UCID- 19473

Preliminary Investigation of Interconnected Systems Interactions for the Safety Injection System of Indian Point-3

H. P. Alesso
D. A. Lappa

Lawrence Livermore National Laboratory

C. F. Smith
Science Applications, Inc.

I. J. Sacks
Analytic Information Processing, Inc.

March 4, 1983

Lawrence Livermore Laboratory

This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy.

ABSTRACT

The rich diversity of ideas and techniques for analyzing interconnected systems interaction has presented the NRC with the problem of identifying methods appropriate for their own review and audit. This report presents the findings of a preliminary study using the Digraph Matrix Analysis method to evaluate interconnected systems interactions for the safety injection system of Indian Point-3.

The analysis effort in this study was subjected to NRC constraints regarding the use of Boolean logic, the construction of simplified plant representations or maps, and the development of heuristic measures as specified by the NRC.

We found the map and heuristic measures to be an unsuccessful approach since they require an effort comparable to a risk assessment study while the exclusion of Boolean logic resulted in a significant reduction in statistical correlation with safety. However, from the effort to model and analyze the Indian Point-3 safety injection system, including Boolean logic in the model, we were successful in identifying singleton and doubleton cut-sets.

We recommend that (a) efforts excluding Boolean logic and utilizying the NRC heuristic measures not be pursued further at LLNL, and (b) that the Digraph Matrix approach (or other comparable risk assessment technique) with Boolean logic included be used to conduct the audit of the Indian Point-3 systems interaction study.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INTRODUCTION

1.1 Background and Motivation

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

The Office of Nuclear Reactor Regulation of the NRC is developing a program to further define and subsequently implement SI regulatory requirements for light water reactors (LWRs). The need to design LWRs against adverse SIs was recognized and formally begun in May, 1978.[1] Assessments of Three Mile Island-2 (TMI-2)[2] and other recent events, including those at Browns Ferry-3[3-6] and Crystal River-3[7] have pointed to the need for increased review efforts in this area. Consequently, the NRC contracted with the Battelle Columbus/Pacific Northwest Laboratories,[8] Brookhaven National Laboratory,[9] and Lawrence Livermore National Laboratory[10] to review the state-of-the-art in SI. The three laboratories examined reported incidents from reactor operating experience, defined a set of criteria for SI, and evaluated existing and potential methodologies for the analysis of SI. The methods evaluated included some based primarily on risk assessment techniques,[11] and others based primarily on the expert judgment of a multidisciplinary team after an on-site inspection.[12] As a result of the state-of-the-art review, the three laboratories unanimously recommended risk assessment techniques, such as event tree/fault tree methods, combined with walk-through inspections for identifying SIs. Various ranking criteria were suggested for evaluating the SIs once they were identified. The Power Authority of the State of New York (PASNY), at about this time, developed its own systems interaction methodology for application to the interconnected systems at Indian Point-3 (IP-3).[13-14] The method was based on "shutdown logic diagrams" which were success-paths of operational sequences.

Preliminary results[15] indicated that there are at least three concepts on how Systems Interactions could be incorporated into an overall Probabilistic Risk Assessment (PRA).

One concept is that systems interactions can be adequately analyzed by enhancing existing PRA techniques. This would be done by expanding the scope and boundary conditions of fault tree analysis and putting additional emphasis on dependency analysis techniques such as generic analysis,[16] minimum cut-set common cause/mode analysis[16] or digraph-fault tree analysis.[17] NRC's initial guidance for this point of view has already begun.[15]

A second, and closely related concept is that systems interactions can be incorporated into a PRA at the event tree stage of analysis. This approach attempts to capture systems interactions at an earlier stage of analysis; by treating dependencies in the event tree analysis portion of a PRA, the requirement of fault tree modeling at additional levels of detail is reduced.[15]

The third concept is based on matrix representation of logic diagrams and is called Digraph Matrix Analysis.[17-18] This technique would be applied after the event tree analysis has identified the accident sequences, but prior to initiating fault tree construction. It treats an accident sequence consisting of several systems along with their support systems as a single success-oriented model. Thus, instead of constructing a reliability block diagram (or equivalent) and a fault tree for each individual system in an accident sequence, as in the Reactor Safety Study,[19] the entire accident sequence is modeled as a single success-oriented operational logic diagram which includes AND and OR gates. The advantage is that such a model can be rigorously separated into independent parts that can be analyzed individually. Once the systems interactions are identified, the fault trees and the rest of PRA could be completed.

A review of the fundamental mathematical aspects of fault-oriented and success-oriented risk analysis (including Digraph-Matrix Analysis) was presented in [20], which offered insight into the trade-off advantages and disadvantages of each.

1.2 Statement of the Problem

This rich diversity of ideas and techniques for utility studies analyzing interconnected systems interaction presented the NRC with the problem of finding a way to evaluate systems interconnections for their own review and audit. It was desired that an independent study be conducted and compared to the licensee submittal. However, the independent study was intended to be performed at a reduced scope.

1.3 Approach

Nuclear power plants are designed and operated such that any given safety function can be achieved through a variety of alternative paths. In other words, for a given safety function, there are typically redundant trains of success paths. Defense-in-depth is achieved in part through design approaches such as redundancy, physical separation, functional diversity, independence, coincidence, quality assurance and testing. If executed properly, these design approaches lead to a level of safety function reliability much higher than can be achieved in a simpler system. However, the resulting system complexity provides the potential for systems interaction. A characteristic aspect of the systems interaction problem is the question of system and/or component independence.

To be useful in a systems interaction assessment, a methodology must be capable of analyzing systems at the component level of detail. It is further desirable that the impact of the interaction on plant safety as a whole be evaluated for ranking purposes.

The identification of the various systems needed to perform the basic safety functions should be followed by the identification of the systems and trains needed to support them. This will involve consideration of support systems, and should extend to the component level. It is likely that interactions resulting from failures of the support systems will be manifested through the components of the systems directly responsible for the safety functions. Interactions at this level often involve "common cause" failures, i.e., multiple component failures due to common single event or failure.

Following the identification of the systems interactions candidates, it is necessary to evaluate their impact on plant safety.

A systematic approach must be taken in exploring the relationships between systems in a nuclear power plant because the plant is complex and the relationships are subtle. At one end of the spectrum of complexity, the systems analysis method could be a detailed fault tree/event tree analysis with an emphasis of dependent (common cause/mode) failures. Other simpler approaches have been discussed elsewhere.[8,9,10,15] A formal structured approach is believed to be desirable and has been recommended.[18,20]

The Indian Point-3 Interconnected systems interaction audit effort to be conducted by LLNL has been subjected to the following NRC constraints:

1. Boolean logic is excluded from modeling efforts (but not necessarily from computer code processing).
2. A "map" of the systems at the train level of detail is to be constructed.
3. Heuristic measures, specified by the NRC, called "connectivity" (degrees of a node) and "levels of dependency" (paths between any node and all others) are to be used to draw statistical correlation between the map and the potential for systems interactions in the systems involved.

The motivation for these constraints was the possible advantages to be found from (1) simpler analyst effort and training, and (2) reduced scope and costs of effort.

This draft report is a preliminary attempt to conduct a systems interaction investigation of the IP-3 safety injection system, and its component cooling, actuation and electrical connections subject to the NRC constraints. We found the specific IP-3 safety injection system design to be particularly difficult to represent in a model subject to the NRC constraints. It contained numerous common pipe-headers and common "passive" components within and between trains. In addition, the numerous plant modes and configurations under differing accident conditions compounded the modeling problems. As a result, we were unable to strictly adhere to the NRC constraints.

In order to identify which components were necessary for successful operation of individual trains, it was necessary to form detailed component level representations of the entire system. This violated constraint 2. In addition, we attempted to apply numerous constraints on the system model such as limiting it to the injection phase following a small LOCA during loss of offsite power. This was done in an attempt to avoid explicit Boolean logic in the modeling. Despite this, the component-level representation required some specific AND conditions in order to differentiate multiple "dependency" conditions from simple hardware connections. This violated constraint 1. After a component-level logical representation of the safety injection and related systems was completed, we attempted to construct a safety injection system "map" (at the component level), and find its "connectivity" and "level of dependency" measures. The "map" became essentially our original component-level logical

representation with the AND and OR logic conditions excluded. However, by excluding Boolean logic, the "connectivity" and "levels of dependency" measures suffer a significant reduction in their ability to provide a statistical correlation with safety. Therefore, for the systems considered in this study, we found the specified measures to be inadequate. This failed constraint 3.

As a result, we found the "map," and the heuristic measures as specified by NRC to be an unsuccessful approach based on the following criteria: (a) they required as much detailed study, training, effort and cost as a comparable risk assessment study, and (b) the evaluation criteria were less informative than a comparable risk assessment result.

It should be noted, however, that the component-level logical representations which we constructed while attempting to overcome the modeling problems (not very different from directed logic diagrams used in Digraph-Matrix Analysis (DMA) or, for that matter, from conventional fault trees) still contain the essential modeling information. From these representations, which were actually the residue of our attempts, we were able to find singleton and doubleton cut-sets for the safety injection system and support systems.

In section 2, we outline the efforts we made to develop a systems interaction audit procedure subject to the NRC constraints. The methodology focuses attention on evaluating the independence of safety system trains and looks for violations of the single failure criterion.

In section 3.1, we briefly describe the IP-3 safety injection system. In section 3.2, we review modeling efforts that we used in attempting to develop a systems interaction audit procedure that would meet the NRC constraints. We illustrate the problem areas that forced us to violate the NRC criteria for this procedure. Finally, in section 3.3, Phoenix-like, we discuss how the detailed component-level logic models, which of necessity were constructed in violation of NRC constraints 1 and 2, were capable of adequately addressing the systems interaction identification problem. From the component-level logic models we found single and doubleton cut-sets (dependent failures) of the system.

2.0 INTERCONNECTED SYSTEMS INTERACTION EVALUATION PROCEDURE

The steps in the systems interaction audit methodology attempted in this report are summarized below.

1. Review plant safety system to identify systems trains
2. Model active components within each train
3. Construct matrix of active components
4. Use matrix to generate map of each train
5. Find "connectivity" and "levels of dependency" measures

First, the plant's safety systems necessary for the plants Engineering Safety Features are identified and reviewed. FSAR, P&ID, system description and electrical wiring information is gathered and reviewed. From this information, the safety systems within the Engineered Safety Features are further delineated into trains. In newer designs, trains are more readily identified. In older designs such as Indian Point-3, however, trains are greatly interrelated due to common headers and common (passive) components. Therefore, as the specific plant design required, modeling of the trains was conducted to the level of detail necessary to assure train identification. In the case of Indian Point-3, it was necessary to model at the individual component level of detail. It was also necessary to limit the study to the high pressure safety injection system with related support systems. Once models of the individual trains were completed, a computer code was used to generate a train "map" and find the system measures "connectivity" and "levels of dependency." In addition, we found singleton and doubleton cutsets.

3.0 INDIAN POINT-3 SAFETY INJECTION SYSTEM EVALUATION

In section 3.1, we summarize the Indian Point-3 Safety Injection and related support systems descriptions. Then in section 3.2, we present the model of the system developed to the train level of detail. In section 3.3, we present the mapping, measures (which proved inadequate), and singleton, doubleton cutset results.

3.1 Indian Point-3 Safety Injection System

The following Indian Point-3 Safety Injections System description borrows from information used in this study including [21-23].

The Safety Injection System is intended to provide adequate emergency core cooling. This system (which constitutes the Emergency Core Cooling System) operates in three modes. These modes are referred to as passive accumulator injection, active safety (or high pressure) injection and residual heat removal recirculation. The system assures that the core will remain intact and in place with its essential heat transfer geometry preserved following a rupture in the Reactor Coolant System.

Redundancy and segregation of instrumentation and components are incorporated to assure that postulated malfunctions will not impair the ability of the system to meet the design objectives. The system is designed to be effective in the event of loss of normal station auxiliary power coincident with the loss of coolant, and is designed to be tolerant of failure of any single component or instrument channel to respond actively in the system.[21]

System Description

The Safety Injection System is designed to provide adequate emergency core cooling following a Loss-of-Coolant Accident. The system components operate in the following possible modes:

a. Injection of borated water by the passive accumulators.

b. Injection of borated water from the Boron Injection Tank and the Refueling Water Storage Tank (RWST) with the safety injection pumps. Thus the two channels of high pressure injection include direct injection (RWST to the Reactor Cooling System) and boron injection through the Boron Injection Tank.

c. Injection by the residual heat removal pumps also drawing borated water from the Refueling Water Storage Tank.

d. Recirculation of spilled reactor coolant, injected water and Containment Spray System drainage back to the reactor from the recirculation sump by the recirculation pumps. (The residual heat removal pumps provide backup recirculation capability.)

To provide protection for large area ruptures in the Reactor Coolant System, the Safety Injection System must respond to rapidly reflood the core following the depressurization and core voiding that is characteristic of large area ruptures. The accumulators act to perform the rapid reflooding function with no dependence on the normal or emergency power sources and also, with no dependence on the receipt of an actuation signal.

The measure of effectiveness of the Safety Injection system is the ability of the pumps and accumulators to keep the core flooded or to reflood the core rapidly where the core has been uncovered for postulated large area ruptures. The result of this performance is to limit any increase in clad temperature below a value where emergency core cooling objectives are met.

With minimum onsite emergency power available (two-of-three diesel generators), the required emergency core cooling equipment is two out of three safety injection pumps, one out of two residual heat pumps, and three out of four accumulators for a cold leg break and four accumulators for a hot leg break. With these systems, the calculated maximum fuel cladding temperature is limited to a temperature less than that which meets the emergency core cooling design objectives for all break sizes up to and including the double-ended serverence of the reactor coolant pipe.

For large area ruptures the clad temperatures are turned around by the accumulator injection. The active pumping components serve only to complete the refill started by the accumulators. Either two safety injection pumps or one residual heat removal pump provides suffient addition of water to continue the reduction of clad temperature initially caused by the accumulator.

Initial response of the injection systems is automatic with appropriate allowances for delays in actuation of circuitry and active component. The active portions of the injection systems are automatically actuated by the

safety injection signal. In addition, manual actuation of the entire injection system and individual components can be accomplished from the Control Room. In analysis of system performance, delays in reaching the programmed trip points and in actuation of components are conservatively established on the basis that only emergency onsite power is available.

The starting sequence of the safety injection and residual heat removal pumps and the related emergency power equipment is designed so that delivery of the full rated flow is reached within 34 seconds after the process parameters reach the set points for the injection signal. Motor control centers are energized and injection valves are opened at the same time as the pumps are started.

The delay time consists of the time intervals:

		Seconds
a.	to initiate the safety injection signal, including instrument lag	1
b.	To start two diesel generators	19
c.	To start two safety injection pumps	8
d.	To start one residual heat removal pump	6
	TOTAL	34

The initiation signal for core cooling by the safety injection pumps is the safety injection signal which is actuated by any of the following: (a) low pressurizer pressure, (b) high containment pressure, (c) high differential pressure between any other two steam generators, (d) high steam flow in any two of the four steam lines coincident with low T_{avg} or low steam pressure, and (e) manual actuation.

For the purpose of this study, analysis has been centered on the high pressure safety injection system as it would be required to function under small break LOCA conditions.

High Pressure Injection Phase

The high pressure safety injection system consists of three safety injection pumps, the boron injection tank, and a network of piping, pipe headers, and valves. The system is dependent upon various electrical, control and component cooling equipment for support. Figure 1 is a schematic diagram of the high pressure safety injection system.

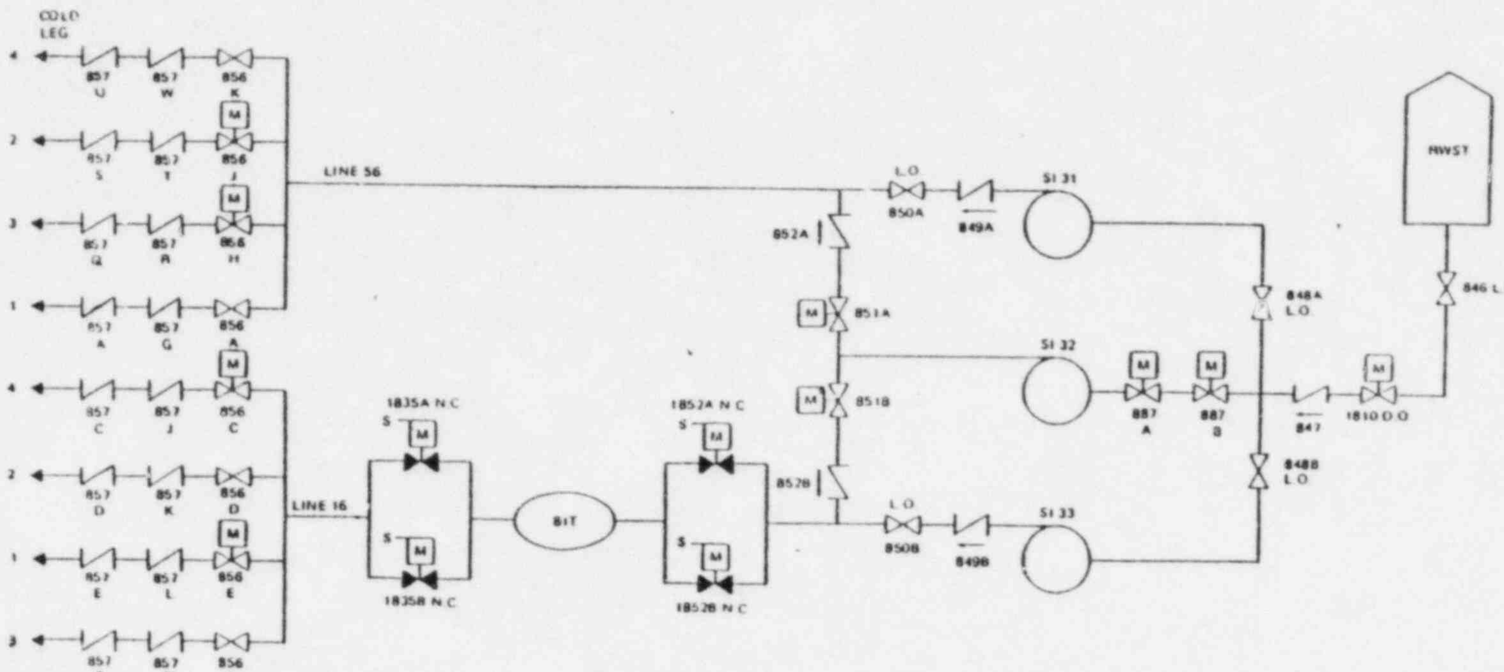


Figure 1. Indian Point-3 High Pressure Safety Injection System (from Reference 23)

The safety injection signal starts the safety injection pumps and opens the Safety Injection System isolation valves. The safety injection pumps deliver borated water to two separate discharge headers. The flow from each header is injected into each of the four cold legs of the Reactor Coolant System (RCS).

One major safety injection flow path contains a boron injection tank (discharge side of pump) for the addition of negative reactivity to the reactor cold legs in the minimum time delay. The tank contains boric acid at a nominal value of 21,000 ppm boron (12 percent solution), and is isolated from the safety injection pump discharge line by redundant, normally closed parallel valves. The valves open upon receipt of a safety injection signal. The refueling water flowing into the tank from the discharge of the high head pumps forces the high boron concentration solution out of the tank and into the RCS.

The second major flow path provides for direct injection of water from the RWST into the RCS. The two flow paths deliver water to the RCS through separate discharge headers, each consisting of four cold leg injection lines.

The three safety injection pumps operate in parallel to provide flow from a common coolant supply through the two major paths into the two injection line headers. Of the three pumps, one is dedicated to each major flow path, while the third (pump 32) provides flow to both paths.

If the four injection lines on a header remain intact, the flow from one safety injection pump is sufficient to meet design requirements for makeup of coolant following a small break which does not immediately depressurize the Reactor Coolant System to the accumulator discharge pressure. Since the small break may be an injection line, two safety injection pumps are required.

Safety Injection Component Cooling

The component cooling system (CCS) is a closed loop system. Water is pumped by three component cooling water (CCW) pumps to two component cooling heat exchangers. Here, heat is exchanged to the service water system. The cooled water which emerges then travels on to various plant locations and

cools numerous components, finally returning as suction for the three CCW pumps.

The component cooling system's support of the safety injection system involves only the cooling of the three safety injection pumps. Considering the case of a unit trip, with loss of off-site power and safety injecti-n, according to the Indian Point PRA (reference 24, page 6):

> "When this condition occurs, all CCS pumps are tripped. Electrical power is reestablished using the emergency diesel generators. The following events will occur in the component cooling loop:
>
> .
> .
> .
>
> - The shaft driven circulating pumps will be running when the safety injection pumps run and will supply cooling services for these pumps."

Thus, for the plant conditions assumed, the only requirement of the CCS is that it provide suction for the shaft driven circulating pumps. On page 3 of the PRA[23] we find:

> "The three safety injection pumps receive flow during all plant conditions.... Each pump drives an attached circulating pump which is capable of supplying the cooling requirements for the safety injection pump using the water contained in the CCS supply headers."

Thus for the assumed plant condition, we conclude that the no active components of the CCS are required to function. Accordingly, we have incorporated the CCS in our modeling of the safety injection system only in terms of the circulating pumps that are driven by the safety injection pumps.

3.2 IP-3 Safety Injection System Modeling

The basic overview of the safety injection system is shown schematically in Figure 1 (page 10). This system was modeled from P&ID,[21] FSAR[22] and PRA[23] information which was used to identify active components in the system and their operation during specified condicions. Note that small diameter piping connections and flow paths were ignored for this analysis. Active components were defined as components that require either a change of state or active

signals, actuation or operation from an external support system. The basic simplifying assumptions imposed on the analysis in order to distinguish a dependency from a simple hardware connection were:

- Small break LOCA
- Loss of off-site power
- Safety Injection (high pressure) phase
- Inactive components and piping ignored except where required to indicate significant interconnection between active components
- The model of the actuation system is developed only to the identification of instrument signal inputs to actuation logic channels
- Only connections representing dependency considered
- Normal system alignment of components.

Successful accomplishment of the high pressure safety injection function was assumed to occur when any one safety injection pump had at least a single flow path to the Reactor Cooling System.

Table 1 gives a list of acronyms used in component modeling. The list shows the components included in the model. The principal support systems for the safety injection system are the electrical and actuation systems, with component cooling consolidated into the safety injection system itself.

The resulting component-level logic models of the safety injection system (see Figure 2), the electrical connections (see Figure 4), the actuation connections (see Figure 6) and their dual representations (see Figures 3, 5, 7 respectively) were then constructed.

The digraphs of the safety injection system (Figures 2 and 3) illustrate the two major flow paths into the RCS via separate discharge headers into cold leg injection lines. The electrical and actuation system inputs into various active elements (valves, pumps, and the boron injection tank) are also included. The pumps are shown to be dependent on their respective electric power buses, component cooling, actuation signals, and coolant flow. Motor operated valves that change state upon initiation of safety injection are shown to be dependent on electric power, actuation signals and flow. The boron injection path requires electric heating for the boron injection tank, heat tracing for the related pipes, and flow.

Table 1

Acronyms Used in Modeling

I. Electrical	
DG31-33	Diesel Generators 31-33
DC31-33	DC battery systems 31-33
BFI5A, 6A, 2A	Bus Fault Interlock on bus 5A, 6A or 2A
UV5A, 6A, 2A	Undervoltage on bus, 5A, 6A or 2A
EP5A, 6A, 2A	Electric Power bus 5A, 6A or 2A
BTB	Bus Tie Breaker
MCC36A, 36B	Motor Control Center 36A or B
II. Actuation	
MSI*	Manual Safety Injection
HSLF*	High Steam Loop Flow
SLDP*	Steam Loop Differential Pressure
LPP*	Low Pressurizer Pressure
HCP*	High Containment Pressure
SILOG1, 2	Safety Injection Logic Channels 1 and 2
SISIG1, 2	Safety Injection Signal Channels 1 and 2
III. Safety Injection	
RWST	Refueling Water Storage Tank
Vxxx	Motor operated valve #xxx
CCW1, 2, 3	Component Cooling Water loop 1, 2 and 3
SIP31, 32, 33	Safety Injection Pumps 31, 32, 33
HDRx	Header #x
MANSW	Manual Switch for Heat Trace
HTRC	Heat Tracing
EHTR	Electric Heaters
BIT	Boron Injection Tank
RCS	Reactor Cooling System

*These actuation signals are not developed further.

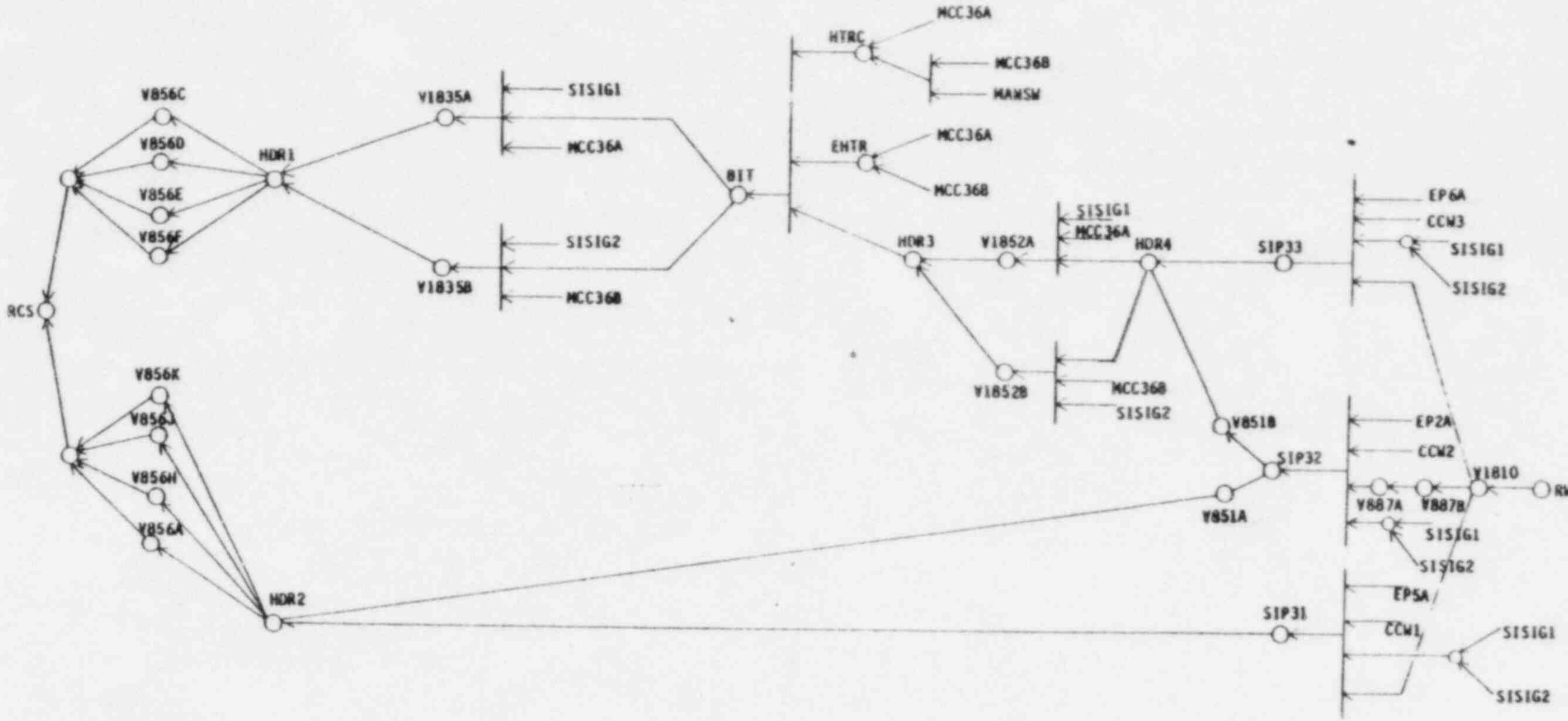


Figure 2. Success Digraph of Safety Injection System

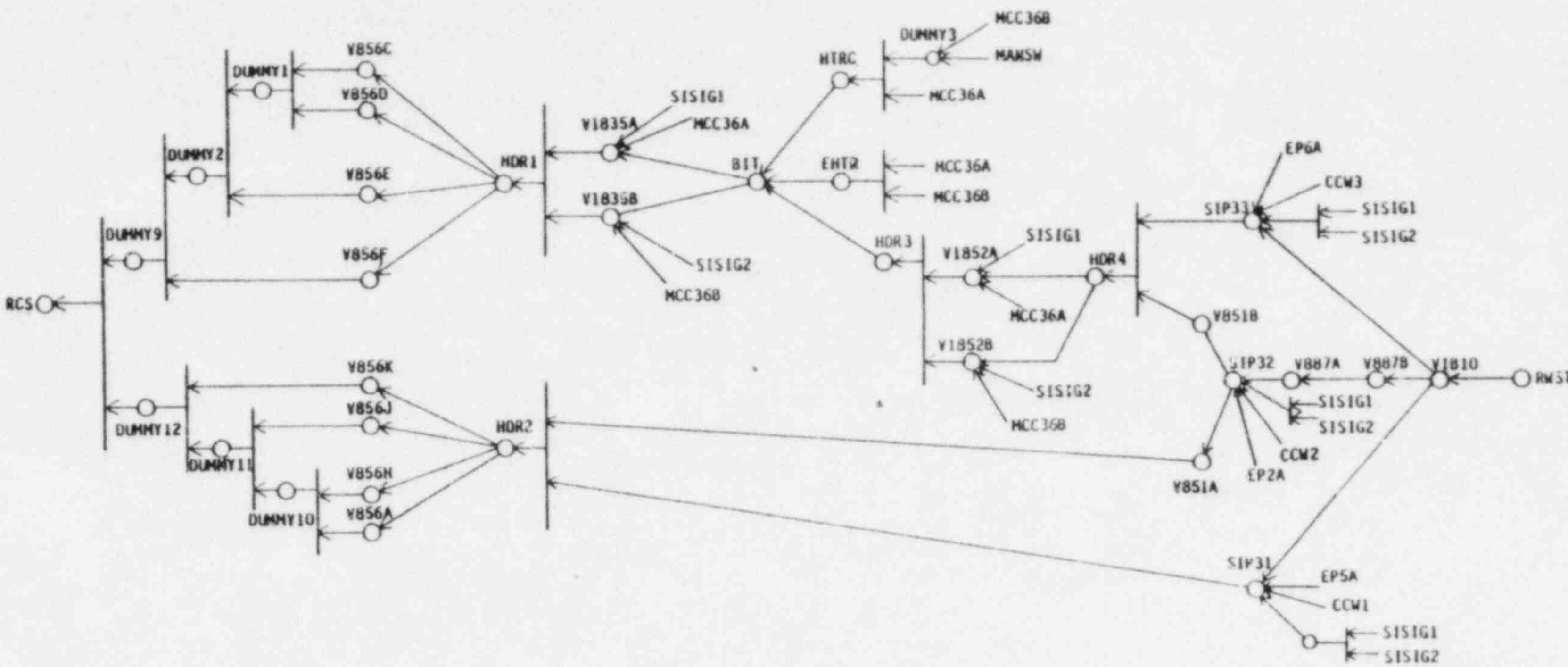


Figure 3 Dual Digraph of Safety Injection System

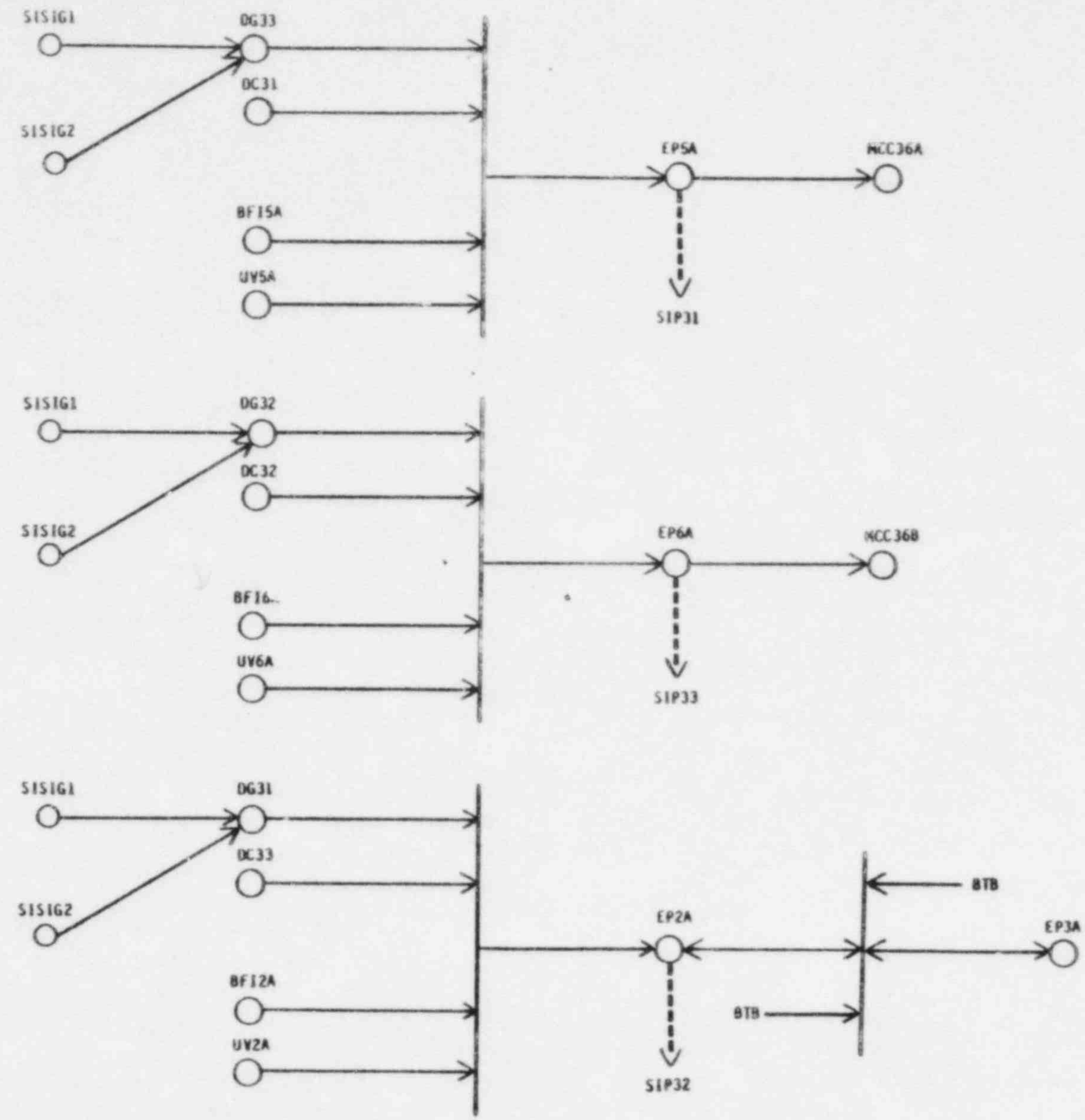


Figure 4. Success Digraph of Electrical Support System

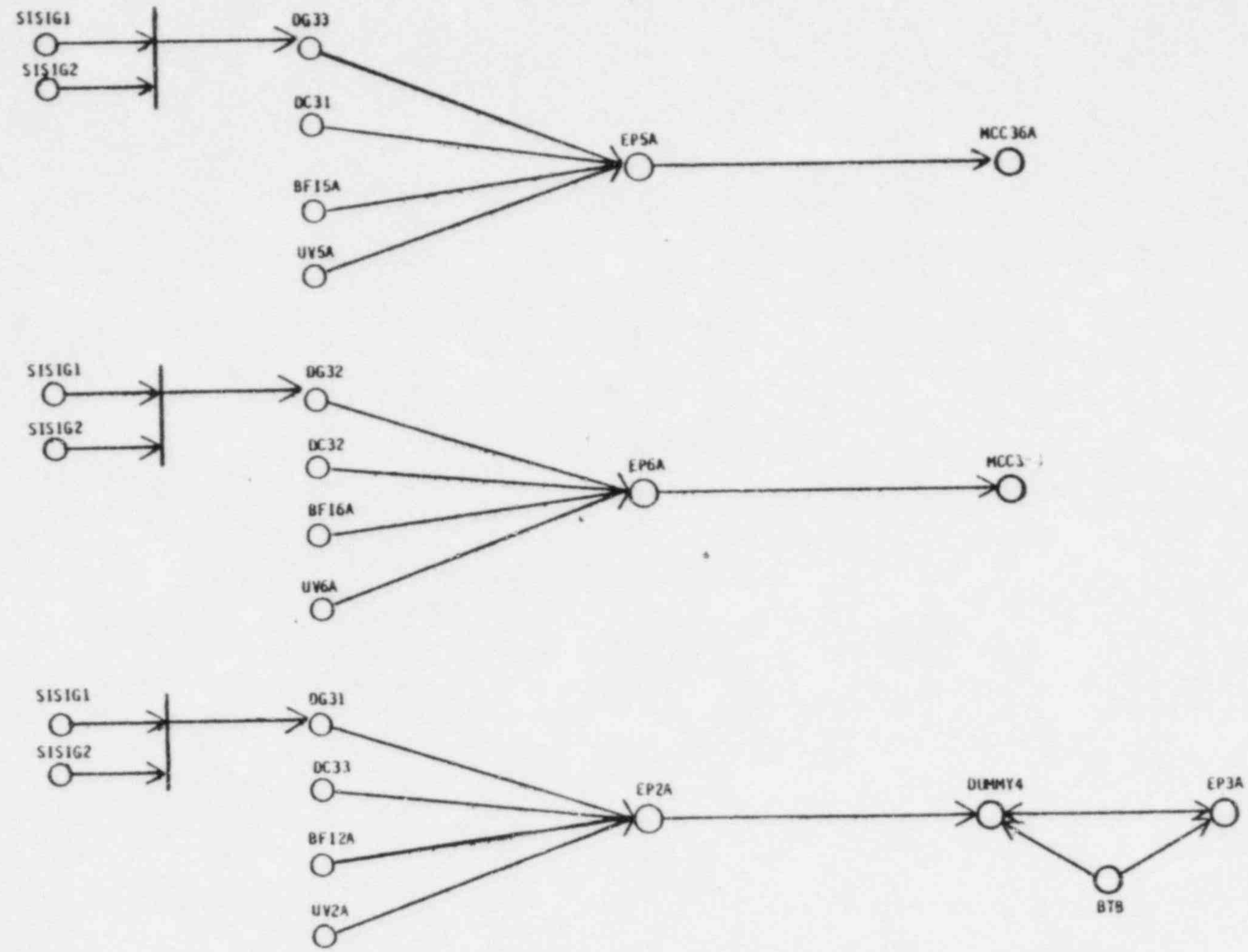


Figure 5. Dual Digraph of Electrical Support System

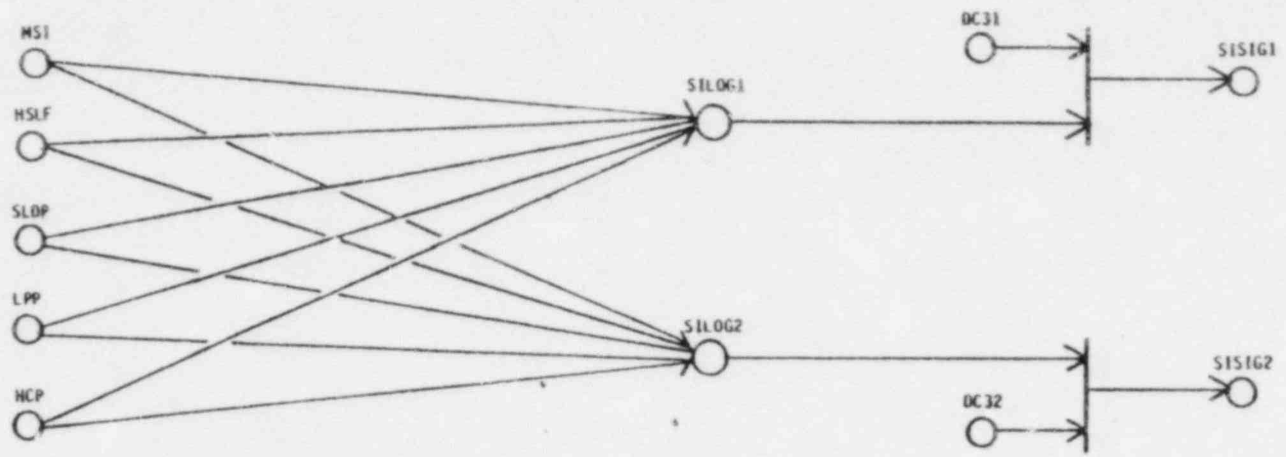


Figure 6. Success Digraph of Safety Injection Actuation

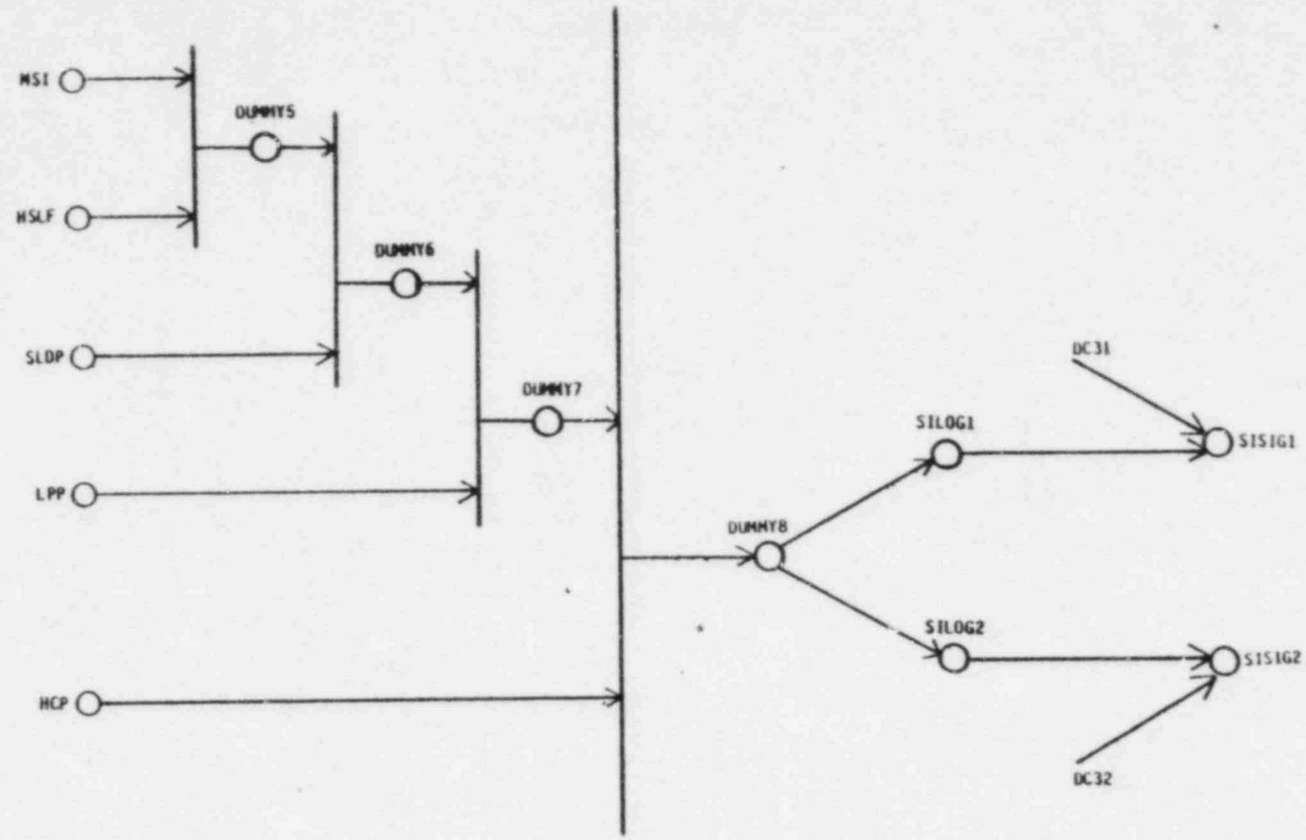


Figure 7. Dual Digraph of Safety Injection Actuation

The digraphs of the electrical support system (Figures 4 and 5) show the interrelationships between 480V power buses, motor control centers, diesel generators and DC power supplies. Also shown are the required actuation signals for diesel startup, and bus fault and undervoltage conditions for diesel connections to the buses.

The digraphs of the safety injection actuation system (Figures 6 and 7) show the instrumentation inputs into two separate logic channels. Also shown are the DC power requirements of the two logic channels for generating the respective actuation signals.

In developing the component level dependency models, it was necessary to incorporate information describing logical states of component interconnections. For example, the operation of a given component might require an actuation signal that could be provided by either actuation channel 1 or 2. In addition to either of these actuation signals, motive power might be required. A logical OR condition applies to the combination of actuation signals, whereas a logical AND condition expresses the mutual dependency where both actuation and motive power are necessary.

The model diagrams indicate OR conditions as directed lines that converge to the appropriate node. AND conditions are represented by the intersection of two or more directed lines with a perpendicular gate. Dummy nodes are used where necessary for computer processing.

The dual representation of a logic model (as discussed in reference 18) is obtained by changing AND gates to OR gates and OR gates to AND gates throughout the diagram. The dual representation of a success diagram is the corresponding fault oriented description. The dual representation is used to develop input for the computer processing of the model.

The computer input that represents the dual component-level logic models for the safety injection and support systems is shown in Table 2. The computer code processed this information and produced a list of components and their computer assigned numerical designators (Table 3) as well as the overall system "maps" (see Figures 8-12 and Overlays A-J).

Table 2

Computer Input Listing of Logic Model

```
RWST,V1810,1      RWST PROVIDES FLOW TO VALVE 1810,NORMALLY OPEN,
                    MOTOR OPERATED VALVE.
V1810,V887B,1           FLOW TO SIP32 IS THROUGH VALVE 887B
V887B,V887A,1           VALVES 887A AND B ARE IN SERIES
V1810,SIP31,1           V1810 PROVIDES SUCTION FOR SIP31
V887A,SIP32,1           V887A PROVIDES SUCTION FOR SIP32
V1810,SIP33,1           V1810 PROVIDES SUCTION FOR SIP33

SISIG1,SIP33,SISIG2     SAFETY INJECTION SIGNAL REQUIRED FOR SIP33
SISIG2,SIP33,SISIG1     SAFETY INJECTION SIGNAL REQUIRED FOR SIP33

SISIG1,SIP32,SISIG2     SAFETY INJECTION SIGNAL REQUIRED FOR SIP32
SISIG2,SIP32,SISIG1     SAFETY INJECTION SIGNAL REQUIRED FOR SIP32

SISIG1,SIP31,SISIG2     SAFETY INJECTION SIGNAL REQUIRED FOR SIP31
SISIG2,SIP31,SISIG1     SAFETY INJECTION SIGNAL REQUIRED FOR SIP31


CCW3,SIP33,1      COMPONENT COOLING PUMP 3 REQUIRED FOR SIP33
CCW2,SIP32,1      COMPONENT COOLING PUMP 2 REQUIRED FOR SIP32
CCW1,SIP31,1      COMPONENT COOLING PUMP 1 REQUIRED FOR SIP31

EP6A,SIP33,1            480V BUS 6A REQUIRED FOR SIP33
EP2A,SIP32,1            480V BUS 2A REQUIRED FOR SIP32
EP5A,SIP31,1            480V BUS 5A REQUIRED FOR SIP31

SIP33,HDR4,V851B         FLOW TO BIT THROUGH HEADER 4
V851B,HDR4,SIP33

SIP32,V851B,1           FLOW PATH FOR SIP32 TO BIT
SIP32,V851A,1           FLOW PATH FOR SIP32 TO DIRECT INJECTION

HDR4,V1852A,1           FLOW THROUGH BORON INJECTION LINE
SISIG1,V1852A,1         ACTUATION SIGNAL FOR BIT VALVE
MCC36A,V1852A,1         POWER SUPPLY FOR BIT VALVE
HDR4,V1852B,1           FLOW THROUGH BORON INJECTION LINE
SISIG2,V1852B,1         ACTUATION SIGNAL FOR BIT VALVE
MCC36B,V1852B,1         POWER SUPPLY FOR BIT VALVE
V1852A,HDR3,V1852B      FLOW TO BIT INPUT HEADER
V1852B,HDR3,V1852A
MCC36B,DUMMY3,1         ALTERNATE POWER SUPPLY FOR HEAT TRACING
MANSW,DUMMY3,1          MANUAL SWITCHOVER FOR HEAT TRACE
DUMMY3,HTRC,MCC36A      POWER SUPPLY FOR HEAT TRACING
MCC36A,HTRC,DUMMY3
MCC36A,EHTR,MCC36B      ELECTRIC HEAT FOR BIT
MCC36B,EHTR,MCC36A

HTRC,BIT,1              HEAT TRACING FOR BORON LINES
EHTR,BIT,1              ELECTRIC HEATING FOR BIT
HDR3,BIT,1              FLOW INTO BIT

BIT,V1835A,1            FLOW PATHS FROM BIT
BIT,V1835B,1
SISIG1,V1835A,1         ACTUATION OF BIT OUTLET VALVES
SISIG2,V1835B,1
MCC36A,V1835A,1         POWER TO BIT OUTLET VALVES
MCC36B,V1835B,1

V1835A,HDR1,V1835B      FLOW FROM BIT OUTLET VALVES
V1835B,HDR1,V1835A

HDR1,V856C,1      FLOW TO COLD LEG INJECTION LINE VALVES
HDR1,V856D,1
HDR1,V856E,1
HDR1,V856F,1

V856C,DUMMY1,V856D      FLOW TO RCS INJECTION LINES
V856D,DUMMY1,V856C
DUMMY1,DUMMY2,V856E
V856E,DUMMY2,DUMMY1
DUMMY2,DUMMY9,V856F
V856F,DUMMY9,DUMMY2

V851A,HDR2,SIP31        DIRECT INJECTION FLOW PATHS
SIP31,HDR2,V851A

HDR2,V856K,1      FLOW TO COLD LEG INJECTION LINE VALVE
HDR2,V856J,1
HDR2,V856H,1
HDR2,V856A,1

V856A,DUMMY10,V856H     FLOW TO RCS INJECTION LINES
V856H,DUMMY10,V856A
DUMMY10,DUMMY11,V856J
V856J,DUMMY11,DUMMY10
DUMMY11,DUMMY12,V856K
V856K,DUMMY12,DUMMY11
DUMMY9,RCS,DUMMY12      FLOW PATHS INTO RCS
DUMMY12,RCS,DUMMY9

SISIG1,DG33,SISIG2
SISIG2,DG33,SISIG1      SISIG STARTS DG33
DG33,EP5A,1             POWER SUPPLY FOR BUS 5A
DC31,EP5A,1             CONTROL POWER FOR BUS CONNECTION
BFI5A,EP5A,1            BUS FAULT INTERLOCK
UV5A,EP5A,1             BUS UNDER VOLTAGE REQUIRED
EP5A,MCC36A,1           POWER SUPPLY FOR MCC36A

SISIG1,DG32,SISIG2
SISIG2,DG32,SISIG1      SISIG STARTS DG32
DG32,EP6A,1             POWER SUPPLY FOR BUS 6A
DC32,EP6A,1             CONTROL POWER FOR BUS CONNECTION
BFI6A,EP6A,1            BUS FAULT INTERLOCK
UV6A,EP6A,1             BUS UNDERVOLTAGE REQUIRED
SISIG1,DG31,SISIG2
SISIG2,DG31,SISIG1      SISIG STARTS DG31

DG31,EP2A,1             POWER SUPPLY FOR BUS 2A
DC33,EP2A,1             BUS FAULT INTERLOCK
UV2A,EP2A,1             BUS UNDERVOLTAGE REQUIRED
EP2A,DUMMY4,1           BUS TIE TO BUS 3A
DUMMY4,EP3A,BTB         BTB IS BUS TIE BREAKER
BTB,EP3A,DUMMY4
EP3A,DUMMY4,BTB         BACK CONNECTION TO BUS 2A
BTB,DUMMY4,EP3A
MSI,DUMMY5,HSLF         SI INSTRUMENTATION
HSLF,DUMMY5,MSI         MSI IS MANUAL SI
DUMMY5,DUMMY6,SLDP      SLDP IS STEAM LINE DIFFERENTIAL PRESSURE
SLDP,DUMMY6,DUMMY5
DUMMY6,DUMMY7,LPP       LPP IS LOW PRESSURE-PRESSURIZER
LPP,DUMMY7,DUMMY6
DUMMY7,DUMMY8,HCP       HCP IS HIGH CONTAINMENT PRESSURE
HCP,DUMMY8,DUMMY7
DUMMY8,SILOG1,1         SILOG1 IS SI LOGIC CHANNEL 1
DUMMY8,SILOG2,1
DC31,SISIG1,1           SISIG1 IS CHANNEL 1 OF SI SIGNAL
SILOG1,SISIG1,1
DC32,SISIG2,1
SILOG2,SISIG2,1
0,0,0
```

Table 3

List Of Variables and Numerical Designators

1	1	37	DUMMY1
2	RWST	38	DUMMY2
3	V1810	39	DUMMY9
4	V887B	40	HDR2
5	V887A	41	V856K
6	SIP31	42	V856J
7	SIP32	43	V856H
8	SIP33	44	V856A
9	SISIG1	45	DUMMY10
10	SISIG2	46	DUMMY11
11	CCW3	47	DUMMY12
12	CCW2	48	RCS
13	CCW1	49	DG33
14	EP6A	50	DC31
15	EP2A	51	BFI5A
16	EP5A	52	UV5A
17	HDR4	53	DG32
18	V851B	54	DC32
19	V851A	55	BFI6A
20	V1852A	56	UV6A
21	MCC36A	57	DG31
22	V1852B	58	DC33
23	MCC36B	59	UV2A
24	HDR3	60	DUMMY4
25	DUMMY3	61	EP3A
26	MANSW	62	BTB
27	HTRC	63	MSI
28	EHTR	64	DUMMY5
29	BIT	65	HSLF
30	V1835A	66	DUMMY6
31	V1835B	67	SLDP
32	HDR1	68	DUMMY7
33	V856C	69	LPP
34	V856D	70	DUMMY8
35	V856E	71	HCP
36	V856F	72	SILOG1
		73	SILOG2

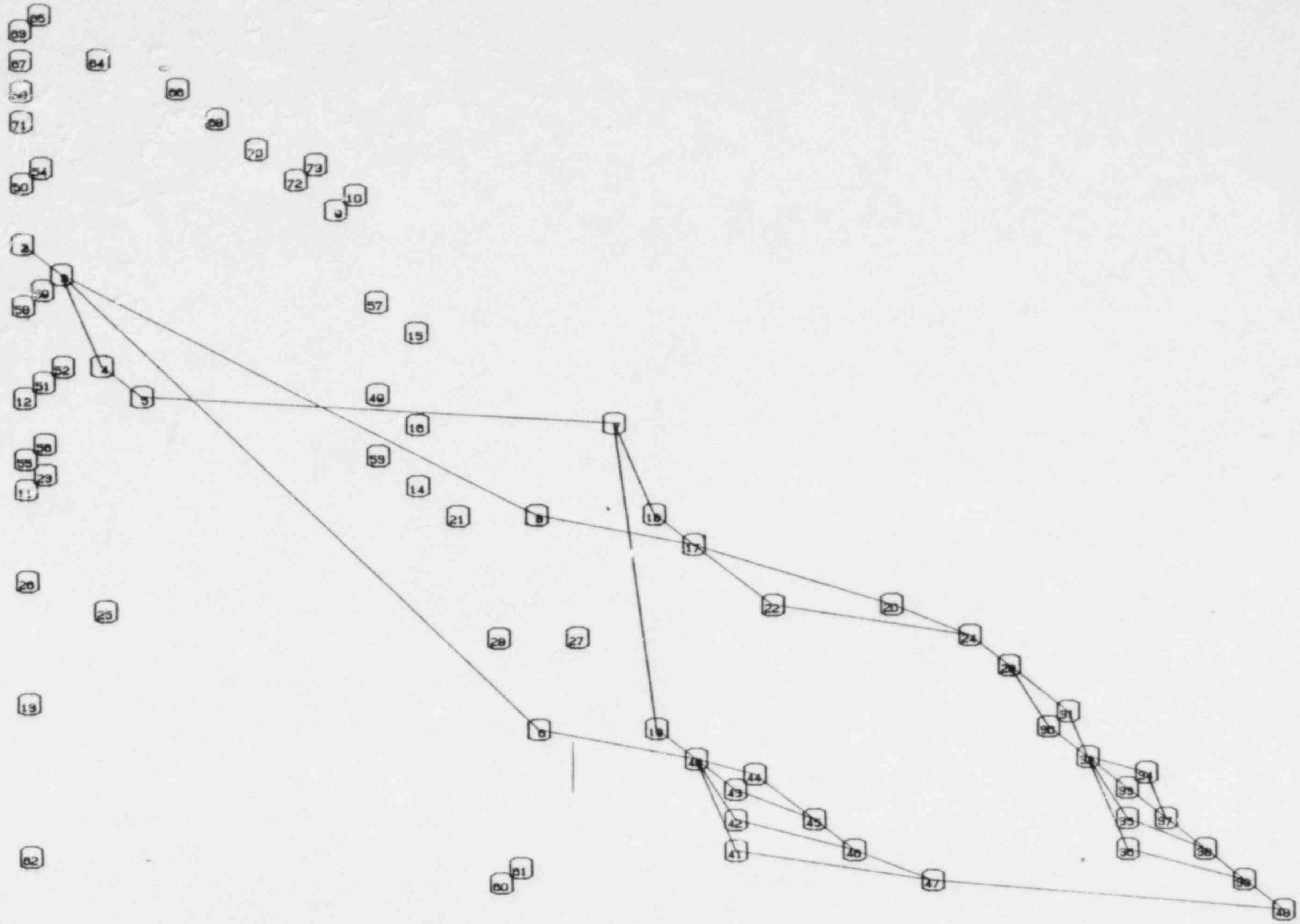


FIGURE 8. INDIAN POINT 3 --- RWST(2) TO RCS(48)

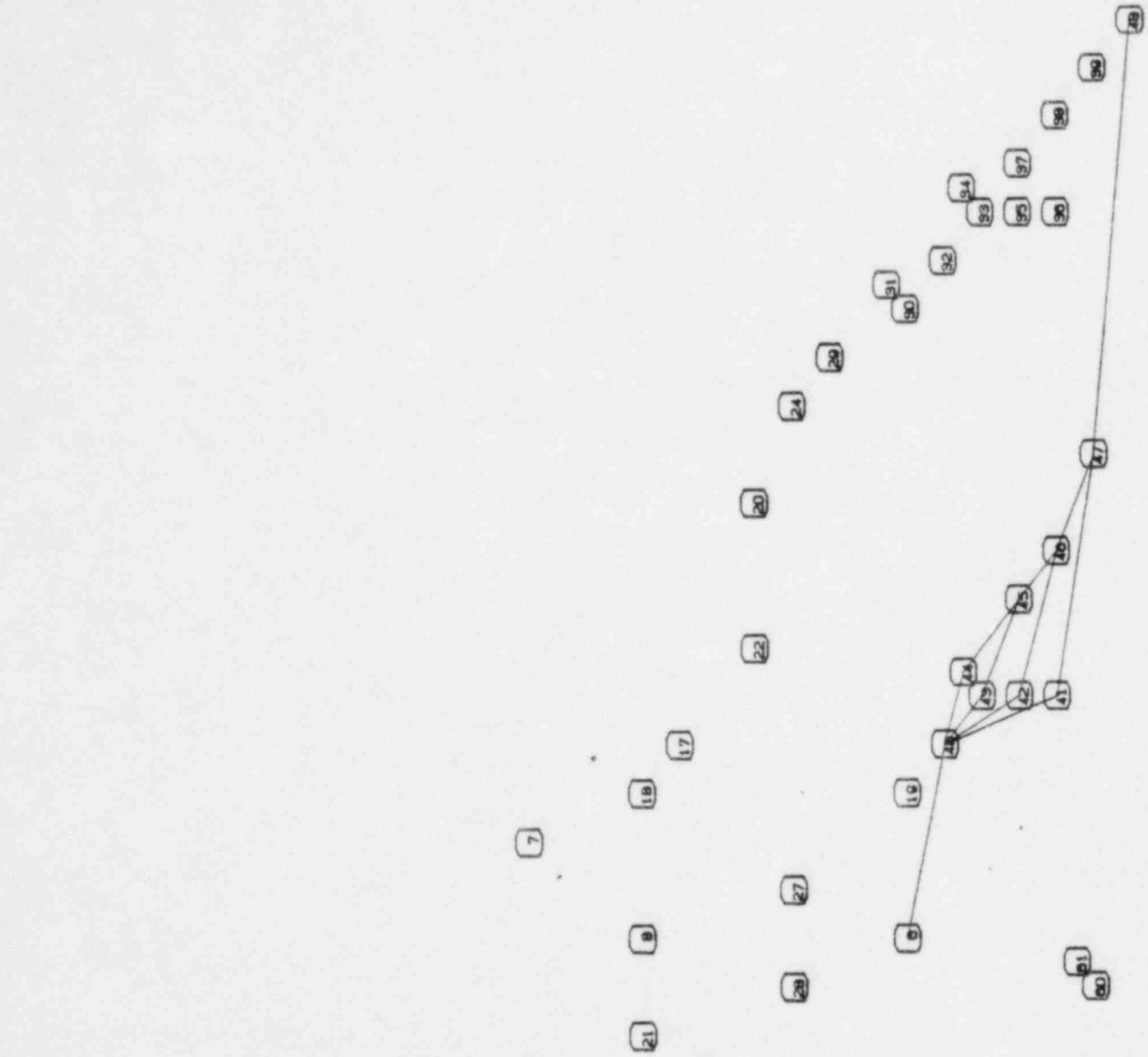


FIGURE 9. INDIAN POINT 3 —— SIP31(6) TO RCS(48)

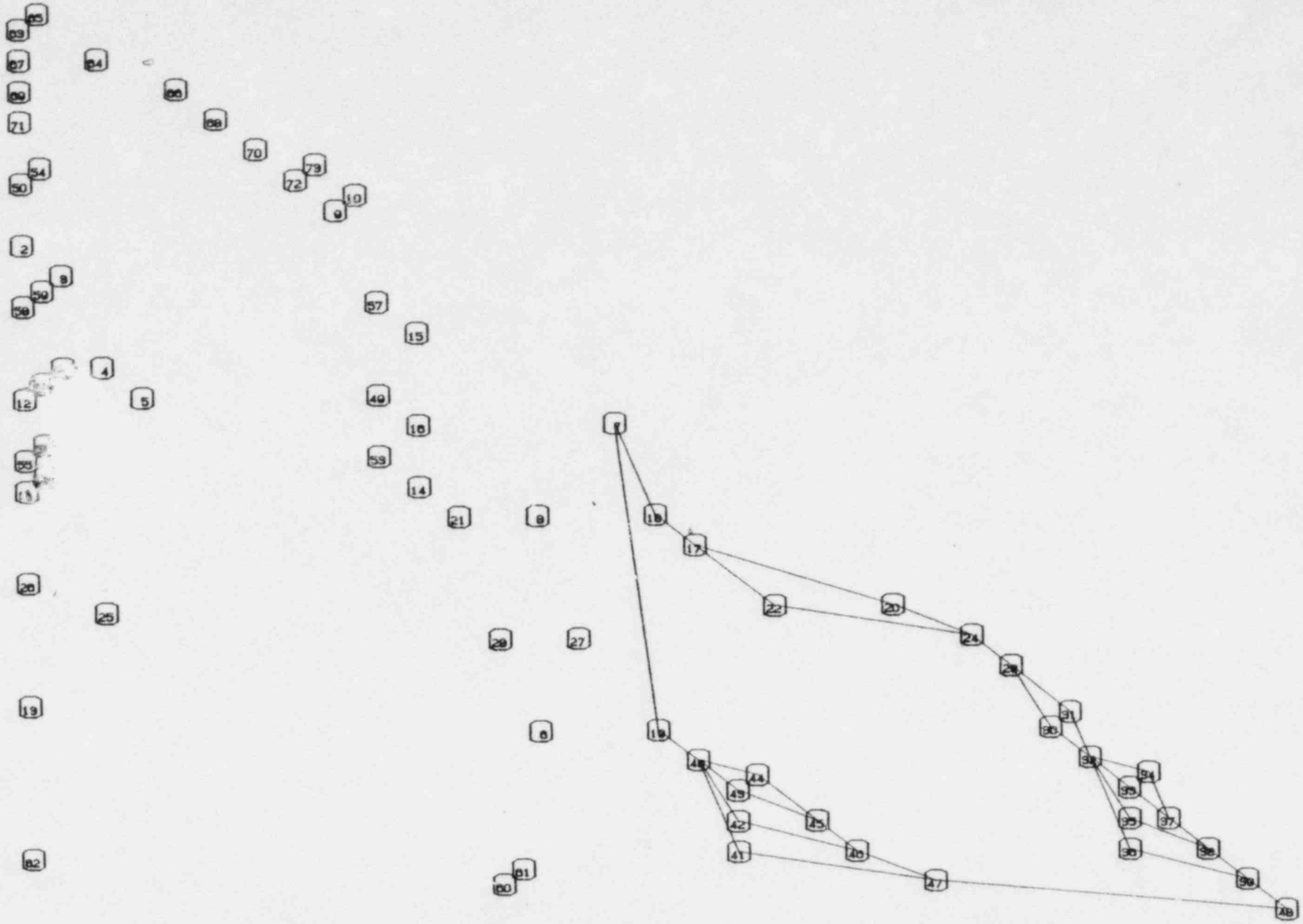


FIGURE 10. INDIAN POINT 3 --- SIP32(7) TO RCS(48)

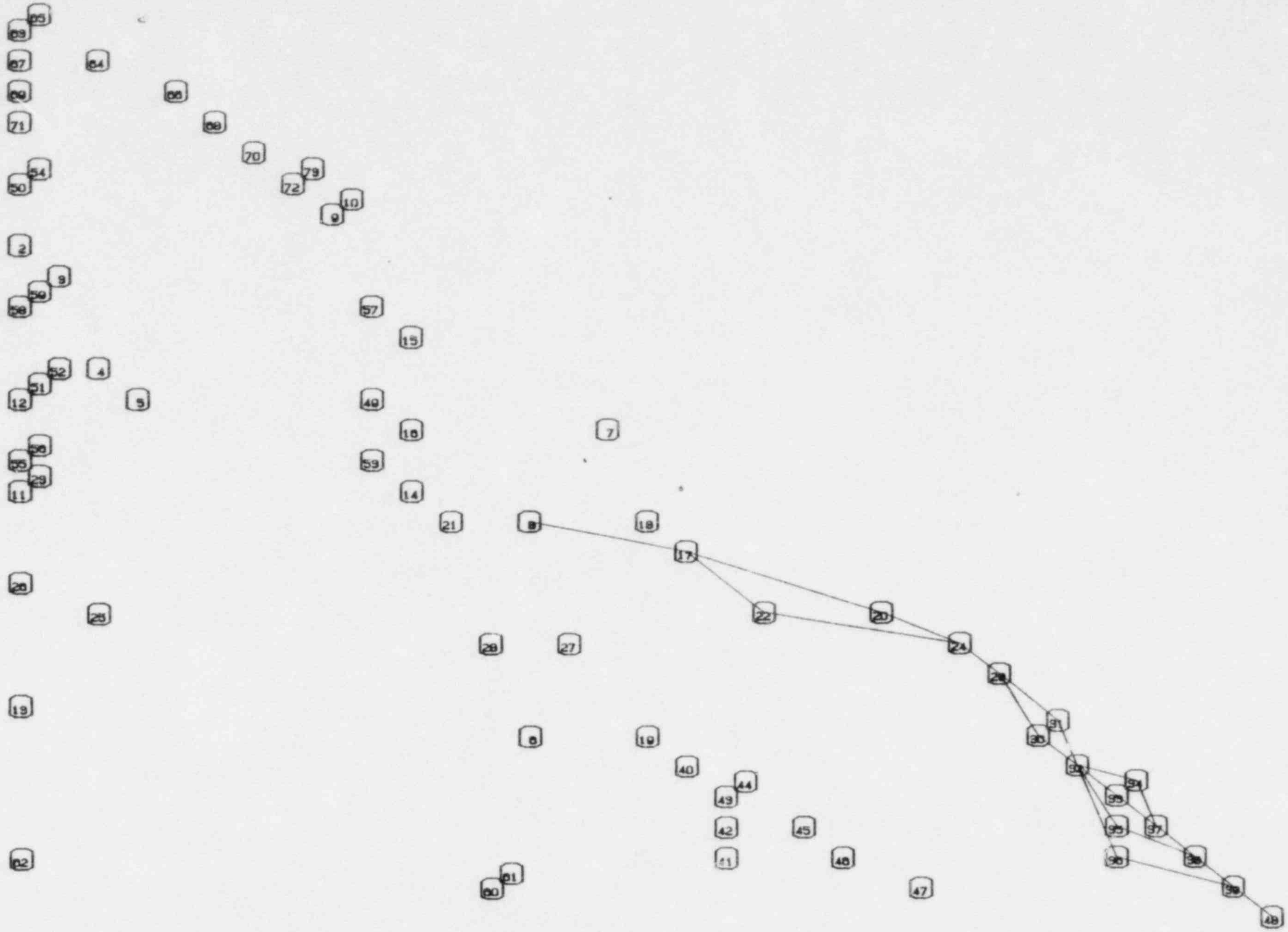


FIGURE 11. INDIAN POINT 3 --- SIP33(8) TO RCS(48)

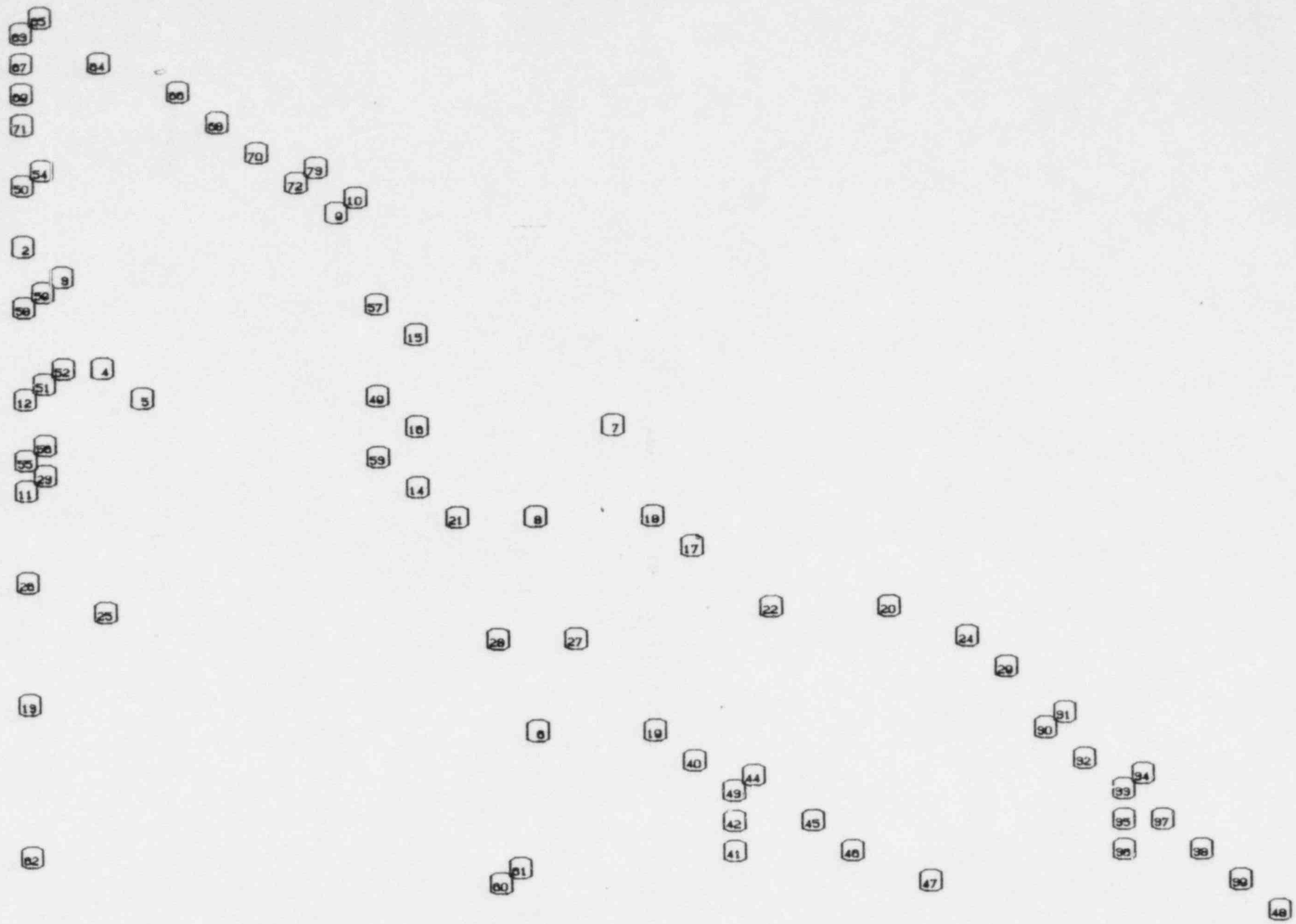


Figure 12. INDIAN POINT 3 --- BASIC COMPONENT POSITIONING

The first step of the computer processing is to produce the raw adjacency information. This information is developed from the inputs shown in Table 2 and presented in deconditioned matrix form in Table 4. The deconditioned matrix is the adjacency matrix where the representation of connections through AND gates has been removed. Reachability processing is then performed which yields the reachability matrix. The row and columns are then summed to yield the number of connections to and from each node. These values are used as the coordinates for the node layout. The upper left region of the map contains nodes with the highest numbers of connections leading from the nodes, while the lower right region contains nodes with the highest numbers of connections leading to the nodes. When two nodes have identical coordinates, one of the nodes is shifted to eliminate overlay.

The logic and physical layout of the system being modeled is generated by the computer using the algorithm described above. Notice that node 48 (reactor core) is the system sink and is at the lower right hand corner of the plot. This location indicates that the node is reachable from the most other nodes and it can reach no other node. The location of node 2 (source) (RWST) indicates it can reach the maximum number of other nodes and can be reached by no other node.

Figure 8 shows the path from the source of cooling water (RWST - node 2) to the sink, the RCS (node 48). Figures 9 through 11 show the paths from each safety injection pump to the RCS. Overlays A through J, intended for use with Figure 12, show similar maps for the diesel generators, power buses, motor control centers, and safety injection signal channels.

Finally, Tables 5 and 6 give the "connectivity" and "levels of dependency" measures specified by NRC. "Connectivity" is a measure of importance based on the degree of a node. The degree of a node is equal to the number of lines directed into the node (called indegree), plus the number of lines directed out of the node (called outdegree), plus the number of undirected lines to a node. If a node has n outdegree but zero indegree, it is a source node. If a node has n indegree, but zero outdegree, it is a sink node. A source node is a possible candidate as a common node or singleton cut-set. However, it is required that the logical relationship of the system be studied before a conclusion can be reached. For example, two source nodes may be required to fail simultaneously in order to fail a system. Thus the logical AND condition precludes our using "connectivity" as a measure for evaluation.

Table 4

Deconditioned Adjacency Matrix

1	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
2	0010000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
3	0001010100	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
4	0000100000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
5	0000001000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
6	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
7	0000000000	0000000110	0000000000	0000000000	0000000000	0000000000	0000000000	000
8	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
9	0000000000	0000000001	0000000001	0000000000	0000000000	0000000000	0000000000	000
10	0000000000	0000000000	0100000000	1000000000	0000000000	0000000000	0000000000	000
11	0000000100	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
12	0000001000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
13	0000010000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
14	0000000100	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
15	0000001000	0000000000	0000000000	0000000000	0000000000	0000000001	0000000000	000
16	0000010000	0000000000	1000000000	0000000000	0000000000	0000000000	0000000000	000
17	0000000000	0000000001	0100000000	0000000000	0000000000	0000000000	0000000000	000
18	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
19	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
20	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
21	0000000000	0000000001	0000000001	0000000000	0000000000	0000000000	0000000000	000
22	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
23	0000000000	0000000000	0100100000	1000000000	0000000000	0000000000	0000000000	000
24	0000000000	0000000000	0000000010	0000000000	0000000000	0000000000	0000000000	000
25	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
26	0000000000	0000000000	0000100000	0000000000	0000000000	0000000000	0000000000	000
27	0000000000	0000000000	0000000010	0000000000	0000000000	0000000000	0000000000	000
28	0000000000	0000000000	0000000010	0000000000	0000000000	0000000000	0000000000	000
29	0000000000	0000000000	0000000001	1000000000	0000000000	0000000000	0000000000	000
30	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
31	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
32	0000000000	0000000000	0000000000	0011110000	0000000000	0000000000	0000000000	000
33	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
34	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
35	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
36	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
37	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
38	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
39	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
40	0000000000	0000000000	0000000000	0000000000	1111000000	0000000000	0000000000	000
41	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
42	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
43	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
44	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
45	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
46	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
47	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
48	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
49	0000000000	0000010000	0000000000	0000000000	0000000000	0000000000	0000000000	000
50	0000000010	0000010000	0000000000	0000000000	0000000000	0000000000	0000000000	000
51	0000000000	0000010000	0000000000	0000000000	0000000000	0000000000	0000000000	000
52	0000000000	0000010000	0000000000	0000000000	0000000000	0000000000	0000000000	000
53	0000000000	0001000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
54	0000000001	0001000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
55	0000000000	0001000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
56	0000000000	0001000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
57	0000000000	0000100000	0000000000	0000000000	0000000000	0000000000	0000000000	000
58	0000000000	0000100000	0000000000	0000000000	0000000000	0000000000	0000000000	000
59	0000000000	0000100000	0000000000	0000000000	0000000000	0000000000	0000000000	000
60	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
61	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
62	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
63	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
64	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
65	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
66	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
67	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
68	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
69	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	011
70	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
71	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
72	0000000010	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000
73	0000000001	0000000000	0000000000	0000000000	0000000000	0000000000	0000000000	000

Table 5

Connectivity Measures: In and Out Degrees of Model Nodes

NODE	OUTDEGREE	INDEGREE
1	0	0
2	1	0
3	3	1
4	1	1
5	1	1
6	[illegible]	5
7	2	5
8	1	5
9	8	2
10	8	2
11	1	0
12	1	0
13	1	0
14	1	4
15	2	3
16	2	4
17	2	2
18	1	1
19	1	1
20	1	3
21	4	1
22	1	3
23	4	0
24	1	2
25	1	2
26	1	0
27	1	2
28	1	2
29	2	3
30	1	3
31	1	3
32	4	2
33	1	1
34	1	1
35	1	1
36	1	1
37	1	2
38	1	2
39	1	2
40	4	2
41	1	1
42	1	1
43	1	1
44	1	1
45	1	2
46	1	2
47	1	2
48	0	2
49	1	2
50	2	0
51	1	0
52	1	0
53	1	2
54	2	0
55	1	0
56	1	0
57	1	2
58	1	0
59	1	0
60	1	3
61	1	2
62	2	0
63	1	0
64	1	2
65	1	0
66	1	2
67	1	0
68	1	2
69	1	0
70	2	2
71	1	0
72	1	1
73	1	1

Table 6

Partial List of Paths
(Levels of Dependency)
from RWST (2) to RCS (48)

```
THE FOLLOWING PATH WAS FOUND

NODE=  48 L=   1
NODE=  47 L=   2
NODE=  46 L=   3
NODE=  42 L=   4
NODE=  40 L=   5
NODE=  19 L=   6
NODE=   7 L=   7
NODE=   5 L=   8
NODE=   4 L=   9
NODE=   3 L=  10
NODE=   2 L=  11
```

```
THE FOLLOWING PATH WAS FOUND

NODE=  48 L=   1
NODE=  47 L=   2
NODE=  46 L=   3
NODE=  45 L=   4
NODE=  43 L=   5
NODE=  40 L=   6
NODE=   6 L=   7
NODE=   3 L=   8
NODE=   2 L=   9
```

```
THE FOLLOWING PATH WAS FOUND

NODE=  48 L=   1
NODE=  47 L=   2
NODE=  46 L=   3
NODE=  45 L=   4
NODE=  43 L=   5
NODE=  40 L=   6
NODE=  19 L=   7
NODE=   7 L=   8
NODE=   5 L=   9
NODE=   4 L=  10
NODE=   3 L=  11
NODE=   2 L=  12
```

```
THE FOLLOWING PATH WAS FOUND

NODE=  48 L=   1
NODE=  47 L=   2
NODE=  41 L=   3
NODE=  40 L=   4
NODE=   6 L=   5
NODE=   3 L=   6
NODE=   2 L=   7
```

```
THE FOLLOWING PATH WAS FOUND

NODE=  48 L=   1
NODE=  47 L=   2
NODE=  41 L=   3
NODE=  40 L=   4
NODE=  19 L=   5
NODE=   7 L=   6
NODE=   5 L=   7
NODE=   4 L=   8
NODE=   3 L=   9
NODE=   2 L=  10
```

```
THE FOLLOWING PATH WAS FOUND

NODE=  48 L=   1
NODE=  47 L=   2
NODE=  46 L=   3
NODE=  42 L=   4
NODE=  40 L=   5
NODE=   6 L=   6
NODE=   3 L=   7
NODE=   2 L=   8
```

```
THE FOLLOWING PATH WAS FOUND

NODE=  48 L=   1
NODE=  47 L=   2
NODE=  46 L=   3
NODE=  45 L=   4
NODE=  44 L=   5
NODE=  40 L=   6
NODE=   6 L=   7
NODE=   3 L=   8
NODE=   2 L=   9
```

```
THE FOLLOWING PATH WAS FOUND

NODE=  48 L=   1
NODE=  47 L=   2
NODE=  46 L=   3
NODE=  45 L=   4
NODE=  44 L=   5
NODE=  40 L=   6
NODE=  19 L=   7
NODE=   7 L=   8
NODE=   5 L=   9
NODE=   4 L=  10
NODE=   3 L=  11
NODE=   2 L=  12
```

"Levels of dependency" is an NRC specified measure of path length between nodes. However, the relationship between path length and safety cannot be correlated without specified logic and consideration of the relative failure probabilities of components involved. Thus, this precludes our using "level of dependency" as an evaluation measure.

3.3 Discussion of Results

The "maps" (see Figures 8-12 and Overlays A-F), "connectivity" (see Table 5), and "levels of dependency" (see Table 6 for partial listing) which we found in the last section proved to be unsatisfactory for identification and evaluation of systems interactions for the systems considered in this study. They were not only as difficult to produce as standard risk assessment results (since they required detailed component level logic models as a starting point), but by excluding Boolean logic, correlation with safety was significantly reduced.

As a result, we attempted to retrieve some useful systems interaction information from the component-level logic representations modeled in Figures 2-7. By using a Digraph Matrix Analysis path-set Boolean reduction computer code, we found all the singleton and doubleton cut-sets of the safety injection system and its support systems as modeled. The results of this subsequent effort are given in Table 7.

Singletons identified in this analysis included the RWST (the ultimate source of safety injection flow), motor operated valve V1810 (the common valve for suction to all three safety injection pumps under normal alignment), and the RCS itself.

Doubletons are displayed in the matrix included in Table 7. Components involved in this matrix include Headers 1, 2, 3 and 4 (Nodes 32, 40, 24 and 17), safety injection signals 1 and 2 (Nodes 9 and 10), Heat Trace (Node 27), electric heat for the boron injection tank (Node 28), the boron injection tank (Node 29), DC power systems 31 and 32 (nodes 50 and 54), and Safety Injection logic channels 1 and 2 (Nodes 72 and 73).

Table 7

Doubleton Matrix and

List of Singletons

	9	10	17	24	27	28	29	32	40	50	54	72	73
9	-	*	-	-	-	-	-	-	-	-	*	-	*
10	*	-	-	-	-	-	-	-	-	*	-	*	-
17	-	-	-	-	-	-	-	-	*	-	-	-	-
24	-	-	-	-	-	-	-	-	*	-	-	-	-
27	-	-	-	-	-	-	-	-	*	-	-	-	-
28	-	-	-	-	-	-	-	-	*	-	-	-	-
29	-	-	-	-	-	-	-	-	*	-	-	-	-
32	-	-	-	-	-	-	-	-	*	-	-	-	-
40	-	-	*	*	*	*	*	*	-	-	-	-	-
50	-	*	-	-	-	-	-	-	-	-	*	-	*
54	*	-	-	-	-	-	-	-	-	*	-	*	-
72	-	*	-	-	-	-	-	-	-	-	*	-	*
73	*	-	-	-	-	-	-	-	-	*	-	*	-

```
***UNSUPPRESSED SINGLETONS***
        2      RWST
        3      V1810
       48      RCS
```

4.0 Conclusions

Lawrence Livermore National Laboratory (LLNL) has been working to develop an interconnected systems interaction audit procedure subject to the following NRC constraints:

1. Boolean logic is excluded from the modeling effort (but may be used for computer code processing).
2. A "map" of the plant at the subsystem, or train, level of detail is to be constructed.
3. Heuristic measures, specified by the NRC, called "connectivity" (degree of a node) and "levels of dependency" (paths between any node and all others) are to be used to draw statistical correlation between the "map" and the potential for systems interaction in the systems involved.

The motivations for this effort were the possible advantages to be found from (1) simpler analyst knowledge and training required, and (2) simpler and less costly effort involved in auditing utility submittals.

In this preliminary systems interaction investigation of the IP-3 safety injection system, and its component cooling, actuation and electrical connections, we found the specific IP-3 safety injection system design to be particularly difficult to represent in a model subject to the NRC constraints. It contained numerous common pipe-headers and common "passive" components within and between trains. In addition, the numerous plant modes and configurations under differing accident conditions compounded the modeling problems. We were unable to strictly adhere to the NRC constraints. In order to identify which components were necessary for successful operation of individual trains it was necessary to form detailed component level representations of the entire system. This violated constraint 2. In addition, we attempted to apply numerous constraints on the system model such as limiting it to a small LOCA during loss of offsite power for just the injection phase. This was done in an attempt to avoid explicit Boolean logic. Despite this, the component-level representation required some specific AND conditions in order to capture "dependency" information. This violated constraint 1. After a component-level logical representation of the safety injection and related systems was completed, however, we attempted to construct a safety injection system "map" (at the component level) and find its "connectivity" and "level of dependency" measures. The "map" became essentially our original component-level logical representation with the

AND and OR logic conditions excluded. However, by excluding Boolean logic, the "connectivity" and "levels of dependency" measures suffer a significant reduction in their ability to provide statistical correlation with safety. Therefore, for the systems considered in this study, we found the specified measures to be inadequate. We, therefore, failed constraint 3.

As a result, we found the "map" and NRC measures to be an unsuccessful approach based on the following criteria: (a) they required as much detailed study, training, effort and cost as comparable risk assessment study, and (b) the evaluation measures were less informative than a comparable risk assessment result.

It should be noted, however, that the component-level logical representations we constructed (not very different from directed logic diagrams used in Digraph-Matrix Analysis (DMA) or, for that matter, from conventional fault trees) still contained the essential modeling information. From these representations, we were able to extract singleton and doubleton cut-sets for the safety injection system and support systems. These results directly address the systems interaction problem.

In conclusion, we make the following recommendations:

(a) further efforts to use contraints excluding Boolean logic from the modeling process and utilizing heuristic measures should be discontinued at Lawrence Livermore National Laboratory, and

(b) the PASNY Indian Point-3 interconnected systems interaction study should be audited by an independent LLNL effort using Digraph-Matrix Analysis (or comparable risk assessment techniques) to find common mode failures.

REFERENCES

1. G. Boyd, et al., Sandia National Laboratories, "Final Report, Phase I, Systems Interaction Methodology Applications Program," U.S. Nuclear Regulatory Commission Report NUREG/CR-1321 (SAND80-0884), April 1980.

2. G.E. Cummings, "Operator/Instrument Interactions During the Three Mile Island Incident," IEEE Symp. Nucl. Power Sys., October 19, 1979.

3. 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.

4. C. Michelson, OAEOD, memorandum to H.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.

5. 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).

6. U.S. Nuclear Regulatory Commission, "Transient Response of Babcock & Wilcox - Designed Reactors," U.S. Nuclear Regulatory Commission Report NUREG-0667, May 1980.

7. Nuclear Safety Analysis Center and Institute of Nuclear Power Operations, "Analysis and Evaluation of Crystal River Unit 3 Incident," Joint NSAC/INPO Report NSAC-3/INPO-1, March 1980.

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

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

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

11. U.S. Nuclear Regulatory Commission, "Interim Reliability Evaluation Program, Phase II, Procedure and Schedule Guide," Draft 2, September 9, 1980.

12. Pacific Gas & Electric Co., "Description of the Systems Interaction Program for Seismically-Induced Events, Diablo Canyon Units 1 and 2, U.S. Nuclear Regulatory Commission Report NUREG 0695, October 1980.

13. Power Authority of the State of New York, <u>Systems Interaction Study</u>, December 1981, Vol. I and II.

References (Cont.)

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

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

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

17. H.P. Alesso and H.J. Benson, "Fault Tree and Reliability Relationships for Analyzing Noncoherent Two-State Systems," Nuclear Engineering and Design, Vol. 56, pp. 309-320, 1980.

18. H.P. Alesso, I.J. Sacks, and C.F. Smith, Initial Guidance on Digraph Matrix Analysis for Systems Interaction Studies at Selected LWR's, Lawrence Livermore National Laboratory UCID 19457, October 1982.

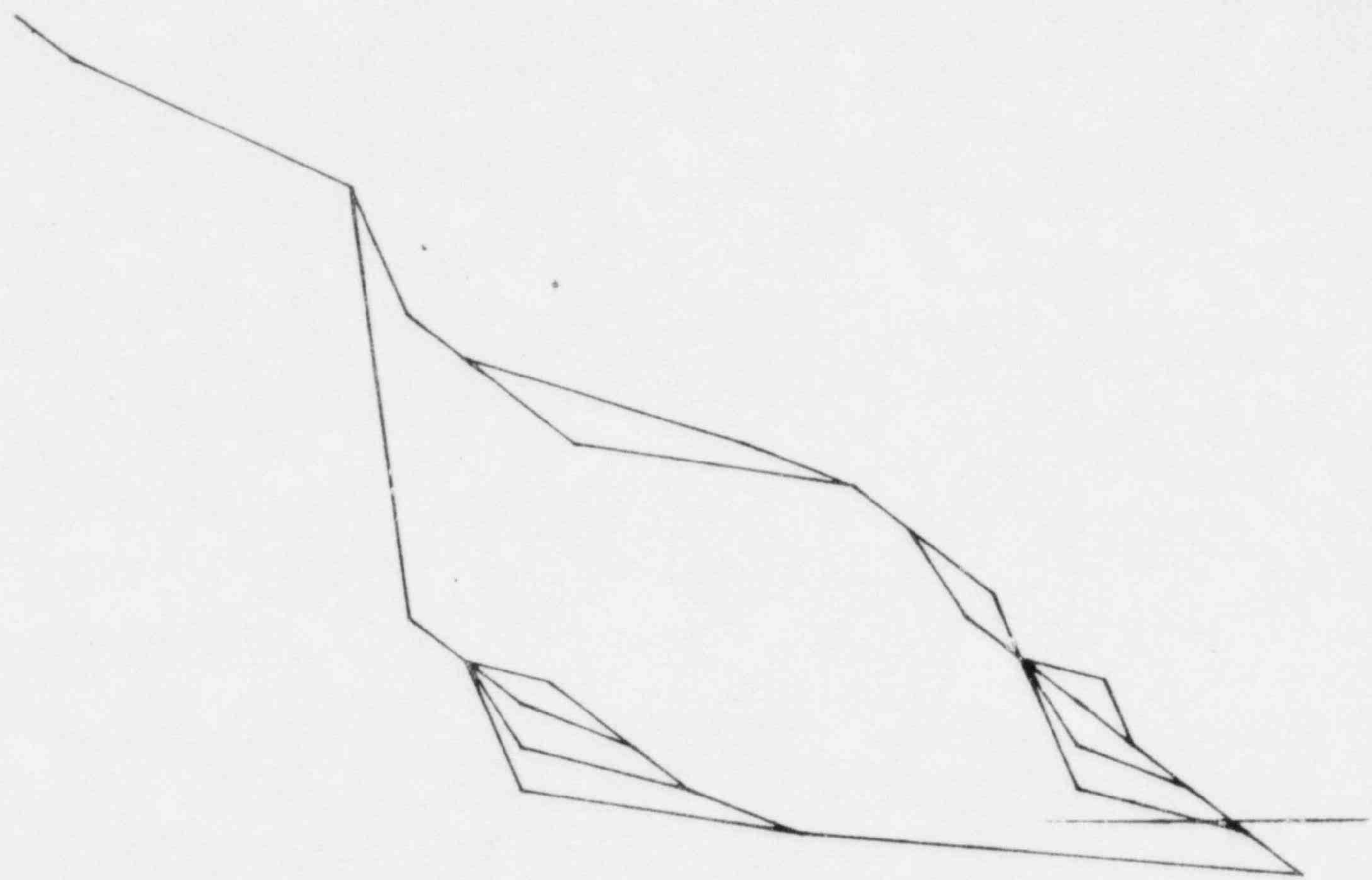
19. U.S. Nuclear Regulatory Commission, "Reactor Safety Study," WASH-1400 (NUREG-75/014), October 1975.

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

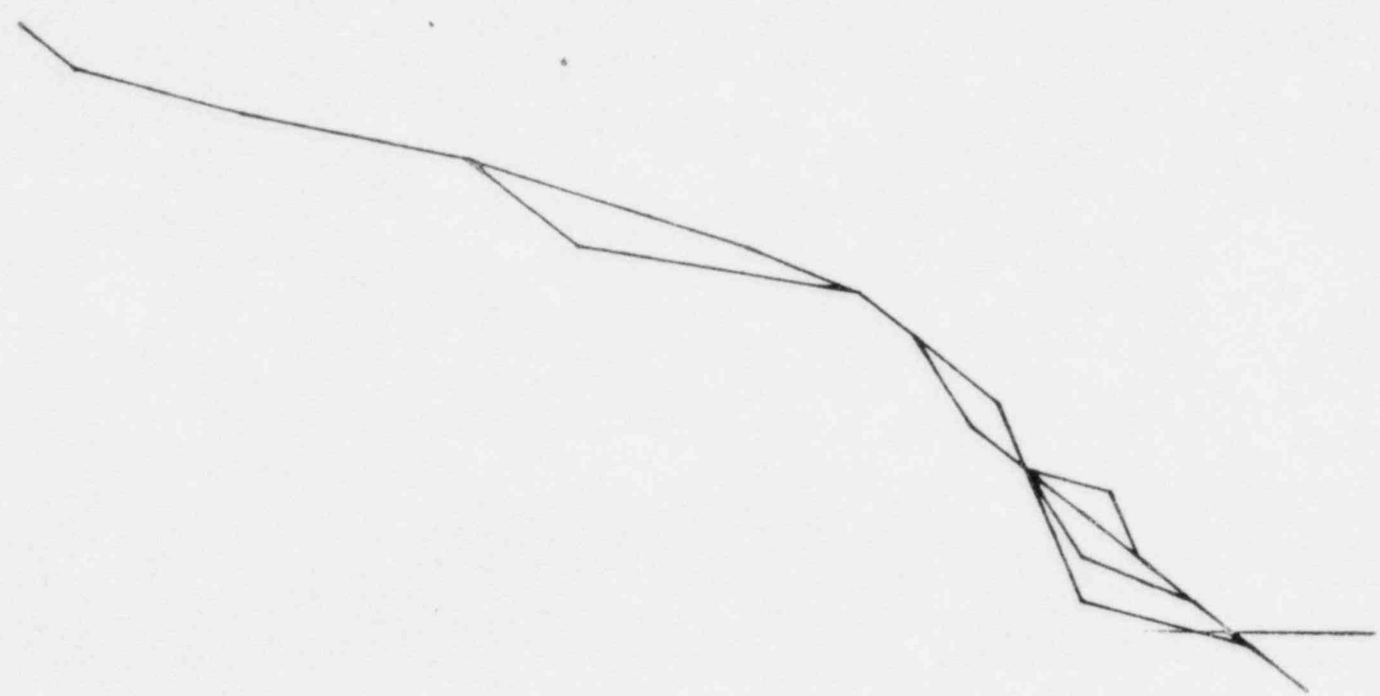
21. Power Authority of the State of New York, Final Safety Analysis Report Indian Point-3, Rev. 0, 7/82, Docket No. 50-286.

22. Power Authority of the State of New York, Piping and Instrumentation Diagrams, 1982.

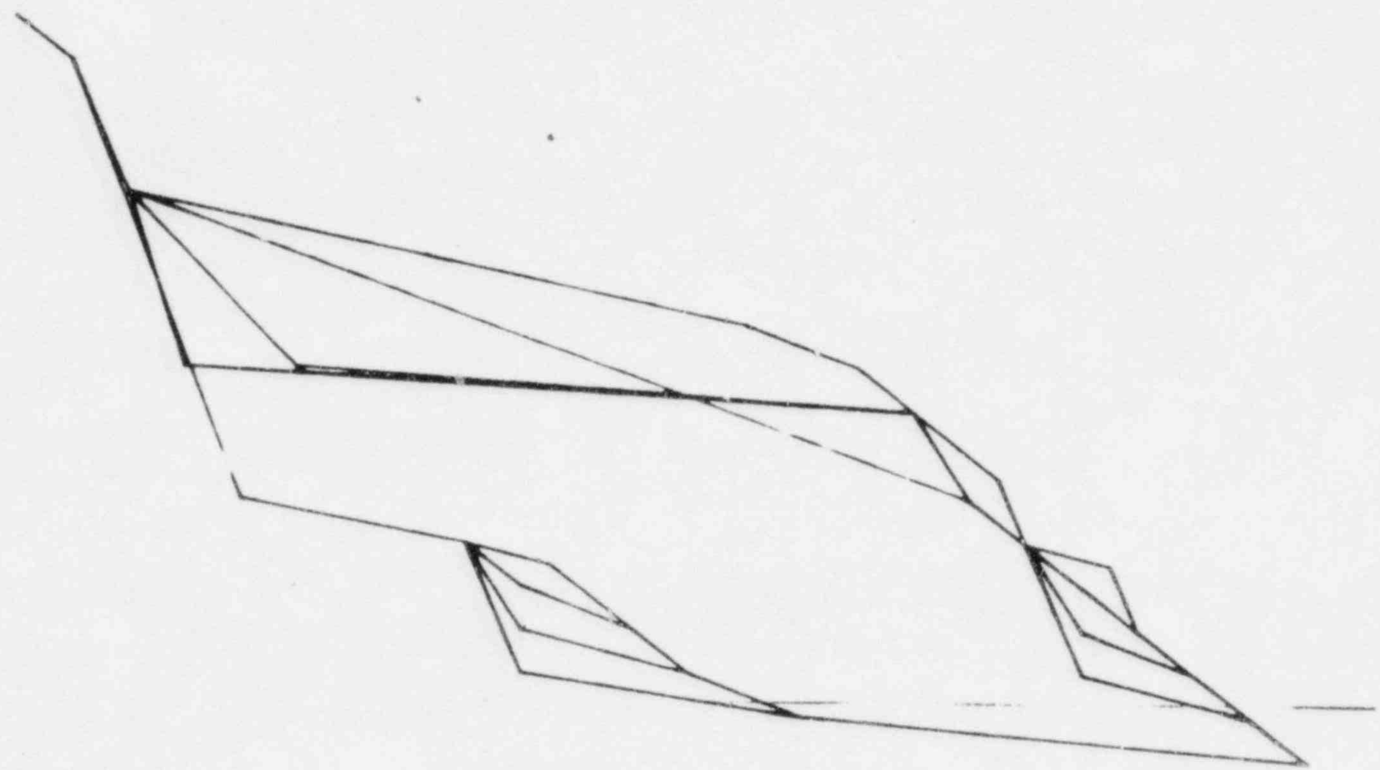
23. Power Authority of the State of New York, Indian Point Probabilistic Safety Study, 1982.



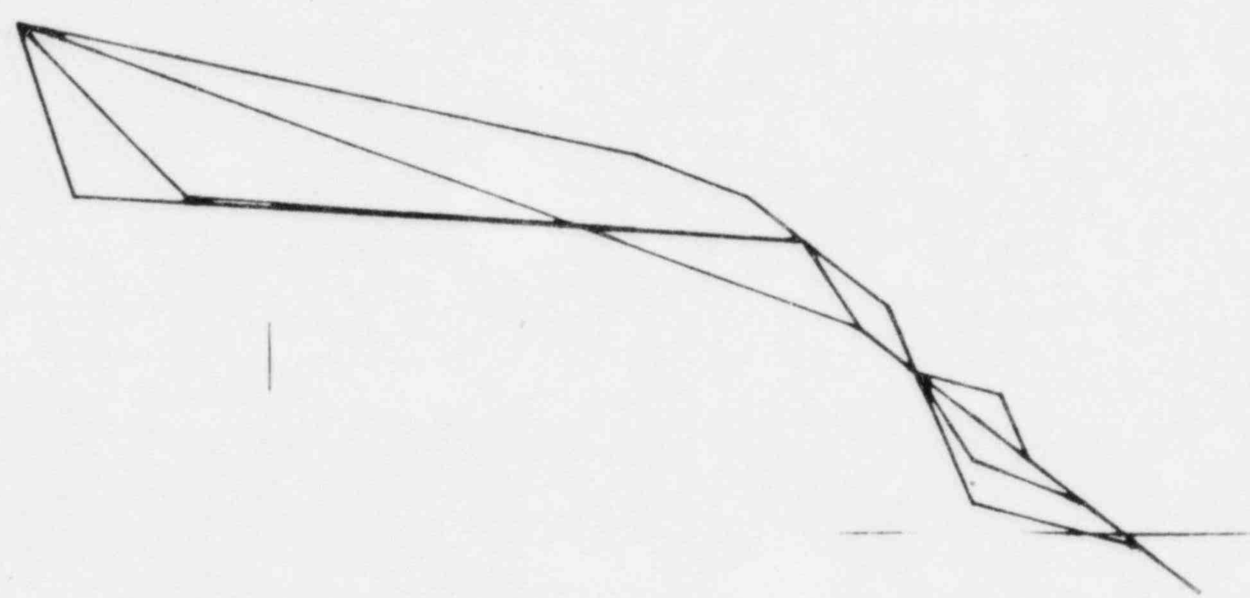
OVERLAY A --- DG31(57) TO RCS(48)



OVERLAY B --- OG32(53) TO RCS(48)

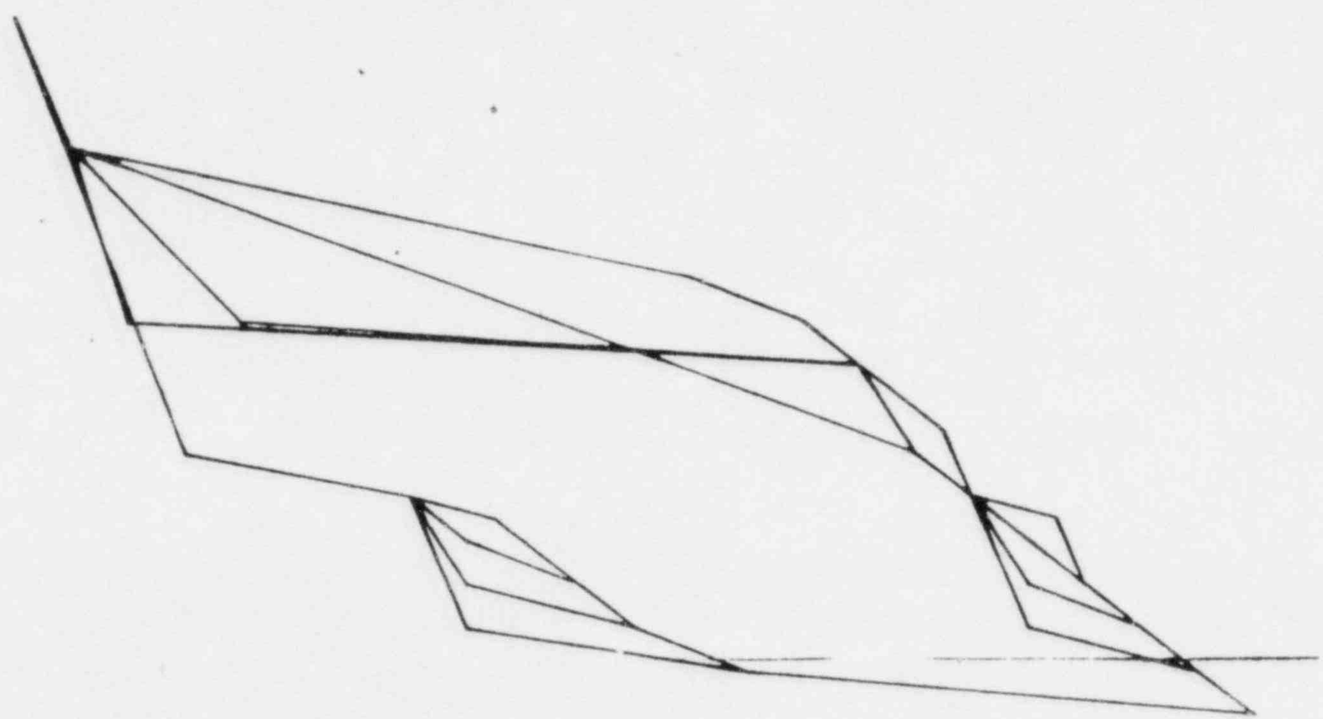


OVERLAY C --- DG33(48) TO RCS(48)



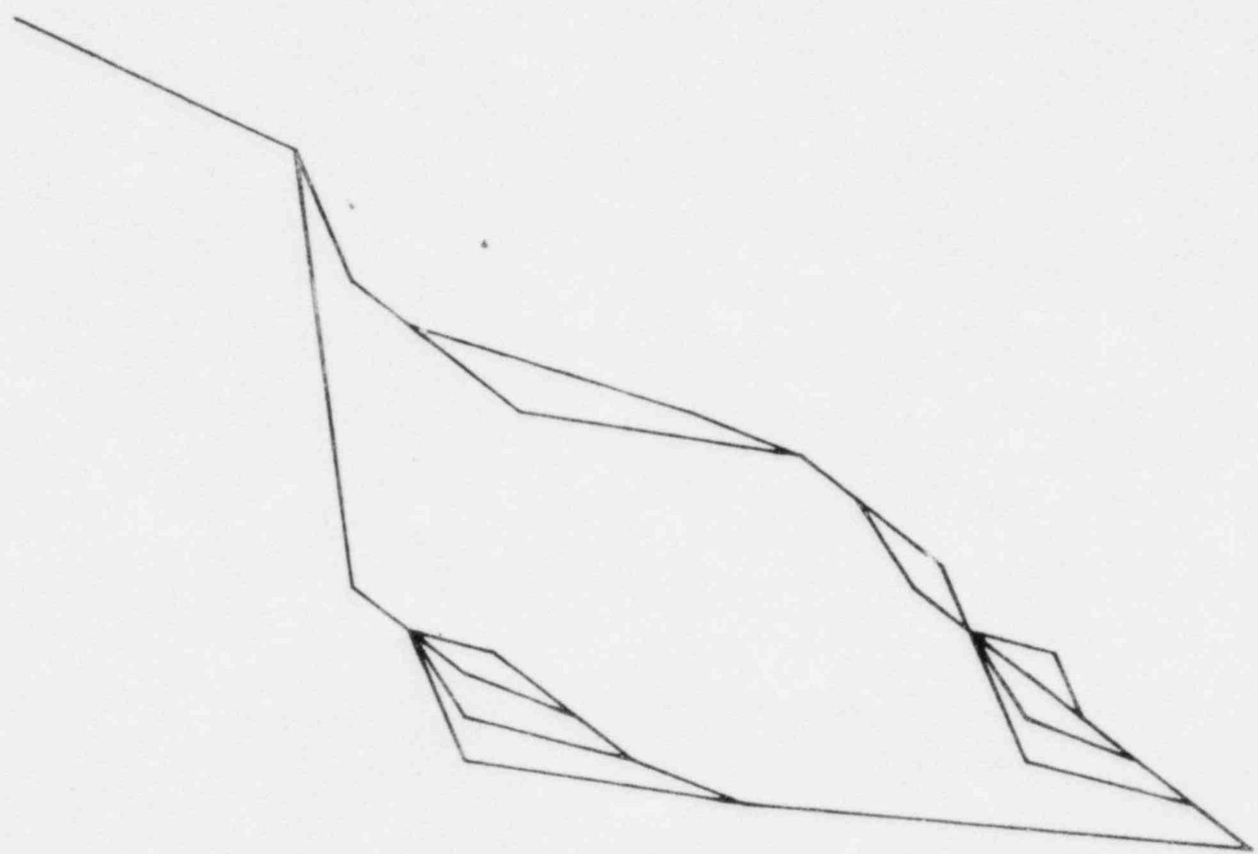
OVERLAY D --- MCC3BA(21) TO RCS(48)

OVERLAY E --- MCC398(23) TO RCS(48)

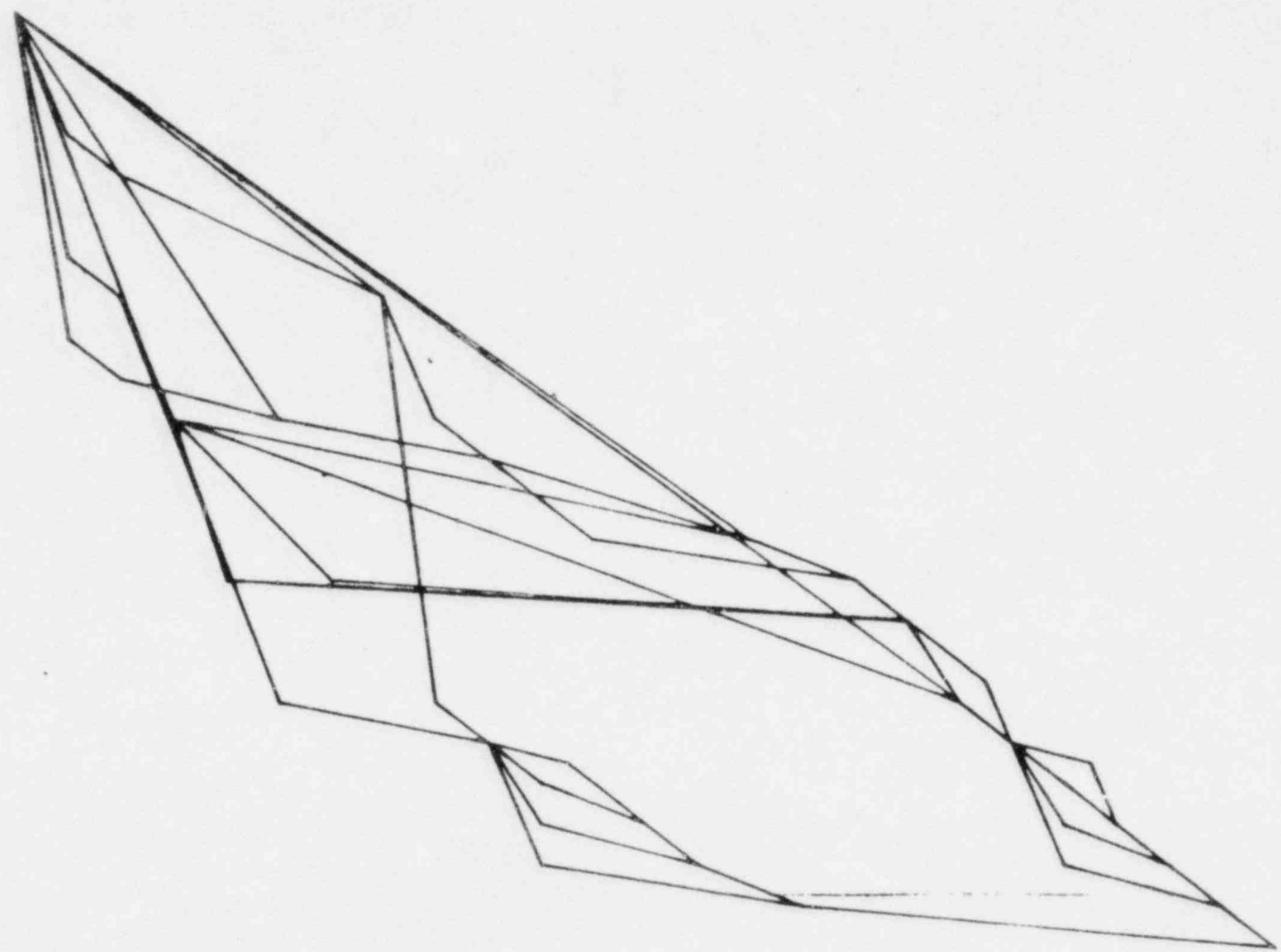


OVERLAY F --- EPSA(16) TO RCS(48)

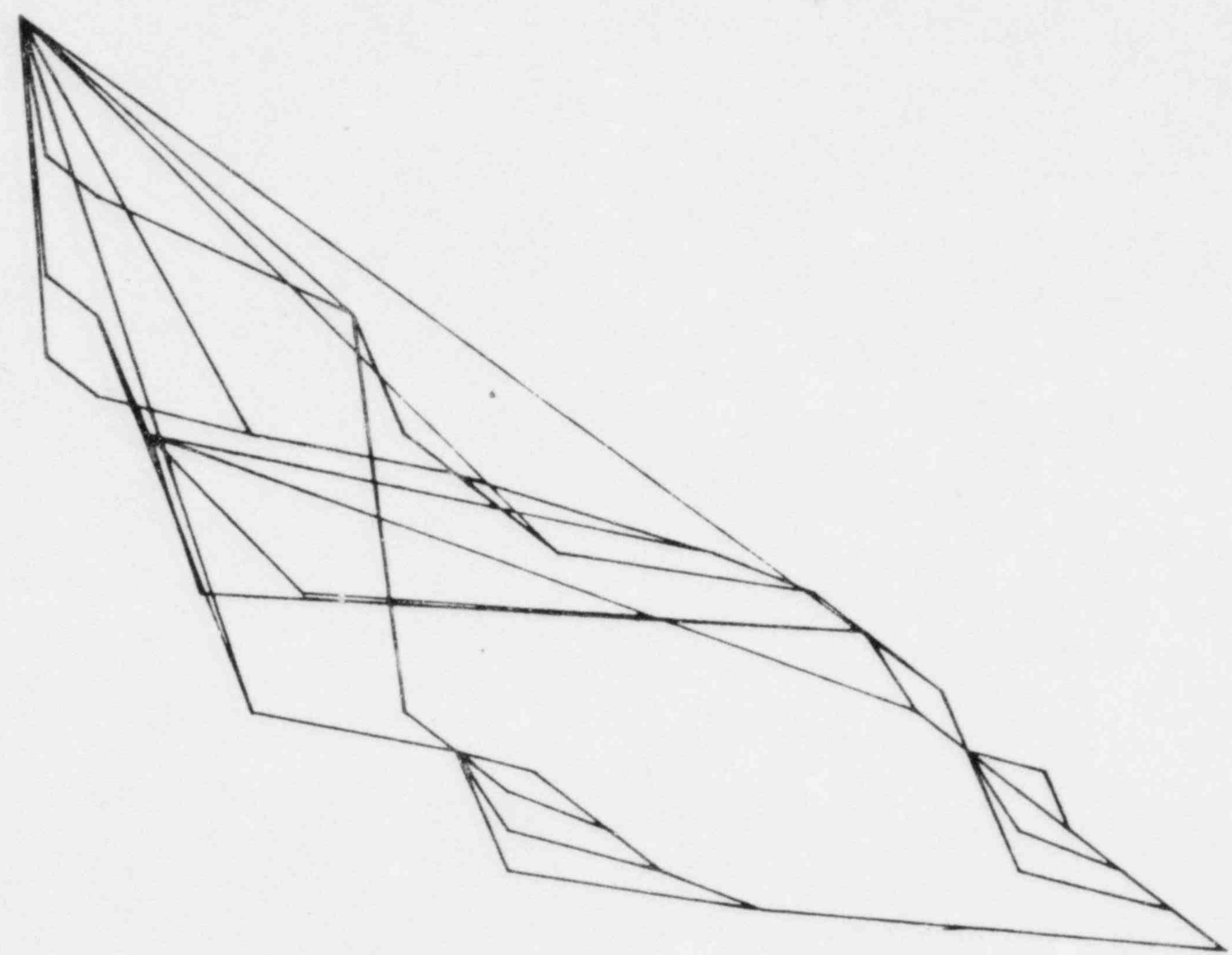
OVERLAY G --- EPBA(14) TO RCS(48)



OVERLAY H --- EP2A(15) TO RCS(48)



OVERLAY I --- SISIG1(8) TO RCS(48)



OVERLAY J --- SISIG2(10) TO RCS(48)