* 1270	LOCCP
* 1274	LOCRP
* 1275	LOCSP
1500	PWRPNL33/P
1551	TRIPMASTER

* INDICATES LOCATION

3.0 GENERAL QUALITATIVE RESULTS

Safety analyses normally attempt to provide two levels of insight into the behavior of complex systems; these two levels involve the qualitative and quantitative interpretation. It is standard practice to obtain and analyze qualitative information in the form of minimal cut sets and important components as a first step to be followed by quantitative results obtained by applying numerical probabilities to the cut set elements. This is the approach taken in this study.

The importance of front-line systems to reactor safety is evident from the definition of the term front-line system: a system that directly performs a vital safety function. For the evaluation of systems interactions, a detailed evaluation of support systems is also essential [18]. Systems interactions can result in the loss of a front-line system function by failure initiation and propagation through the support systems. Therefore, both qualitative and quantitative assessments of systems safety must consider front-line as well as support systems and their potential for systems interactions.

The qualitative evaluation of system safety is centered on the identification and review of minimal cut sets and important components. A cut set is a component or group of components whose failure would cause system failure. Of primary concern in the system combinations considered in this study are the minimal cut sets for the indicated front-line system function. These failure cut sets cross system boundaries and potentially include components from front-line as well as related support systems.

DMA processing is capable of identifying singleton (first order), doubleton (second order) and selected tripleton (third order) cut sets for each system combination.

3.1 Summary of Safety Significant Results

Table 1-1 in Section 1.0 provided an overall summary of the number of cut set results identified by system combination and according to the four cases of analysis considered, the first case evaluated the front-line systems themselves. The second case includes support systems as well as the front-line systems. The third case included location commonalities in addition to the complete combinations of systems. The final case included human/operator actions by incorporating procedures. The complete set of singleton and doubleton cut sets for each system combination was presented in the associated enclosures in Section 2.4.

Discussion of Results

Within the scope and limitations of the Digraph Matrix analysis to find Systems Interactions at Indian Point-3, we have reached the following conclusions:

I. When we evaluated the front-line systems while assuming that the support systems' probability of failure was zero, we found that the safety injection and feedwater front-line systems were robust.

II. When we evaluated the interactions of both front-line and support systems, we found the following significant systems interactions:

A. Interlock Failures in the IP-3 480 V Electrical System

There are two interlocks in the 480 V electrical system which can cause serious systems interactions should either one fail during particular accident sequences.

The interlocks in question are on the manual 480 V crosstie breakers 2AT5A and 3AT6A. In the event of bus undervoltages such as caused by a loss of offsite power, failure of these interlocks prevents the diesel generators from being automatically loaded onto the buses, bringing about a loss of ac power condition. This condition requires operator action to correct.

The interlocks are modeled as in Figures B 6.1 - B 6.13. Node ITLBKR3AT6A is directly connected to the automatic closing mechanism for BKR2AT3A, the automatic 480 V crosstie, and for BKRE62, the diesel generator supply breaker for bus 6A. Node ITLBKR2AT5A is directly connected to the automatic closing mechanism for BKREG3 and BKREG1, the diesel generator supply breaker for bus 5A and bus 2A respectively.

If the diesel generators are called on to start, as in a loss of offsite power condition for example, failure of the 3AT6A interlock prevents breakers 2AT3A and EG2 from closing, thereby causing a loss of all components powered from buses 3A and 6A. Failure of the 2AT5A interlock prevents closure of breakers EG3 and EG1, thereby causing a loss of all components powered from buses 5A, 2A, and 3A. Note the operator can restore power to the buses by closing the breakers either from switches in the control room or diesel building, or manually at the breakers.

Both interlocks function similarly. They are known as "b" contact auxiliary switches. When the manual crosstie breakers are open, the "b" contacts are closed and the closing circuits for the interlocked breakers may be completed, providing dc power is available and all other interlocks are satisfied. If a manual crosstie is closed or if the interlock fails such that the "b" contacts do not close the circuit when the breaker is open, then the interlocked breakers will not close automatically. 480V switchgear schematic diagrams show the interlocks in the automatic closing circuits for these breakers. Refer also to IP-3 System Description No. 27.1, pages 65A-65C, for substantiation of this interlock function explanation.

The effects of an interlock failure can be quite serious. In a loss of offsite power automatic case, the 3AT6A interlock is a singleton to buses 3A and 6A. Note that auxiliary feedwater pumps 31 and 33 are affected, leaving only the steam driven pump in this case. Also, both residual heat removal pumps (31 and 32) are lost.

Failure of the 2AT5A interlock under the above conditions causes the loss of components on buses 5A, 2A, and 3A. This includes safety injection pumps 31 and 32, essential service water pumps 31 and 32 or 34 and 35, and component cooling pumps 31 and 32. In this case, three safety systems, safety injection, service water, and component cooling, are each left with only one pump functioning.

The effects of the 3AT6A interlock failure can be easily mitigated if the motor driven auxiliary feedwater pump 31 and RHR pump 31 are powered from bus 5A or 2A instead of 3A. However, failure of the 2AT5A interlock is devastating and the best solution is to remove it from the breaker closing circuits. The 2AT5A crosstie should then be removed or locked open so that it cannot be inadvertently closed.

B. Service Water Valves SWN-98 and SWN-99

The Indian Point-3 Nuclear Plant has three diesel generators (DGs). The DGs must be cooled in order to keep from failing due to overheating. The cooling is accomplished by transferring heat to the Service Water System (SWS) which is designed to circulate river water through DG heat exchangers when the DGs are in use. Loss of this cooling will result in failure of the DGs due either to protective shut off or damage due to overheating within a few minutes of loss of heat removal.

To ensure heat removal capability during an accident, the SWS is configured into two redundant piping trains, each with its own dedicated set of three service water pumps (SWPs). In preparation for automatic response during accident, one pump train is preselected as "Essential" and the other as "Non-essential". One train uses pumps 31-33 and the other uses pumps 34-36. Almost always, pumps 34-36 are selected as essential. Only two pumps are required for heat removal immediately after an accident. During normal plant operation, pumps from both sets are generally running, though not through the DGs. In the event of high DG oil or jacket water temperature or of safety injection (SI) signal, valves on the common downstream side of the DGs are opened to allow service water flow through. The non-essential pumps are tripped and the essential pumps are powered (during a blackout, the essential pumps are powered by the DGs before the DGs become too hot). The two SWP trains are normally isolated from each other and the valves on the non-essential train are normally aligned to preclude DG cooling by the non-essential pumps. This relationship also holds after the blackout or SI. Therefore, after an accident, the DGs are normally cooled by a single SWP train. This presents some noteworthy vulnerabilities.

Failure of DGs to Generate Power Due to Misaligned Valves: Each SWP train has two butterfly valves in series, either of which if closed and undetected, would mean failure of DGs to be cooled immediately after an accident, should that train have been selected as essential. If SWPs 31-33 are selected as essential, then the valves are SWN-98 and SWN-30. If SWPs 34-36 are selected as essential, then the valves are SWN-99 and SWN-29. Misalignment of any of the valves could result from inaccurate application of the checkoff list or of a maintenance or testing error. However, the means of detecting misalignment of SWN-98, 99 is very different from that of SWN-29, 30.

A misalignment in the first set is fairly easily detected since there is normally flow through each valve and just downstream of each valve is a pressure meter which is connected to an indicator light and annunciator in the central control room. Therefore, during normal plant operation a misalignment would be indicated automatically. Misalignment of either of the other valves (SWN-29, 30), however, is not automatically detected. After the initial procedure of following the checkoff list, inspection of the valve position consists of monitoring a local pressure gauge every 8 hours. The location of the pressure tap is shown in Figure 2-7 which is a copy of a section of the main SWS P&ID 9321-F-27223-21. Also noted are butterfly valves 29 and 30. The other butterfly valves mentioned above, numbers 98 and 99, are off the page. If SWRs 31-33 are selected as essential, then SWN-30 is normally open as are SWNs-62A, C, and E, which lie just upstream of each diesel heat exchanger pair.

III. When we evaluated front-line and support systems with location vulnerabilities, we identified several key locations though we did not find initiating events.

Locations LOCDP (480 V bus location), LOC001 (AFW pump room), LOCSIPRM (SI pump room), were vitally important and presently secure.

IV. When we evaluated front-line and support systems together with their location vulnerabilities and their interactions with operator actions, we concluded:

A. Operator actions that initiate safety actions, such as starting pumps and opening valves, greatly improves reliability and should generally be recommended for both safety injection and feedwater systems.

B. Operator actions that terminate safety actions, such as stopping pumps or closing valves, should only be allowed with the concurrence of a supervisor.

C. That there is a significant difference between operator actions dealing with front-line systems instead of support systems.

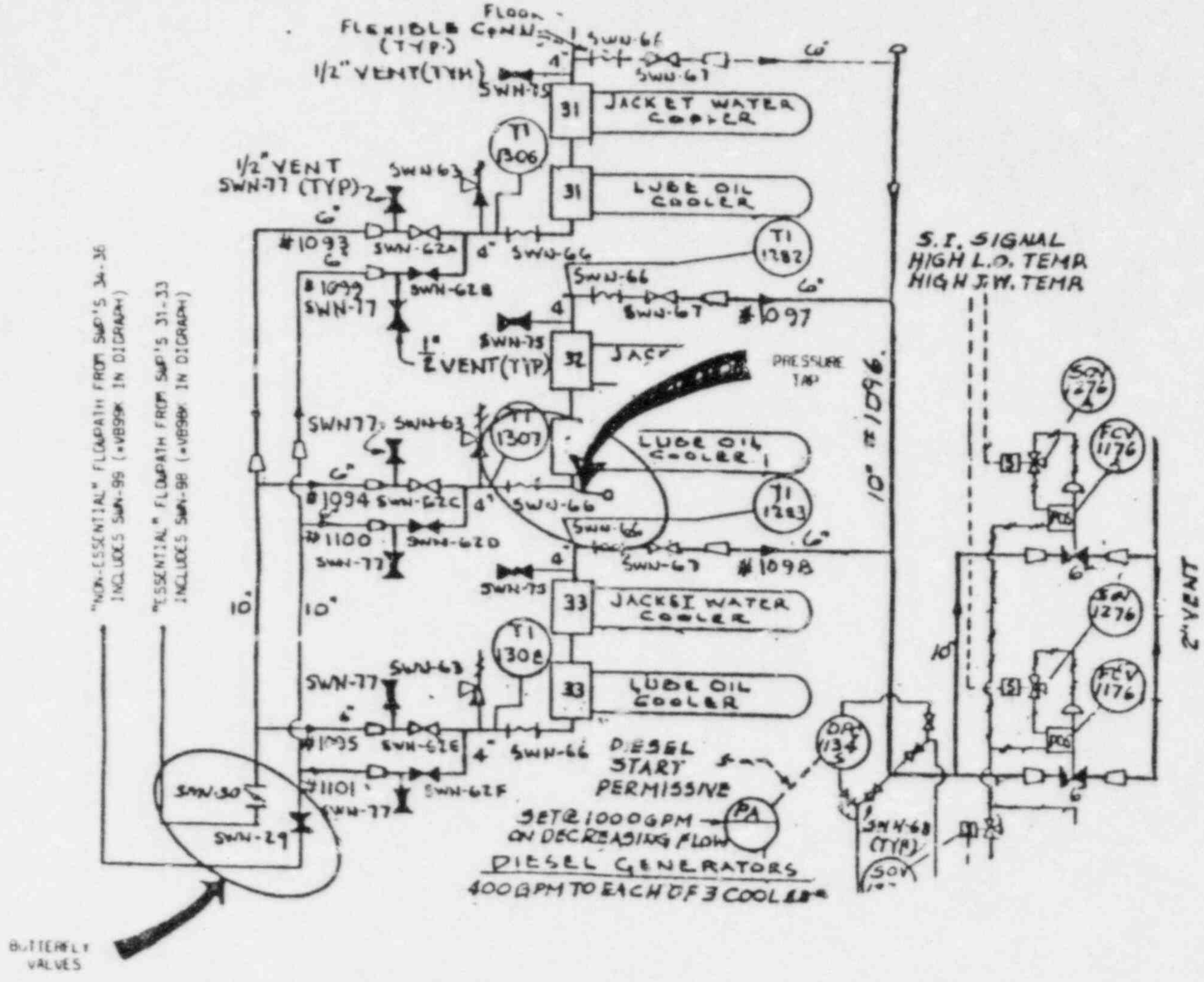


FIGURE 2-7 FLOWPATHS TO DIESEL GENERATOR HEAT EXCHANGERS CORRESPONDING TO SELECTION OF SWP'S 31-33 AS "ESSENTIAL" ⧓ = NORMALLY CLOSED (FROM U.E. AND C. DWG. NO. 9321-F-27223-21 AND CHECK-OFF LIST COL-RW-2)

4.0 QUANTITATIVE ANALYSIS

In order to determine the significance of the singleton and doubleton cut sets, 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, IEEE Standard 500, the Zion Seismic Safety Study, and the Indian Point Probabilistic Safety Study. Where available, Indian Point data was used to allow comparison to the IP PSS. Four cases were analyzed. In the first three cases, we considered only the fully automatic action. In the fourth case, the operator was able to take mitigating action and allowed to make errors.

In the subsections which follow, the results of the quantitative analysis of the ten system combinations are presented. These results are based on the component failure and unavailability data given in Appendix D. For the most part this data was taken from the Indian Point Probabilistic Safety Study [14] in order to maintain comparability. Exceptions to the use of Indian Point data are given in the data of Appendix D. Four cases were analyzed for each system combination. These are listed in Table 4-1.

Case	Mode	Description
I	Automatic	Front-line Systems Only
II	Automatic	Front-line + Support Systems
III	Automatic	Front-line + Support Systems + Locations
IV	Manually Assisted	a. Positive Operator Intervention b. Positive and Negative Operator Intervention

Table 4-1 Cases Analyzed for Quantitative Results

As shown in Table 4-1, system combinations were analyzed for two types of operation, fully automatic and manually assisted. In the fully automatic case, no credit was given to operator circumvention of the effects of failed components and/or systems. In the manual case, two types of operator intervention are allowed; operator actions to mitigate the effects of component failures; and operator errors. Operator errors were assumed to be independent. That is, no attempt was made to analyze the effect of coordinated errors. The variable names for the first type of operator interaction with the system always includes the prefix OPR (operator right) where as the second type starts with OPW (operator wrong). Appendix D.2 contains a more complete discussion of the two types of operator actions.

In all cases, a count of the number of singletons and doubletons are given. This count includes only failure sets which have nonzero probability. For example, some of the singletons shown earlier in this report include test nodes. Since no failure probability is assigned to these nodes, they are not counted in the failure set totals. Other singletons not included in these counts arise from components which are subcomponents of components for which there is failure data. For example, a part of a motor actuated valve may show up as a singleton, but since the failure data base did not break MOV failure to failure of its subcomponents, only the MOV failure itself was counted.

- In general, component failure probability and unavailablity data was taken from the Indian Point Probabilistic Safety Study (IP-PSS) section 1.6 (primarily Table 1.6.1-4). This data base contains (Bayesian) updated failure rates for the IP components based on actual operating IP experience.

In using this data base, no statement is made about its accuracy. The IP PSS data base was used only to allow a direct comparison to be made between the results of the DMA and those of the IP PSS.

The tables in Appendix D contain the probability data bases as used for each system combination. The format of these tables is:

MOV822BL	MOV221	2	0.151E-02 -0.915E-07
Component Name	Generic Type	Number of Probability Terms	Minus sign indicates rate (failures/hr)

@ MOTOR OPERATED VALVE

Thus, valve MOV822BL is of generic class MOV221, a motor operated valve, normally closed, which must change state, and has a failure to operate on demand probability of 0.15E-02 per demand and a blockage failure rate of 0.915E-07 failures per hour. Lines in the data base which begin with a @ symbol contain explanatory information.

To compute the overall failure probability for a specific component in the data base, all of the failure terms are combined using the rules for combinations of probability for independent events. That is

$$P_{TOTAL} = 1-\prod_{i=1}(1-P_i)$$

where Ptotal is the total failure probability for the component
P_i is the probability of the ith failure mode.

The probability of failure for components which had hourly rates was determined by multiplying the failure rate by the action time of the accident sequence.

As stated above, failure and unavailability data was taken from the IP PSS when available. In some cases, specific data was not available. We have assumed in most of these cases, that the component was operational at the time of the accident, hence its failure probability is simply the duration of the accident times its failure rate (failure/hr). This calculation yields a lower bound for the component failure probability.

The data base listed in Appendix D was adjusted for the conditions of each system combination.

4.1 Quantitative Analysis of System Combination 1-Medium LOCA with Low Pressure Injection

Introduction

The probability that the Indian Point-3 Low Pressure Injection system will be available and function through the one-half hour required response to a medium LOCA has been evaluated. This analysis included both fully automatic operation and performance with operator assistance. The effects of failures in support systems were explicitly included in this analysis. Because of the completeness of the DMA model, no assumptions were made about the availability of offsite electrical power, safety injection actuation, service water, or component cooling. All components in these systems were included in the basic digraph model. Unavailability (and failure) contributions from these systems and combinations of these support systems are explicitly included in the failure sets.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Water from the Refueling Water Storage Tank (RWST) is available.

2. Success of Low Pressure Injection is defined as the injection of water into at least two cold legs of the Reactor Coolant System with at least one Residual Heat Removal Pump operating.

3. The time requirement for LPI is 0.5 hours.

Probability Data Base

The data used for the quantitative analysis of System Combination 1 is listed in Appendix D. This data was taken (for the most part) from the Indian Point Probabilistic Safety Study. Exceptions to Indian Point data are noted in the data base of Appendix D. Operator error was assigned a probability of 1 x 10^{-3}. Operators were allowed to disable any component which could be turned off except for components located inside of containment which had no control room remote switches. For the manually assisted cases studied, it was assumed that an operator would take a correct override action with a probability of 1.0.

Results

There were four cases studied:

1. Automatic Operation, Front-line systems only,

2. Automatic Operation, Front-line and support systems,

3. Automatic Operation, Front-Line, support systems, and locations, and

4. Manual Operation

    1. Operator Override of Failed Components

    2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

Table 4-2 contains a summary of the results from the four cases analyzed. The data in the rows referred to "probability" is the probability that a system will be available and continue to function during the accident. As can be seen from this table, in all cases the bulk of the failure probability (and unavailability) is due to single component failures. The ability of the operators to override failed components does not significantly improve the reliability of the Low Pressure Injection System. The LPI is however, significantly less reliable when the effects of operator errors are considered. In this system combination, it appears that the safest mode of operation would be to prevent the operators from taking any action. It should be stated that the above result probably overestimates the effect of detrimental operator actions, since the DMA model did not include any safequards which would prevent some of these incorrect actions. Each case will now be briefly discussed.

Case I - Front-Line Systems Only

The most risk significant singletons from an analysis of the front-line systems alone are shown along with their failure probabilities in Table 4-3 (The complete list of singleton and doubletons is given in Enclosure 1). The failure probabilities shown in this table include both unavailability at the time of the accident and failure during the 0.5 hour mission time.

Component	Mean Failure Contribution
MOV882D	6.01E-04
VC881D	6.91E-05
VC741D	6.91E-05
MOV744D	3.29E-05
VGA846D	3.29E-05

Table 4-3 Most Risk Significant Singletons in System Combination One

CASE	I	II	III	IV	
Description	AUTOMATIC	AUTOMATIC	AUTOMATIC	MANUAL	
	Front Line Alone	Front Line + Support*	Front Line + Support + Location	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	17	17	28	16	18
Singleton Probability Contribution	8.05E-4	9 [illegible]E-4	N/A	8.05E-4	2.81E-3
Number of Doubletons	84	2465	2180	1854	2128
Doubleton Probability Contribution	2.50E-6	3.79E-6	N/A	2.77E-6	2.39E-5
Singleton + Doubleton Failure Probability	8.07E-4	8.14E-6	N/A	8.08E-4	2.83E-3

* Includes Battery 32 Singleton.

Table 4-2 Summary of Quantitative Results for System Combination One - Low Pressure Safety Injection in Response to Medium LOCA

These components were also identified as singletons in the Indian Point Probabilistic Safety Study. The remaining 12 singletons are pipe sections with individual failure probabilities on the order of 4E-9. These remaining singletons do not contribute significantly to the overall failure probability.

The doubletons are dominated by the failure of the two Residual Heat Removal pumps, RHRP31Z and RHR32Z. This failure set has a failure probability of 2.06E-06. The IP PSS quotes a value of 3.29E-06 for this doubleton. The IP-3 RHR doubleton however includes a check valve and manual valve for each pump which we have modeled as separate components and therefore appear in other failure sets (e.g., VC738AB * RHRP32Z).

The remaining doubletons can be grouped into "order of magnitude" sets. The 10^{-8} magnitude group includes:

RHRP31Z	VC738BD	9.92E-08
VC738AD	RHRP32Z	9.92E-08
MOV747B	HCV640B	1.80E-08
MOV747B	MOV746B	1.80E-08
VGA742D	MOV745BD	1.80E-08
MOV899BB	MOV899AB	1.80E-08
MOV747B	MOV899AB	1.80E-08
HCV638B	HCV640B	1.80E-08
VGA742D	MOV745AD	1.80E-08
HCV638B	MOV746B	1.80E-08
MOV899BB	MOV746B	1.80E-08
MOV899BB	HCV640B	1.80E-08
HCV638B	MOV899AB	1.80E-08
RSI2H	RHRP31Z	1.67E-08
RSI21XZ	RHRP31Z	1.67E-08

The total failure probability due to doubletons for the Front-Line System Low Pressure Injection in response to a medium LOCA is 2.50E-6. Since the IP PSS did not consider front-line systems alone, no comparison can be made.

Case II - Front-line and Support Systems

The addition of the support systems to the analysis of the failure of low pressure injection does not change the number of singletons (17) but does significantly increase the number of doubletons (from 84 to 2349). The large increase in the number of doubletons does not significantly raise the failure probability of the system (from 2.5E-6 to 3.65E-6). The most significant added doubletons are:

STAUXXFMRP * SW123456P	3.41E-07
STAUSSFMRP * COL-RW-2K	3.41E-07

The variable name STAUXXFMRP includes both the failure of the station auxiliary transformer and the loss of offsite power. The loss of offsite power dominates the failure of the transformer (3.41E-04 to 0.84E-06/hr). Variable SW123456P refers to an incorrect setting of the service water mode switch prior to the accident. The variable

COL-RW-2K is an error in the manual checkoff procedure for the sevice water pumps prior to the accident. The prominence of offsite power in the doubletons implies that this system combination would have a significantly larger failure probability (singletons in the 10E-2 to 10E-3 range) during an offsite power outage. This would occur because doubletons with offsite power would become singletons.

Again the results of the DMA of the Low Pressure Injection system yield quantitative results of the same order as the IP PSS (3.65E-6 to 6.09E-6).

Case III - Front-Line, Support Including Locations

The addition of locations to the front-line plus support systems adds 11 singletons and 75 doubletons to the failure sets. These locations were discussed earlier.

Case IV - Manual Operation

The Indian Point Low Pressure Safety Injection System was designed with ample opportunity for operators to override failed components. The cases studied here assume that if an automatic system fails, the operators will take the appropriate corrective action. Failure to take this corrective action has been assigned a probability of 0.0. Thus it would be expected that the low pressure injection system becomes more reliable in this manual case.

Two subcases were considered in the manual case; only operator corrective action, and both corrective and detrimental operator actions. The results of each of these subcases will now be discussed.

Case IVa - Manual Operation - Corrective Action Only

In this subcase, operators are allowed to take corrective action. The probability of taking these actions has been taken to be 1.0. The ability to take these corrective actions did not change the singleton failure probability from the automatic case (II). However, the failure contributions from the doubletons decreased from 3.49E-6 to 2.77E-6. This insignificant decrease results from operator override of failed components.

It should be noted here that the operators do not have a significant positive effect on the reliability of Low Pressure Safety Injection.

Case IVb - Corrective and Detrimental Actions

In this subcase, the operators are allowed to take both corrective and detrimental actions. These detrimental actions are "errors of commission" since they require an action by the operator to cause an error. The probability of each of these types of errors was taken to be 1.0E-3.

These errors of commission increased the singleton probability from 8.05E-4 in case IVa to 2.81E-3 and the doubleton probability from 2.77E-6 to 2.39E-5. The singletons with the largest value are incorrect operator actions in closing valves

VGA846D,
MOV882D, and
MOV744D.

These three failures dominate the singleton failure probability.

4.2 Quantitative Analysis of System Combination 2-Medium LOCA with High Pressure Injection

Introduction

The failure of the Indian Point-3 High Pressure Injection system to respond to and function during the low range of a medium LOCA has been evaluated.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Water from the Refueling Water Storage Tank (RWST) is available.
2. Success of High Pressure Injection for the low range of the LOCA is defined as the injection of water into the Reactor Coolant System by at least two of the three high head safety injection pumps.
3. The time requirement for HPI is 0.5 hours.

Results

There were four cases studied:

1. Automatic Operation, Front-line systems only,
2. Automatic Operation, Front-line and support systems,
3. Automatic Operation, Front-Line, support systems, and locations, and
4. Manual Operation
    1. Operator Override of Failed Components
    2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

Table 4-4 contains a summary of the results from the four cases analyzed. As can be seen from this table, in all cases the bulk of the failure to successfully function is due to single component failures. The ability of the operators to override failed components does not significantly improve the reliability of High Pressure Injection System. High Pressure Injection, however, is significantly less reliable when the effects of operator errors are considered. In this system combination, as with low pressure injection, it appears that the safest mode of operation would be to prevent the operators from taking any action. It should be stated that the above result probably overestimates the effect of detrimental operator actions,

CASE	I	II	III	IV	
Description	AUTOMATIC	AUTOMATIC	AUTOMATIC	MANUAL	
	Front Line Alone	Front Line + Support	Front Line + Support + Location	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	9	28	34		
Singleton Probability Contribution	7.03E-4	7.03E-4	N/A	1.03E-7	1.03E-7
Number of Doubletons	535	4426	4552		
Doubleton Probability Contribution	2.97E-5	4.46E-4			1.04E-4
Singleton + Doubleton Failure Probability	7.32E-4	11.49E-4	N/A		1.04E-4

Table 4-4 Summary of Quantitative Results for System Combination Two - High Pressure Safety Injection in Response to Medium LOCA

since the DMA model did not include any safeguards which would prevent some of these incorrect actions. Each case will now be briefly discussed.

Case I - Front-Line Systems Only

The risk significant singletons from an analysis of the front-line systems alone are shown along with their failure probability in Table 4-5. (The complete list of singletons and doubletons is given in Enclosure 2.)

Component	Mean Failure Contribution
MOV1810D	6.01E-04
VGA846D	3.29E-05
VC847D	6.91E-05

Table 4-5 Risk Significant Singletons in System Combination Two

These components were also identified as singletons in the Indian Point Probabilistic Safety Study. The remaining singletons are pipe sections with individual failure probabilities on the order of 4E-9. These remaining singletons do not contribute significantly to the overall failure probability.

The doubletons are dominated by the failure of combinations of the safety injection pumps, SIP31Z, SIP32Z, and SIP33Z. Each of these has a failure probability (including unavailability) of 5.08E-6.

The remaining doubletons in the 10^{-6} group are listed below.

SIP31Z	SIP33Z	5.08E-06
SIP32Z	SIP33Z	5.08E-06
SIP31Z	SIP32Z	5.08E-06
MOV887AD	SIP33Z	1.35E-06
MOV887BD	SIP33Z	1.35E-06
SIP31Z	VGA848BA	1.35E-06
VGA848AA	SIP33Z	1.35E-06
SIP32Z	VGA848BA	1.35E-06
MOV887AD	SIP31Z	1.35E-06
MOV887BD	SIP31Z	1.35E-06
VGA848AA	SIP32Z	1.35E-06

The total failure probability due to doubletons for the Front-Line System Low Pressure Injection in response to a medium LOCA is 3.02E-6. Since the IP PSS did not consider front-line systems alone, no comparison can be made.

Case II - Front-Line and Support Systems

The addition of the support systems to the analysis of the failure of high pressure injection significantly increases the the number of singletons (9 to 28) and also significantly increases the number of doubletons (from 535 to 4504). The large increase in the number of doubletons significantly raises the failure probability of the system (from 3.02E-5 to 4.47E-4). The most significant added doubleton is:

STAUXXFMRP * ITLBKR2AT5AP 4.15E-04

The variable STAUXXFMRP includes the failure of the station auxiliary transformer and the loss of offsite power. The loss of offsite power dominates the failure of the transformer (3.41E-04 to 0.84E-06/hr). Variable ITLBKR2AT5AP refers to the failure of an interlock in the IP-3 Electrical Power System. The prominence of offsite power in the doubletons implies that this system combination would have a significantly larger failure probability (singletons in the 1.E-2 to 1.E-3 range) during an offsite power outage.

The results of the DMA of the High Pressure Injection system yield quantitative results higher than those of the IP PSS (4.80×10^{-4} to 1.81×10^{-4}). Also it should be noted that the contribution of the doubletons is over one order of magnitude greater than the singletons. The loss of offsite power - interlock doubleton alone is an order of magnitude greater than the singleton. This doubleton was not identified in the IPS PSS.

Case III - Front-Line, Support Including Locations

The addition of locations to the front-line plus support systems adds 6 singletons and 126 doubletons to the failure sets. These locations were discussed earlier.

Case IV - Manual Operation

Two subcases were considered in the manual case; only operator corrective action, and both corrective and detrimental operator actions. The results of each of these subcases will now be discussed.

Case IVa - Manual Operation - Corrective Action Only

In this subcase, operators are allowed to take corrective action. The probability of taking these actions has been taken to be 1.0. The ability to take these corrective actions did not change the singleton failure probability from the automatic case (II). However, the failure contributions from the doubletons decreased from 4.46E-4 to 2.265E-5. This significant decrease results from operator override of failed components.

Case IVb - Corrective and Detrimental Actions

In this subcase, the operators are allowed to take both corrective and detrimental actions. These detrimental actions are "errors of commission" since they require an action by the operator to cause an error. The probability of each of these types of errors was taken to be 1.0E-3.

These errors of commission increased the singleton probability from 3.3E-5 in Case IVa to 1.03E-3 and the doubleton probability from 2.25E-5 to 8.06E-5. The singleton with the largest value is an incorrect operator action in closing valve VGA846D. This failure dominates the singleton failure probability.

4.3 Quantitative Analysis of System Combination 3-PORV Induced LOCA with High Pressure Injection

Introduction

The reliability (and unavailability) of the combination of the Indian Point-3 PORV and High Pressure Injection system is discussed in this section. The singletons which should result from this analysis are the intersection of the singletons from the failure of the PORV and the singletons from the failure of high pressure injection. This analysis included both fully automatic operator and performance with operator assistance.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Success of High Pressure Injection is defined as the injection of water into at least two cold legs of the Reactor Coolant System with at least one Residual Heat Removal Pump operating.

2. The time requirement for HPI is 0.5 hours.

Results

There were four cases studied:

1. Automatic Operation, Front-line systems only,

2. Automatic Operation, Front-line and support systems,

3. Automatic Operation, Front-Line, support systems, and locations, and

4. Manual Operation

   1. Operator Override of Failed Components

   2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

Table 4-6 contains a summary of the results from the four cases analyzed. As can be seen from this table, in all cases the bulk of the failure probability (and unavailability) is due to single component failures. The ability of the operators to override failed components does not significantly improve the reliability of the High Pressure Injection System. Each case will now be briefly discussed.

Case I - Front-Line Systems Only

There were no front-line singletons found which would induce a PORV failure and also cause the failure of High Pressure Injection.

CASE	I	II	III	IV	
Description	AUTOMATIC	AUTOMATIC	AUTOMATIC	MANUAL	
	Front Line Alone	Front Line + Support	Front Line + Support + Location	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	0	0	0	0	0
Singleton Probability Contribution	0	0	0	0	0
Number of Doubletons	28	28	63	12	12
Doubleton Probability Contribution	2.30E-6	2.30E-6	0	9.87E-7	9.87E-7
Singleton + Doubleton Failure Probability	2.30E-6	2.30E-6	0	9.87E-7	9.87E-7

Table 4-6 Summary of Quantitative Results for System Combination Three - PORV Induced LOCA with High Pressure Injection

Each doubleton in the combination front-line system, as expected, arises from one singleton from HPI and one singleton from the PORV. The doubletons can be grouped into "order of magnitude" sets. The 10^{-7} magnitude group includes:

VGA846D	PCV464I	3.29E-07
VGA846D	PCV455CI	3.29E-07
VGA846D	SOV455CI	3.29E-07
VGA846D	PCV468I	3.29E-07
VGA846D	PCV456I	3.29E-07
VGA846D	PCV466I	3.29E-07
VGA846D	SOV456I	3.29E-07

The total failure probability due to the 28 doubletons for the Front-Line System High Pressure Injection failure in combination with a PORV failure is 2.30E-6.

Case II - Front-Line and Support Systems

The addition of the support systems to the analysis of the failure of high pressure injection does not add any singletons or doubletons.

Case III - Front-Line, Support Including Locations

The addition of locations to the front-line plus support systems adds 35 doubletons to the failure sets. These locations were discussed earlier.

Case IV - Manual Operation

The Indian Point High Pressure Safety Injection System was designed with ample opportunity for operators to override failed components. The cases studied here assume that if an automatic system fails, the operators will take the appropriate corrective action. Thus, it would be expected that the high pressure injection system becomes more reliable in this manual case.

Two subcases were considered in the manual case; only operator corrective action, and both corrective and detrimental operator actions. The results from each subcase are identical. The ability to take these corrective actions completely eliminated all doubletons in the combination of a PORV failure and HPI failure for front-line systems alone. It was found that allowing the operator to override failed components decreased the number of doubletons from 28 to 12 with a corresponding decrease in failure probability from 2.30E-6 to 9.87E-7. There were no doubletons found which include an operator act of commission.

4.4 Quantitative Analysis of System Combination 4-Reactor Coolant Pump Seals Induced S2 LOCA with High Pressure Injection

Introduction

The reliability of the Indian Point-3 High Pressure Injection system to an S2 LOCA induced by a failure of the Reactor Coolant Pump Seals has been evaluated. In this case, we analyzed whether there was a systems interaction which could cause a failure of the RCP seals and also prevent successful functioning of HPI. In order to accomplish this analysis, two plant operating modes were analyzed, each with its own model. The first mode is normal automatic plant operation. From that model, singletons and doubletons are found which result in the failure of the RCP seals, thus initiating a LOCA. The second operating mode is the plant's automatic response to the LOCA. From that model, singletons and doubletons are found which keep the safety injection system from succeeding. Thus, failure sets common to the models represent failure(s) that both cause the LOCA AND keep the safety injection system from responding.

That is, in this system combination, singletons and doubletons which are common to the RCP seals and the High Pressure Injection system are analyzed. Components in the service water system were found to be common to both systems. It should be noted that the reliability numbers found for this system combination are qualitatively different from those for injection alone. In the earlier discussions, the reliablity results have to be multiplied by the probability of the externally caused LOCA. In this case, the reliability answer includes the probability of the initiator (LOCA due to loss of RCP seals). In the earlier results the frequency of core damage is given by

$$C_f = I_f * P_s$$

where

C_f is the frequency of core damage,
I_f is the initiator frequency, and
P_s is the probability that the safety system does not function.

In the Indian Point PSS, the initiator (the LOCA) frequency was in the range of 10E-3. Thus, the core damage probabilities would be in the 10^{-6} range. In this case, that of a LOCA and failure to respond due to the same systems interaction, the resulting core damage frequency is the same as the system combination frequency.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Water from the Refueling Water Storage Tank is available.

2. Success of High Pressure Injection for this LOCA* is defined as the injection of water into the Reactor Coolant System by at least one of the three high head safety injection pumps.

3. The time requirement for HPI is 0.5 hours.

Results

There were four cases studied:

1. Automatic Operation, Front-line systems only,

2. Automatic Operation, Front-line and support systems,

3. Automatic Operation, Front-Line, support systems, and locations, and

4. Manual Operation

    1. Operator Override of failed Components

    2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

In the fourth case, it was assumed that the operator would correctly set the service water system valves. Table 4-7 contains a summary of the results from the four cases analyzed. As can be seen from this table, in all cases the bulk of the failure probability (and unavailability) is due to single component failures. The ability of the operators to override failed components does not significantly improve the reliability of High Pressure Injection System. High pressure injection is however, significantly less reliable when the effects of operator errors are considered.

Case I - Front-Line Systems Only

There were no singletons between the RCP seals and the safety injection system. (The complete list of singletons and doubletons is given in Enclosure 4.)

The front-line system doubletons are risk insignificant with the highest doubleton on the order of 8.72E-12.

The total failure probability due to doubletons for the Front-Line System High Pressure Injection in response to RCP Seals induced small LOCA is 1.39E-10.

----

* It was determined that the four RCP seals would leak at a rate of about 2000 gpm.

CASE	I	II	IV	
Description	AUTOMATIC	AUTOMATIC	MANUAL	
	Front Line Alone	Front Line + Support	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	0	0	0	0
Singleton Probability Contribution	0	0	0	0
Number of Doubletons	0	3	0	0
Doubleton Probability Contribution	0	See Text	0	0
Singleton + Doubleton Failure Probability	0	See Text	0	0

Table 4-7 Summary of Quantitative Results for System Combination Four – High Pressure Injection in Response to RCP Seals Induced LOCA

Case II - Front-Line and Support Systems

As discussed earlier, this sytem combination occurs across two time phases; before the LOCA, and after the LOCA. There were no singletons found which were common to the RCP seals prior to their failure and to the safety injection system after seals failure.

There were, however, doubletons found which were common to systems used in both plant modes. These were shown in Figures 2-11a and 2-11b and are the

offsite electrical power * service water valve

and

offsite electrical power * interlock 2AT5A

The total failure probability arises from the doubletons. This calculation is difficult since the first time phase has an indefinite period. That is, the offsite electrical power could fail at any time from the resulting of the service water valve. The service water valves are "administrately controlled" and checked by a (very) downstream pressure reading every eight hours. We can not assign a failure probability to these doubletons given the indefinite time span and our lack of knowledge about valve setting and checking procedures.

Case III - Front-Line, Support Including Locations

The addition of locations to the front-line plus support systems adds 1 singleton and 630 doubletons to the failure sets. These locations were discussed earlier.

Case IV - Manual Operation

The Indian Point High Pressure Safety Injection System was designed with ample opportunity for operators to override failed components. The cases studied here assume that if an automatic system fails, the operators will take the appropriate corrective action. This operator action eliminates the service water singletons.

4.5 Quantitative Analysis of System Combination 5-Turbine Trip with Main and Auxiliary Feedwater

Introduction

The reliability (and unavailability) of the Indian Point-3 Main and Auxiliary Feedwater Systems after a turbine trip system has been evaluated.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Success of Auxiliary Feedwater depends on the start of one motor-driven or turbine-driven pump.

2. The time requirement for feedwater in response to the turbine trip is 0.5 hours.

Results

There were four cases studied:

1. Automatic Operation, Front-line systems only,

2. Automatic Operation, Front-line and support systems,

3. Automatic Operation, Front-Line, support systems, and locations, and

4. Manual Operation

    1. Operator Override of failed Components

    2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

Table 4-8 contains a summary of the results from the four cases analyzed. As can be seen from this table, there were no singletons or doubletons detected in the manually assisted case (IVa). Only when operators were allowed to make errors of commission did any doubletons appear. These were risk insignificant.

The entire contribution in the automatic case is due to four singletons in the front-line systems which will now be discussed.

CASE	I	II	III	IV	
Description	AUTOMATIC	AUTOMATIC	AUTOMATIC	MANUAL	
	Front Line Alone	Front Line + Support	Front Line + Support + Location	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	4	4	8	0	0
Singleton Probability Contribution	1.04E-4	1.04E-4	N/A	0	0
Number of Doubletons	0	0	35	0	4
Doubleton Probability Contribution	0	0	N/A	0	4.74E-10
Singleton + Doubleton Failure Probability	1.04E-4	1.04E-4	N/A	0	4.74E-10

Table 4-8 Summary of Quantitative Results for System Combination Five - Main and Auxiliary Feedwater with Turbine Trip

All Automatic Cases (I, II, and III)

The singletons from an analysis of all cases are shown along with their failure probability in Table 4-9. (The complete list of singletons and doubletons is given in Enclosure 5.)

Component	Mean Failure Contribution
VGA64F	8.02E-5
VBVT6F	2.36E-5
TANKCSTF	7.12E-8
HDR1072X1073F	4.30E-9

Table 4-9 Singletons in System Combination Five

The addition of locations to the front-line plus support systems adds 8 singletons to the failure sets. These locations were discussed earlier.

Case IV - Manual Operation

The Indian Point Feedwater systems were designed with ample opportunity for operators to override failed components. The cases studied here assume that if an automatic system fails, the operators will take the appropriate corrective action. Failure to take this corrective action has been assigned a probability of 0.0. Thus, it would be expected that the high pressure injection system becomes more reliable in this manual case.

Two subcases were considered in the manual case; only operator corrective action, and both corrective and detrimental operator actions. The results of each of these subcases will now be discussed.

Case IVa - Manual Operation - Corrective Action Only

In this subcase, operators are allowed to take corrective action. The probability of taking these actions has been taken to be 1.0. The ability to take corrective action eliminated all singletons.

Case IVb - Corrective and Detrimental Actions

In this subcase, the operators are allowed to take both corrective and detrimental actions. These detrimental actions are "errors of commission" since they require an action by the operator to cause an error. The probability of each of these types of errors was taken to be 1.0E-3.

These errors of commission increased the doubleton probability from 0 in case IVa to 4.74E-10.

4.6 Quantitative Analysis of System Combination 6-Loss of Feedwater with Turbine Trip and Loss of Offsite Power

Introduction

The reliability of the Indian Point-3 Feedwater systems has been evaluated for response to a turbine trip with the loss of offsite power.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Success of Auxiliary Feedwater depends on the start of at least one motor-driven or turbine-driven feedwater pump in response to the turbine trip.

2. The time requirement for feedwater is 0.5 hours.

Results

There were four cases studied:

1. Automatic Operation, Front-line systems only,

2. Automatic Operation, Front-line and support systems,

3. Automatic Operation, Front-Line, support systems, and locations, and

4. Manual Operation

    1. Operator Override of failed Components

    2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

Table 4-10 contains a summary of the results from the four cases analyzed. As can be seen from this table, the bulk of the failures are due to the contributions of component failures. The ability of the operators to override failed components significantly improves the reliability of the feedwater systems in the case of the loss of offsite power. Each case will now be briefly discussed.

CASE	I	II	III	IV	
Description	AUTOMATIC	AUTOMATIC	AUTOMATIC	MANUAL	
	Front Line Alone	Front Line + Support	Front Line + Support + Location	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	4	4	8	0	0
Singleton Probability Contribution	1.04E-4	1.04E-4	N/A	0	0
Number of Doubletons	0	942	977	4	4
Doubleton Probability Contribution	0	5.48E-6	N/A	4.75E-10	4.75E-10
Singleton + Doubleton Failure Probability	1.04E-4	1.09E-4	N/A	4.75E-10	4.75E-10

Table 4-10 Summary of Quantitative Results for System Combination Six - Feedwater in Response to Turbine Trip with Loss of Offsite Power

Case I - Front-Line Systems Only

The singletons from an analysis of the front-line systems alone are shown along with their failure probabilities in Table 4-11. (The complete list of singletons and doubletons is given in Enclosure 6.)

Component	Mean Failure Contribution
VGA64F	8.02E-5
VBVT6F	2.36E05
TANKCSTF	7.12E-8
HDK1072X1073F	4.30E-9

Table 4-11 Most Risk Significant Singletons in System Combination Six

There were no front-line system doubletons detected.

Case II - Front-Line and Support Systems

The addition of the support systems to the analysis of the failure of feedwater with the loss of offsite power does not change the number of singletons (4) but does cause doubletons (942). These doubletons do not significantly raise the failure probability of the system (from 1.04E-4 to 1.09E-4).

Case III - Front-Line, Support Including Locations

The addition of locations to the front-line plus support systems adds 4 singletons and 35 doubletons to the failure sets. These locations were discussed earlier.

Case IV - Manual Operation

The Indian Point Feedwater Systems were designed with ample opportunity for operators to override failed components. The cases studied here assume that if an automatic system fails, the operators will take the appropriate corrective action. Failure to take this corrective action has been assigned a probability of 0.0. Thus it would be expected that the low pressure injection system becomes more reliable in this manual case.

Two subcases were considered in the manual case; only operator corrective action, and both corrective and detrimental operator actions. The results of the analysis of the two subcases were the same.

Case IVa and IVb Manual Operation

As stated above, the results of both manual intervention subcases were the same. In both cases, the operators could reduce failure probability of feedwater with turbine trip and loss of offsite power to insignificance (4.75E-10).

4.7 Quantitative Analysis of System Combination 7-Main and Auxiliary Feedwater in Response To A Reactor Coolant Pump Seals Induced LOCA

Introduction

The reliability (and unavailability) of the Indian Point-3 Main and Auxiliary Feedwater Systems in response to a RCP seals induced LOCA system has been evaluated. This analysis included both fully automatic operator and performance with operator assistance. The effects of failures in support systems were explicitly included in this analysis. Because of the completeness of the DMA model, no assumptions were made about the availability of electrical power, service water, or component cooling. Unavailability (and failure) contributions from these systems and combinations of these support systems are explicitly included in the failure sets. There were no single failures detected which were common to both the RCP seals and the feedwater systems. The doubletons in this system combination arise from a singleton in each of the two systems.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Success of Auxiliary Feedwater depends on the start of one motor-driven or turbine-driven pump.

2. The time requirement for feedwater in response to the turbine trip is 0.5 hours.

Probability Data Base

The data used for the quantitative analysis of System Combination 7 is listed in Appendix D. This data was taken (for the most part) from the Indian Point Probabilistic Safety Study. In this data base, an operator error was assigned a probability of 1×10^{-3}. Operators were allowed to disable any component which could be turned off except for components located inside of containment which had no control room remote switches. For the manual cases studied, it was assumed that an operator would take a correct override action with a probability of 1.0.

Results

There were four cases studied:

1. Automatic Operation, Front-line systems only,

2. Automatic Operation, Front-line and support systems,

3. Automatic Operation, Front-Line, support systems, and locations, and

4. Manual Operation

   1. Operator Override of failed Components

   2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

Table 4-12 contains a summary of the results from the four cases analyzed. As can be seen from this table, there were no singletons detected in any of the cases studied. The ability of the operators to override failures in the feedwater systems eliminated all doubletons in the manually assisted case (IV).

Case I - Front-Line Systems Only

There were no front-line singletons found which would cause both an RCP seals failure and the failure of the feedwater systems.

Each doubleton in the combination front-line system, as expected, arises from one singleton from RCP seals and one singleton from the feedwater systems.

The doubletons can be grouped into "order of magnitude" sets. The highest group of these doubletons was of the order of magnitude of 10^{-11} and included valve VGA64F in the feedwater system with a upper motor bearing failure in the RCP seals.

The total failure probability due to the 228 doubletons for the Front-Line System was 4.3E-10.

Case II - Front-Line and Support Systems

The addition of the support systems to the analysis of the failure of System Combination 7 added 424 doubletons and which caused an insignificant increase in the failure probability.

Case III - Front-Line, Support Including Locations

The addition of locations to the front-line plus support systems adds 755 doubletons to the failure sets. These locations were discussed earlier.

CASE	I	II	III	IV	
Description	AUTOMATIC	AUTOMATIC	AUTOMATIC	MANUAL	
	Front Line Alone	Front Line + Support	Front Line + Support + Location	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	0	0	0	0	0
Singleton Probability Contribution	0	0	0	0	0
Number of Doubletons	228	712	1467	0	0
Doubleton Probability Contribution	4.30E-10	4.80e-10	0	0	0
Singleton + Doubleton Failure Probability	4.30E-10	4.80E-10	0	0	0

Table 4-12 Summary of Quantitative Results for System Combination Seven - RCP Seals Induced LOCA with Feedwater

4.8 Quantitative Analysis of System Combination 7-Main and Auxiliary Feedwater in Response To A PORV Induced LOCA

Introduction

The reliability (and unavailability) of the Indian Point-3 Main and Auxiliary Feedwater Systems in response to a PORV induced LOCA has been evaluated. This analysis included both fully automatic operator and performance with operator assistance. The effects of failures in support systems were explicitly included in this analysis. Because of the completeness of the DMA model, no assumptions were made about the availability of electrical power, service water, or component cooling. Unavailability (and failure) contributions from these systems and combinations of these support systems are explicitly included in the failure sets. There were no single failures detected which were common to both the PORV and the feedwater systems. The doubletons in this system combination arise from a singleton in each of the two systems.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Success of Auxiliary Feedwater depends on the start of one motor-driven or turbine-driven pump.

2. The time requirement for feedwater in response to the LOCA is 0.5 hours.

Probability Data Base

The data used for the quantitative analysis of System Combination 8 is listed in Appendix D. This data was taken (for the most part) from the Indian Point Probabilistic Safety Study. In this data base, an operator error was assigned a probability of 1×10^{-3}. Operators were allowed to disable any component which could be turned off except for components located inside of containment which had no control room remote switches. For the manual cases studied, it was assumed that an operator would take a correct override action with a probability of 1.0.

Results

There were four cases studied:

1. Automatic Operation, Front-line systems only,

2. Automatic Operation, Front-line and support systems,

3. Automatic Operation, Front-Line, support systems, and locations, and

4. Manual Operation

   1. Operator Override of failed Components

   2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

Table 4-13 contains a summary of the results from the four cases analyzed. As can be seen from this table, there were no singletons detected in any of the cases studied. The ability of the operators to override failures in the feedwater systems eliminated all doubletons in the manually assisted case (IV).

Case I - Front-Line Systems Only

There were no front-line singletons found which would cause both failure in the PORV and the failure of the feedwater systems.

Each doubleton in the combination front-line system, as expected, arises from one singleton from the PORV and one singleton from the feedwater systems.

The doubletons can be grouped into "order of magnitude" sets. The highest group of these doubletons was of the order of magnitude of 10^{-7} and included valve VGA64F in the feedwater system with various relief valves in the PORV system.

The total failure probability due to the 21 doubletons for the Front-Line Systems was 5.61E-06.

Case II - Front-Line and Support Systems

The addition of the support systems to the analysis of the failure of System Combination 8 added no doubletons.

Case III - Front-Line, Support Including Locations

The addition of locations to the front-line plus support systems added no doubletons to the failure sets.

CASE	I	II	III	IV	
Description	AUTOMATIC	AUTOMATIC	AUTOMATIC	MANUAL	
	Front Line Alone	Front Line + Support	Front Line + Support + Location	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	0	0	0	0	0
Singleton Probability Contribution	0	0	0	0	0
Number of Doubletons	21	21	21	0	0
Doubleton Probability Contribution	5.62E-06	5.62E-06	0	0	0
Singleton + Doubleton Failure Probability	5.62E-06	5.62E-06	0	0	0

Table 4-13 Summary of Quantitative Results for System Combination Eight - PORV Induced LOCA with Feedwater

4.9 Quantitative Analysis of System Combination 9-Large LOCA with Low Pressure Recirculation

Introduction

The reliability of the Indian Point-3 Low Pressure Recirculation System has been evaluated for response to a large LOCA. Recirculation requires manual initiation and must continue for a long time hence only Case IV was analyzed. A period of 24 hours of active recirculation was chosen as the minimum time required before natural convection might suffice.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Success of Recirculation is defined as at least one recirculation pump supplying water to the core.

2. The time requirement for recirculation is 24.0 hours.

Results

Only the manual operation cases were studied including:

1. Operator Override of failed Components

2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

Table 4-14 contains a summary of the results from the two subcases analyzed. As can be seen from this table, in all cases the bulk of the failure probability (and unavailability) is due to single component failures. Recirculation is also not seriously impacted by the effect of operator errors. The results of the two manual operation subcases will now be discussed.

Case IVa - Manual Operation - Initiating and Correct Action Only

In this subcase, operators are take the actions neccessary to initiate the recirculation phase and to take corrective action if a failure should occur. The probability of taking these actions has been taken to be 1.0. In this case it was found that the probability of failure (and unavailability) due to singletons was 2.46E-05. The failure probability which results from doubleton failures was 2.20E-07. The dominant contribution to failure found in the IP PSS was failure of the operator to switch to the recirculation phase. We did not include this particular failure in our quantitative analysis.

CASE	IV	
Description	MANUAL	
	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	7	7
Singleton Probability Contribution	2.46E-05	2.46E-05
Number of Doubletons	929	1055
Doubleton Probability Contribution	2.20E-07	5.55E-06
Singleton + Doubleton Failure Probability	2.22E-05	3.01E-05

Table 4-14 Summary of Quantitative Results for System Combination Nine - Recirculation in Response to Large LOCA

Case IVb - Corrective and Detrimental Actions

In this subcase, the operators are allowed to initiate recirculation and take both corrective and detrimental actions. These detrimental actions are "errors of commission" since they require an action by the operator to cause an error. The probability of each of these types of errors was taken to be 1.0E-3.

These errors of commission did not change the singleton probability from the prior case but did increase the doubleton probability to 5.55E-06.

4.10 Quantitative Analysis of System Combination 10-Medium LOCA with Loss of Both High and Low Pressure Injection

Introduction

The reliability of the combination of Indian Point-3 Low and High Pressure Injection Systems has been evaluated for response to a medium LOCA. This analysis included both fully automatic operator and performance with operator assistance.

Assumptions

The following assumptions were made for the purpose of this quantitative analysis:

1. Water from the Refueling Water Storage Tank is available.
2. Success is defined as the injection of water into at least two legs of the Reactor Coolant System by at least one Residual Heat Removal Pump or two Safety Injection Pumps.
3. The time requirement for injection is 0.5 hours.

Results

There were four cases studied:

1. Automatic Operation, Front-line systems only,
2. Automatic Operation, Front-line and support systems,
3. Automatic Operation, Front-Line, support systems, and locations, and
4. Manual Operation
    1. Operator Override of Failed Components
    2. Operator Override of Failed Components plus operator inadvertent errors (errors of commission).

Table 4-15 contains a summary of the results from the four cases analyzed. As can be seen from this table, in all cases the bulk of the failure probability is due to single component failures. The ability of the operators to override failed components does not significantly improve the reliability of the combination of the high and low pressure injection systems. Injection however, was significantly less reliable when the effects of operator errors are considered. In this system combination, it appears that the safest mode of operation would be to prevent the operators from taking any action. It should be stated that the above result probably overestimates the effect of detrimental operator actions, since the DMA model did not include any safequards which would prevent some of these

CASE	I	II	III	IV	
Description	AUTOMATIC	AUTOMATIC	AUTOMATIC	MANUAL	
	Front Line Alone	Front Line + Support	Front Line + Support + Location	a. Positive Operator Action Only	b. Positive Operator Action Errors of Commission
Number of Singletons	6	6	8	4	4
Singleton Probability Contribution	3.29E-5	3.29E-5	N/A	3.29E-5	1.03E-3
Number of Doubletons	54	424	430	219	300
Doubleton Probability Contribution	5.17E-7	1.22E-6	N/A	6.12E-12	1.47E-11
Singleton + Doubleton Failure Probability	3.34E-5	3.31E-5	N/A	3.29E-12	1.03E-3

Table 4-15 Summary of Quantitative Results for System Combination Ten - All Safety Injection in Response to Medium LOCA

incorrect actions. In all but Case IVb, the results of this DMA found the injection system response to a medium LOCA to be extremely reliable. Each case will now be briefly discussed.

Case I - Front-Line Systems Only

The only risk significant singleton from an analysis of the front-line systems alone is shown along with its failure probabilities in Table 4-16. (The complete list of singletons and doubletons is given in Enclosure 10.)

Component	Mean Failure Contribution
VGA846D	3.29E-05

Table 4-16 Most Risk Significant Singletons in System Combination Ten

The remaining 2 singletons are pipe sections with individual failure probabilities on the order of 4E-9. These remaining singletons do not contribute significantly to the overall failure probability.

The doubletons are dominated by the failure of the two motor operated valves MOV1810D and MOV882D. This failure set has a failure probability (including unavailability) of 3.61E-07.

The remaining doubletons can be grouped into "order of magnitude" sets. The 10^{-8} magnitude group includes:

VC847D	MOV882D	4.15E-08
MOV1810D	VC881D	4.15E-08
MOV1810D	VC741D	4.15E-08
MOV1810D	MOV744D	1.98E-08

The total failure probability due to doubletons for the front-line injection systems in response to a medium LOCA is 5.17E-7. The reliability for the combination of these injection systems is significantly better than for low pressure alone.

Case II - Front-Line and Support Systems

The addition of the support systems to the analysis of the failure of all injection systems in response to a medium LOCA does not change the number of singletons (from 6 to 9) but does significantly increase the number of doubletons (from 54 to 424). The large increase in the number of doubletons raises the failure probability of the system (from 5.17E-7 to 1.22E-6). The three singletons added are double pipe breaks in the component cooling system with an insignificant probability of occurrence hence were not counted as singletons. The most significant added doubletons, as in system combination one, are:

STAUXXFMRP * SW123456P	3.41E-07
STAUSSFMRP * COL-RW-2K	3.41E-07

The variable STAUXXFMRP includes the failure of the station auxiliary transformer and the loss of offsite power. The loss of offsite power dominates the failure of the transformer (3.41E-04 to 0.84E-06/hr). Variable SW123456P refers to an incorrect setting of the service water mode switch prior to the accident. The variable COL-RW-2K is an error in the manual checkoff procedure for the service water pumps prior to the accident. The prominence of offsite power in the doubletons implies that this system combination would have a significantly larger failure probability (singletons in the 10E-2 to 10E-3 range) during an offsite power outage.

Case III - Front-Line, Support Including Locations

The addition of locations to the front-line plus support systems adds 2 singletons and 14 doubletons to the failure sets. These locations were discussed earlier.

Case IV - Manual Operation

Case IVa - Manual Operation - Corrective Action Only

In this subcase, operators are allowed to take corrective action. The probability of taking these actions has been taken to be 1.0. The ability to take these corrective actions did not change the singleton failure probability from the automatic case (II). However, the failure contributions from the doubletons decreased dramatically from 1.22E-6 to 6.12E-12. This decrease results from the number of alternate pumps and paths available for this accident sequence given that injection from one residual heat removal pump or two SI pumps is adequate.

Case IVb - Corrective and Detrimental Actions

In this subcase, the operators are allowed to take both corrective and detrimental actions. These detrimental actions are "errors of commission" since they require an action by the operator to cause an error. The probability of each of these types of errors was taken to be 1.0E-3.

These errors of commission increased the singleton probability from 3.29E-5 in case IVa to 1.03E-3 and the doubleton probability from 6.12E-12 to 1.47E-11. The singleton with the largest value is an incorrect operator action in closing valve VGA846D. This failure dominates the singleton failure probability.

4.11 Extract from Appendix D--Failure Data Base

The component failure data base used for this DMA of the Indian Point Three power reactor is explained and listed in Tables D.1-1 through D.1-10 in section D.1 of this appendix.* The inclusion of human failure data into the DMA quantitative analysis is explained in Section D.2 of this appendix.

----

* In this extract, we have included only the data base for System Combination One.

D.1 Component Failure Data Base

In general, component failure probability and unavailability was taken from the Indian Point Probabilistic Safety Study (IP-PSS) Section 1.6 (primariiy Table 1.6.1-4). This data base contains (Bayesian) updated failure rates for the IP components based on actual operating IP experience. Exceptions to this rule are described in the listings of the data base for each system combination.

In using the IP PSS data base, no statement is made about its accuracy. The IP PSS data base was used only to allow a direct comparison to be made between the results of the DMA and those of the IP PSS.

The following tables contain the probability data bases as used for each system combination. The format of these tables is shown in Figure D.1-1 and explained below.

```
                                        DEMAND      OPERATING
MOV822BL     MOV221       2        0.151E-02 -0.915E-07

Component    Generic  Number               Minus  sign indicates
  name        type      of                 rate (failures/hr)
                      Probability
                      Terms
@ MOTOR OPERATED VALVE
```

Figure D.1-1 Explanation of Probability Data Base Format

Thus valve MOV822BL is of generic class MOV221, a motor operated valve, normally closed, which must change state, and has a failure to operate on demand probability of 0.15E-02 per demand and a blockage failure rate of 0.915E-07 failures per hour. Lines in the data base which begin with a @ symbol contain explanatory information.

To compute the overall failure probability for a specific component in the data base, all of the failure terms are combined using the rules for combinations of probability for independent events. That is

$$P_{total} = 1 - \prod_{i=1} (1-P_i) \quad \text{unless}$$

where P_{total} is the total failure probability for the component

P_i is the probability of the ith failure mode

The probability of failure for a component which had an hourly rate was determined by multiplying the failure rate by the action time of the accident sequence. This action time was the time over which the component must function. For example, the action time for high pressure injection was taken to be 0.5 hours.

Care was taken in assembling this data base to include only exclusive failure modes for any specific component.

As stated above, failure and unavailability data was taken from the IP PSS when available. In some cases specific data was not available. We have assumed in most of these cases, that the component was operational at the time of the accident, hence its failure probability is simply the duration of the accident times its failure rate (failure/hr). This calculation yields a lower bound for the component failure probability.

The failure data bases for the components used in each system combination are found in Tables D.1-1 through D.1-10. Careful review of the data bases will show differences in the failure data for the same component used in different accident sequences.

DATA BASE FOR SYSTEM COMBINATION ONE

```
 SC1.PRB       MEDIUM LOCA 12-JUN-84
       TEXT FAIL TO DESCRIBE EACH COMPONENT FAILURE
       REFERENCE IP PSS  P1.6-505  TABLE 1.6.2.3.2-6
       (BASIC REFERENCE PSS TABLE 1.6.1-4 PAGE 1.6 -56/63)
 ***************************************************************
 HTRC846ZD        N       1  0.000E+00
@
 VGA846D          VGA112   1  3.290E-05
@
 MOV882D          MOV112   1  6.010E-04
@  FAILS CLOSED (DEEN OPEN) 9.15E-08/HR*13140/2
 VC881D           VC120    1  6.910E-05
@  FAILS TO OPEN
 MOV744D          MOV112   1  3.290E-05
@  FAILS CLOSED (DEENER OPEN) MEANOF 30DAYTESTPERIOD  9.15E-08*24HR/DAY*30DAY/2
 VC741D           VC120    1  6.910E-05
@  FAILS TO OPEN
 VGA759BL         VGA111   1 -0.915E-07
@
 VGA765BL         VGA111   1 -0.915E-07
@
 VGA759AL         VGA111   1 -0.915E-07
@
 STRCTRINTKK      N        1  0.100E-07
@
 VGA765AL         VGA111   1 -0.915E-07
@
 VGA735BD         VGA112   1 -0.915E-07
@
 VGA739BD         VGA112   1 -0.915E-07
@
 VGL736BL         VGA111   1 -0.915E-07
@
 VGL1871AL        VGA111   1 -0.915E-07
@
 VGL1871BL        VGA111   1 -0.915E-07
@
 VGL737BL         VGA111   1 -0.915E-07
@
 VGA735AD         VGA112   1 -0.915E-07
@
 VGA739AD         VGA112   1 -0.915E-07
@
 VGL736AL         VGA111   1 -0.915E-07
@
 VGL1871DL        VGA111   1 -0.915E-07
@
 VGL1871CL        VGA111   1 -0.915E-07
@
 VGL737AL         VGA111   1 -0.915E-07
@
 MOV899AB         MOV111   1  1.340E-04
@  TRANSFERS CLOSED
 MOV746B          MOV111   1  1.340E-04
@  TRANSFERS CLOSED
```

```
 MOV899BB         MOV111   1  1.340E-04
@  TRANSFERS CLOSED
 MOV747B          MOV111   1  1.340E-04
@  TRANSFERS CLOSED
 MOV745BD         MOV111   1  1.340E-04
@  TRANSFERS CLOSED
 MOV745AD         MOV111   1  1.340E-04
@  TRANSFERS CLOSED
 VGA742D          VGA112   1  1.340E-04
@  TRANSFERS CLOSED
 RHRP31Z          RHP120   2  0.136E-02 0.075E-03
@   FAIL TO START   FAIL TO RUN 0.5
 RHRP32Z          RHP120   2  0.136E-02 0.075E-03
@   FAIL TO START   FAIL TO RUN 0.5
 STAUIIFMRP       IMR110   3 -0.839E-06 3.890E-08 3.410E-04
@       transformer failure and
@  LOSS OF OFFSITE POWER  PSS P1.6-217 LOSS OF OFFSITE POWER
@                                PSS P1.6-217 FAILURE GIVEN UNIT TRIP
@
 VC738AD          VC120    1  6.910E-05
@   FAILS TO OPEN
 VC738BD          VC120    1  6.910E-05
@   FAILS TO OPEN
 VC750DL          VC120    1  6.910E-05
@   FAILS TO OPEN
 VC750EL          VC120    1  6.910E-05
@   FAILS TO OPEN
 HCV638B          VGA111   1  1.340E-04
@  TRANSFERS CLOSED
 HCV640B          VGA111   1  1.340E-04
@  TRANSFERS CLOSED
 PSHIR1871BL      HIR000   1 -0.973E-06
@
 PSHIR1871DL      HIR000   1 -0.973E-06
@
 RHIR31Z          HIR000   1 -0.973E-06
@
 RHIR32Z          HIR000   1 -0.973E-06
@
 J735BD           PP3000   1 -0.860E-08
@
 J735AD           PP3000   1 -0.860E-08
@
 J1810D           PP3000   1 -0.860E-08
@
 PPI846D          PP3000   1 -0.860E-08
@
 PPR846D          PP3000   1 -0.860E-08
@
 PPR1810D         PP3000   1 -0.860E-08
@
 J898D            PP3000   1 -0.860E-08
@
 J1863D           PP3000   1 -0.860E-08
@
 JRHRD            PP3000   1 -0.860E-08
@
 J883D            PP3000   1 -0.860E-08
@
 J745BD           PP3000   1 -0.860E-08
```

```
@
 J1871AL          PP1000   1 -0.860E-09
@
 J736BL           PP1000   1 -0.860E-09
@
 PPR736BL         PP1000   1 -0.860E-09
@
 PPR750DL         PP1000   1 -0.860E-09
@
 J750DL           PP1000   1 -0.860E-09
@
 PPI1871AL        PP1000   1 -0.860E-09
@
 PPI1871BL        PP1000   1 -0.860E-09
@
 PPR1871BL        PP1000   1 -0.860E-09
@
 PPI1739AD        PP3000   1 -0.860E-08
@
 J1871CL          PP1000   1 -0.860E-09
@
 J736AL           PP1000   1 -0.860E-09
@
 PPR736AL         PP1000   1 -0.860E-09
@
 PPR750EL         PP1000   1 -0.860E-09
@
 J750EL           PP1000   1 -0.860E-09
@
 J838RB           PP3000   1 -0.860E-08
@
 J838QB           PP3000   1 -0.860E-08
@
 J641AB           PP1000   1 -0.860E-09
@
 J899AB           PP3000   1 -0.860E-08
@
 J899BB           PP3000   1 -0.860E-08
@
 J889BB           PP3000   1 -0.860E-08
@
 J889D            PP3000   1 -0.860E-08
@
 J1869BD          PP3000   1 -0.860E-08
@
 J101XD           DEGRAD   1  0.000E-00
@
 J103XD           DEGRAD   1  0.000E-00
@
 J104D            DEGRAD   1  0.000E-00
@
 J107D            DEGRAD   1  0.000E-00
@
 J110XD           DEGRAD   1  0.000E-00
@
 J111XD           DEGRAD   1  0.000E-00
@
 J200D            DEGRAD   1  0.000E-00
@
 J290AD           DEGRAD   1  0.000E-00
 @
  J1866BD          DEGRAD   1  Ø.ØØØE-ØØ
 @
  J1866DD          DEGRAD   1  Ø.ØØØE-ØØ
 @
  J636D            DEGRAD   1  Ø.ØØØE-ØØ
 @
  J638B            DEGRAD   1  Ø.ØØØE-ØØ
 @
  J639B            DEGRAD   1  Ø.ØØØE-ØØ
 @
  J64ØB            DEGRAD   1  Ø.ØØØE-ØØ
 @
  J74ØAD           DEGRAD   1  Ø.ØØØE-ØØ
 @
  J1867AD          DEGRAD   1  Ø.ØØØE-ØØ
 @
  J1867BD          DEGRAD   1  Ø.ØØØE-ØØ
 @
  J641B            DEGRAD   1  Ø.ØØØE-ØØ
 @
  J733AB           DEGRAD   1  Ø.ØØØE-ØØ
 @
  J733BB           DEGRAD   1  Ø.ØØØE-ØØ
 @
  J74ØBD           DEGRAD   1  Ø.ØØØE-ØØ
 @
  J889AB           DEGRAD   1  Ø.ØØØE-ØØ
 @
  CHNLDS3K         CHANNL   1  Ø.ØØØE-ØØ
 @
  CHNLDSK          CHANNL   1  Ø.ØØØE-ØØ
 @
  COL-RW-2K        PROCED   1  1.ØØØE-Ø3
 @  ERROR IN LOGGING CHECKOFF LIST SERVICE WATER CHECKOFF LIST PROCEDURE
  HTRC846YD        HEATTR   1  Ø.ØØØE-ØØ
 @
  PP1735D          PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  J95AK            PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  J1Ø96AK          PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  J95BK            PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  J95CK            PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  J95DK            PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  J95FK            PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  VB3ØK            VGA111   1 -Ø.915E-Ø7
 @
  J1Ø93AK          PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  J1Ø93BK          PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  J1Ø93DK          PP3ØØØ   1 -Ø.86ØE-Ø8
 @
  J1Ø94K           PP3ØØØ   1 -Ø.86ØE-Ø8
```

```
@
 J1095K          PP3000   1 -0.860E-08
@
 J1096BK         PP3000   1 -0.860E-08
@
 J1190K          PP3000   1 -0.860E-08
@
 J98AK           PP3000   1 -0.860E-08
@
 J106BK          PP3000   1 -0.860E-08
@
 J1221K          PP3000   1 -0.860E-08
@
 J131K           PP3000   1 -0.860E-08
@
 J409K           PP3000   1 -0.860E-08
@
 J4K             PP3000   1 -0.860E-08
@
 VB98K           VGA111   1 -0.915E-07
@
 VC98K           VC120    1  6.910E-05
@  FAILS TO OPEN
 RL27-3AX1I      SAR110   1 -2.430E-07
@
 RL27-3AX3I      SAR110   1 -2.430E-07
@
 RL27-3AX4I      SAR110   1 -2.430E-07
@
 RL27-6AX1I      SAR110   1 -2.430E-07
@
 RL27-6AX2I      SAR110   1 -2.430E-07
@
 RL27-6AX4I      SAR110   1 -2.430E-07
@
 RL3-13AI        SAR120   2  1.150E-05-2.430E-07
@  RELAY FAIL TO ACTUATE,  TRANSFER OPEN
 BKRDPNL34/P     WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND
 BKRDPNL31/P     WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND
 BUS3A/P         WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND
 BUS6A/P         WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND
 PWRPNL32/P      WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND
 PWRPNL33/P      WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND
 J017AL          PP3000   1 -0.860E-08
@  BREAK
 J017BL          PP3000   1 -0.860E-08
@  BREAK
 J1805L          PP3000   1 -0.860E-08
@  BREAK
 J1871BL         PP3000   1 -0.860E-08
@  BREAK
 J1871DL         PP3000   1 -0.860E-08
@  BREAK
 J601AL          PP3000   1 -0.860E-08
```

```
  @  BREAK
   J601BL          PP3000   1 -0.860E-08
  @  BREAK
   J601CL          PP3000   1 -0.860E-06
  @  BREAK
   J601DL          PP3000   1 -0.860E-08
  @  BREAK
   J602AL          PP3000   1 -0.860E-08
  @  BREAK
   J602BL          PP3000   1 -0.860E-08
  @  BREAK
   J602CL          PP3000   1 -0.860E-08
  @  BREAK
   J627AL          PP3000   1 -0.860E-08
  @  BREAK
   J627BAL         PP3000   1 -0.860E-08
  @  BREAK
   J627BBL         PP3000   1 -0.860E-08
  @  BREAK
   J627BCL         PP3000   1 -0.860E-08
  @  BREAK
   J627BL          PP3000   1 -0.860E-08
  @  BREAK
   J760AL          PP3000   1 -0.860E-08
  @  BREAK
   J760CL          PP3000   1 -0.860E-08
  @  BREAK
   J762AL          PP3000   1 -0.860E-08
  @  BREAK
   J762CL          PP3000   1 -0.860E-08
  @  BREAK
   J763AL          PP3000   1 -0.860E-08
  @  BREAK
   J763BL          PP3000   1 -0.860E-08
  @  BREAK
   J764AL          PP3000   1 -0.860E-08
  @  BREAK
   J764BL          PP3000   1 -0.860E-08
  @  BREAK
   J765AL          PP3000   1 -0.860E-08
  @  BREAK
   J765BL          PP3000   1 -0.860E-08
  @  BREAK
   J830AL          PP3000   1 -0.860E-08
  @  BREAK
   J830BL          PP3000   1 -0.860E-08
  @  BREAK
   JA10L           PP3000   1 -0.860E-08
  @  BREAK
   JA14AL          PP3000   1 -0.860E-09
  @  BREAK
   JA14L           PP3000   1 -0.860E-08
  @  BREAK
   JA2L            PP3000   1 -0.860E-08
  @  BREAK
   JA3L            PP3000   1 -0.860E-08
  @  BREAK
   JA501AL         PP3000   1 -0.860E-08
  @  BREAK
   JA501L          PP3000   1 -0.860E-08
```

```
@ BREAK
 JA502L          PP3000   1 -0.860E-08
@ BREAK
 JA55L           PP3000   1 -0.860E-08
@ BREAK
 JA57L           PP3000   1 -0.860E-08
@ BREAK
 JA7L            PP3000   1 -0.860E-08
@ BREAK
 JA8L            PP3000   1 -0.860E-08
@ BREAK
 PPI1871DL       PP3000   1 -0.860E-08
@ BREAK
 PPI765AL        PP3000   1 -0.860E-08
@ BREAK
 PPR1805L        PP3000   1 -0.860E-08
@ BREAK
 PPR1871DL       PP3000   1 -0.860E-08
@ BREAK
 VC761CL         PP3000   1 -0.860E-08
@ BREAK
 VGA760AL        PP3000   1 -0.860E-08
@ BREAK
 VGA760CL        PP3000   1 -0.860E-08
@ BREAK
 VGA762AL        PP3000   1 -0.860E-08
@ BREAK
 VGA762CL        PP3000   1 -0.860E-08
@ BREAK
 JTIC627L        PP3000   1 -0.860E-08
@ BREAK
 CCWP31L         PP3000   1 -0.860E-08
@ BREAK
 CCWP33L         PP3000   1 -0.860E-08
@ BREAK
 PWLDIS31/P      WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND
 PWLDIS34/P      WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND
 PWRPNL31/P      WIR000   1 -7.520E-06
@  SHORT CIRCUIT TO GROUND
 SW123456P       SWT000   1  1.000E-03
@  MODE SELECT SWITCH TO SERVICE WATER PUMPS ERRONEOUSLY PRESELECTED
 RSI11XZ         SAR120   2  1.150E-05-2.430E-07
@  SLAVE  SAFEGUARDS ACTUATION RELAY
 RSI21XZ         SAR120   2  1.150E-05-2.430E-07
@  SLAVE  SAFEGUARDS ACTUATION RELAY
 RSI1H           SAR120   2  1.150E-05-2.430E-07
@  SAFEGUARDS ACTUATION RELAY
 RSI2H           SAR120   2  1.150E-05-2.430E-07
@  SAFEGUARDS ACTUATION RELAY
 CCHXRS31Z       HXR000   1 -0.973E-06
@COMPONENT COOLING HEAT EXCHANGER BREAK
 CCHXRS32Z       HXR000   1 -0.973E-06
@COMPONENT COOLING HEAT EXCHANGER BREAK
 RL3-16AI        SAR120   2  1.150E-05-2.430E-07
@  RELAY FAILS TO CHANGE STATE AND HOLD
 VC761AL         PP3000   1 -0.860E-08
@ CHECK VALVE RUPTURES
 ITLBKR2ATSAP    SAR111   1 -2.430E-07
```

```
@       ELECTRICAL INTERLOCK FAILURE  RELAY FAIL TO OPERATE
@       SIMILAR TO IP3 PSS ITEM 3E
 ITLDKR3AT6AP     SAR111   1 -2.430E-07
@       ELECTRICAL INTERLOCK FAILURE  RELAY FAIL TO OPERATE
@       SIMILAR TO IP3 PSS ITEM 3E
 J132BK           PP3000   1 -0.860E-08
 J133K            PP3000   1 -0.860E-08
 J745BD           PP3000   1 -0.860E-08
 ORFC760CL        PP3000   1 -0.860E-08
 ORFC760AL        PP3000   1 -0.860E-08
 ORFC645AL        PP3000   1 -0.860E-08
 ORFC645BL        PP3000   1 -0.860E-08
 ORFC646AL        PP3000   1 -0.860E-08
 ORFC645BL        PP3000   1 -0.860E-08
 ORFCCCW31L       PP3000   1 -0.860E-08
 ORFCCCW33L       PP3000   1 -0.860E-08
 RL27-3AI2I       SAR110   1 -2.430E-07
@       CONTACTS INADVERTENTLY CLOSE
 RL27-6AI3I       SAR110   1 -2.430E-07
@        CONTACTS INADVERTENTLY CLOSE
 ORFC646BL        PP3000   1 -0.860E-08
@       PIPE > 3"
 J745AD           PP3000   1 -0.860E-08
@       PIPE > 3"
 J1829D           PP3000   1 -0.860E-08
@       PIPE > 3"
@
 J203AD           PP3000   1 -0.860E-08
@       PIPE > 3"
 J203D            PP3000   1 -0.860E-08
@       PIPE > 3"
 J204D            PP3000   1 -0.860E-08
@       PIPE > 3"
 J887AD           PP3000   1 -0.860E-08
@       PIPE > 3"
 LF888D           LOC000   1  1.000E-15
@       LOCATION
 LFRHRD           LOC000   1  1.000E-15
@
 LFRHIRB          LOC000   1  1.000E-15
@
 LFSIPD           LOC000   1  1.000E-15
@
 LOCCP            LOC000   1  1.000E-15
@
 LOCDP            LOC000   1  1.000E-15
 LOCRP            LOC000   1  1.000E-15
 LOCSP            LOC000   1  1.000E-15
@
 LS888D           LOC000   1  1.000E-15
@
 LSRHRD           LOC000   1  1.000E-15
@
 LSRHIRB          LOC000   1  1.000E-15
@
 LSSIPD           LOC000   1  1.000E-15
@
 LW888D           LOC000   1  1.000E-15
@
 LWRHRD           LOC000   1  1.000E-15
```

```
@
 LWRHXRB          LOCØØØ   1  1.ØØØE-15
@
 LWSIPD           LOCØØØ   1  1.ØØØE-15
@
 MOV181ØD         MOV111   1  6.Ø1ØE-Ø4
@    FAILS CLOSED (LOCKED OPEN) MEANOF 3ØDAYTESTPERIOD
@       9.15E-Ø8*24HR/DAY*3ØDAY/2
@
 MOV887AD         MOV111   1  6.Ø1ØE-Ø4
@    FAILS CLOSED (LOCKED OPEN) MEANOF 3ØDAYTESTPERIOD
@       9.15E-Ø8*24HR/DAY*3ØDAY/2
@
 MOV887BD         MOV111   1  6.Ø1ØE-Ø4
@    FAILS CLOSED (LOCKED OPEN) MEANOF 3ØDAYTESTPERIOD
@       9.15E-Ø8*24HP/DAY*3ØDAY/2
@
 OPW1871AL        OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
 OPW1871BL        OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
 OPW1871CL        OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
 OPW1871DL        OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
 OPW736BL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW737AL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW737BL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW759AL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW759BL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW76ØAL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW76ØCL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW762AL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW762CL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW765AL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW765BL         OPWØØØ   1  Ø.ØØØE-Ø1
@       IMPOSSIBLE OPERATOR ACTION
@
 OPW181ØD         OPWØØØ   1  Ø.ØØØE-Ø3
@     DEENGERIZED OPEN
```

```
 OPW739AD        OPW000   1  1.000E-03
@
 OPW735AD        OPW000   1  1.000E-03
@
 OPW735BD        OPW000   1  1.000E-03
@
 OPW739BD        OPW000   1  1.000E-03
@
 OPW742D         OPW000   1  1.000E-03
@
 OPW744D         OPW000   1  1.000E-03
@
 OPW745AD        OPW000   1  1.000E-03
@
 OPW745BD        OPW000   1  1.000E-03
@
 OPW846D         OPW000   1  0.000E-03
@      LOCKED OPEN
@
 OPW882D         OPW000   1  1.000E-03
@
 OPW887AD        OPW000   1  1.000E-03
@
 OPW887BD        OPW000   1  1.000E-03
@
 OPW898D         OPW000   1  1.000E-03
@
 OPWRHRP31D      OPW000   1  1.000E-03
@
 OPWRHRP32D    . OPW000   1  1.000E-03
@
 OPWRHRP32E      OPW000   1  1.000E-03
@
 SWRS3P          OPW000   1  1.000E-03
@      OPERATOR INADVERTENTLY SWITCHES TO RECIRCULATION MODE
 VC847D          VC128    1  6.910E-05
@  CHECK VALVE FAILS TO OPEN
@
 V6A898D         V6A111   1 -0.915E-07
@      MANUAL VALVE IN ALTERNATE PATH NORMALLY CLOSED HAS TO BE
@      OPENED BY OPERATOR  FAILURE IS VALVE TRANSFERS CLOSED AFTER
@      BEING OPENED
```

D.2 Human Reliability Model

Most safety systems rely on human operators as backup to the automatic functioning of safety and support systems. The DMA model explicitely includes nodes for these operator backup operations. These nodes are shown as OPR***'s in the digraphs. A simplified examp!e of the use of an OPR node is shown in Figure D.2-1.

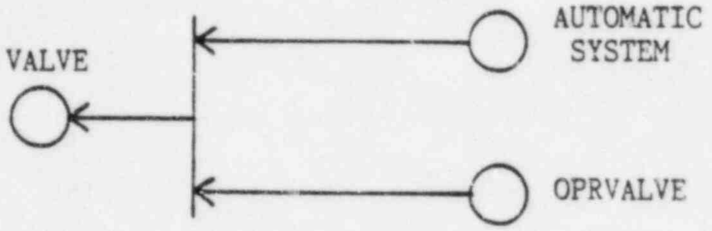


Figure D.2-1 Use of the OPR Node to Represent Operator Backup of an Automatic System

In this figure, the valve is usually opened by an automatic system, however, in the case of the failure of the automatic system, an operator could manually open the valve. Hence, two failures are required for the valve to fail, failure of the automatic system and failure of the operator to manually open the valve.

In the earlier sections, results from two broad clases of system operation were presented: Fully Automatic and Manually Assisted. In the fully automatic runs the OPR nodes are constrained to be true, thus allowing automatic system failures to propagate into front-line systems. In the manually assisted runs, it is assumed that an operator will take the correct action to override an automatic system failure if this opportunity has been designed in. For the purposes of the quantitative analysis, it was assumed that the probability of an operator taking a needed corrective action was 1.0. Thus, the probability of an error of omission is 0.0. The failure of an operator to perform a required backup operation appears as a node labeled OPR*** in the singleton and doubleton results.

A second type of operator error is the inadvertent disabling of a system component. This type of operator action is labeled OPW*** in the digraphs and is illustrated in Figure D.2-2.

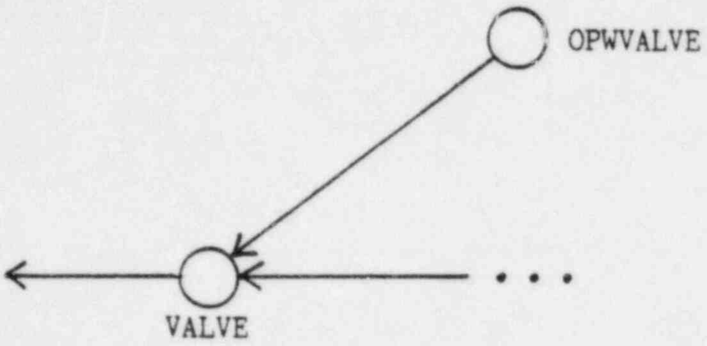


Figure D.2-2 Use of OPW Node To Represent Operator Error In Disabling Component Function

In this figure, the operator OPWVALVE closes the VALVE and thus causes the system to fail. The OPW*** node thus represents an error of commission. The set of digraphs contains an OPW*** node everywhere there is an opportunity for an operator error of commission. The probability of this type of error was arbitrarily set to 1.0 x 10^{-3}. A much more extensive analysis of human error rates was performed by the authors of the IP PSS (Section 1.6.1.4.1) using other data.* The human error rates used in the IP PSS are generally greater than 1 x 10^{-3}. In doubleton failure sets which include two OPW's, the errors of commission were taken to be independent.

We have split the human errors of commission into two time periods: 1) time from some semiarbitrary initial time (perhaps last maintenance) to the beginning of the accident and 2) from the beginning of the accident to the end. The probability data for a specific component includes data for mechanical component failure for the second time period and data, if applicable, for human errors prior to the accident. It does not include a term for an operator error of commission in the second time period. These errors are explicitly broken out as OPW***. This is shown in Figure D.2-3 for a diesel generator with the corresponding data base entries in Table D.2-1.

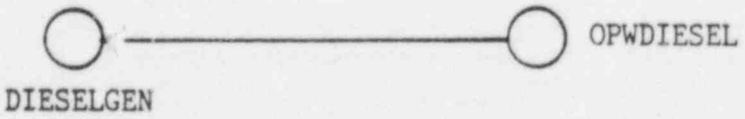


Figure D.2-3 Diesel Generator Digraph

----

* A.D. Swain, H.E. Guttman, "Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Application," NUREG/CR-1278 Draft Oct 1980.

COMPONENT		
DIESEL GENERATOR	1.44E-02/Demand	Failure to start
	9.37E-04/Hour	Failure during Operation
	2.51E-05/Demand	Left in Non Auto Position
	1.09E-03/Demand	Unavailability/Maint
OPWDIESEL	1.00E-03/Demand	Operator turns off

Table D.2-1 Data Base Entries for Diesel Generator

The only human error term in the data base for the diesel is "Left in Non Auto Position" which is an error prior to the accident. The data for the component OPWDIESEL contains the probability that an operator might turn the diesel off once the accident has begun.

If a component is designed such that an operator could not inadvertently change its state or if that component is in containment with no remote controls, the probability of its OPW*** will be 0.

5.0 CONCLUSION

Events such as Three Mile Island-2, Browns Ferry-3, and Crystal River-3 have demonstrated that complex systems interactions can occur as a result of unanticipated dependent failure. The primary objective of this study was to provide information for the comparison of the effectiveness of Digraph Matrix Analysis (DMA) to two other methodologies in discovering systems interactions. These were the "traditional" Probabilistic Risk Assessment performed earlier by the Power Authority of the State of New York (IP-PSS) and a concurrent Fault Tree/Failure Modes and Effects Analysis performed by Brookhaven National Laboratory. A complete comparison to the BNL study can not be made at the present time since that study has not been completed.

The primary objective of this study has been to evaluate part of the Indian Point Plant, Unit 3 for systems interactions using Digraph Matrix Analysis.

Within the scope and limitations oif this Digraph Matrix Analysis to find Systems Interactions at Indian Point-3, we have reached the following conclusions:

(1) When only the front-line systems involved in safety injection and feedwater are evaluated, we found no failure sets not included in the IP-PSS. Both we and PASNY found the front-line systems robust.

(2) The inclusion of detailed support system models into the analysis significantly increased the number of failure sets over those found in the IP-PSS for all system combinations which could be compared. In particular important systems interactions were found in System Combinations 1 and 4 which were not found in the IP-PSS.

The system interaction found in System Combination 1, Low Pressure Injection in response to a medium LOCA was first identified by BNL. After correction of the electrical load shedding model in the DMA model, we also identified the same systems interaction. This S.I. involved the failure of BATTERY 32 preventing the RHR pumps from running given the nonfailure of offsite electrical power.

In System Combination 4, High Pressure Injection in response to an RCP seal LOCA, we found two types of significant systems interactions. In this case we were looking for a single failure or pair of failures which would cause a seals failure (hence a LOCA) <u>and</u> also prevent safety injection from functioning successfully. These two systems interactions were:

(A) The incorrect manual setting of a valve in the service water system would cause the diesel generators to fail. Thus in the effect of the loss of offsite power, the plant 480V electrical system will fail resulting in an RCP seals LOCA. Since there is no 480V electrical power, safety injection will not function resulting in a core damage incident. The "initiator" in this case is loss of offsite power. This systems interaction was not discovered by PASNY in the IP-PSS.

(B) The failure of interlock ITLBKR3AT6A in the auto closing circuits for breakers EG2 and 2AT3A prevents closure of these breakers unless breaker 3AT6A is open. Physically, the interlock is a "b" contact breaker auxiliary switch. If breaker 3AT6A is closed, or if the "b" contact fails to close when that breaker is open, then the interlock fails and EG2 and 2AT3A will not close automatically. Under Loss of Offsite Power circumstances, this can cause the loss of multiple trains of front-line systems. In particular, Auxiliary Feedwater pumps 31 and 33 and two of the three safety injection pumps as well as Residual Heat Removal pumps 31 and 32 will not start automatically. Similarly, a "b" contact interlock on breaker 2AT5A prevents diesel supply breakers EG1 and EG3 from closing automatically (see Section 3.2 for details). This S.I. was not discovered by PASNY.

(3) When we evaluated front-line and support systems with location vulnerabilities, we identified several key locations though we did not find initiating events.

Locations LOCDP (480 V bus location), LOC001 (AFW pump room), LOCSIPRM (SI pump room), were vitally important and presently secure.

(4) When we evaluated front-line and support systems together with their location vulnerabilities and their interactions with operator actions, we concluded:

(A) Operator actions that initiate safety actions, such as starting pumps and opening valves, greatly improves reliability and should generally be recommended for both safety injection and feedwater systems.

(B) Operator actions that terminate safety actions, such as stopping pumps or closing valves, should only be allowed with the concurrence of a supervisor.

(C) That there is a significant difference between operator actions dealing with front-line systems instead of support systems.

In conclusion, we feel that this demonstration of DMA at an operating reactor showed the effectiveness of detailed system modeling and analysis. In particular, the structured methodology of DMA forced us to model the electrical system and service water system in greater detail than anyone had done before. As a result of this detailed modeling, we found two significant systems interactions. The first discovery of the BATTERY 32 problem by BNL demonstrated to us two things:

(1) Better coordination between modellers was needed (to correct the load shedding model)
(2) Knowledgeable analysts (such as at BNL) are invaluable in any safety study.

REFERENCES

1. U.S. Atomic Energy Commission, "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants," WASH-740, 1957.

2. U.S. Nuclear Regulatory Commission, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG 75/014), October 1975.

3. G. E. Cummings, "Operator/Instrument Interactions During the Three Mile Island Incident," IEEE Symp. Nucl. Power Sys., October 19, 1979.

4. G. Lanik, U.S. Nuclear Regulatory Commission, "Report on the Interim Equipment and Procedures at Browns Ferry to Detect Water in the Scram Discharge Volume," September 1980.

5. U.S. Nuclear Regulatory Commission, Verbatim Transcript of Advisory Committee on Reactor Safeguards, Fluid Dynamics Subcommittee Meeting, Tuesday, August 19, 1980, Inglewood, California.

6. C. Michelson, OAEOD, memorandum to R. R. Denton, NRR, "Potential for Unacceptable Interaction Between the Control Rod Drive System and Non-Essential Control Air System at the Browns Ferry Nuclear Plant," August 18, 1980.

7. S. Rubin and G. Lanik, U.S. Nuclear Regulatory Commission, "Report on the Browns Ferry 3, Partial Failure to Scram Event on June 28, 1980," July 30, 1980 (with Executive Summary).

8. U.S. Nuclear Regulatory Commission, "Transient Response of Babcock & Wilcox - Designed Reactors," NUREG-0667, May 1980.

9. Nuclear Safety Analysis Center and Institute of Nuclear Power Operations, "Analysis and Evaluation of Crystal River Unit 3 Incident," Joint NSAC/Impo Report NSAC-3/INPO-1, March 1980.

10. U.S.N.R.C., "Action Plan Developed as a Result of the TMI-2 Accident," NUREG-0660, May 1980.

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

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

13. J. J. Lim, H. P. Alesso, T. R. Rice, R. K. McCord, J. E. Kelly, "Systems Interaction Evaluation Procedure for Application to Indian Point-3," Lawrence Livermore National Laboratory, Livermore, CA, U.S. Nuclear Regulatory Commission Report NUREG/CR-2050 (May 1981).

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

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

16. D. M. Rasmussen, G. R. Burdick, and J. R. Wilson, "Common Cause Failure Analysis Techniques: A Revision and Comparative Evaluation," EG&G Idaho, Inc., TREE 1349 (September 1979).

17. F. D. Coffman, "Initial Guidance for the Performance of Systems Interaction Reviews at Selected LWRs," U.S. Nuclear Regulatory Commission October 1, 1981 (Draft).

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

19. H. P. Alesso, I. J. Sacks and C. F. Smith, "Initial Guidance on Digraph Matrix Analysis for Systems Interaction Studies, NUREG/CR-2915, UCID-19457, January 1983.

20. I. J. Sacks, B. C. Ashmore and H. P. Alesso, "Systems Interaction Results from the Digraph Matrix Analysis of a Nuclear Power Plant's High Pressure Safety Injection Systems," Vol. 1 and 2, NUREG/CR-3593, UCRL 53467, July 1984.

21. Power Authority of the State of New York, "Indian Point Probability Safety Study," 1983.

22. Final Safety Analysis Report, Indian Point Three Nuclear Power Plant, Power Authority of the State of New York, Docket No. 50286, July 1982, Revision 2.

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

24. G. J. Kolb, Review and Evaluation of Indian Point Probabilistic Safety Study, U. S. Nuclear Regulatory Commission, NUREG/CR-2934, Dec. 1982.

NRC FORM 335
(2-84)
NRCM 1102,
3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER *(Assigned by TIDC, add Vol. No., if any)*
NUREG/CR-4179
UCID-20350
Vol. 1

2. TITLE AND SUBTITLE
Digraph Matrix Analysis for Systems Interactions at Indian Point Unit 3

3. LEAVE BLANK

4. DATE REPORT COMPLETED
MONTH: August YEAR: 1984

5. AUTHOR(S)
H.P. Alexxo, et al.

6. DATE REPORT ISSUED
MONTH: January YEAR: 1986

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Lawrence Livermore National Laboratory
Livermore, CA 94550
Subcontractors: Analytic Information Processing, Inc.
and
Science Applications, Inc.

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER
A0445

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

11a. TYPE OF REPORT
Technical

b. PERIOD COVERED *(Inclusive dates)*

12. SUPPLEMENTARY NOTES
Pertain to Docket No. 50-286

13. ABSTRACT *(200 words or less)*

Digraph Matrix Analysis (DMA) has been under development as a tool to search for systems interactions at nuclear power plants. This report presents the DMA methodology and the results of the analysis of selected safety system combinations at the Indian Point Unit 3 so as to allow a comparison with a competitive analysis performed by Brookhaven National Laboratory. The plant specific results of this study were as follows:

1. No new systems interactions were found in the front-line safety injection or feedwater systems when analyzed separately.
2. The analysis of the complete systems including support systems such as electrical power and service water uncovered the following significant systems interactions:
   a. Improper alignment of a manually set valve in the service water system in conjunction with the loss of offsite power will cause the failure of the diesel generators resulting in a RCP seals failure along with the failure of safety injection leading to reactor core damage.
   b. Failure of an electrical interlock (a set of contacts) in conjunction with the loss of offsite power will cause the loss of multiple trains of front-line systems.

14. DOCUMENT ANALYSIS – a. KEYWORDS/DESCRIPTORS
Indian Point 3
Systems Interactions
Digraph Matrix Analysis

b. IDENTIFIERS/OPEN-ENDED TERMS

15. AVAILABILITY STATEMENT
Unlimited

16. SECURITY CLASSIFICATION
(This page)
Unclassified
(This report)
Unclassified

17. NUMBER OF PAGES

18. PRICE

(317) 318 blank