NUREG/CR-1896
BMI-2073

Review of Systems Interaction Methodologies

Prepared by P. Cybulskis, R. S. Denning, R. Gallucci,
P. Pelto, A. M. Plummer, R. D. Widrig

Battelle Columbus Laboratories

Prepared for
U.S. Nuclear Regulatory
Commission

Available from

GPO Sales Program
Division of Technical Information and Document Control
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Printed copy price: $5.50

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-1896
BMI-2073

Review of Systems Interaction Methodologies

Manuscript Completed: December 1980
Date Published: January 1981

Prepared by
P. Cybulskis, R. S. Denning, R. Gallucci,
P. Pelto, A. M. Plummer, R. D. Widrig

Battelle Columbus Laboratories
505 King Avenue
Columbus, OH 43201

Prepared for
Division of Systems Integration
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN B2335

ABSTRACT

The results of a study of methodologies with possible applications to systems interaction analysis are presented. A definition of systems interaction is developed and various methodologies and their applicability to systems interaction analysis are discussed and compared. The recommended approach is based on the concept of principal safety functions and employs logic models to identify and evaluate systems interactions candidates. The approach is applied to actual operating incidents to demonstrate its capabilities.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

The Systems Interaction Branch of the NRC's Office of Nuclear Reactor Regulation has among its responsibilities the consideration of the potential effects of systems interactions in the review of reactor license applications. This is a new thrust for the NRC which derives from the several analyses of the TMI incident and the development of the NRC Action Plan (NUREG-0660). As a means of fulfilling this responsibility the development of an independent methodology for identifying and evaluating systems interactions is being considered. Such a methodology would have two broad applications:

a) it would define the information requirements, procedures, and criteria that could be used by the applicant in the development and review of the plant design, and
b) it would provide the framework for the NRC review of the plant design for systems interaction considerations.

At the present time there are no regulatory guidelines and requirements for systems interaction evaluations for nuclear power plants, except within the narrow context of potential common cause effects noted in 10CFR50, Appendix A, General Design Criteria, 2, 23, and 24. Further, it is not clear that a concensus definition of systems interaction is available at this time, much less an agreement on applicable methodologies. It is the objective of the initial effort described here to review applicable methodologies that may have potential for relatively near-term use in systems interaction evaluations. The work described here was undertaken by Battelle's Columbus Laboratories and Pacific Northwest Laboratories. Parallel efforts are being performed by two other organizations.

The broad objective of this project is to develop methods that hold the best potential for further development and near-term use by industry and NRC on systems interaction evaluations for future as well as operating plants. More specifically, the objectives of the work described here include:

a) development of a definition of systems interaction and corresponding safety failure criteria,
b) review and assessment of current systematic methods that have been used, or considered feasible for use, on any complex system comparable to a light water reactor plant,

c) provision of an inventory of a range of systems interaction scenarios with emphasis on actual operating experience to:
   (1) better focus on the definition of systems interaction, and
   (2) serve as a basis for evaluating the ability of the various methodologies to predict these examples, and

d) recommendation of a methodology or alternatives that have the best potential for further development and near-term use by industry and the NRC on systems interaction evaluations.

e) application of candidate methodologies to actual occurrences to demonstrate their ability to predict systems interactions' effects.

The effort undertaken under this task should provide the basis for follow-on studies; the latter may include application of the recommended methodologies to selected cases as well as further methodology development.

DEFINITION OF SYSTEMS INTERACTION

Before attempting to derive a definition of systems interaction it is useful to consider a number of concepts. For the present purposes, a "system" is a collection of components which perform some function; generally the function defines the system. One component is not a system. Several systems can support a single function. Clearly, systems are designed to interact with each other in various ways. Most of these interactions are intentional and well recognized. The concern is with a limited set of potential interactions. In the present context an "interaction" of concern results when the conditions in one system affect (degrade) the ability of another system to perform its safety function. It should be recognized that such "interactions" need not necessarily imply or require failure in the normal sense of the affected system, e.g., a system may be misled by faulty instrumentation or actuation signals. Since the operator, used here in a very broad sense, can have an impact on the availability of any and all safety as well as supporting systems in the plant, it is imperative that his role be properly recognized. The operator may be considered as a component or a subsystem that can impact on the other systems in the plant.

As was noted earlier the definition of systems interaction includes consideration of some safety failure criterion. The failure criterion selected must recognize potential as well as actual hazard or risk that may result from the systems interaction. The Crystal River incident, for example, did not release any radioactivity to the environment, though it clearly represents a situation of interest from the systems interaction viewpoint. The inclusion of potential hazard or risk in systems interaction consideration, while deemed necessary, has the potential of substantially broadening the scope of this effort. In order to focus the systems interaction considerations it will be useful to consider the concept of safety functions. The use of this concept is not unique to this study. The present discussion draws heavily on the work of Reference (1). This concept provides a certain hierarchy of plant protection and a systematic approach to mitigating the consequences of an

upset event. A safety function may be defined as a group of actions that maintain the defense-in-depth concept and minimize the potential of radioactivity release to the environment. Ten basic safety functions can be defined which are required to maintain the desired level of protection to the public. These basic safety functions and their specific purposes are given below.

Safety Function	Purpose
Reactor Control	Maintain desired power level and shutdown reactor when required.
Reactor Coolant System Inventory Control	Maintain a suitable coolant medium around the core.
Reactor Coolant System Pressure Control	Maintain the coolant in the proper state.
Core Heat Removal	Transfer heat from the core to the coolant.
Reactor Coolant System Heat Removal	Remove heat from the primary system.
Containment Isolation	Maintain containment integrity to prevent radiation releases.
Containment Temperature and Pressure Control	Avoid potential damage to containment and vital equipment.
Combustible Gas Control	Remove and/or redistribute hydrogen to avoid potentially damaging reactions.
Maintenance of Vital Auxiliaries	Maintain operability of systems needed to support safety systems.
Indirect Radioactivity Release Control	Contain miscellaneous stored radioactivity to protect the public and the environment.

The safety functions and their respective purposes as they are given above are quite straightforward and a detailed discussion of each is not deemed necessary here. However, some discussion of the intent of defining these functions may be appropriate. In the application of the safety function concept it will be necessary to define all the systems (and perhaps ultimately all the components) that are required to perform each of these functions. It will be essential that all the required systems are in fact identified, e.g., the maintenance of reactor coolant inventory in an operating PWR requires not only the charging pumps with a supply of water, but also motive power, instrument power, cooling and lubrication, as well as environmental control for these systems. While this systems identification may be reasonably straightforward for some of the functions, it could get quite complicated in such areas as the maintenance of vital auxiliaries. The latter, however, could be a principal source of difficult-to-recognize systems interdependencies. The safety functions as defined above would apply to reactors in general, i.e., all plants must perform these basic safety functions. However, the specific systems and components used to achieve these functions can be quite different from plant to plant. While these safety functions are general enough to apply to all modes of reactor operation, the nature of a function as well as the function priority will clearly change with the operating mode. For example, reactor coolant system pressure control is an essential function during power operation whereas during refueling it is not required. Reactor coolant system heat removal is required at all times, but the means used to achieve this function will vary. During power operation it is accomplished by means of the power conversion system; during shutdown but with the system at elevated pressure and temperature the power conversion system and/or the high pressure recirculation may be used. With the system at low temperature and pressure, however, only the low pressure residual heat removal system may be available. The plant operating modes of interest include: startup, power operation, hot standby, hot shutdown, cold shutdown, and refueling.

Given the foregoing discussion of systems, interactions, and safety functions we can pose a definition of systems interaction as it will be used in the subsequent discussion:

> Systems Interaction (SI) - a system failure combination that can reduce the effectiveness of any one of a number of basic safety functions.

A key aspect of the above definition is "system failure combination". Within the present context multiple independent hardware failures do not constitute systems interactions, neither does a single external event that fails multiple systems.

Nuclear power plants are designed and operated such that there are normally several ways that can be used to achieve any given safety function, i.e., for each safety function there are typically several possible success paths. This is an essential ingredient of the defense-in-depth approach to reactor safety. The defense-in-depth is achieved through the use of such design approaches as redundancy, coincidence, functional diversity, independence, physical separation, quality assurance and testing. If it were not for such approaches, the potential for systems interaction would not exist. In that case, the reliability of the system would be governed by single failures. The potential for systems interaction (and also common mode/common cause failure) is the result of the complexity of the system. If executed properly this complexity leads to a level of safety function reliability much higher than can be achieved in a simple system. If the potential pitfalls of this complexity (such as systems interaction) are not recognized and properly addressed, the desired gains in reliability may not be achieved.

A key aspect of any reliability assessment and one of particular importance to the problem at hand is the question of system and/or component independence. As is well recognized, reliability assessments based on the assumption of independent failures lead to optimistic predictions of system reliability. Certain types of dependencies among systems and/or components are fairly readily recognized; among these may be such items as common location, power supply, actuation, etc. These have received much attention in the recent past in the context of common mode/common cause failures. Certain other types of dependencies are much more difficult to recognize and evaluate; among the latter are the extremely broad area of human factors and subtle dependencies in functionally widely separated systems. These are the areas of primary concern from the systems interaction viewpoint. In a sense, systems interaction analysis can be considered as a search for hidden dependencies.

DESIRABLE SYSTEMS INTERACTION METHODOLOGY ATTRIBUTES

The recognition of the need to consider the potential effects of systems interaction reflects a desire to identify hazards that otherwise would be missed or to highlight "everything that we forgot". In this light the best hope for a successful approach for the identification and evaluation of systems interactions would appear to be the development of a formal methodology for this purpose. Broadly speaking such a methodology should have the following attributes: systematic, complete, flexible, reproducible, simple, and visible or scrutable. These desired attributes are discussed below.

The methodology is "systematic" if it follows a clearly defined sequence of analysis. A "complete" methodology would cover all the significant areas within its range of applicability. "Flexibility" is the ability to adapt to elements of varying complexity as well as varying situations. A method is "reproducible" if its application in an independent analysis will yield equivalent results. A "simple" methodology will be characterized by ease and consistency of application. "Visibility or scrutability" implies that the basis for the method and the results obtained can be presented to and understood by others.

Among other attributes that the methodology should have are both an identification as well as an evaluation function. The identification may be thought of as the qualitative and the evaluation as the quantitative aspect of the analysis. This distinction is not strictly appropriate, but is useful in emphasizing the need to first identify (recognize) and then to assess potential systems interactions. In the context of fault tree analysis, the qualitative part of the evaluation may consist of the identification of minimum cut sets; the quantitative part would incorporate failure rate data and consequence assessment into the analysis. The identification should focus on fundamental relationships among systems and subsystems as they relate to the execution of a safety function. The evaluation is required to screen according to their safety significance as well as to determine system sensitivity to data and model uncertainties.

The desirable systems interaction methodology attributes discussed above are to a great extent mutually exclusive. As an approach tends to get more complete, it generally also gets more complex and less scrutable; the simpler methodologies may tend to be more reproducible, but less complete, etc. The more powerful methodologies require greater skill on the part of the analyst and have greater support requirements, such as computer capabilities.

Since the definition of systems interactions as used here is quite broad, it can be expected that many such potential interactions will be identified by whatever methodology that may be utilized. In such a case, it may be essential to be able to screen and rank the potential interactions in order to reduce to a reasonable level the number of detailed evaluations and/or the number of actions aimed at mitigating such interactions. An obvious way of screening is on the basis of probability. This, however, would require quantitative evaluation of all potential interactions prior to screening and thus could not aid in reducing the extent of detailed analysis required. If rough estimates of failure rate data are used as the basis for this screening, the conclusions could be sensitive to the data assumed. Thus, other means of screening and ranking potential interactions may be required. Other bases for screening might be the importance of the safety function affected, time dependence (e.g., the immediacy of the required action), and screening by categories. The systems interaction methodology selected should facilitate, or at least not preclude, screening of potential interactions at an early stage of analysis. If the number of potential systems interactions that have to be considered in depth is too large, the approach may be self-defeating.

It may be recalled that the systems interaction methodology to be developed is aimed at two broad applications; the first is the reactor license applicant's use of such a methodology in the development and review of the plant design, the second is the NRC's review of license applications from the systems interaction viewpoint. It may be useful to note that the methodology used by the applicant need not be the same as that used by the NRC. While the applicant's use of a methodology familiar to the NRC may facilitate its review, the use of a common or similar approach by both may suffer from generic deficiencies. Further, it is likely that the depth and breadth of the analysis utilized by the applicant may very well be different from that of the NRC. It is possible, for example, that the NRC review may emphasize the qualitative aspects of systems interaction evaluation whereas the applicant would cover the quantitative aspects as well.

APPLICABILITY OF POTENTIAL METHODOLOGIES TO SYSTEMS INTERACTIONS

Appendix A of this report gives a review of potential systems interaction methodologies. While not necessarily exhaustive, this review describes in some detail the strengths and weaknesses of a variety of formal as well as less structured methodologies. Table 1 lists some of the more important basic characteristics of the methodologies under three major headings. "Basic Approach" refers to the major techniques used in the method. Fault trees are considered "logical" because they are based on logic models (AND/OR gates, etc.). Weighting factors are "mathematical" because they are based on numerical approximations (α, β, and γ factors). "Capabilities" refers to the types of analysis for which each methodology is appropriate. Physical survey involves a "walk-through" procedure coupled with some sort of checklist, primarily appropriate for a qualitative analysis. Marshall-Olkin specialization involves failure-rate models based on an exponential distribution, most appropriate toward a quantitative analysis. The GO methodology considers multiple event states corresponding to output occurrence times, appropriate when analyzing a time sequence of operation. "Applicability" refers to the level of plant detail which a methodology can examine. A physical survey is mainly limited to identifying component interactions, while a cause-consequence analysis can span the full range from components through functions.

In Table 2, some of the important aspects of the methodologies are qualified. In considering this table, it must be remembered that each methodology has its own range of applicability. Thus, any comparison among them based on these aspects must bear in mind the areas in which each is applied. For example, both FMEA and cause-consequence analysis are "complete". However, FMEA is "complete" on its prime level of identifying major failure modes for components, while cause-consequence analysis is "complete" in analyzing accident sequences.

TABLE 1. CHARACTERISTICS OF POTENTIAL METHODOLOGIES

Methodology	Basic Approach		Capabilities			Applicability		
	Logical	Mathematical	Qualitative	Quantitative	Time-Sequential	Components	Systems	Functions
Operational Survey			X			X	X	X
Physical Survey			X			X		
FMEA	X		X	X		X	X	
Digraph Method	X		X			X		X
Fault Trees	X		X	X		X	X	X
Phased Mission	X		X	X	X	X	X	X
Event Trees*	X		X	X	X		X	X
Cause-Consequence	X		X	X	X	X	X	X
GO	X	X		X	X	X	X	X
Markov Modelling		X		X	X	X	X	
Generic Analysis	X		X	X		X		
Weighting Factors		X		X		X	X	
Marshall-Olkin		X		X		X		

* Refers to event trees only. Event trees plus conditional fault trees are considered to be cause-consequence analysis.

TABLE 2. ASPECTS OF POTENTIAL METHODOLOGIES

Methodology	Systematic	Complex	Complete	Reproducible	Flexible	Visible
Operational Survey	Potentially	Potentially	Somewhat	Somewhat	Yes	Yes
Physical Survey	Somewhat	No	Somewhat	Somewhat	Yes	Yes
FMEA	Yes	Somewhat	Yes	Yes	Somewhat	Somewhat
Digraph Method	Yes	No	Yes	Yes	Yes	Yes
Fault Trees	Yes	Yes	Yes	Yes	Somewhat	Somewhat
Phased Mission	Yes	Yes	Somewhat	Yes	Somewhat	No
Event Trees*	Yes	Somewhat	Somewhat	Yes	Somewhat	Yes
Cause-Consequence	Yes	Yes	Yes	Yes	Somewhat	Somewhat
GO	Yes	Yes	Yes	Somewhat	Yes	No
Markov Modelling	Yes	Somewhat	Yes	Somewhat	Somewhat	Somewhat
Generic Analysis	Somewhat	Somewhat	Somewhat	Somewhat	Yes	Somewhat
Weighting Factors	Slightly	No	No	Slightly	Yes	Slightly
Marshal-Olkin	Slightly	No	No	Slightly	Somewhat	Slightly

* Refers to event trees only. Event trees plus conditional fault trees are considered to be cause-consequence analysis.

Systems interactions can take place either on the system level or through the component level. Consider Figure 1. Systems B & C interact at the system level, while systems C & D interact through components C_2 & D_1. As an illustrative example, consider the small LOCA accident scenario in Figure 2. This is most easily transformed into the event tree of Figure 3. From there, it can be seen that if both HPCI and APR fail ($\overline{H}$ & $\overline{A}$), the LP-ECC systems cannot be used to mitigate the potential consequences. This is a result of the failure of APR to reduce vessel pressure in the event of HPCI failure. Both LP-ECC systems may be available, but their design precludes operation at an elevated pressure. This represents a system interaction on the system level.

Figure 4 is a consequence fault tree for this same scenario. Here, the failures of the LPCI and the RHR systems have been resolved to the component level. For illustration, both the LPCI and the RHR pumps have been assumed to receive electric power from the same bus (bus A). Should this bus be lost, both the LPCI and the RHR pumps will fail due to loss of power, thereby failing their respective systems. This represents a systems interaction through the component level, a type of failure often referred to as "common-cause" because two or more components (LPCI and RHR pumps) failed due to a single, common cause (loss of power bus A).

To be useful in a systems interaction assessment, the methodology must be capable of identifying at least some of the interactions on at least one of the two levels (component or system). It is further desirable that the impact of the interaction on plant safety as a whole be evaluated for ranking purposes. The following discussion views the methodologies in this framework - identification and evaluation of systems interactions.

1. Identification of Systems Interactions

As previously mentioned, systems interact either at the system level or at the component level. Most of the methodologies examined are capable of identifying interactions on at least one of these levels, while some are applicable to both. The plant review necessary in a systems interaction assessment would begin at the most general level of plant safety, shown at the top of the hierarchy in Figure 1. Next would come definition of the various safety functions contributing to plant safety

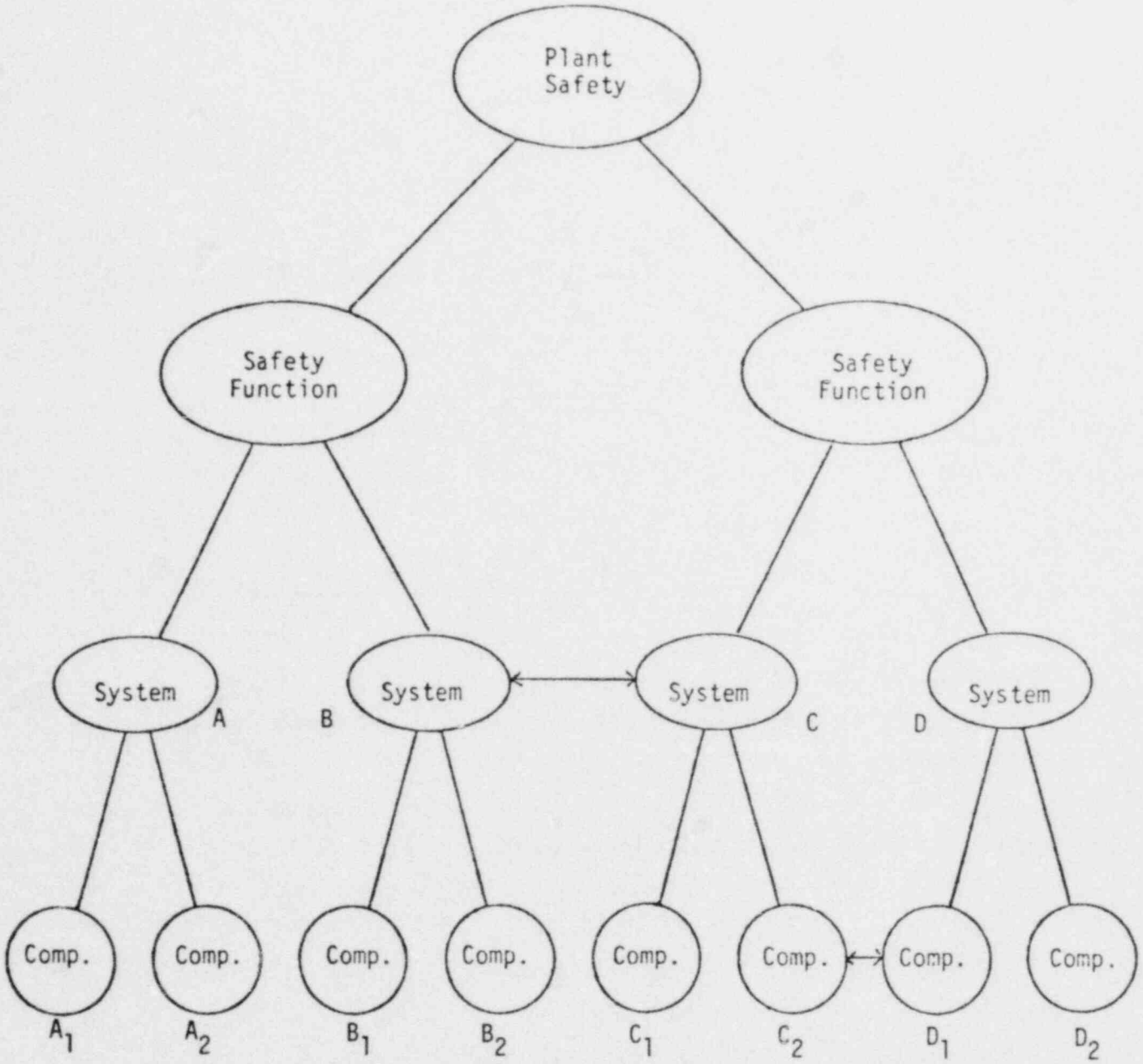


FIGURE 1. General Hierarchy for Plant Safety, Showing Levels at Which Systems Interactions May Occur

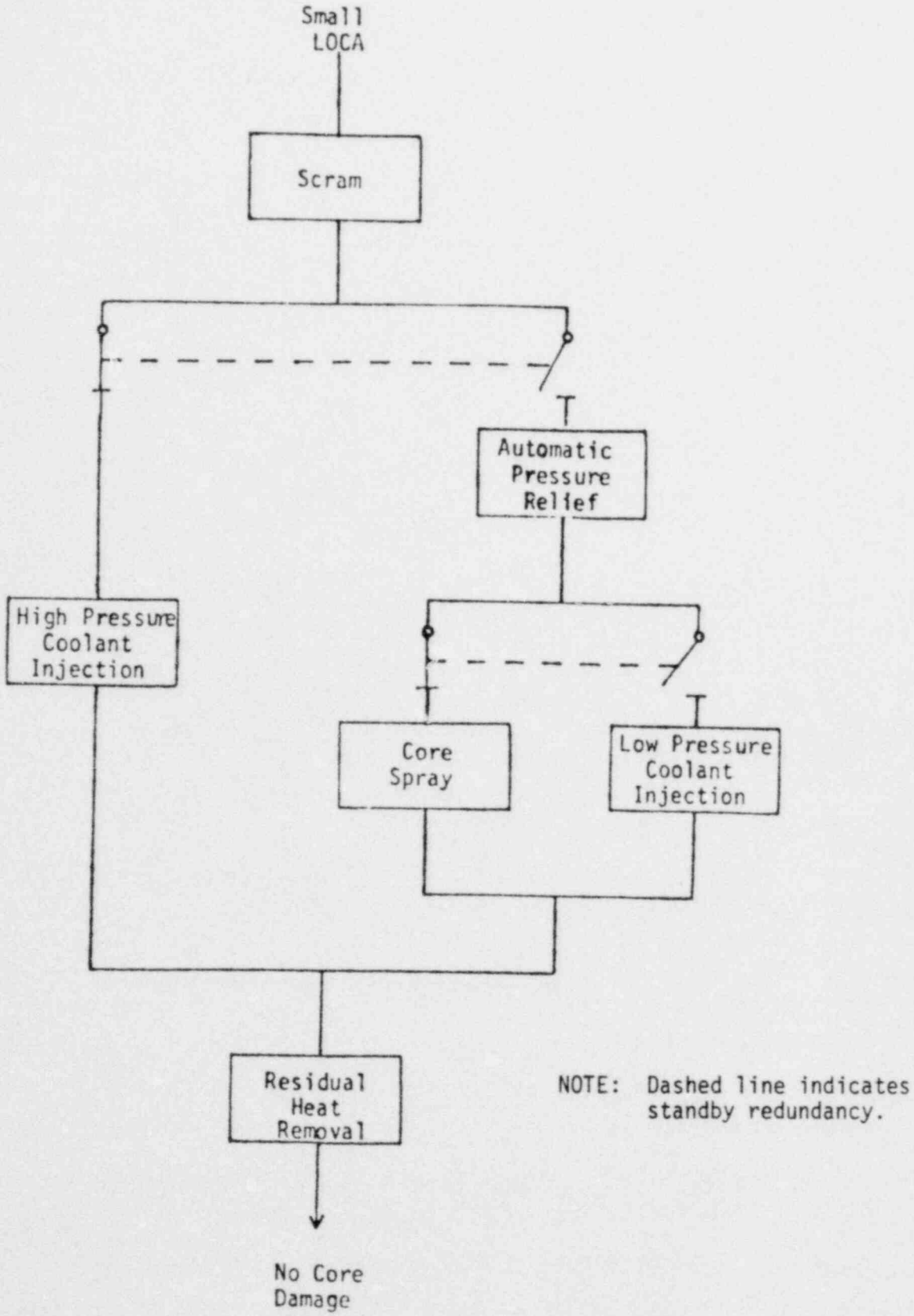
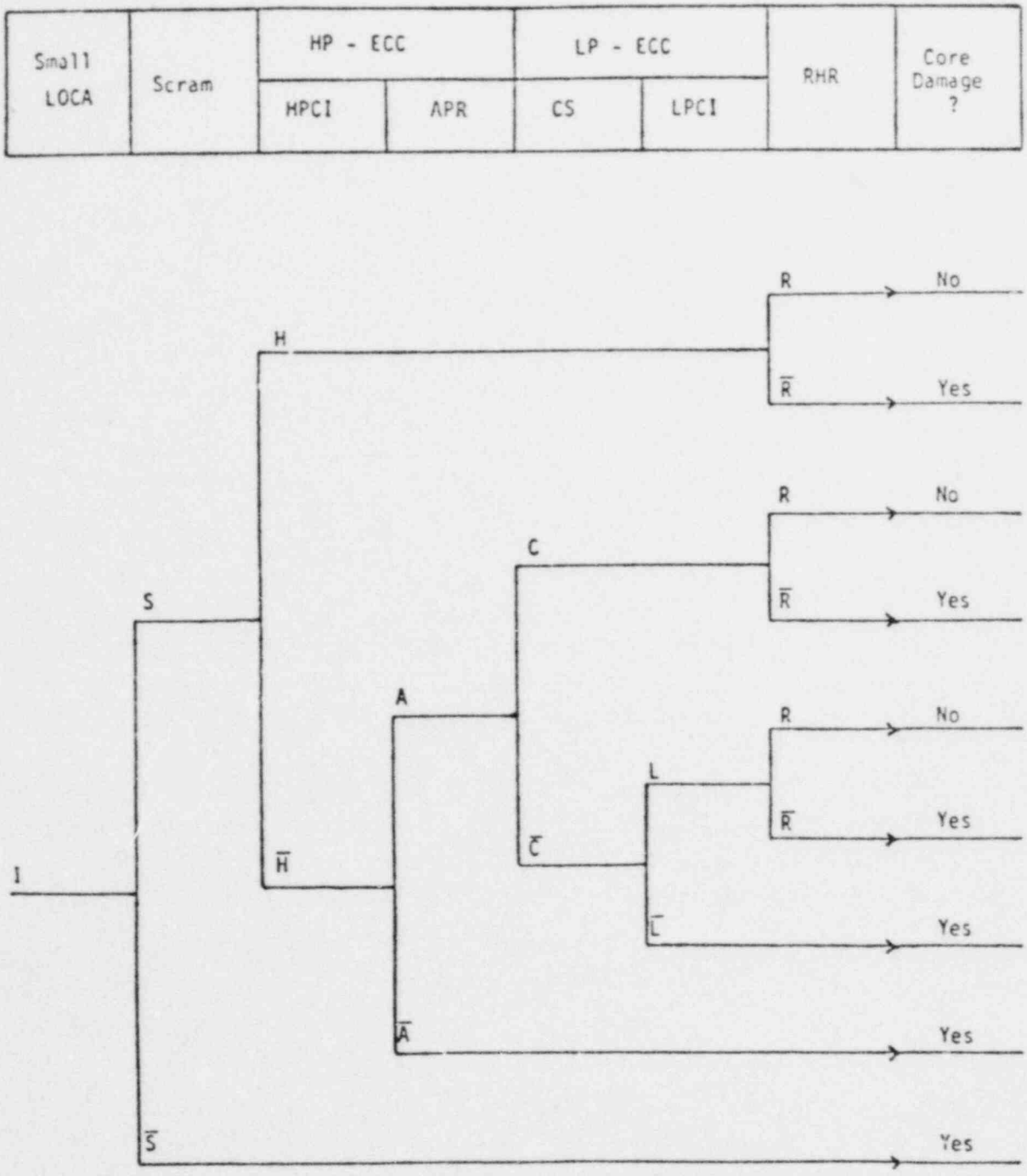


FIGURE 2. Block Diagram Showing Operation of Emergency Safety Systems Following Small LOCA



NOTE: At each branching point, the upper branch denotes success, the lower failure.

Figure 3. Event Tree for Small LOCA Accident (reference Figure 2)

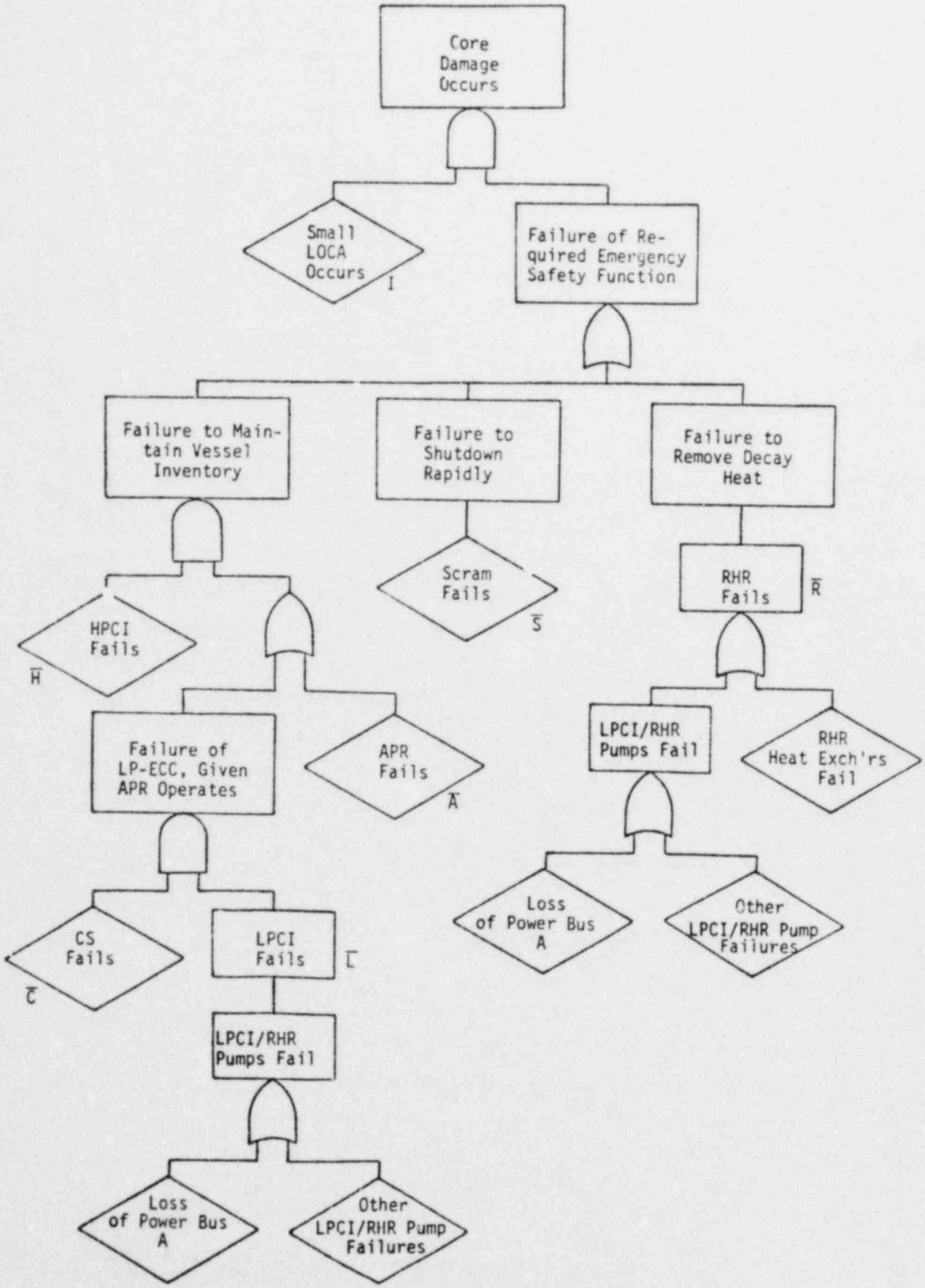


Figure 4. Consequence Fault Tree for Small LOCA Accident (reference Figure 2)

in all operating modes. Following this would be identification of the various systems needed to perform the safety functions. It is at this level where the systems interaction assessment should begin.

At the system level, the analyst seeks to identify interactions occurring at this level (such as APR and LP-ECC systems in the small LOCA accident scenario). Table 3 lists the methodologies capable of identifying these. An operational survey coup'ed with an FMEA on the systems rather than components could serve as a good starting point, especially since some sort of operational survey would be necessary to go from the top level of general plant safety down to the system level. The system FMEA could be helpful in identifying potential modes of interaction.

The identification of the various systems needed to perform the basic safety functions should be followed by the identification of the systems and subsystems needed to support them. This may involve consideration of secondary, tertiary, and other support systems and may to some extent extend to the component level. It is likely that interactions resulting from failures of the supporting 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 or dependent component failures due to common single events.

Table 3 lists the methodologies capable of identifying interactions at the component level. The operational survey would extend to this level and, coupled with a physical survey, would form a good starting point for identifying component interactions. Component FMEA and the digraph method would aid in systematizing the identification process, while a generic analysis should reasonably ensure that no major component dependencies have been overlooked.

Note that not all component interactions need result in systems interactions. If the interacting components are totally contained within a single system, their failure may affect only that system. This would not necessarily constitute a systems interaction unless failure of that system affected others. Thus, generally more component interactions are identified than actually lead to systems interaction. Only those leading to systems interaction need be retained for subsequent analysis.

TABLE 3. APPLICABILITY OF POTENTIAL METHODOLOGIES TO SYSTEMS INTERACTIONS

Methodology	Identification		Evaluation		
	Components	Systems	Components	Systems	Plant Modes
Operational Survey	X	X			
Physical Survey	X				
FMEA	X	X			
Digraph Method	X				
Fault Trees			X	X	
Phased Mission			X	X	X
Event Trees*				X	
Cause-Consequence			X	X	
GO			X	X	X
Markov Modelling			X	X	X(limited)
Generic Analysis	X		X		
Weighting Factors			X(limited)		
Marshall-Olkin			X(limited)		

* Refers to event trees only. Event trees with conditional fault trees are considered cause-consequence analysis.

2. Evaluation of Systems Interactions

Following the identification of the systems interactions candidates, it is necessary to evaluate their impact on plant safety. This involves analyzing the interactions on both the component and system levels and extending the results up through the function level to overall plant safety. Some of the methodologies are particularly suited toward analysis over this full hierarchal structure while others are more suited to one level.

Cause-consequence analysis, or the equivalent event tree-conditional fault tree analysis, is probably the best known methodology for analysis over the total hierarchy. This is essentially the technique employed in the Reactor Safety Study. The event trees are especially suitable for modelling functional losses in terms of contributing system failures. These can subsequently be extended to the component level through conditional fault trees for the systems. This is amenable for both qualitative and quantitative evaluation, but it suffers somewhat from a difficulty of keeping track of component interactions since they are generally indicated on separate fault trees.

Consequence fault trees reduce this difficulty by integrating the entire analysis onto single fault trees. Both system and component level interactions are indicated on one tree for each accident consequence. The amount of representation is basically the same since one large tree must be drawn for each consequence. (The cause-consequence analysis requires one dual tree for each initiating event.) However, fault trees are generally more difficult to conceptualize than event trees, a problem magnified by the large size of consequence fault trees. Thus, even to perform an analysis using consequence fault trees, it may be necessary to first construct event trees to aid the analyst in visualizing the situation.

Perhaps the most powerful methodology is the GO method, capable of total hierarchal analysis with the added advantages of time-modelling and integration of hardware operation with logic functions into a single analytical structure. However, the cost of such increased capability is additional complexity, which may be prohibitive when attempting to utilize its full potential. The GO methodology has an advantage over a fault tree approach in that it works from a success viewpoint, generally easier to visualize than failure combinations. The allowance for multiple event states also gives it the potential for partial failure analysis, as opposed to the

total success/failure analyses inherent in the other methods allowing only for binary states. Unlike consequence fault trees and cause-consequence diagrams, it does not readily lend itself to qualitative analysis.

Other methods do not span the total hierarchy of Figure 1, but they are capable of evaluating certain aspects of systems interactions. A reasonably versatile method that can be applied on both the system and component levels is Markov modelling. Interactions on these levels can be mathematically modelled by transitions among states with varying redundancy. Being a mathematical technique, Markov modelling is inappropriate for qualitative analysis. It is primarily a probabilistic technique. The simplifying assumption that succeeding states depend solely on their immediate predecessors may be too restrictive for some more complex interactions. However, it does provide for time-dependency, although not as extensively as does GO (or with as much complexity).

Somewhat empirical are the weighting factor method and the Marshall-Olkin specialization. They are applicable primarily on the component level, although the β-factor technique can be extended to interacting systems. They do not attempt to identify dependencies. Rather, they are designed to provide a quantitative means of approximating failure rates for dependent components and would be applicable only during probabilistic evaluation of systems interactions. They are inappropriate for qualitative analysis.

A thorough, qualitative method for evaluation of component interactions is the generic analysis approach, specifically through the Boolean transformation technique. Used primarily in conjunction with minimal cut sets from a fault tree analysis, generic analysis identifies component interactions and traces their effect on system failure by the Boolean transformation technique. Quantitative evaluation can be incorporated through the Boolean expression for system failure, which is basically an algebraic representation of an equivalent fault tree.

Systems interactions may sometimes involve changes in plant operating modes and similar time-related phenomena. Both the GO methodology and Markov modelling have been mentioned as possessing time-modelling capability. Another technique, which is an extension of fault tree analysis, is phased mission analysis. Although not as powerful (or complex) as GO, it provides

a means of analyzing a system or function which performs different roles during different plant modes. Being a fault tree technique, it can model both component and system level interactions, but it is restricted to modelling only the same systems and non-repairable components throughout the mission time.

Table 3 summarizes the methodologies which have evaluation, as well as identification, potential for systems interactions based on their level of applicability (system and/or component). Also included are those applicable to evaluating interactions involving changes in plant mode.

SYSTEMS INTERACTIONS IN PAST OPERATING EXPERIENCE

Several sources of descriptions of safety-related occurrences[2-8] have been reviewed to find examples of events involving systems interactions. The purpose of this review was to test and improve the definition of systems interactions and, in a cursory way, to test the applicability of proposed methodologies. Much more complete methodology applications are found in Appendices B and C, which are examples of the analysis of the Brown's Ferry failure-to-scram and Crystal River LOCA events. The Brown's Ferry event was not identified in the review discussed here because published accounts were not sufficiently detailed to suggest the involvement of a systems interaction; Appendix B shows the degree of detail required to anlayze this event.

The events identified in this review are summarized in Appendix D. In some cases, the actual existence of a systems interaction is tenuous; these have been included because they illustrate some aspect of systems interactions. One such case is example G of Appendix D, in which a diesel generator failed to run because of water-contaminated fuel. Rainwater had accumulated in an area above the main supply tank, had leaked into the supply tank, and been transferred to the diesel's day tank; a water detector failed to detect the water. On one hand, this event could be considered as a design deficiency (accumulation and in-leakage of water) and a random failure (water detector). On the other hand, the accumulation of water should be considered at least as a systems interaction candidate because it is a situation that could disable both (or all, as the case may be) of the emergency diesel generators. Evaluation of the situation might well discount it as a valid systems interaction, but it is also interesting to speculate that the failure of the water detector was also caused by the accumulation of rainwater!

Example E of Appendix D has some implications of interest, although the interpretation of the systems interaction aspects is somewhat flimsy. An alternate DC source was disconnected by an operator at a time when the principal bus was isolated for battery charging. One result was a temporary loss of emergency power to Engineered Safety Features due to loss of contactor control power. The major result was severe damage to a diesel generator due to the loss of capability to transfer and shed loads; this was not particularly safety-related.

It could be argued that the loss of DC power resulted from a systems interaction because the bus failed in a manner against which it was not protected. The failure appears to have resulted from a combination of procedural deficiencies, however, and would probably be difficult to predict by any analysis.

One relatively minor aspect of this event illustrates an extremely important example of a systems interaction. In the course of the event, the operator was able to return the plant to a stable condition by restoring power to the DC bus. However, he was hampered and delayed in this action by the fact that the DC bus alarms are powered by the bus itself. In the context of the event, this lack of information was of minor importance but the principle it represents is very important from the standpoint of systems interactions: the combination of the operator, the information supplied to him, and the manual controls actuated by him constitute a vital support function, which can be violated by the degradation of any one of its three components. Systems interaction analysis should be especially concerned with failures and their combinations that can deprive the operator of information he needs to cope with these failures.

RECOMMENDED APPROACH

In considering the various methodologies and their attributes as discussed above, it appears that the most promising techniques are those utilizing logic models such as fault trees or event trees. These highly structured approaches provide a framework for describing the system and for a step-by-step examination of system behavior at a fine level of detail. This ability to treat the system in very fine detail can be both an asset and a liability. It permits tracing the causes of system (function) failure (and presumably systems interactions) to failures or deficiencies at the fundamental component level. The detail of analysis permitted by these methods requires an understanding and modeling of the structures of the system, the operation of each of the components, the inputs that control the system, and the resultant outputs in commensurate detail. In a system as complex as a nuclear power plant, this level of detail can be overwhelming. In order to make the analysis tractable, the analyst is very quickly forced into compromises such as making simplifying assumptions, ignoring "unimportant" systems, limiting operating modes under consideration, working on only portions of the system at a time, etc. All these compromises reduce the practical utility of the basic methodology. In the extreme, if enough such compromises are made, the analysis is reduced to that of the effect of independent hardware failures in redundant trains, neglecting such key aspects as potential internal dependencies and human interaction. Thus, a conceptually powerful methodology can be reduced to a trite exercise due to the sheer magnitude of the problem.

Fault tree based approaches to systems interaction evaluation, such as the SETS method, are generally based on the premise that potential systems interactions can be found by identifying commonalities between the components of the systems. In principle, this premise should be quite valid since, generally speaking, systems interact through components. The realization of the full potential of such approaches would require that all components and all potential linking characteristics be included in the analysis. This is where the practical difficulties may become controlling. By immediately focusing on the components that comprise the system, the methodology is confronted with a problem of enormous magnitude. In a system as complex as the nuclear power plant, just the sheer number of components may overwhelm even the most powerful analytical methods and computer facilities. Thus, compromises in the analytical approach must be

made, particularly in the depth of evaluation that is performed. Among the earliest casualties of these compromises are the support systems to the principal safety functions. The sheer number of components that must be considered does not necessarily preclude the use of such methodologies, e.g., the identification of components that may be shared by several systems, or components that share the same location may still be quite feasible. Other linking characteristics such as those associated with calibration, test, and maintenance would be difficult to evaluate on a component-by-component basis.

The need to consider systems interaction effects stems from the realization that it is the reliability of a system (function) that is the principal safety concern. The reliability of a system depends not only on the state of components but also on potential dependencies among seemingly independent systems and also on design deficiences. The human factor is probably the dominant linking characteristic and could very well be the most likely source of systems interactions. Physical interdependencies which are not recognized are obviously also possible, these can be expected to result from subtle and obscure causes.

The human factor can affect the plant safety functions in a dynamic or a latent fashion. The dynamic mode results from the fact that the human may be required and/or permitted to act in the event of a plant upset. The situations in which a human is required to act are more easily recognized and evaluated; these are generally covered by specific procedures and criteria. The situations in which human intervention is permitted can be much more difficult to assess since they raise the question as to whether the human will act as well or whether he will act correctly, and the implication of each potential action. The Three Mile Island accident is replete with examples of permitted human intervention, some good and some bad. The latent mode of human interaction may go all the way back to design and manufacturing deficiencies, but most likely will be associated with calibration, test, maintenance, and related activiites that can leave affected portions of the plant in a degraded condition. Such degradation may not manifest itself until the affected system is required to mitigate the effects of some abnormality.

The unrecognized physical interdependencies can originate anywhere in the plant, but the more likely places are in secondary, tertiary, and other support functions; these areas typically are subject to less scrutiny during the design and review processes than are the primary systems. As has been noted by others, systems interaction evaluation cannot stop at so-called "safety related" systems; all systems that contribute to the basic safety functions are potentially important.

Since the requirements on a methodology to identify and evaluate systems interactions are broad it is suggested that the methodology initially focus on the basic safety functions rather than addressing the plant on the component level. It is further suggested that logic models such as fault trees be adapted to evaluate system behavior and potential systems interactions on a functional or systems level. The suggested approach is outlined in Figures 5 and 6.

A discussion of the qualitative systems interaction assessment as outlined in Figure 5 is given below. The initial steps consist of specifying the basic safety functions and the plant operating modes. The breakdown of the basic safety functions suggested in this report is not unique; clearly other definitions are possible. The plant operating modes suggested here correspond to the generally accepted definitions. For each of the principal safety functions and operating modes it will be necessary to determine all the possible success paths for the plant. These success paths will then be the points of departure for the subsequent analyses. This is a key point since faiulre modes can only be clearly identified if the corresponding success states are known. For each of the success paths it will be necessary to identify each of the redundant trains of the safety systems that comprise that path. For each safety system it will be necessary to identify the trains of vital auxiliaries that are needed to support it. Given the number of safety functions, operating modes, redundant safety trains, and support systems, it can be seen that even at a very broad level of consideration the problem becomes very large. In order to keep the problem tractable it will be necessary to develop a system of identifiers to track the systems and subsystems in each of the above success paths. Recognizing the needs of the subsequent analyses, this sytem of identifiers should include (or at least permit the

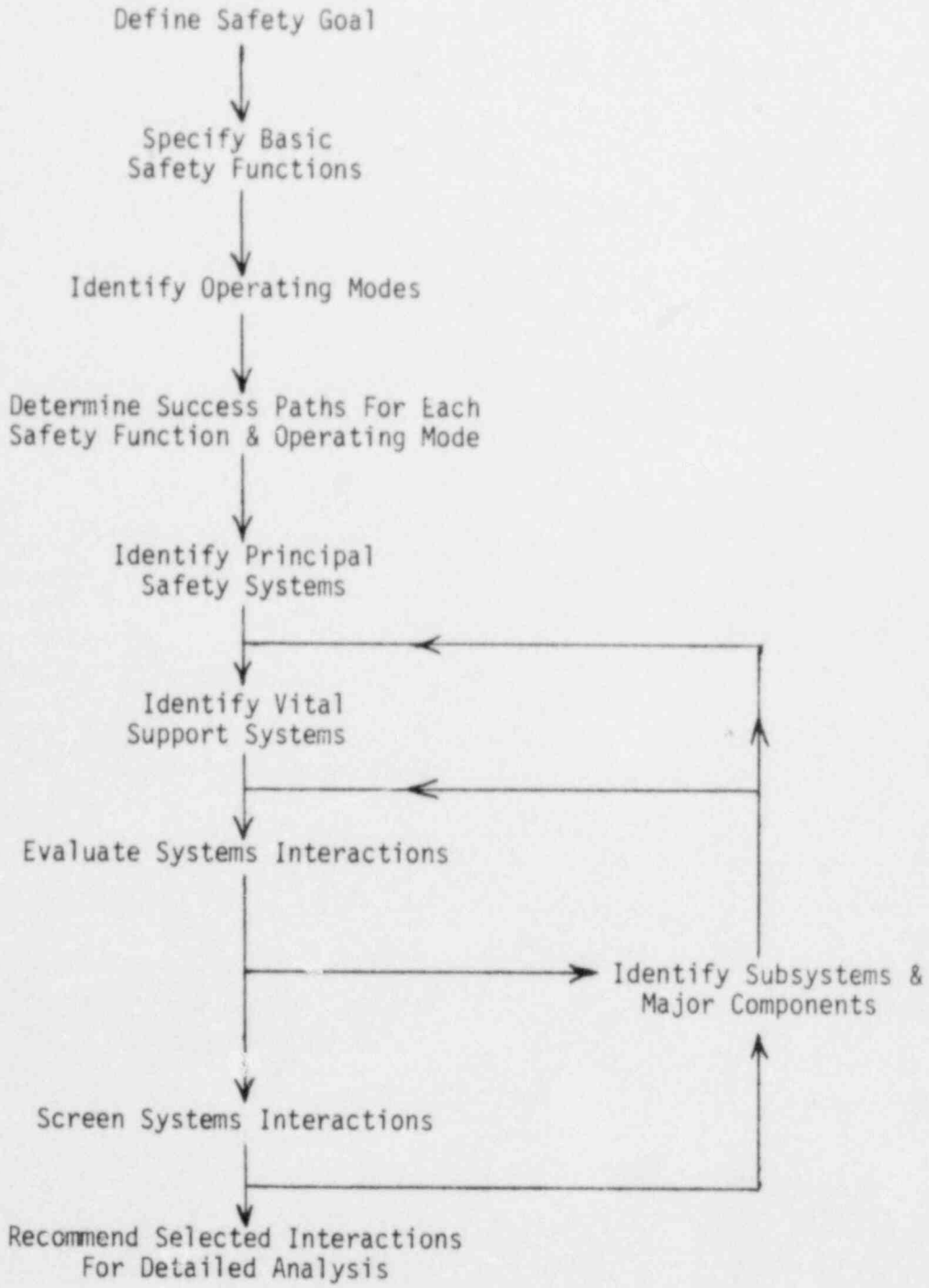


Figure 5. Qualitative Systems Interaction Assessment

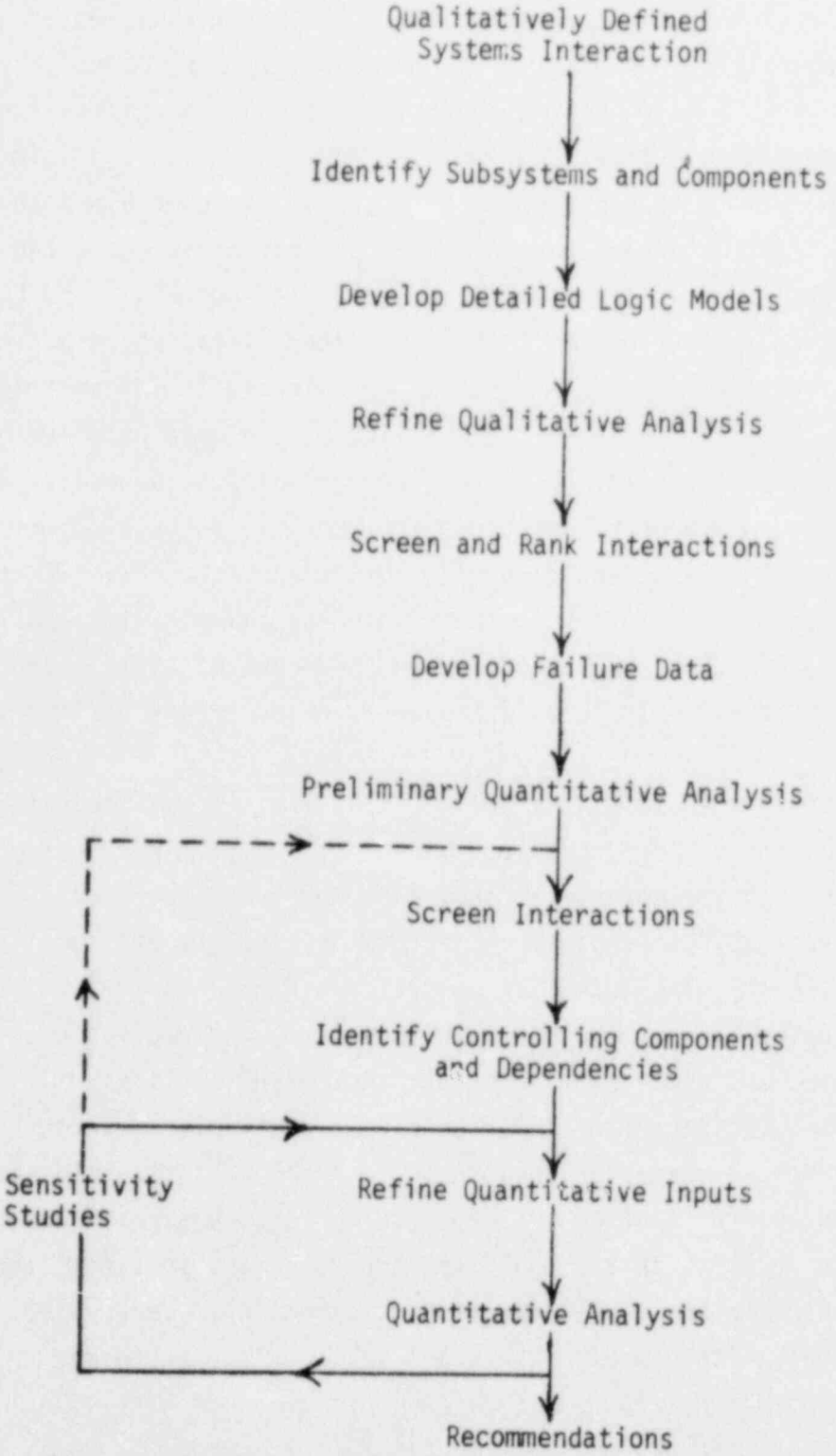


Figure 6. Quantitative Systems Interaction Assessment

addition of) the potential linking characteristics between the systems, subsystems, and components in the plant. The principal linking characteristics are given in Table 4. The preceding definitions and identifications provide the basis for the initial evaluation of systems interactions. This evaluation would probably be best performed by means of logic models such as fault trees, though other approaches such as FMEA, digraphs, etc., can also contribute. This is illustrated by the examples in Appendix B and C. The initial qualitative evaluation may lead to the identification of potential interactions of varying significance. It will be desirable to screen this list of interactions to minimize the number carried on for more detailed analysis. Some of the possible ways of screening were discussed earlier in this report. However, the means of screening and ranking potential systems interactions is one of the key areas requiring further development. Figure 5 also indicates the potential need for iteration if, for example, the analysis indicates the need for further resolution in the breakdown of systems and subsystems. Such iteration could conceivably be required in any part of the process.

The quantitative systems interaction assessment as outlined in Figure 6 follows the general logic previously outlined. It is predicated on some degree of qualitative assessment having preceded it. Whereas the foregoing qualitative analysis would be facilitated by the use of logic models (e.g., fault trees), the quantitative analysis would require them. In the successful application of logic models to systems interaction evaluation the recognition and incorporation of all the potential linking characteristics will be of paramount importance. Of particular interest and importance will be the characterization of the human factors, both latent and dynamic; this is an area that can be expected to require significant development. As was the case in the qualitative part of the analysis, the need to screen and rank potential interactions is expected to carry into this phase of the evaluation. Again, the bases for such screening and ranking will require development.

By focusing on the basic safety functions, the safety systems required to perform these functions, and the vital support systems, it is felt that the approach can identify the requisite depth of analysis before

TABLE 4. SYSTEM, SUBSYSTEM, AND COMPONENT LINKING CHARACTERISTICS

Physical
Electrical
Mechanical
Hydraulic
Pneumatic
Spatial
Thermal
Fluid
Mechanical
Radiation
Inherent
Common Manufacturer
Similar Technology
Equal Aging or Wear
Shared Components
Human
Dynamic
Latent

proceeding to the detail associated with basic components. Of the available methodologies, the event tree approach appears to be most suited for application at the functional or systems level. An event tree begins with some initiating event and maps out a variety of sequences involving faults at the system level, each of which represents a particular consequence. A complete event tree analysis would require identification of all significant initiating events and the development of an event tree for each. Extensive overlap of consequences among the branches of the several trees can be expected. Each accident sequence leading to a particular consequence in an event tree is somewhat analogous to a cut set on a fault tree. Whereas a cut set represents a combination of failures leading to the top, or undesired, event; an accident sequence represents represents a combination of system successes and/or failures leading to a given consequence. The difference in reference points between event tree and fault tree analysis suggests that event trees may be more appropriate when the initiating events are known, while fault trees may be more appropriate when the consequences can be identified more easily. The latter is the situation with the problem at hand. Thus, it is suggested that the fault tree approach be adapted for application to the identification and evaluation of systems interactions.

Although traditionally fault trees have been used to model system failure in terms of failure of its basic components, fault trees should also be useable to model accident sequences with the top event being some consequence of those sequences. The use of fault tree methodologies in this context is being suggested for the evaluation of systems interactions. It is further suggested that resolution of the analysis be initially limited to the system or subsystem level. Most previous applications of fault tree analysis have tended to resolve systems to the component level, where failure data is more readily available. For qualitative analyses where the identification of potential systems interactions is the most importnat aspect, the lack of failure rate data at this level is not particularly important. Those interactions that are considered to be significant after screening of the qualitative results can subsequently be subjected to a more detailed analyses, including detailed fault trees. A further motivation for initially focusing

on the systems level is the realization that in complex systems the validity of reliability estimates may be govered more by the assumptions used in modelling the system than by the failure data utilized. By limiting the initial analysis to the systems level it is hoped that the modelling approach can retain many of the subtle interdependencies that may be lost due to the truncations and compromises that are necessary when a high degree of detail for the entire system is attempted.

The use of the same basic methodology for both the qualitative as well as the quantitative portions of the analysis, e.g., use of fault trees for both rather than a combination of event trees and fault trees, would have the following advantages:

a) it should facilitate a consistent transition from the qualitative to the quantitative mode of analysis,
b) it should permit whatever degree of iteration may be required, as later analyses indicate the need for more resolution, particularly for the more important interactions that may be identified,
c) the depth of analysis can be carried out to whatever level of detail is desired, or stopped at any level of interest, and
d) the presentation of the results and the scrutability of the methods should be enhanced.

Some further thoughts on addressing the systems interaction problem from the systems or functional level are as follows. As was noted earlier, human interaction can be expected to be a major linking factor leading to potential systems interactions. The latent mode of human interaction deals with such aspects as calibration, testing, and maintenance. While all these activities relate to individual components, it is the function of the system that contains the affected components that is concern. Further, the above activities are more often than not conducted in the context of checking, testing, or repairing a system. E.g., it is the ECC system set points that are calibrated, though the actual calibration is performed on a very specific set of components; it is the ECC train "A" that is being tested and/or repaired and thus taken out of service. Thus, it may be natural to assign the linking characteristics due to human interactions to the system or subsystem level rather than that of the individual components. The fact that there are far fewer systems than components facilitates the initial consideration of these interactions at the systems level.

The application of fault tree methodology to system reliability assessment and, to a more limited extent, common cause/common mode failure analysis is broadly accepted. There are numerous automated techniques for developing fault trees as well as evaluating them. For the reasons cited previously, most fault tree analyses have focused on the hardware and aimed at system failures originating due to component failures. The use of fault trees at the system level as suggested here has received only limited attention. Again, for reasons cited previously, the "traditional" fault tree analyses approaches are felt to have practical limitations for application to systems interaction evaluation. However, in view of the demonstrated capabilities of this methodology and the existence of a base of capability in terms of experience and analytical tools, it is felt prudent to take advantage of this basis in the further development of a systems interaction methodology. This is the intent of the suggested approach.

Since the recommended methodology for addressing systems interactions concerns has not been demonstrated to be fully applicable, further development will be required. The key areas of further development include: application of the fault tree methodology at the functional or systems level, characterization of the system, subsystem, and component linking due to both latent and dynamic human effects, and methods for screening and ranking potential systems interactions at early stages in the analysis. These needs will be further defined in subsequent phases of the program.

AN INTERIM APPROACH TO SYSTEMS INTERACTION EVALUATION

The review of the methodologies potentially available for systems interaction evaluation clearly indicates that a major analysis effort will be involved to analyze a plant in the breadth and depth required to find systems interations. If a structured systems analysis were made a requirement of the license application, the effort required by the utility applicants would be substantial. Considering the state-of-the-art of these types of analyses it is highly unlikely that the utilities would have access to a sufficient number of qualifed analysts over the next few years to meet such a requirement. Similarly, a very large quantity of information would be submitted to the NRC for review, implying a large committment of NRC staff. In view of these considerations an alternate approach to systems interaction evaluation is suggested which would be less formal and structured than that recommended in the previous section, but which could be implemented while the formal methodologies are undergoing further development.

The objective of the interim approach is not to abandon more structured methods but rather to use them, with other sources of information on systems interactions, to develop general principles and to identify specific problem areas. These general principles could then be used to formulate guidelines for the regulatory review of plant applications.

The sources of information available on systems interactions are:

1) detailed systems analyses (which either have been performed or are in progress,e.g., as part of the NRC research effort), and
2) operational experiences.

In the suggested interim approach, detailed systems analysis methods would continued to be developed, particularly with regards to their ability to identify systems interactions. These methods would be applied by the NRC contractors to some specific plant designs. For example, the effort currently being undertaken for the first set of IREP plants could be extended to examine the potential for systems interactions in greater detail. Similarly, Licensee Event Reports would be reviewed in some detail to identify the systems interactions that have occurred. Events would be identified which had either resulted in degradation of a safety function or which had the potential to

do so as the result of common cause relationships. Having identified important types of interactions from the analyses and from the review of events, general guidelines would be developed which could be applied in the regulatory review of applications. These guidelines could be developed into a generic checklist of potential systems interactions.

The following elements could form the basis for a regulatory review process which focused on system interactions.

1) Simplified Systems Analysis

A systematic approach must be taken in exploring the relationships between systems in a nuclear power plant. The plant is too complex and the relationships are too subtle for the reviewer to evaluate without the assistance of systems analysis techniques. At one end of the spectrum of complexity, the systems analysis method could be a detailed fault tree/event tree analysis. While such a formal structured approach is believed to be desirable and has been recommended in the previous section, it does not appear practical in the short term. What is being suggested for this review would be much less complex. The steps of a method of this type are presented in Table 5. The analyses would be performed by the utility and submitted with the license application. The results would guide the reviewer through the important functional relationships in the plant. The reviewer could identify interactions at the systems level and some interactions at the component level. Such a method would clearly not be as effective in identifying interactions as a formal structured analysis. To aid in the review, however, the reviewer would be provided with a generic list of specific interactions for which to look as well as some general guidelines. In this manner, the results of detailed systems analyses and operational experiences can be used to augment the capability of the simple systems analysis approach. Presumably, the majority of important systems interactions can thus be identified.

Table 6 presents the types of connections that can lead to systems interaction in complex systems. The systems analysis approach involved in this element of the review would attempt to identify physical and inherent interactions.

TABLE 5. FUNCTIONAL SUCCESS TREE APPROACH TO SIMPLIFIED SYSTEMS ANALYSIS

Analysis Steps

(1) For each of the prinicpal safety functions as previously defined, determine possible success paths for the plant starting from the principal operating modes.

(2) Identify each redundant train of the safety systems in the success paths.

(3) List all subsystems and major components within each train using unique identifiers.

(4) Define trains of vital auxiliaries providing motive power, control power, actuation, cooling, lubrication and environmental control for all components listed in Step 3.

(5) Scan system to identify:

(a) single failures that can disable two or more safety trains

(b) subsystems and components which are common to different safety trains or vital auxiliaries

(c) subsystems and component which are common to different safety functions in the same success path

(d) subsystems and components in different safety trains or different safety functions that are related by the potential linking characteristics of Table .

TABLE 6. REGULATORY REVIEW OF COMMON CAUSE CONNECTIONS

Connections[9]	Review Element
Physical	Simplified Systems Analysis
Electrical	
Mechanical	
Hydraulic	
Pneumatic	
Spatial	Plant Walk-Through
Thermal	
Fluid	
Mechanical	
Radiation	
Inherent	Simplified Systems Analysis
Common Manufacturer	
Similar Technology	
Equal Aging or Wear	
Shared Components	
Human	Review of Procedures, Technical
Dynamic	Specifications and Training
Latent	Requirements

2) Review of Procedures, Technical Specifications, and Training Requirements

Human interactions are the most difficult aspect of systems interactions with which to deal. They transcend the entire plant and provide the potential for linkage between all components and systems. Although all plant management practices can affect the performance of plant personnel to some degree, many aspects of plant management are difficult to influence by regulatory control. For example, the regulator can have little affect on the quality of the environment (relationship between management and staff) in which the operators work, although this probably has a close relationship to the incidence of human errors. The regulator can, however, affect two of the most important factors that influence personnel performance. Through the review process, he can help to assure that the training of plant personnel is adequate and that the procedures by which the plant is operated are written in a manner to reduce the occurrence of operator error as well as to reduce the potential impact of such error.

In this element of review, technical specifications, operating procedures, emergency procedures, and test and maintenance procedures would be reviewed to assure that the potential for interactions which can be introduced by the human is minimized. For example, well-written procedures should not permit a single operator/technician to calibrate all of the corresponding instruments in redundant trains of a safety system; if systems have to be disabled for test or maintenance, the return-to-service procedures become extremely important; etc. Guidelines of this type would be provided to aid the reviewer. Consideration would also be given to the adequacy of training plans.

3) Plant Walk-Through

The final element of the review program would be a walk-through of the plant. The reviewer would be provided in advance with detailed drawings of the equipment location in the plant. The systems providing each of the principal safety functions and vital auxiliary functions could be identified

separately on the drawings to aid the reviewer in recognizing potential interactions. The review plan would provide specific guidance on relationships for which to look. The types of common cause connections (see Table 6) that could be identified in a walk-through would involve the spatial proximity of components to one another and to energy sources.

The elements of the suggested interim approach to the regulatory review of systems interactions have some capability to address each of the four major forms of common cause connections as described in Table 6. This approach would rely heavily on lessons learned from the review of operational experience and the study of detailed systems analyses. It is difficult to project how successful such an approach would be in identifying novel systems interactions which had not been found previously in other designs. This recommended interim approach parallels the more structured systems interaction evaluation methodology suggested earlier. The former minimizes the reliance on novel analysis techniques and exploits capabilities that are readily available. Although there are aspects of detailed systems analyses that are more promising, the alternative approach described above could be implemented within a comparatively short time. In addition, the approach could make use of the results of detailed systems analyses in a generic sense while these methods are being developed for application to specific design reviews, assuming that at some time in the future that would be practical.

SUMMARY

The broad objective of this study is to identify methods suitable for near-term use and future development for the evaluation of systems interactions by industry and NRC. Consideration was given to existing systematic methods that have been used or could be used on systems having complexity comparable to light water reactor plants.

The definition of systems interaction posed as a result of this study is as follows:

> A system failure combination that can reduce the effectiveness of any one of a number of basic safety functions.

This definition contains three important features. First, the concept of "failure combination" places multiple independent failures outside of the boundaries of systems interactions. Second, the concept of "reduction of effectiveness" incorporates the recognition that potential, as well as real, hazards can result from systems interactions. This concept significantly broadens the scope of analysis, but is deemed necessary to provide for the identification of all important systems interactions. Third, the concept of "basic safety functions" provides a general framework for analyses that can be applied to all light water plants, regardless of design.

A methodology developed to identify and evaluate systems interactions should be systematic, complete, flexible, reproducible, simple, and visible or scrutable. The number of systems interactions identified in an analysis could be quite large, so it apperas desirable that the methodology perform as much as possible of the identification and screening processes on a qualitative basis. The effort involved in the detailed evaluations (performed by probabilistic methods, for example) would thus be reduced and would include only those systems interactions of importance.

Existing analytical methods were reviewed to assess their applicability to a systems interaction methodology; these methods are discussed in Appendix A. None of those considered can be considered as unsuitable. Some of the more complex methods would not be practical for most analyses, but could be useful and perhaps necessary in the analysis of some situations. It appears certain

that any methodology must begin with a review of plant descriptions and drawings, and must include a physical survey of the plant.

Valuable insights into the nature of systems interactions can be gained by reviewing operating experiences of nuclear power plants. The most readily available sources of information on operating experience are Licensee Event Reports (LER's). At the p esent time, it is often difficult to identify actual systems interactions in LER's because of the reporting format and brevity of the reports. However, improvements in event reports have been proposed (these are too recent to be considered in this study), which appear to make the LER's of greater value from the systems interaction standpoint. Reports of a number of events were reviewed to identify systems interactions; in a number of these, no actual hazard existed, but they included the types of failure combinations that are of interest in systems interactions. These experiences could form part of a historical data base for future analyses.

The recommended methodology for systems interaction analysis is comprised of two general parts: (1) a qualitative part to identify and screen systems interactions candidates, and (2) a quantitative part to evaluate the importance of identified systems interactions. In consideration of the complexity of the systems involved and the need for completeness in the analysis, identification and screening form the crucial part. Event and fault trees, perhaps supplemented by methods such as FMEA and digraphing, appear to offer the best approach to this part of the methodology. A key factor here is that the methodology must incorporate a provision for iteration so the analysis can begin at a fairly broad level and proceed to greater detail as required. Similarly, screening should closely follow identification so only items of known or potential interest are subjected to the complete analysis; these steps are necessary to maintain the analysis at a manageable size and still achieve the required completeness. Existing methods can be used for the quantitative evaluation of identified systems interactions. The introduction of failure rates is a logical extension of the use of fault trees in the qualitative part of the analysis.

REFERENCES

1. Corcoran, W. R., et al, "The Operator's Role and Safety Functions", Combustion Engineering, Inc. Report No. TIS-6555.

2. "Review of Licensee Event Reports (1976-1978)", NUREG-0572, USNRC, ACRS (September, 1979).*

3. Power Reactor Events, Vol. 2, No. 4, USNRC (July 1980).

4. "Reactor Operating Experiences 1975-1977", NUREG/CR-0369, ORNL (October 1978).**

5. Scott, R. L., and Gallaher, R. B., "Annotated Bibliography of Safety-Related Events in Boiling-Water Nuclear Power Plants as Reported in 1977", NUREG/CR-0462, ORNL (November 1978).**

6. Scott, R. L., and Gallaher, R. B., "Annotated Bibliography of Safety-Related Events in Pressurized-Water Nuclear Power Plants as Reported in 1977", NUREG/CR-0466, ORNL (November 1978).**

7. Nuclear Safety, USNRC (1977-1979).

8. Bertini, H. W., et al, "Description of Selected Accidents That Have Occurred at Nuclear Reactor Facilities", ORNL/NSIC-176, (April 1980).

9. Boyd, G. J., et al, "Final Report - Phase I Systems Interaction Methodology Applications Program", NUREG/CR-1321 (April 1980).*

*Available for purchase from the NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission, Washington, DC 20555, and the National Technical Information Service, Springfield, VA 22161.

**Available for purchase from the National Technical Information Service.

APPENDIX A

REVIEW OF POTENTIAL SYSTEMS INTERACTION METHODOLOGIES

Because systems interactions form a vital part of any thorough safety assessment, more general safety analysis methods form a convenient starting point from which to choose specific methodologies applicable to analysis of systems interactions. Both identification and analysis of system interactions must be provided for in any method or combination of methods selected for examination of these interactions. With this perspective in mind, it is convenient to divide the potential methods into two categories: qualitative and quantitative. This categorization does not necessarily imply that one group is more rigorous or formalized than the other, although this may be true for specific methods. The two categories are not mutually exclusive, since some methods have both qualitative and quantitative capabilities, such as fault trees.

A.1. Qualitative Methods

Four methods are discussed: operational survey, physical survey, failure modes and effects analysis (FMEA), and digraph method. Of the four, the first two refer to somewhat informal review processes while the latter pair represent more formal techniques. As was previously mentioned, these methods may also possess limited quantitative capabilities. However, since their prime role is qualitative, they have been classified as such.

A.1.1. Operational Survey

"Operational survey" is a rather formalized name given to the detailed review process involved in ascertaining the functional relationships among systems. The analyst studies relevant documentation, including such information as found from system schematics, plant technical specifications and administrative procedures, and systematically identifies potential areas for interactions. This identification can incorporate more formal techniques, such as the digraph method, or can be as informal as merely producing some sort of tabulation. The analyst probably would tend toward more formalization as the number and/or complexity of systems interactions increased. For a large-scale survey, it may be advantageous to utilize a computerized data base. To supplement the documentation study, the analyst can procure expert opinion, presumably from plant personnel. An example of a type of operational survey that may serve as a convenient starting point in the review process is Appendix G of reference 27.

A.1.2 Physical Survey

The physical survey is basically a "walk-through" inspection of the appropriate areas of the plant coupled with some sort of systematic accounting of identified areas for interaction. A typical example can be found in the Diablo Canyon seismic review.[1] Tabulation may be in a columnar format or possibly involve marking sensitive locations on diagrams of the plant layout. The survey should be thorough enough to identify potential interactions unique at the plant due to modifications not specified on schematics. However, it should not become encumbered with highly unlikely interactions. This latter criterion also applies to the operational survey. However, since functional interactions tend to be more clearly defined and less speculative than spatial ones, a checklist prepared from the operational survey can be used to guide the physical. This reduces its potential for becoming encumbered with trivial interactions.

A.1.3 FMEA[2,3,4]

FMEA is a qualitative induction technique for identifying hazardous conditions and determining their importance. As commonly used in reliability and safety analyses, the FMEA identifies failure modes for the components of concern and traces their effects upon other components, sub-systems, and systems. Emphasis is placed on identifying the problems which result from hardware failure. Typically, a columnar format is employed in an FMEA, as shown in Table A.1. Specific entries for the columns include descriptions of the component, its failure modes, causes of failure, possible effects, and actions to reduce the failures and their consequences.

Although traditionally developed from a component level, a type of FMEA can be envisioned which would start at a system level to trace out interactions and their effects upon plant safety functions and, eventually, on plant safety itself. Such a modified FMEA is illustrated in Table A.2. Note that it can be designed to integrate with an operational and a physical survey.

A.1.4. Binary Matrices and Digraphs

The use of hierarchies to portray relationships among elements of complex systems is common in many fields, especially in the business and social sciences. The nature of SI and the complexity of nuclear power plants suggests that the concept of hierarchies could be a valuable part of a methodology for SI analysis.

TABLE A.1[25] Sample FMEA for Components

PART ASSEMBLY OR PROCESS				P/N					PREPARED BY R. C. Pertucio	DATE 2/25/76	
ITEM NO.	PART, ASSEMBLY OR PROCESS NUMBER	PART, ASSEMBLY OR PROCESS NAME	PART, ASSEMBLY OR PROCESS FUNCTION	FAILURE MODE(S)	FAILURE CAUSE(S)	PROBABILITY	CRITICALITY	FAILURE EFFECT(S)	CORRECTIVE ACTION OR PREVENTIVE ACTION	PART, ASSEMBLY OR PROCESS INTERFACINGS AND REMARKS
1.1	Reactor Vessel		Provides support for fuel assemblies Contains sodium	Leakage, rupture	Corrosion, erosion, thermal shock, excessive loads			Sodium fills guard vessel. Decay heat removal possible.		Failure not critical unless there is a coincident failure of guard vessel.
2.1	Shutdown Heat Removal System Piping, Valving, and Components		Includes piping, drain valves vent valves manual isolation valves	External leakage, rupture (represents total unavailability of a SHRS loop due to leakage of all components)	Bending fatigue, creep strain, thermal or mechanical loads, weld failure, thermal shock, thermal stresses, and corrosion			Sodium spills into cell. Loop drained and repaired; unavailable for decay heat removal		If the system is at negative pressure at the point of leak, gas enters the coolant.
2.2	EM Pump			Fails to operate	Loss of electrical power supply. Short circuit in MG set windings fail. Loss of cooling to windings. Structural failure of MG set.			Loss of forced convection in SHRS loop. Heat transport by natural circulation.	Redundant EM pumps would protect against random independent failures of the pump.	Option 2, 3, and 4 would possibly not naturally circulate if there was pony motor flow. ΔP would close checkvalve.
2.3	SHRS Checkvalve		Prevent reverse flow in loop during normal operation	Fails to open	Contamination, mechanical distortion			Prevents flow in SHRS loop. No decay heat removal capability.	Positive pressure from pump head will very often open stuck valve, thereby reducing true failure rate.	
3.1	PHTS Piping Valving, and Components			Leak, rupture	Bending fatigue, creep strain, thermal or mechanical loads, weld failure, corrosion, nozzle weld failures.			Sodium spills into PHTS cell. Loop drained and repaired.		Loop unable to provide pony motor flow through core.
	PHTS Pump			Seal leakage, failure	Thermal cycling, fatigue, wear, corrosion			Sodium leaks into cell. Pump drained and repaired.		Loop unavailable to provide pony motor flow through core.
				Bearing seizure	Wear, corrosion, contamination			No forced convection in PHTS loop.		Loop unavailable to provide pony motor flow through core.
				Shaft failure, structural failure of pump internals	Thermal shock; excessive loading.			No forced convection in PHTS loop.		Precludes pony motor operation.

TABLE A.2 Sample Modified FMEA for Systems Interactions

Systems Interaction	Interaction Type	Plant Operating Mode	Systems' Failure Modes	Consequences		
				System Level	Function Level	Plant Level
APR & LP-ECC	Operational	Scrammed due to small LOCA	Given HPCI failure, APR failure to depressurize vessel prevents operation of LP-ECC	LP-ECC inoperable, although available	Failure to maintain vessel inventory	Possible core damage, leading to potential breach of containment
LPCI & RHR	Operational	Scrammed due to small LOCA	Failure of LPCI/RHR Pumps used by both LPCI and RHR, leaves both systems inoperable	LPCI & RHR inoperable	Failure to remove decay heat from containment	Possible containment overpressure, unless vented
General non-safety system & SC	Physical	Cold Shutdown	Fire in cables of non-safety system spreads to nearby, non-redundant cables of SC	SC inoperable	Failure to lower primary coolant temperature to < 212°F	None, if plant can be returned to Hot Shutdown & maintained there

APR = Automatic Pressure Relief

LP-ECC = Low Pressure Emergency Core Cooling

LPCI = Low Pressure Coolant Injection

RHR = Residual Heat Removal

SC = Shutdown Cooling

HPCI = High Pressure Coolant Injection

The tools associated with the concept are the binary matrix and the directional graph, or digraph. The binary matrix contains information on the relationships between the elements of a system and the digraph is graphical presentation of the structure of the system. Formal procedures involving very elementary matrix operations are available to generate the digraph from the binary matrix.

The relationships contained in the binary matrix are "subordination relations"; the binary entry in each intersection of the matrix indicates whether or not one element is subordinate to another. An important aspect of the indicated relationships is that they have an associated direction, i.e., given elements A and B, if A is subordinate to B, then B is not subordinate to A. The word "subordinate" should be interpreted broadly; for example, (1) the flow of fluid through a pipe is subordinate to (depends on) the position of a valve in the pipe, and (2) the output signal of an amplifier is subordinate to the operating state of the amplifier and to its input signal. In the application of the binary matrix to the analysis of complex systems, it is important to note that although the matrix must indicate all levels of subordination, the analyst need supply only direct first-level relationships and provide a computer code to deduce any consequent levels of subordination. An additional advantage is that the elements can appear in any order in the matrix; the matrix processing procedures are capable of rearranging the matrix into separate hierarchies.

Another feature of the binary matrix that makes it particularly attractive for SI analysis is that an element of the matrix can be any entity of interest; an entire system, a system function, a subsystem, a component, a physical location, a maintenance crew, or an electrical connection, to name a few of the possibilities. Elements of any level of detail can be intermixed.

The digraph (or digraphs, if the binary matrix represents more than one independent system) is generated directly from the binary matrix and provides a convenient graphical presentation of the ordered arrangement of the elements of the system. From the standpoint of SI analysis, potential interactions appear as linking elements between systems (subsystems, etc.). To determine whether such linkage represents valid SI requires further review because the

digraph shows only the direction of element associations, and not their nature. If more detailed analysis (fault tree analysis, for example) is to be performed, the digraph can be used as a guide and visual checklist in the processes of determining pertinent failure modes and establishing logical relationships between elements.

An example of the application of the binary matrix to two simple, linked flow systems (shown in Figure A.1) is presented in Figure A.2.

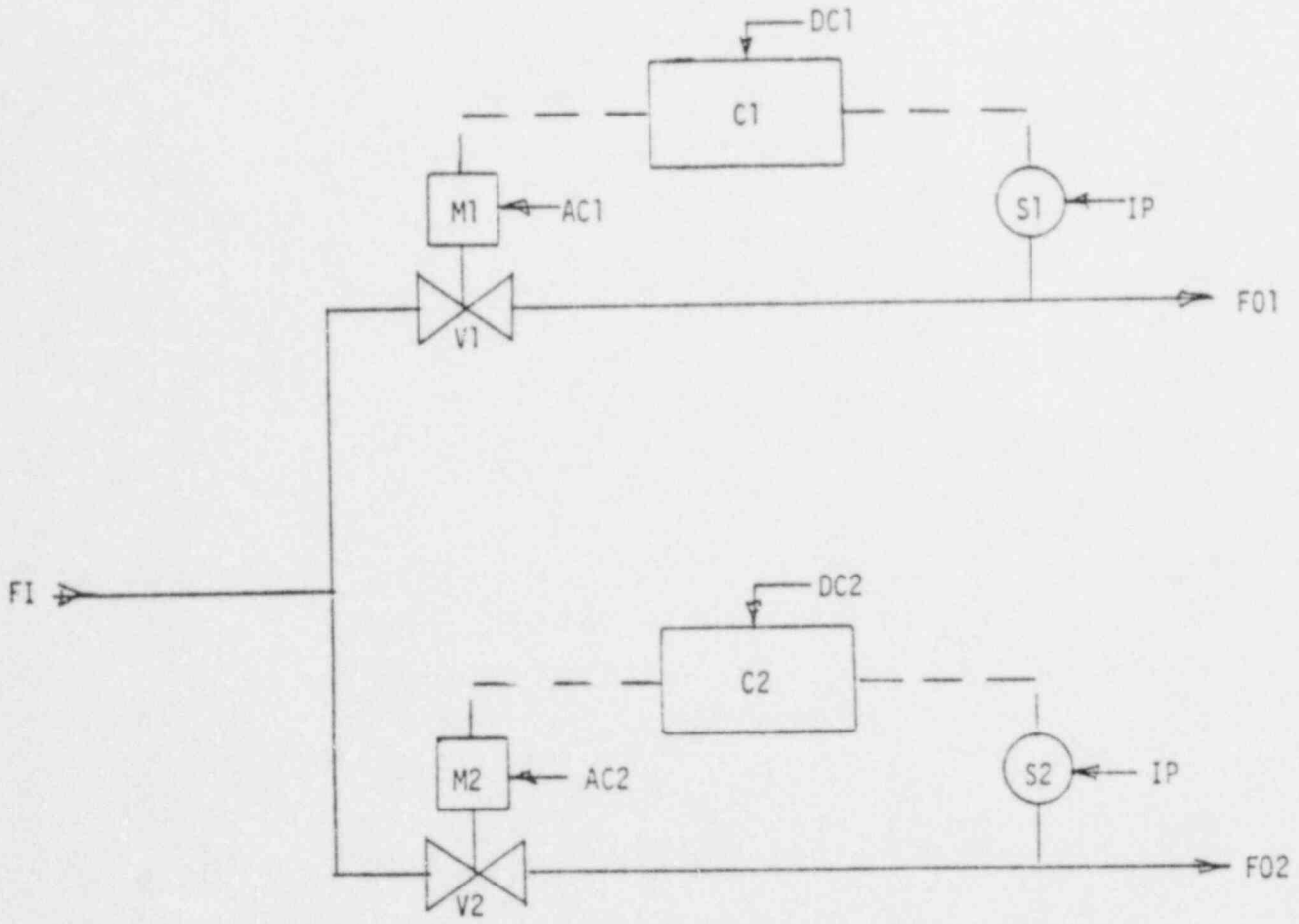
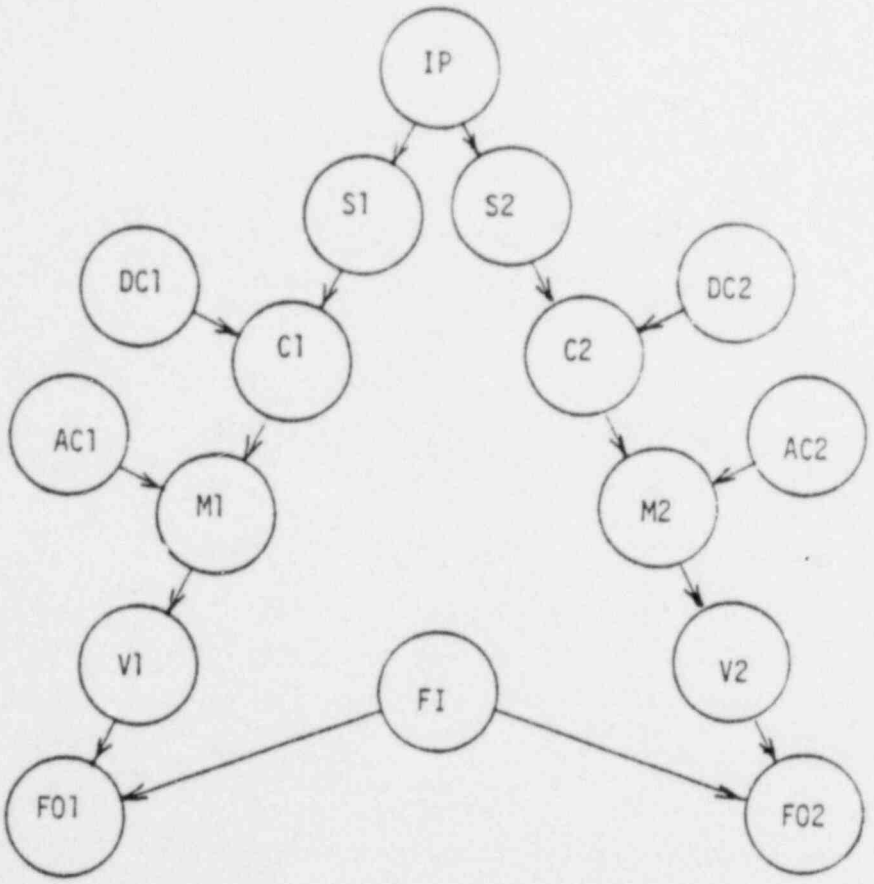


FIGURE A.1 Sample Flow Circuit with Common Power (IP)



	FI	AC1	DC1	IP	AC2	CD2	V1	M1	C1	S1	V2	M2	C2	S2	FO1	FO2
FI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AC1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DC1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AC2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DC2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V1	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0
M1	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0
C1	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0
S1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
V2	0	0	0	1	1	1	0	0	0	0	0	1	1	1	0	0
M2	0	0	0	1	1	1	0	0	0	0	0	0	1	1	0	0
C2	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0
S2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
FO1	1	1	1	1	0	0	1	1	1	1	0	0	0	0	0	0
FO2	1	0	0	1	1	1	0	0	0	0	1	1	1	1	0	0

FIGURE A.2 Digraph and Binary Matrix for Flow Circuit Showing Linkage Through IP

A.2 Quantitative Methods

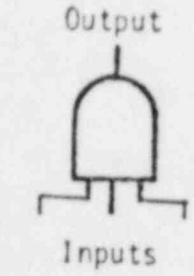
Nine methods are discussed: fault trees, phased mission analysis, event trees, cause-consequence diagrams, GO methodology, Markov modelling, generic analysis, weighting factors, and Marshall-Olkin specialization. With the possible exception of certain weighting factor methods, the remainder tend to be rather formal techniques. Most possess qualitative capabilities also; but, as was previously mentioned, they have been categorized as quantitative because they possess significant capability for such analysis.

A.2.1 Fault Trees[2,5,6,7,26]

Fault tree analysis is a deductive logic technique which diagrammatically models the various combination of basic failure events which contribute to some overall failure event. A fault tree begins at the TOP with the definition of this ultimate failure event, which is expanded downward through subsequent levels of contributing failures until the desired level of basic failure events has been reached. These contributory failures are combined by logical AND and OR gates at the appropriate levels. Fault trees are normally used to model events having binary failure states (total failure vs. total success), as opposed to those having partial failures. The symbols used in fault trees are shown in Figures A.3 and A.4.

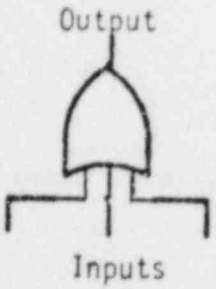
The means by which the TOP event can occur are known as "cut sets," the combination of basic events leading to the TOP. Of particular importance, especially in evaluating failure probabilities associated with the TOP event, is the concept of a minimal cut set - one in which return of any one of the basic failure events to a success mode precludes the occurrence of the TOP event. By assigning probabilities to the basic failure events, the probability of the TOP event can be found as the Boolean sum of the probabilities for each of the minimal cut sets.

Fault trees are often used to model system failure in terms of failure of its basic components. Component malfunctions are divided into two types: failures and faults. Failures are malfunctions which require repair (or replacement) of the component to correct the malfunction. Faults are malfunctions that can be corrected without maintenance of the component in question. Repair refers to the reversal of a basic event state from failed to unfailed. For example, an electrical short due to defective wiring would be considered a failure, while one due to moisture presence would be a fault (since removal of the moisture would presumably remove the short). Replacing the defective wires or removing the moisture would constitute repair. Both failures and faults can be designated as primary or secondary. A primary malfunction is one in which the component itself is responsible (such as a switch sticking closed). A secondary malfunction is one



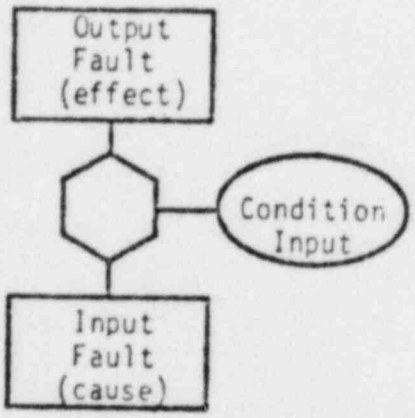
AND Gates

Coexistence of all inputs required to produce output.



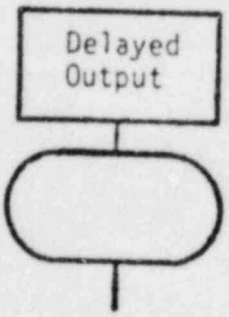
OR Gates

Output will exist if at least one input is present.



INHIBIT Gates

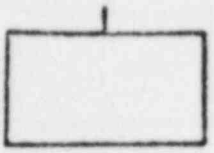
Input produces output directly when conditional input is satisfied.



DELAY Gates

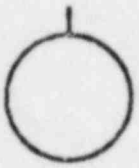
Output occurs after specified delay time has elapsed.

FIGURE A.3(10) Fault Tree Logic Symbols



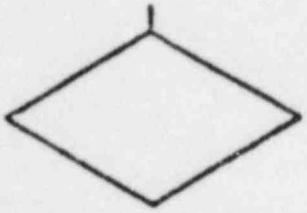
RECTANGLE

A Fault Event resulting from the combination of more basic faults acting through logic gates.



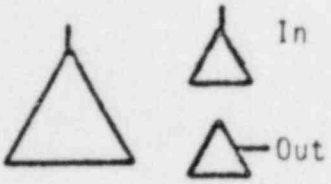
CIRCLE

A basic component fault - an independent event.



DIAMOND

A Fault Event not developed to its cause.



TRIANGLE

A connecting or transfer symbol.

HOUSE

An event that is normally expected to occur or to never occur. Also useful as a "trigger event" for logic structure change within the fault tree.

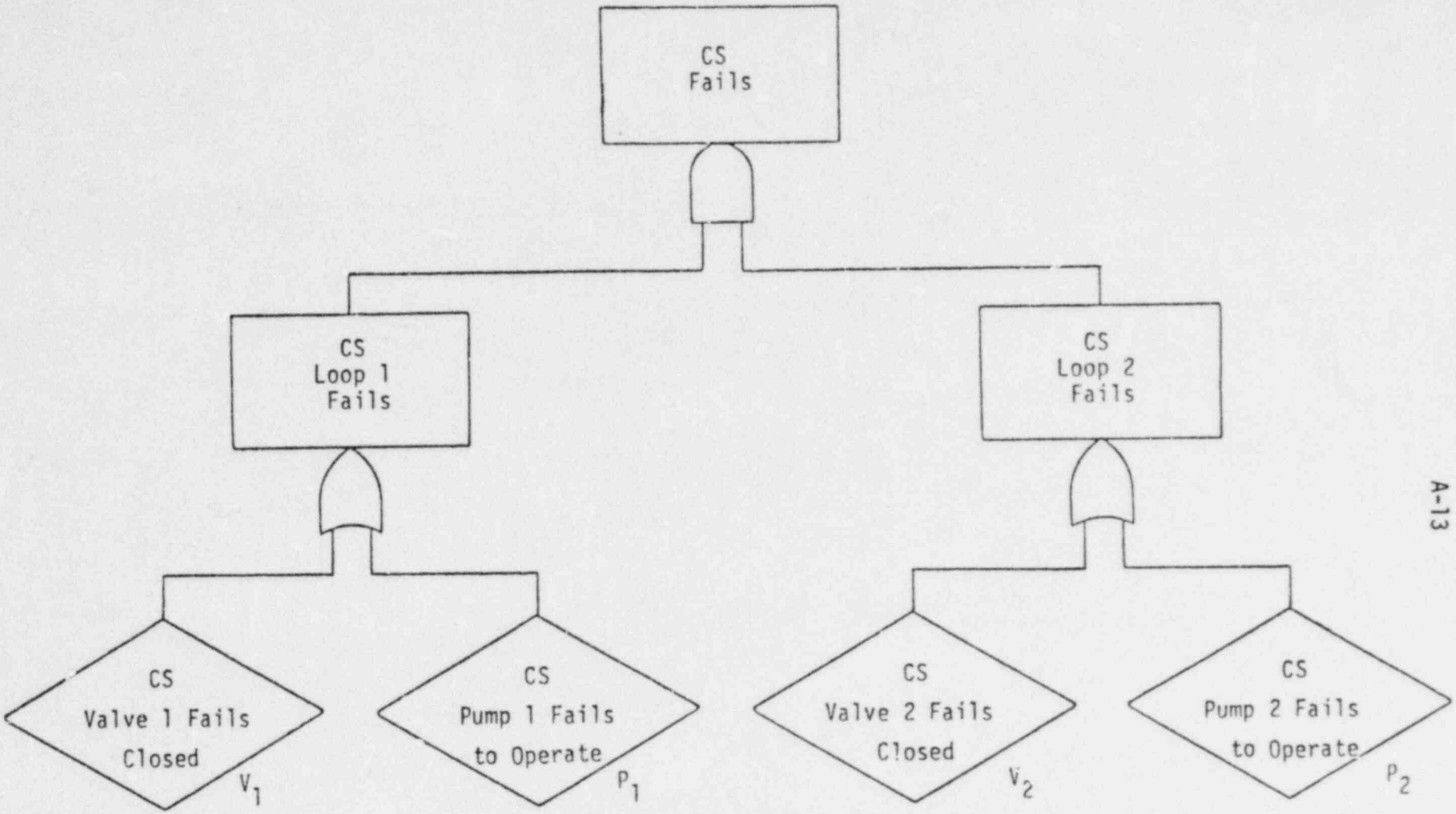
FIGURE A.4[10] Fault Tree Event Symbols

in which the component is not held accountable (such as a switch being welded closed). A special type of secondary fault is a "command" fault, in which the component functions properly immediately upon repair of the causes of the secondary fault. An illustrative fault tree for system failure is shown in Figure A.5.

Although traditionally used to model system failures, fault trees can also be used to model accident sequences, where the TOP event becomes some consequence of those sequences. Usually, this involves combining several system fault trees which contribute to the overall consequence. When a consequence fault tree is constructed for each of the various consequences of the accident sequences, the complete analysis is equivalent to a complete event tree analysis (with conditional fault trees) covering all initiating events, or a corresponding cause-consequence analysis. To illustrate a consequence fault tree, consider the operating sequence of emergency safety systems following a small LOCA shown in Figure A.6 as a block diagram. The equivalent consequence fault tree for core damage is shown in Figure A.7.

Dependencies often exist among different components within a system. Failure of one component, such as a pump, may increase the load on another, thereby increasing its likelihood of failure. Or, two components, each requiring support from some other component or system, can fail simultaneously if that support fails. Such dependencies can be incorporated directly onto a fault tree by further resolving the basic failures subject to a common failure into an independent component failure and the common failure.

Consider the fault tree for Core Spray (CS) failure in Fig. A.5. Suppose the pumps each receive electric power from the same power bus, whose failure is denoted as B in Figure A.8. (Note that this is not a representative case, but rather has been selected only for illustration.) Should this bus fail, both pumps will fail due to the common failure, thereby failing both loops and CS. Thus, the redundancy of the two loops has been circumvented. This is represented by creation of a new, single-event (B) minimal cut set derived from the fault tree by resolving former basic events P_1 and P_2 into independent pump failures P_1' and P_2' and a common failure B. Such a case would represent very poor design, because CS loop redundancy has been eliminated at the pump level, and is not characteristic of plant design. However, some dependencies may exist at more subtle and obscure levels and can go unaccounted for during system design.



Note: The CS system has been assumed to consist of two redundant loops, each with full capacity. Thus, only failure of both constitutes failure of CS.

Minimal Cut Sets: $\{V_1, V_2\}$, $\{V_1, P_2\}$, $\{P_1, V_2\}$, $\{P_1, P_2\}$

FIGURE A.5 Sample Fault Tree for Core Spray System

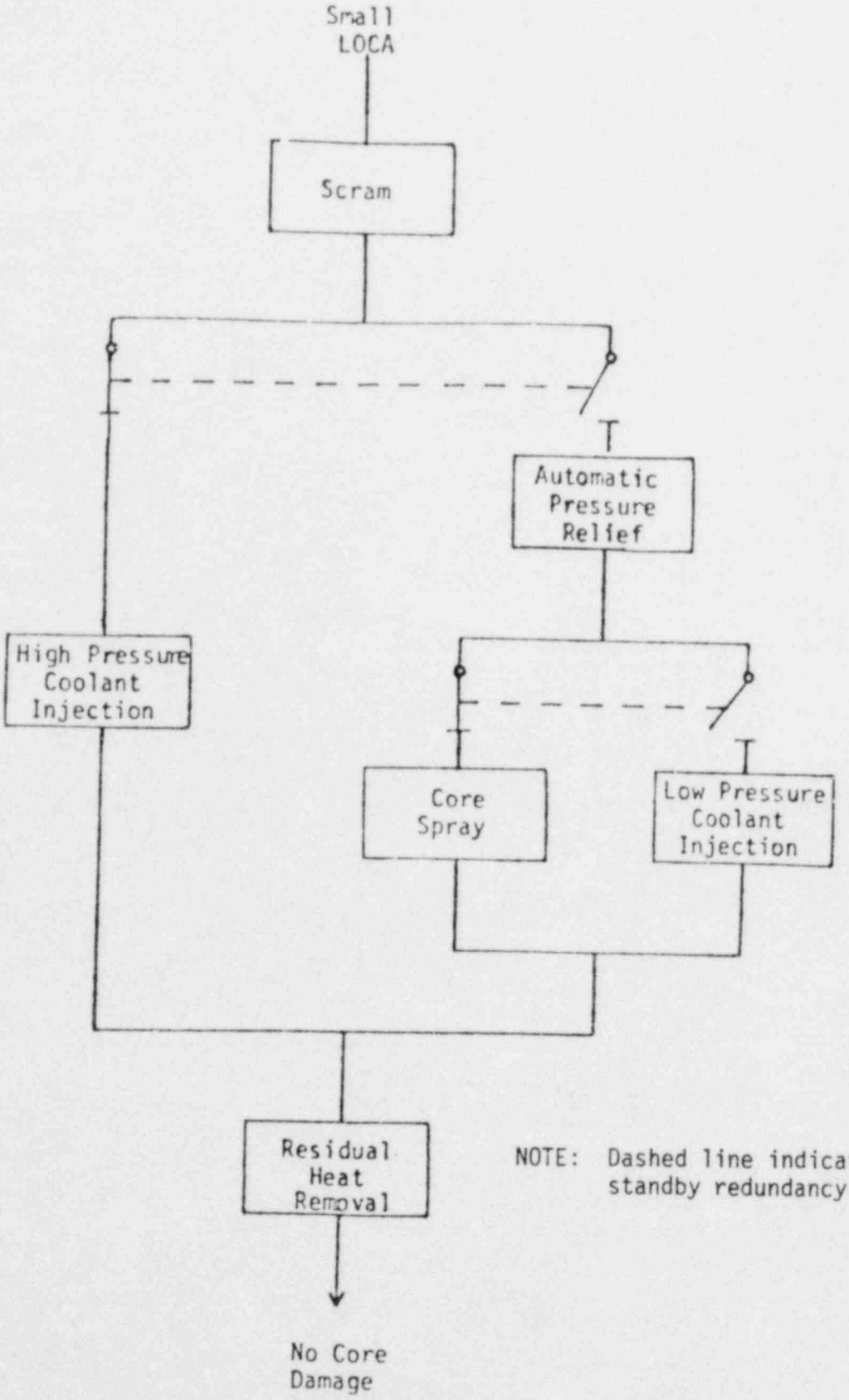


FIGURE A.6 Block Diagram Showing Operation of Emergency Safety Systems Following Small LOCA

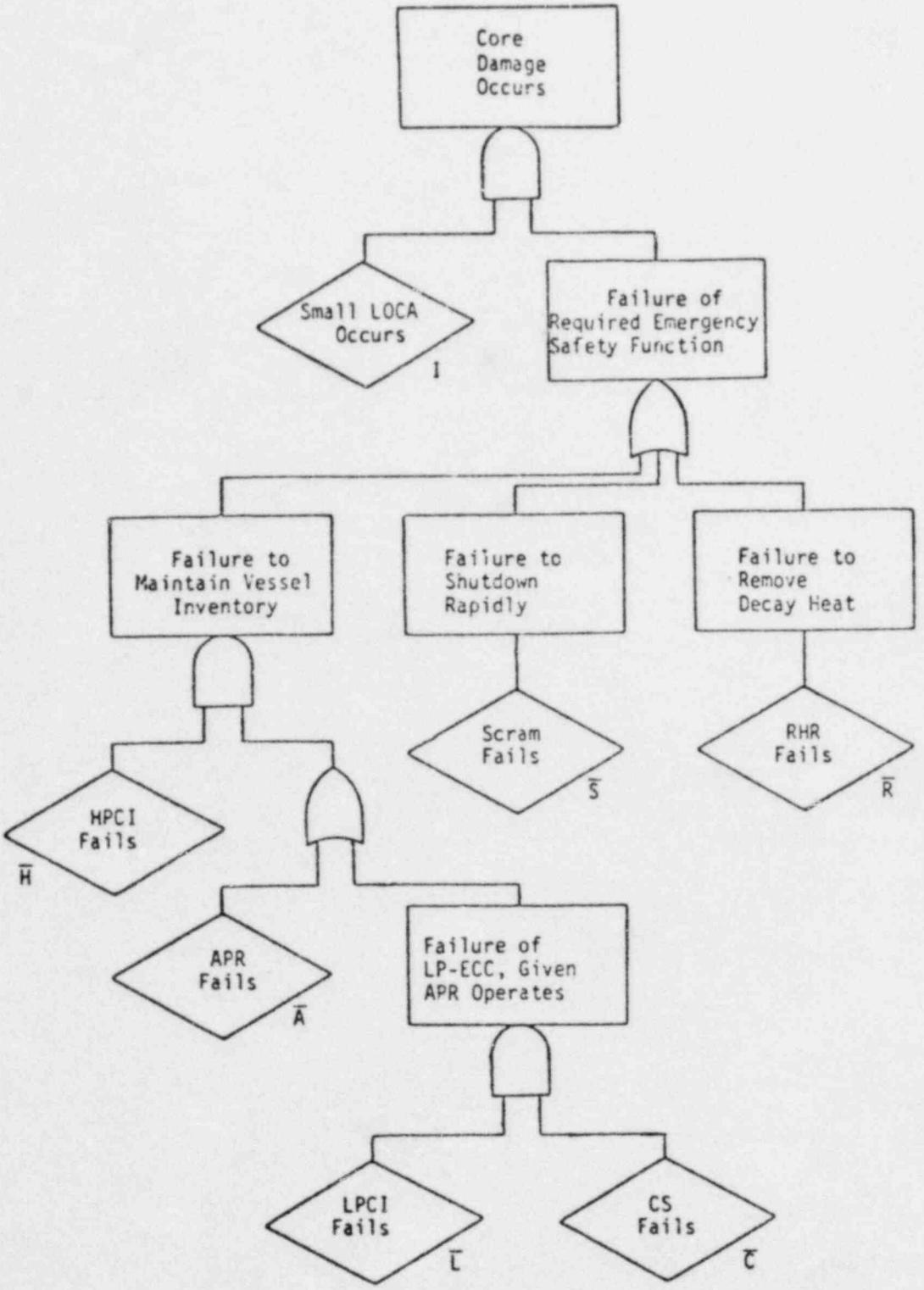
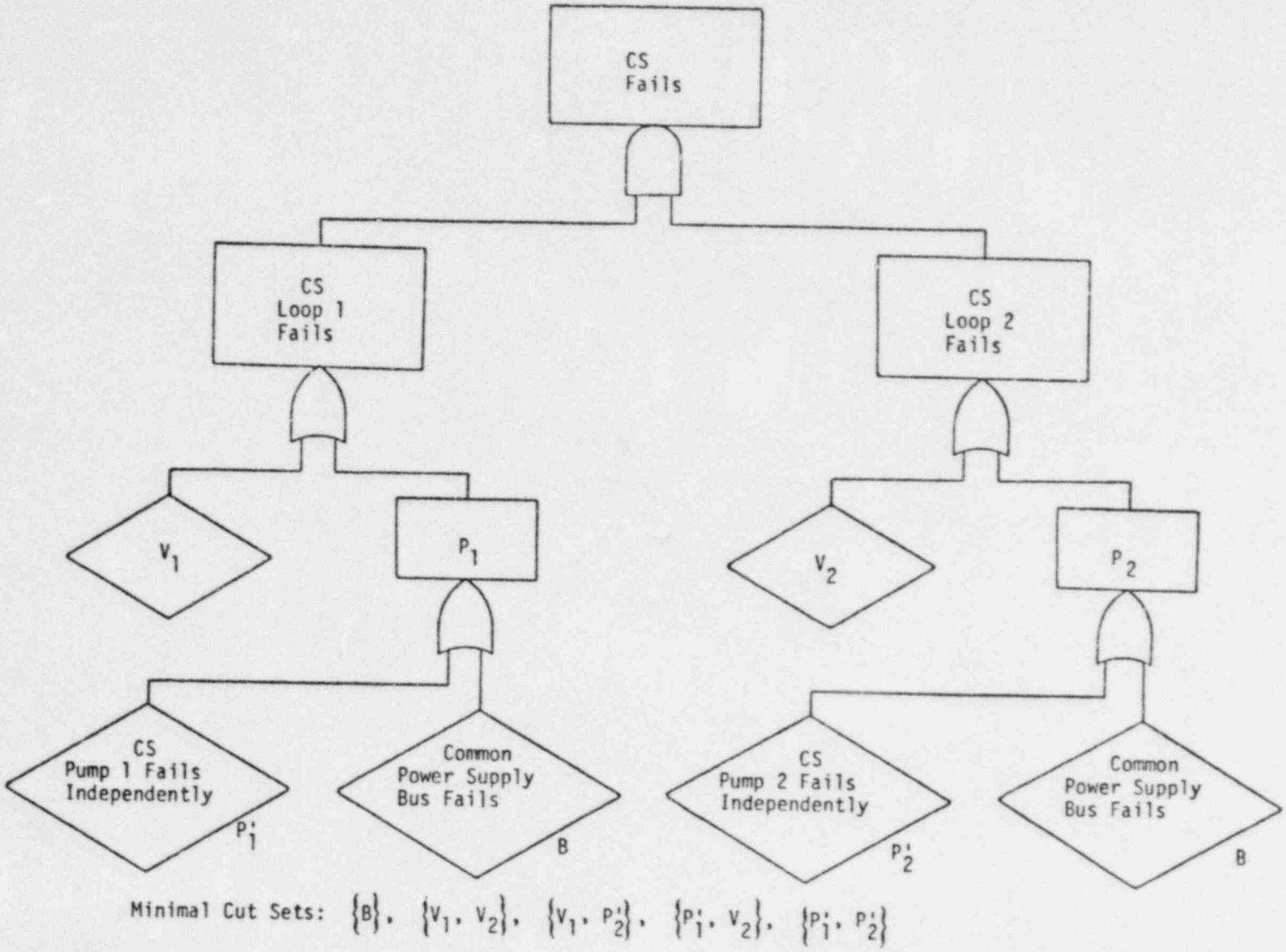


Figure A.7 Consequence Fault Tree for Core Damage due to Small LOCA Accident (reference Figure A.6)



Minimal Cut Sets: $\{B\}$, $\{V_1, V_2\}$, $\{V_1, P'_2\}$, $\{P'_1, V_2\}$, $\{P'_1, P'_2\}$

Figure A.8 Sample Fault Tree for Core Spray System with Common-Cause Failure (reference Figure A.5)

A.2.2. Phased Mission Analysis[8]

Fault trees are not particularly suited to modelling failures in a time sequence. Compensating somewhat for this is phased mission analysis. As discussed in reference 8, a phased mission is a system task during the execution of which the system is altered such that the logic model changes at specific times. In performing an overall safety function, a system may have to operate in different modes as time progresses. The goal of phased mission analysis is to reduce the original multiphase mission into an equivalent single phase one. Overall mission failure, defined as a TOP event, is represented by a fault tree, whose individual branches correspond to different system logic in each phase. By performing various logical operations, this fault tree can be simplified into one for a single phase with a single logic structure.

Phased mission analysis is applicable to a multi-function system with nonrepairable components (at least over the time span of the overall mission). By manipulation of the minimal cut sets, the multiphase mission can be reduced to an equivalent single phase one. To illustrate this, consider the primary reactor coolant (PRC) system during an ascent from low to full power operation. During low-power operation, the heat generated is lower than during full-power operation. Thus, cooling requirements are less.

For illustration purposes, consider only the PRC pumps, assuming there is just a pair. During low power, only one of them is needed. However, during full power, both are necessary. Thus, two distinct operating phases for the same system exist, and the requirements change with time. The multiphase mission fault tree is shown in Figure A.9a. Note that there are three minimal cut sets, two single-element ones and one with two elements. Through procedures involving cut-set cancellation and component transformation, this multiphase mission can be reduced to a single phase one, as shown in Figure A.9b. Note that there are now four minimal cut sets, but each one contains only a single element. The total number of basic events (4) has remained the same, but the logic structure has been simplified and the basic elements directly reflect their phase-dependence. Time dependence has been incorporated within a simplified fault tree structure.

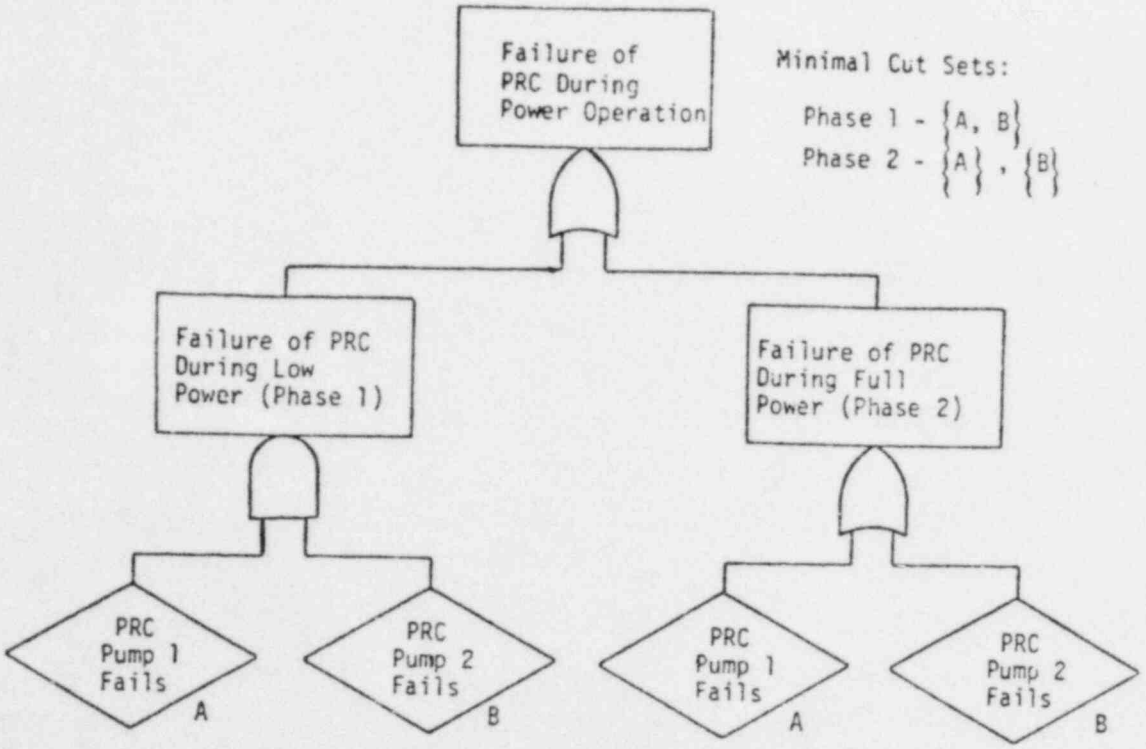


Figure A.9a Failure of Primary Reactor Coolant System During Power Operation, Shown as Multiphase Mission

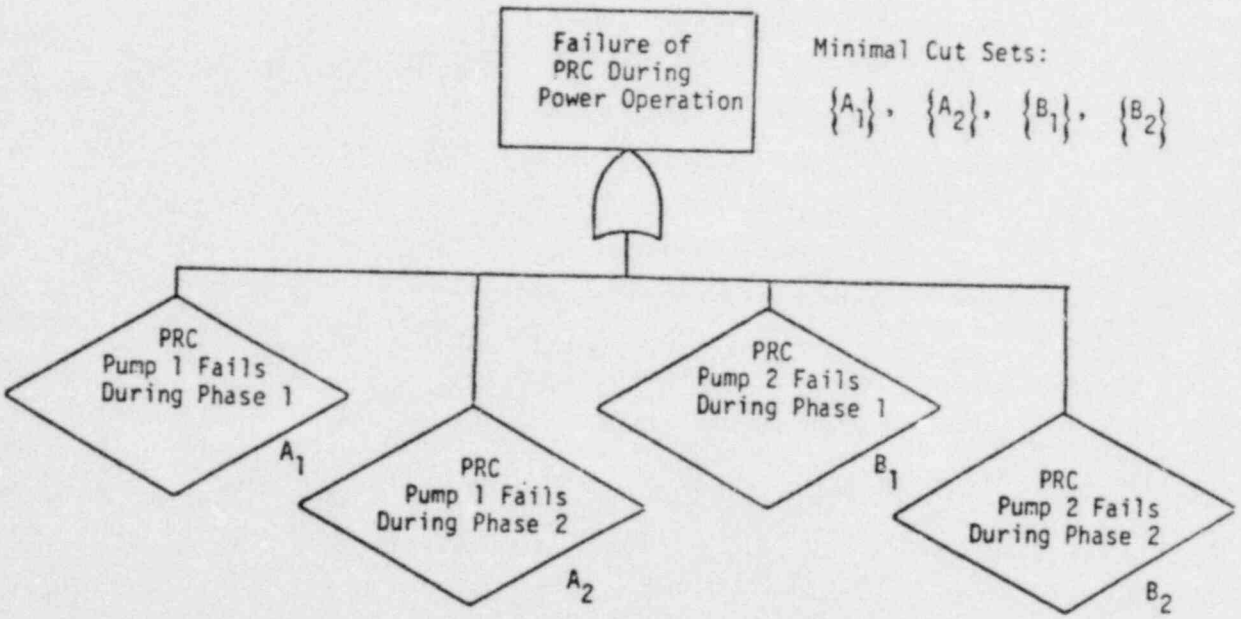


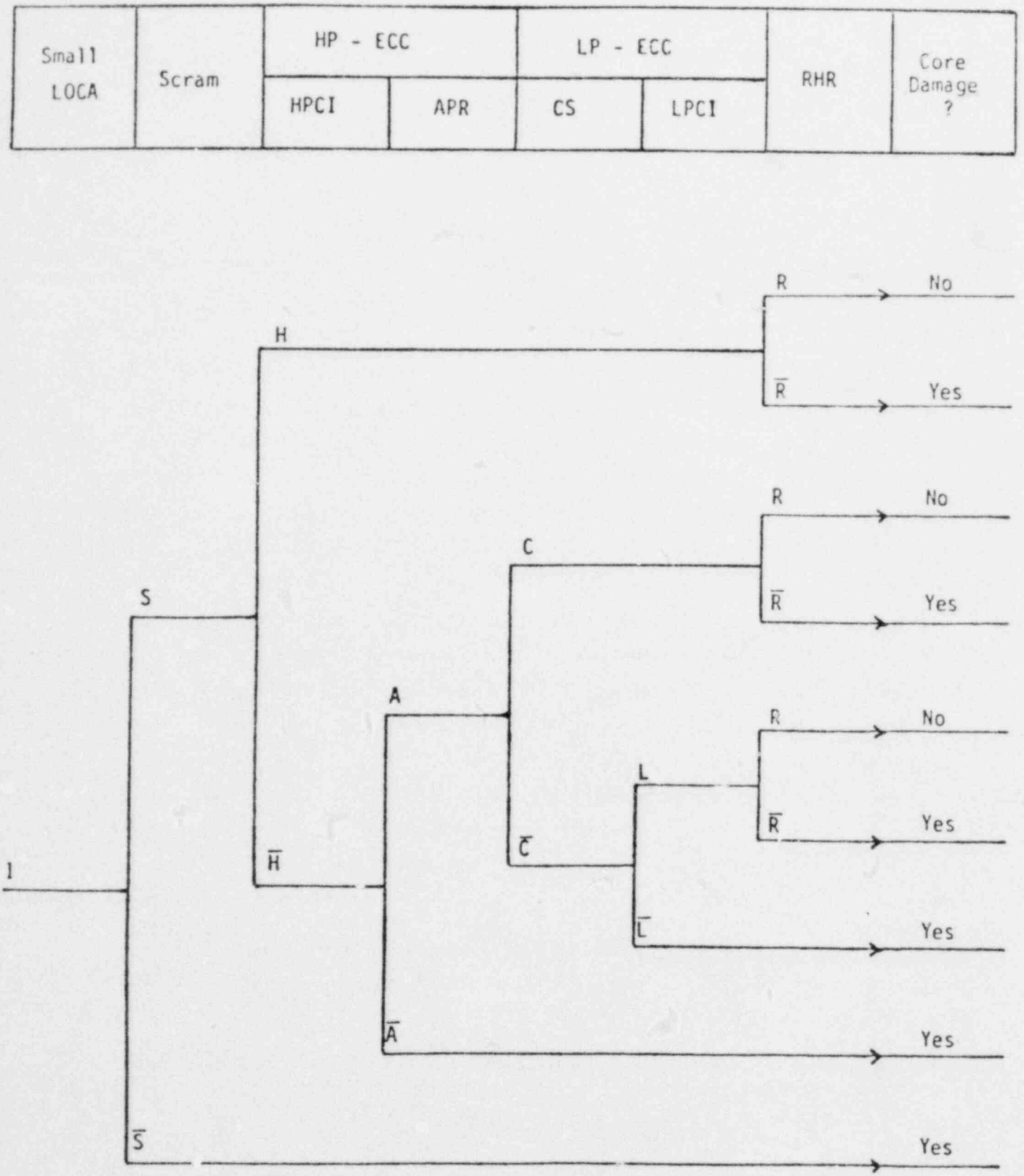
Figure A.9b Failure of Primary Reactor Coolant System During Power Operation, Shown as Single-Phase Mission

A.2.3. Event Trees

Event tree analysis is an inductive logic technique which sequentially models the progression of events, both success and failure, leading from some initiator to a series of logical outcomes. An event tree begins with some initiating failure, usually on a component level, and maps out a sequence of events, usually on the system level, to form a set of branches, each of which represents a specific accident sequence whose outcome, or consequence, corresponds directly to the events contained in the sequence. Like fault trees, event trees are normally used to model events having binary failure states, these events usually corresponding to total success or failure of a system.

Each accident sequence leading to a particular undesired consequence is somewhat analogous to a cut set on a fault tree. Whereas a cut set represents a combination of failures leading to the TOP event, an accident sequence represents a combination of sequential events (successes and/or failures) leading to a particular consequence. This suggests a possible equivalence between event trees and consequence fault trees, i.e. fault trees whose TOP events correspond to consequences of accident sequences. Complete event tree analysis requires identification of all possible and distinct initiating events and development of an event tree for each. There tends to be an extensive overlap of consequences among the various trees. Consequence fault tree analysis requires identification of all possible and distinct consequences and development of a fault tree for each. There tends to be an extensive overlap of initiating events among the various trees. The difference in reference points between event tree and consequence fault tree analysis seems to suggest that event trees are more appropriate when the initiating events are more readily identifiable, while consequence fault trees are more appropriate when the consequences can be identified more easily.

An event tree for the accident sequence depicted in Figure A.6. is shown in Fig. A.10. Note that the degree of core damage will vary from branch to branch, but this has been ignored for the sake of simplicity in illustration. Evaluation of the degree of core damage for each accident sequence would involve analysis of the physical phenomena taking place during each sequence.



NOTE: At each branching point, the upper branch denotes success, the lower failure.

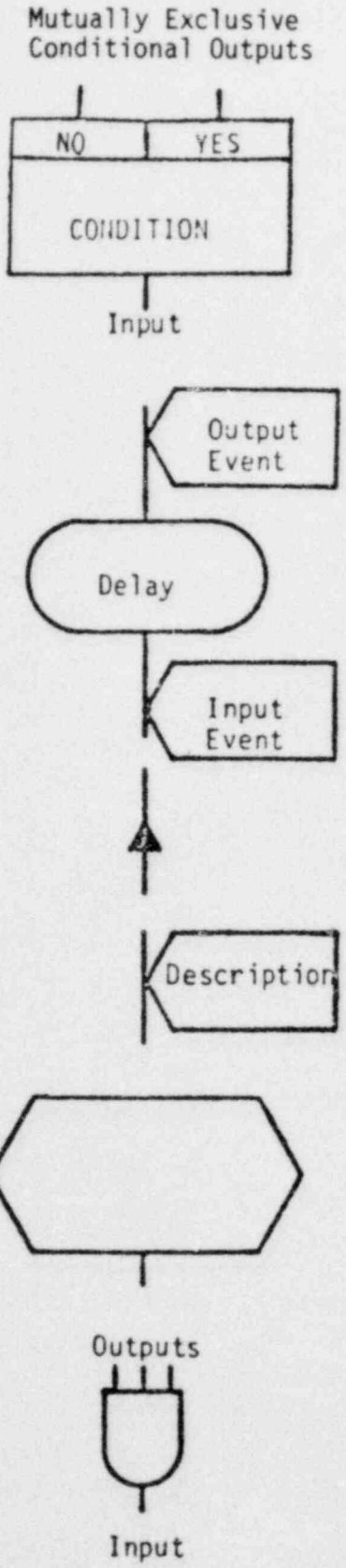
FIGURE A.10 Event Tree for Small LOCA Accident (reference Figure A.6)

Event trees, using system successes and failures as the basic events at the branching points, tend to view overall consequences to a limited degree of resolution, that being the system level. Fault trees, both those for system failures as well as for consequences, tend toward a greater degree of resolution, that being the component level. To obtain true equivalence between event trees and consequence fault trees, it is necessary to resolve the system failures on the event tree to their contributing component failures. The usual technique involves development of a system fault tree for each branching point, the events on this tree being conditional upon what has occurred earlier in the event tree sequence. The formal combination of event trees with conditional fault trees forms the basis of cause-consequence analysis and is examined in the next section.

It must be noted that, unless failure data is available on the system level, probabilistic analysis involving event trees usually necessitates resolution to the component level, where failure data may be more readily available. Due to the sequential nature of event trees, quantitative evaluation necessitates the use of conditional probabilities, those whose values reflect the occurrence or non-occurrence of preceding events. This can pose some computational difficulty when events are not independent.

A.2.4. Cause-Consequence Diagrams[9,10]

Cause-consequence analysis is a formalized combination of event tree and conditional fault tree analysis. The event tree is used to map out the sequence of events leading to the various consequences. The causes of these events, usually system failures, are modelled by conditional fault trees. Cause-consequence diagrams are basically event trees with the conditional fault trees directly attached to the branching points. The fault tree symbolism is the same, while the event tree symbolism is somewhat formalized (see Figure A.11). As with an event tree, cause-consequence diagrams begin with an initiating event except that now this event may be expanded into its contributory failures. The combination of event trees with conditional fault trees, although not formalized into cause-consequence diagrams, formed the basis of the Reactor Safety Study. For illustration, the event tree of Figure A.10 has been developed into a cause-consequence diagram in Figure A.12. Again, for simplicity, the degree of core damage has been excluded from the consequence descriptions.



BRANCHING OPERATOR

Output is "yes" if condition is met; "no" otherwise.

DELAY OPERATOR

Indicates the amount of time delay required for output event to result from the input event.

DIRECTOR

Indicates the direction of event flow.

EVENT DESCRIPTOR

Describes the event present at specified position in chart.

CONSEQUENCE DESCRIPTOR

Describes the consequence. A terminal Symbol.

Inverse AND Gate

All outputs occur if the input occurs.

FIGURE A.11[10] Symbols for Event Tree Segment of Cause-Consequence Diagram

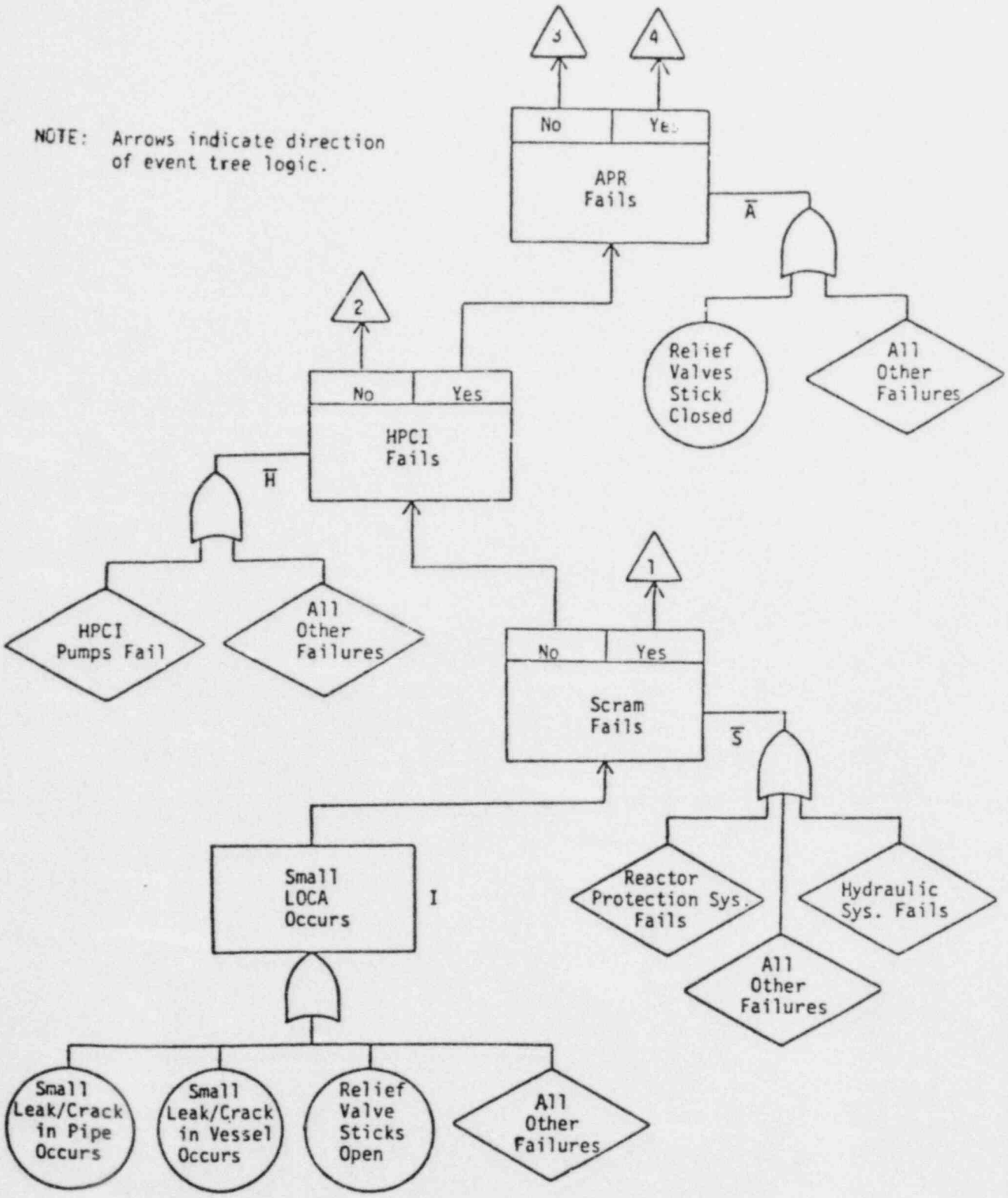


Figure A.12 Cause-Consequence Diagram for Small LOCA Accident (reference Figures A.6, A.7, & A.10)

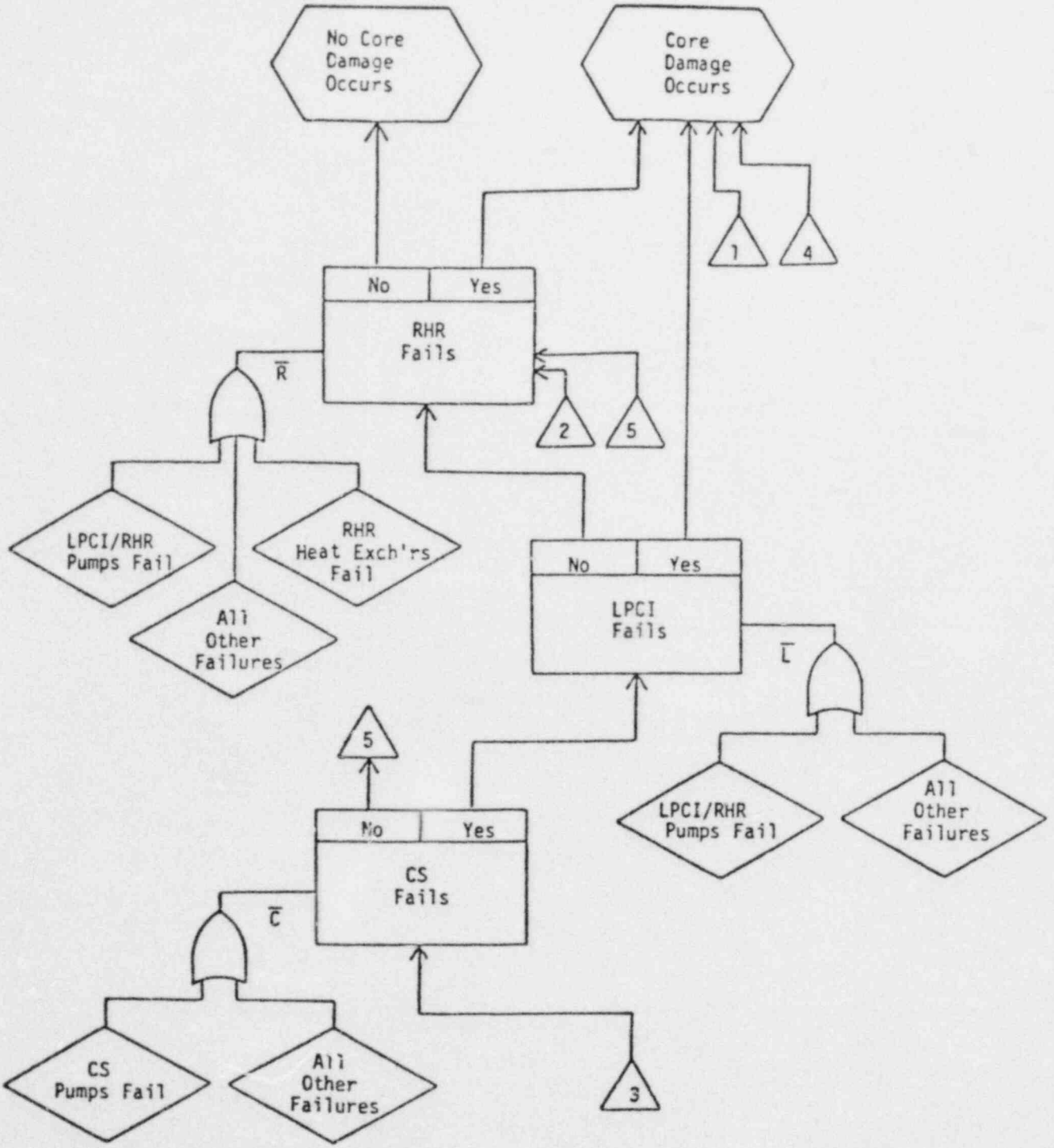


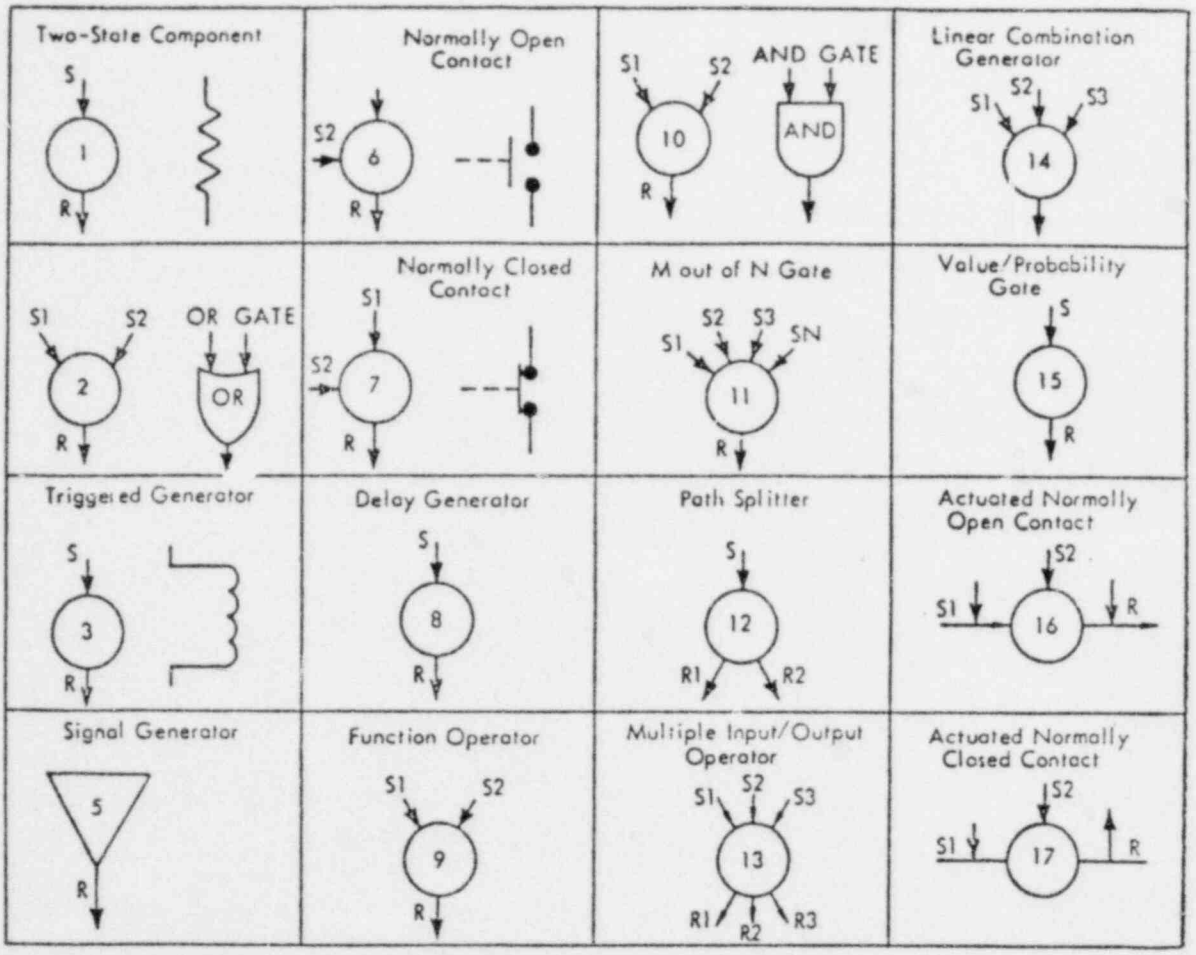
Figure A.12 (continued)

As previously mentioned, a lack of failure data on the system level will usually necessitate resolution to the component level, where such data may be available, in performance of a quantitative assessment. The cause-consequence diagram has this capability. It also is better suited to identification of potential system dependencies on the component level than is the event tree alone. However, these dependencies must be shown on separate, conditional fault trees, while the consequence fault tree is capable of including all of them within a single logic structure. Nevertheless, no matter which of these methods is used, complete analysis requires many of the individual trees, one event tree, or cause-consequence diagram, for each initiating event, or one consequence fault tree for each accident consequence.

A.2.5. GO Methodology[11]

The GO methodology is a combined simulation and logic technique which models both hardware and logic operations on an overall flow chart. It is basically a success tree approach. (A success tree is analogous to a fault tree except that success rather than failure events comprise its makeup at all levels, including the TOP.) A GO flow chart consists of "events" linked by hardware and logic operators to form some overall sequence of operation. Each "event" corresponds to the occurrence of output from a GO operator and can occur in several states, each corresponding to an occurrence time for an output. Up to 128 states are possible, with 0 representing premature or spurious operation while the highest state represents a failure to operate (operation delayed over the entire mission time). As mentioned, the GO operators correspond to both hardware, such as electrical components, and logic gates. Each is normally represented by a circle whose included numeral represents the type of operator. Figure A.13. shows some of the more commonly used GO operators.

Being essentially a logic technique with additional capability to directly assimilate hardware operation, the GO methodology possesses the capabilities of fault and event trees plus the capacity to model time-dependency through the various event states. These event states may also be used to simulate partial failures, alleviating the limitation of binary failure states prevalent in fault and event tree analyses. Although the hardware-related GO operators are designed to model components, the GO methodology can be extended beyond system operation to functions, consisting of operation of various systems, by enlarging the overall GO flow chart. Whereas cause-consequence diagrams require two logic models, event and fault trees, to accomplish this functional modelling, a GO flow chart can include this within one basic logic structure. Note that consequence fault trees also possess this capability.



Operator	Characteristic
1	Success/failure state
2, 10	Up to 10 inputs allowed
3	Initiates spurious signal
5	Initial input on flow chart
6, 7	Output only if both inputs are present
8	Adds/subtracts an integer to/from input value
9	Output determined by (S1-S2); NAND/exclusive OR gate
12	Mutually exclusive outputs
14	Output is linear combination of inputs
15	Output only if input within specified limits

Figure A.13[11] GO Operators

For illustration, a GO flow chart has been constructed in Figure A.14 to model the small LOCA accident depicted in Figure A.6. Note that some components have been included for illustration without any attempt to be complete. For simplicity, the GO operators corresponding to logic gates (numbers 2, 9, and 10 in Figure A.14) have been shown as gates rather than circles; the GO numbering convention has been maintained. For a quantitative analysis using GO, probabilities are assigned to the various event states. These may be success or failure probabilities depending upon the nature of each state. Thus, probabilities for partial failures can be accommodated without special provisions which may be necessary when attempting to adjust logic models for binary failures to handle partial failures.

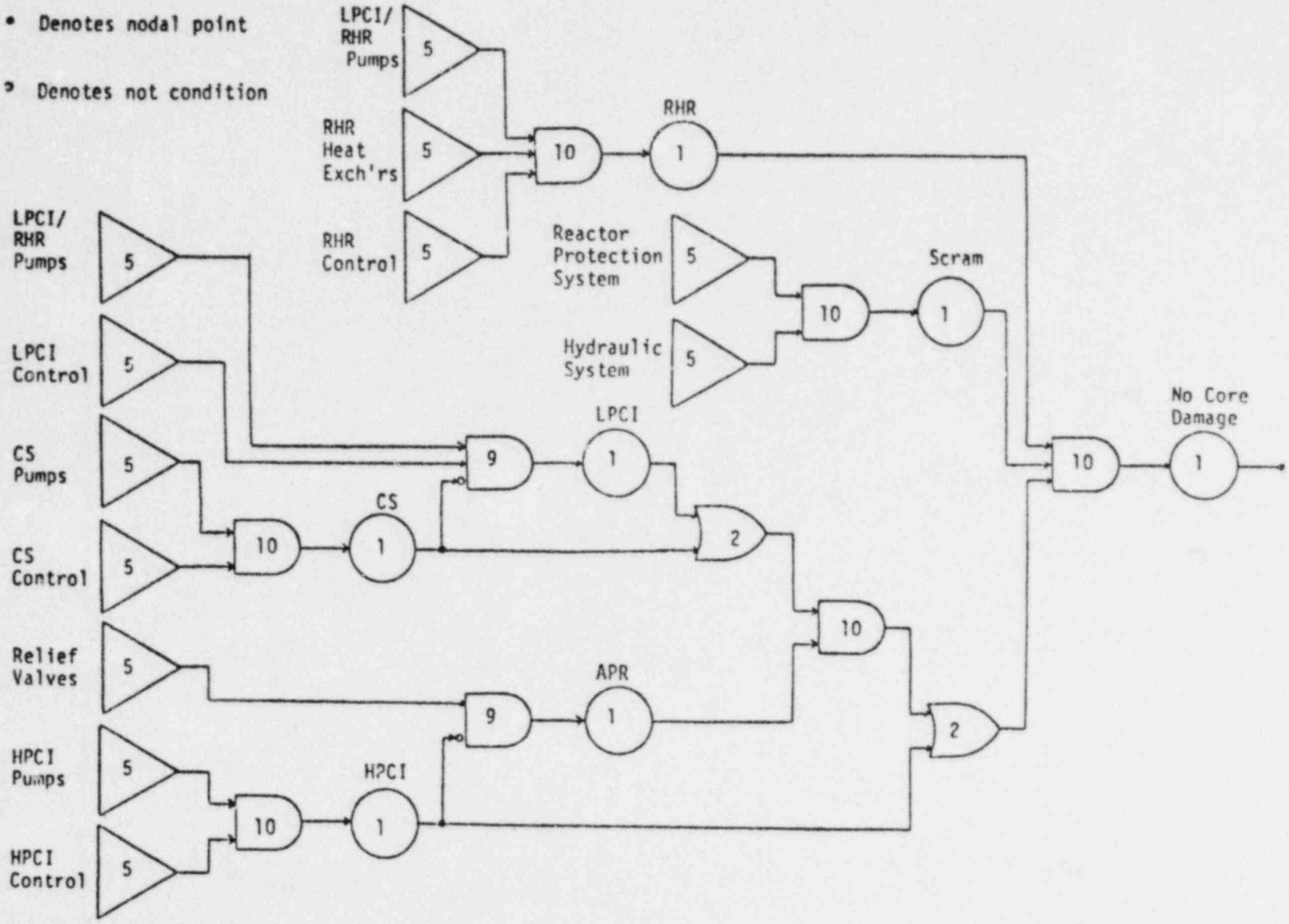


Figure A.14 GO Flow Chart for Small LOCA Accident (reference Figure A.6)

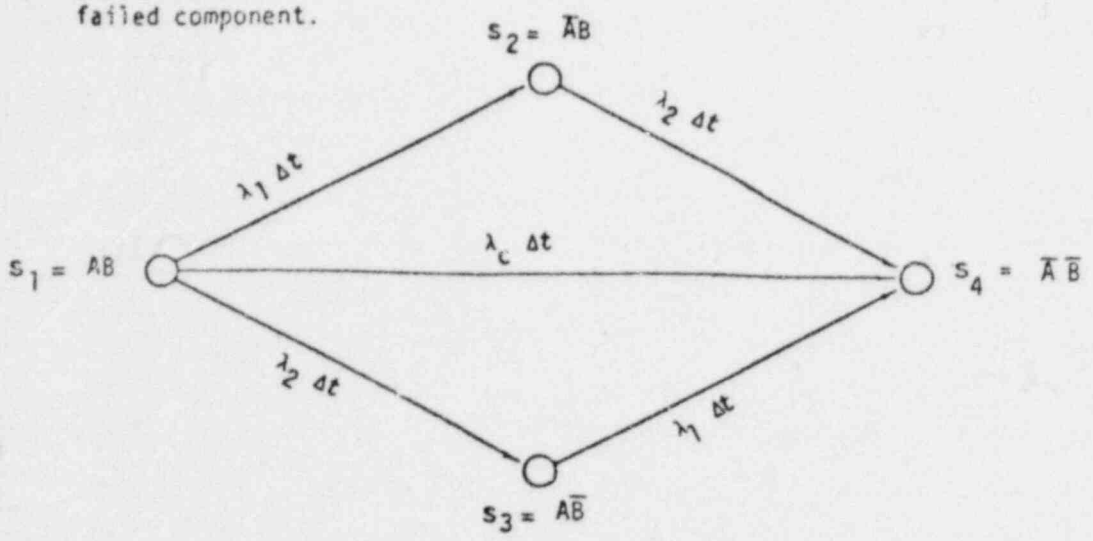
A.2.6. Markov Modelling[12,13,14,26]

Markov modelling is a mathematical inductive analysis procedure which reduces a system of many stochastic processes, effects, and paths to a single stochastic relationship characterized by a series of discrete time processes. As described in reference 26, Markov models are functions of two random variables - the state of the system, and the time of observation. Any Markov model is defined by a set of probabilities P_{ij} which define the probability of transition from any state i to any state j. Another important feature of any Markov model is that transition probability P_{ij} depends only on states i and j, and is completely independent of all past states except the last one, state i.

A Markov process can be specified by a set of differential equations and their associated initial conditions. Because of the basic Markov assumption that only the last state is involved in determining the probabilities, the analysis always yields a set of first-order differential equations. The constants in these equations can be specified by constructing a transition-probability matrix. The rows of the matrix represent the probability of being in any state i at time t, and the columns represent the probability of being in state j at time $t + \Delta t$. The former are called initial states and the latter final states. The transition probability P_{ij} is the probability that in time Δt, the system will undergo a transition from initial state i to final state j. Each P_{ii} term, on the main diagonal, is the probability that the system will remain in the same state during one transition. The sum of the P_{ij} terms in any row must be unity, since this is the sum of all possible transition probabilities. The probability that the system will be in a state i at time t is denoted by $P_i(t)$.

To illustrate Markov modelling, consider a system comprised of two components, A and B, which have binary states (total success or total failure). These could be the two PRC pumps used in the illustration of phased mission analysis in section A.2.2. As shown in Figure A.15., four system states are possible (both components operable or inoperable, or either inoperable while the other is operable). The arrows indicate the allowed transitions between states. (Note that the components have been assumed to be nonrepairable.) λ_1 and λ_2 represent the independent failure rates of components A and B respectively. λ_c represents the failure rate of both components together. Whether or not each state represents a success or failure state of the overall system depends upon the overall system logic, which must be determined external to the Markov model.

NOTE: Bar indicates failed component.



Final - State Vector		Transition-Probability Matrix		Initial-State Vector
$\begin{bmatrix} Ps_1(t+\Delta t) \\ Ps_2(t+\Delta t) \\ Ps_3(t+\Delta t) \\ Ps_4(t+\Delta t) \end{bmatrix}$	=	$\begin{bmatrix} P_{11} & P_{12} & P_{13} & P_{14} \\ P_{21} & P_{22} & P_{23} & P_{24} \\ P_{31} & P_{32} & P_{33} & P_{34} \\ P_{41} & P_{42} & P_{43} & P_{44} \end{bmatrix}$		$\begin{bmatrix} Ps_1(t) \\ Ps_2(t) \\ Ps_3(t) \\ Ps_4(t) \end{bmatrix}$

Probabilities:

Allowed Transitions → $P_{12} = P_{34} = \lambda_1 \Delta t$
$P_{13} = P_{24} = \lambda_2 \Delta t$
$P_{14} = \lambda_c \Delta t$

Disallowed Transitions → $P_{21} = P_{23} = P_{31} = P_{32} = P_{41} = P_{42} = P_{43} = 0$

Non-Transitions → $P_{ii} = 1 - \sum_{\substack{j=1 \\ j \neq i}}^{4} P_{ij}$ for $i = 1, 2, 3, 4$

Figure A.15[26] Markov Model for Two-Component States

State S_1 clearly represents a success state for the system while S_4 represents a failed state. With respect to the PRC system used to illustrate phased mission analysis (see Figure A.9a), states S_2 and S_3 represent success states during low-power operation. However, during full-power operation, they represent failed states for the system.

Markov models can be resolved to either the component or system level. When the overall states correspond to system states, the specific transitions involve changes in individual component states leading potentially to changes in system states. Similarly, transitions involving changes in individual system states potentially lead to changes in overall function states. The states dealt with in Markov models are usually binary, although the potential exists for some partial failure analysis. Transitions between states could involve individual changes from success to partially-failed modes. By its very nature, Markov modelling involves time-dependency. Time-varying probabilities can be modelled through the transition-probability matrices linking various states.

Markov modelling has the potential to quantitatively account for multiple failures due to a single common cause. Consider the example in Figure A.15. The transition from S_1 to S_4 results from dual failure of both components due to a single event, as reflected by the failure rate λ_c. If the components are the two PRC pumps, λ_c could represent failure of both due to a common event, such as loss of electric power. The Markov model can provide a convenient means for probabilistic representation of the common cause event.

A.2.7. Generic Analysis

Generic analysis involves reviewing the minimal cut sets from a fault tree or similar analysis for dependencies among the basic failure events using a standard checklist of potential linking characteristics. Subsequently, the results can be used to identify new modes of overall failure by Boolean transformation of the minimal cut sets to accommodate these dependencies. Although a major portion of this technique is qualitative, it has been included among the quantitative methods because it follows an analysis procedure such as fault trees rather than preceding it, as the other qualitative methods tend to do. Also, the Boolean transformation possesses quantitative capabilities.

Generic analysis is usually performed on the component level, as reflected by the standard checklists for dependencies. Starting from a list of basic

events from minimal cut sets, the analyst identifies common linkages among these events based on some standard checklist. One such checklist[17] identifies four major generic cause categories:

1. Mechanical/Thermal
2. Electrical/Radiation
3. Chemical/Miscellaneous
4. Other common links

These are detailed in Tables A.3 - A.6.

Sandia[18] uses another checklist, consisting of three categories:

1. Physical - electrical, mechanical, hydraulic
2. Spatial- propagation of an adverse environment through a common spatial medium
3. Inherent - common manufacturer, similar technology, equal age/wear, identical or similar components

The two checklists overlap almost totally and are representative of the types of dependencies requiring identification.

A convenient technique for cataloguing dependencies involves overlaying domains for the generic causes on a plant floor plan. This technique is especially adaptable to computer codes, such as BACFIRE.[19] As described in reference 26, given a specific generic cause, an analyst can examine a building floor plan and identify each area of the building where a single occurrence of that generic cause could affect all building components. This area is called a common location. Thus, a common location requires an area and the potential occurrence of a specific generic cause. The domain of a specific generic cause is the set of all common locations involving that generic cause. Most buildings contain barriers such as walls, floors, and cabinets. An oil spill can generally be confined to the room in which the spill occurred. Vibration from a large compressor, on the other hand, could affect every room in the building. Acid vapors can become distributed throughout several rooms by the air conditioning system. Most secondary causes have a distinct domain because boundaries containing the effects of one cause often do not contain the effects of another.

The dependencies identified for the basic events can be attached to the fault tree, as discussed in section A.2.1. and shown in Figure A.8., or incorporated into the minimal cut sets by means of a Boolean transformation of the variables for the basic events. In essence, these two techniques are equivalent, since the final

TABLE A.3[26]

MECHANICAL OR THERMAL GENERIC CAUSES

Symbol	Generic Cause	Example Sources
I	Impact	Pipe whip, water hammer, missiles, earthquakes, structural failure
V	Vibration	Machinery in motion, earthquake
P	Pressure	Explosion, out-of-tolerance system changes (pump overspeed, flow blockage)
G	Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances, crystallized boric acid from chemical control system
M	Moisture	Condensation, pipe rupture, rainwater
S	Stress	Thermal stress at welds of dissimilar metals, thermal stresses and bending moments caused by high conductivity and density of liquid sodium
T	Temperature	Fire, lightning, welding equipment, cooling system faults, electrical short circuits
F	Freezing	Liquid sodium solidifying, water freezing

TABLE A.4[26]

ELECTRICAL OR RADIATION GENERIC CAUSES

Symbol	Generic Cause	Example Sources
E	Electromagnetic interference (EMI)	Welding equipment, rotating electrical machinery, lightning, power supplies, transmission lines
R	Radiation damage	Neutron sources, charged particle radiation
M	Conducting medium	Moisture, conductive gases
V	Out-of-tolerance voltage	Power surge
I	Out-of-tolerance current	Short circuit, power surge

TABLE A.5[26]

CHEMICAL OR MISCELLANEOUS GENERIC CAUSES

Symbol	Generic Cause	Example Sources
A	Corrosion (acid)	Boric acid from neutron control system, acid used in maintenance for removing rust and cleaning
O	Corrosion (oxidation)	In a water medium or around high temperature metals (for example, filaments)
R	Other chemical reactions	Galvanic corrosion; complex interactions actions of fuel cladding, water, oxide fuel, and fission products; leaching of carbon from stainless steel by sodium
C	Carbonization	Hydrocarbon (hydraulic fluid, lubricating oils, diesel fuel) in liquid sodium
B	Biological	Poisonous gases, explosions, missiles hazards

a. Sodium-water and sodium-air reactions have been left out of the table because the resulting failure modes can be represented by other generic causes included in the other tables, e.g., temperature and biological hazards. However, the analyst, for clarity, may expand the table to include sodium reactions.

TABLE A.6[26]

COMMON LINKS RESULTING IN DEPENDENCIES AMONG COMPONENTS

Symbol	Common Link	Example Situations
E	Energy source	Common drive shaft, same power supply
C	Calibration	Misprinted calibration instructions
I	Installations	Same subcontractor or crew contractor
M	Maintenance	Incorrect procedure, inadequately trained person
O	Operator or operation	Operator disabled or overstressed, faulty operating procedures
P	Proximity	Location of all components of a cut set in one cabinet (common location exposes all of the components to many unspecified common causes)
T	Test procedure	Faulty test procedures which may affect all components normally tested together
N	Energy flow paths	Location in same hydraulic loop, location in same electrical circuit

goal is a listing of the "new" minimal cut sets, i.e., all the sets including not only independent component failures but also failures due to commonalities. For illustration, consider again the CS system whose fault tree is shown in Figure A.3. Suppose all the components have common actuation (failure of which is denoted by A), while each pair of valves and each pair of pumps receives power from a common electrical bus (failures of which are denoted by B_1 and B_2 respectively), as indicated in Table A.7. The basic events are transformed as indicated into independent failures and failures due to the commonalities. (Note that this is analogous to attaching the common failure to the fault tree, as shown in Figure A.8.). The transformed variables are substituted into the minimal cut sets to yield "new" cut sets, not necessarily minimal. Finally, these are summed in a Boolean expression for the TOP event (CS failure) to yield the "new" minimal cut sets. In the example, these "new" sets consist of three single-element ones for the commonalities and four dual-element ones for the independent component failures. This is the method advocated by Sandia,[18] who utilize the SETS[20] computer code to facilitate the Boolean algebra. Probabilistic analysis may then proceed from these "new" minimal cut sets in the same procedure as with any minimal cut sets from a fault tree or similar analysis.

A.2.8. Weighting Factors[21,22,26]

Weighting factors can be used to mathematically adjust independent failure probabilities for the presence of some common failure event. Unlike the generic approach, the emphasis is not on identifying the commonalities, although this is necessary to some degree, but rather on obtaining a quantitative estimate of the degree of dependency between two failure events. The most basic approach is to multiply the product of independent failure probabilities by a factor α (≥ 1) to obtain an estimate of the "true" failure probability, i.e. after commonalities have been accounted for. The amount by which α exceeds unity reflects the degree of dependence between the two events.

For example, the probability that both CS valves fail (from Figure A.5.) is greater than the product of their independent failure probabilities if some commonality exists between them. Using Table A.7. for illustration, the joint failure probability for both valves may be written as:

$$P(V_1 \wedge V_2) = P(V_1)P(V_2) > P(V_1')P(V_2')$$

because: $P(V_1) = P(V_1' + A + B_1) > P(V_1')$

$$P(V_2) = P(V_2' + A + B_1) > P(V_2')$$

TABLE A.7 Sample Generic Analysis & Boolean Transformation for Core Spray System Failure (reference Figure A.5)

Basic Event	Generic Commonality	
	Actuation	Power
V_1	A	B_1
V_2	A	B_1
P_1	A	B_2
P_2	A	B_2

Boolean Transformation of Basic Events:

$V_1 = V_1' + A + B_1$

$V_2 = V_2' + A + B_1$

$P_1 = P_1' + A + B_2$

$P_2 = P_2' + A + B_2$

NOTE: Prime indicates independent component failure.

Boolean Transformation of Minimal Cut Sets:

$V_1V_2 = A + B_1 + V_1'V_2'$

$V_1P_2 = A + B_1B_2 + B_1P_2' + B_2V_1' + V_1'P_2'$

$P_1V_2 = A + B_1B_2 + B_1P_1' + B_2V_2' + P_1'V_2'$

$P_1P_2 = A + B_2 + P_1'P_2'$

"New" System Failure Definition & Minimal Cut Sets:

$$\text{CS Failure} = V_1V_2 + V_1P_2 + P_1V_2 + P_1P_2$$
$$= A + B_1 + B_2 + V_1'V_2' + V_1'P_2' + P_1'V_2' + P_1'P_2'$$

where each term represents a "new" minimal cut set

therefore: $P(V_1 \wedge V_2) = P(V_1')P(V_2')\alpha$

where: $\alpha > 1$

The value of α must be determined by the analyst. This is the key to accurate representation of dependencies using this weighting scheme. His choice of method for evaluating α will depend upon the qualitative and quantitative information available to him. He may use a fault tree-generic analysis approach if he has sufficient detail or may merely make a subjective estimate of α based on expert opinion.

While the α-factor method is general enough to be applied at the system as well as the component level, a somewhat more specific approach is particularly appropriate on the component level. Two types of dependencies are identified:

1. Multiple failures attributable to a single cause
2. Subsequent failures resulting from preceding ones

For example, two pumps, each of 50% capacity during normal operation but capable of 100% for a limited time during emergency operation, are powered from the same electrical bus. Failure of that bus will fail both pumps--multiple failures due to a single cause. If one pump fails independently, the other must operate at the increased load. If forced to do so beyond a certain time period, it too could fail--a subsequent failure resulting from a preceding one.

As discussed in reference 26, when multiple component failures can be traced to a single event, such as an external event or the design of the system itself, the fraction of the component failures is represented by β. The use of the β-fraction is illustrated by Figures A.16 and A.17. Figure A.16 is a success block diagram for a one-out-of-two system, where r denotes component reliability. The failure rate λ in Figure A.16 is assumed to be constant, a consequence of the simple assumption that equipment failure is random and therefore governed by the exponential distribution.

The failure rate λ can be divided into two mutually exclusive elements: independent failure (with failure rate λ_1) and common-cause failure (with failure rate λ_2). Thus:

$$\lambda = \lambda_1 + \lambda_2$$

The fraction of common-cause failures (β) is defined as:

$$\beta = \frac{\lambda_2}{\lambda}$$

where:

β = the conditional probability that a common-cause failure occurs, given that an equipment failure has occurred.

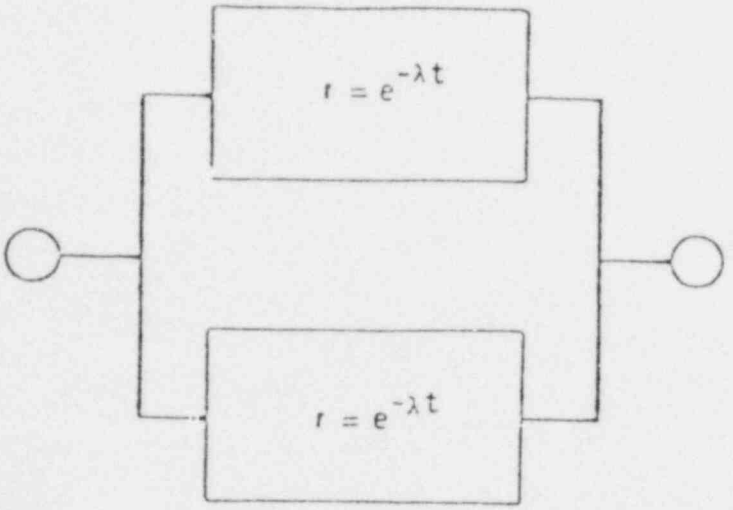


FIGURE A.16[26] Independent Failure Model for One-out-of-Two System

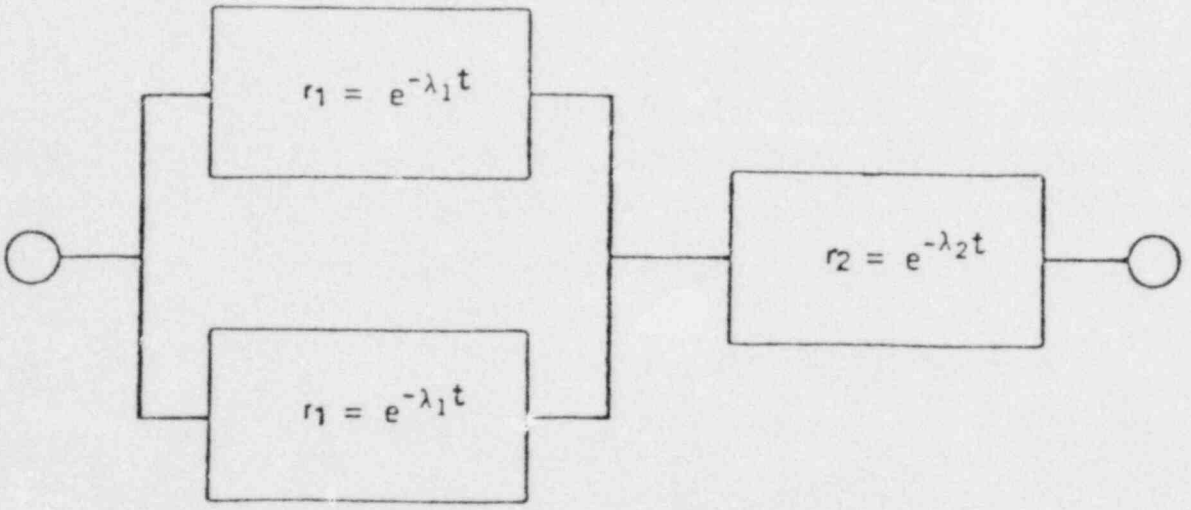
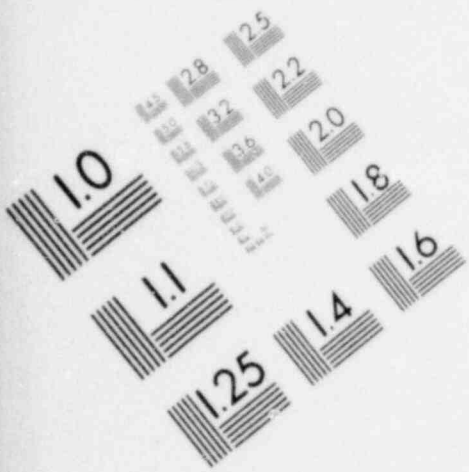


FIGURE A.17[26] Common-Cause Failure Model for One-out-of-Two System

IMAGE EVALUATION TEST TARGET (MT-3)

6″



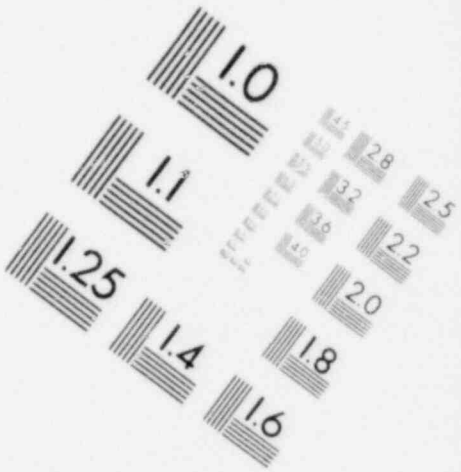
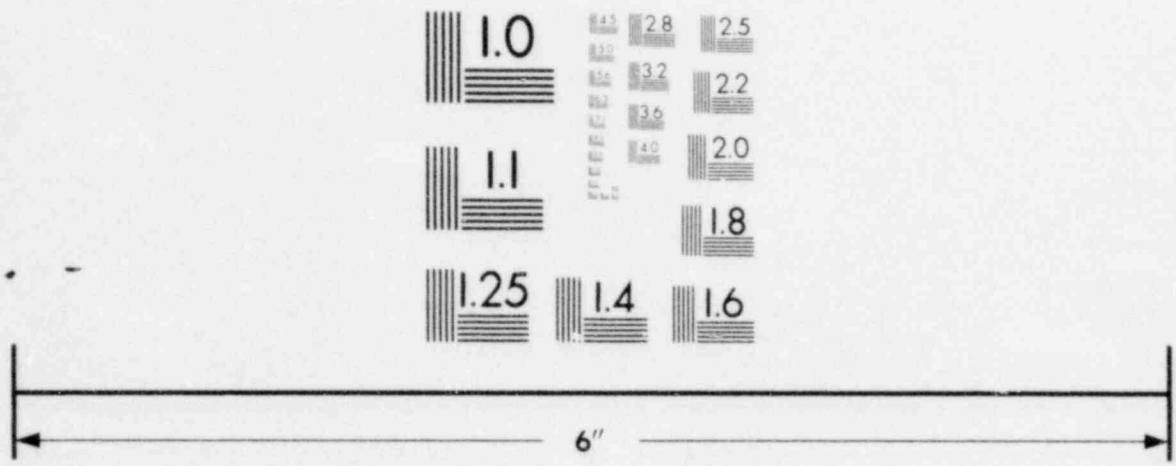
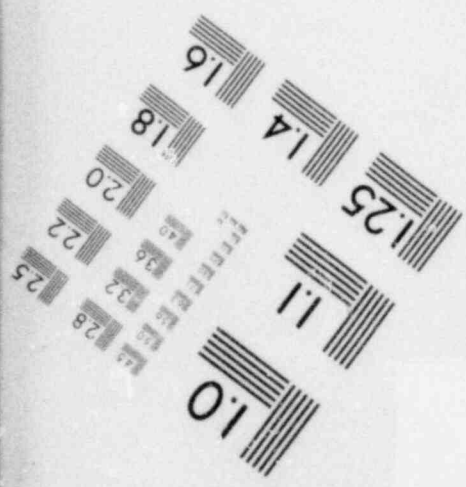


IMAGE EVALUATION TEST TARGET (MT-3)





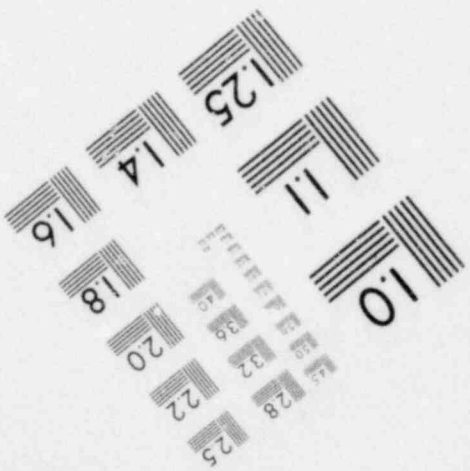


Figure A.17 depicts independent failure and common-cause failure as three independent "components." Implicit in Figure A.17 is that, when a common-cause failure occurs, all redundant units are failed with probability one. This is the extreme case of common-cause failure with complete coupling between the random variables representing time to failure for each redundant unit. Any error due to this assumption will lead to a pessimistic reliability prediction in contrast to the optimistic predictions associated with the assumption of independent failures.

The second type of dependency is causal failure, in which an equipment failure originates independently, but propagates, resulting in additional equipment failures. It is important to consider causal failures as originating only from independent failures and not from common-cause ones. Although a common-cause failure could conceivably damage additional equipment, system failure has already occurred and care must be taken to avoid double accounting of system failure modes. A category for causal failures is formed by leaving the definition of common-cause failures the same, and breaking up independent failures into two subcategories:

1. Isolated = a failure that is completely independent and does not propagate into additional failures (failure rate = λ_{1a})
2. Causal = a failure that originates as an independent failure but propagates, resulting in additional failures (failure rate = λ_{1b})

As in the previous case:

Common-Cause = an occurrence of multiple failures, where the failures are caused by a single common event (failure rate = λ_2)

The fraction of causal failures is represented by γ and defined as follows:

$$\gamma = \frac{\lambda_{1b}}{\lambda_{1a} + \lambda_{1b}}$$

where

γ = the probability that a unit will initiate a causal failure, given that it has failed, and given that the failure is not common-cause.

The β-factor method can be extended to the system level to treat intersystem dependencies. If two systems, with independent failure rates λ_{i1} and λ_{i2}, have a dependency, with failure rate λ_d, their overall failure rates (λ_{S1} and λ_{S2}) may be written as:

$$\lambda_{S1} = \lambda_{i1} + \lambda_d$$

$$\lambda_{S2} = \lambda_{i2} + \lambda_d$$

The intersystem β's become:

$$\beta_{S1} = \lambda_d/\lambda_{S1}$$

$$\beta_{S2} = \lambda_d/\lambda_{S2}$$

The β factor accounts for a large class of failure causes without explicitly identifying them.

As with the α-factor method, the β-γ-factor method also requires that the analyst determine β and γ. However, because the mathematical formulation in this method is more structured than in the α-factor method, less subjectivity need be used in the case where appropriate failure data is available.

A.2.9. Marshall-Olkin Specialization[23,24,26]

Marshall-Olkin specialization is a mathematical technique for adjusting a multiple failure rate for some dependency among the failure events. It is based on the Marshall Olkin multivariate exponential distribution and has been developed for the component level. For illustration, consider a three-component system, as discussed in reference 26. If a shock hits the system, seven ways exist for the components to fail:

(1), (2), (3), (1,2), (1,3), (2,3), or (1,2,3).

The failure of a single component represents independent failure, while failure of two or more components due to the shock represents failure due to a common cause. Each set can have its own failure rate and is assumed to be independent of the others.

Let $\underline{x}$ denote the vector, or set, of component failures, of which there are seven distinct ones, each corresponding to one of the failure groupings previously identified. The Marshall-Olkin model is specialized by assuming that $\lambda_{\underline{x}}$, the failure rate associated with the cause producing $\underline{x}$, depends only on the number of components failed. Therefore $\lambda_{\underline{x}} = \lambda_x$ where x is the total number of components failed by the cause. The assumption $\lambda_{\underline{x}} = \lambda_x$, x = 1, . . . m, implies that the components in the population are similar and are subject to similar failure causes. This specialized model is referred to as the homogeneous Marshall-Olkin model, in which common-cause failures are most likely to occur.

Within the homogeneous model, the common-cause failure rates may be independent of the failure numbers,

$$\lambda_x = \lambda, \; x \geq x_1$$

where the equality is only assumed for numbers of failures greater than or equal to some value x_1. This is referred to as the constant-rate case. The constant-rate case allows simple evaluations to be performed. The restriction upon it is the assumption that $\lambda_x = \lambda$, which involves engineering and failure cause considerations.

When the constant-rate case does not seem applicable, then another special case within the homogeneous model can be considered - the binomial-rate case. Here, the equation for λ_x is obtained by factoring the common-cause failure rate into an overall occurrence rate and a detailed effect probability. It assumes that, given a common-cause failure occurrence, each component has a constant probability of failing from the common cause. The binomial-rate case is more involved than the constant-rate case. The analyst must evaluate each component's probability of common-cause failure, unnecessary in the constant-rate case. However, it is more widely adaptable. Note that the constant-rate case is a special case within the binomial-rate model. The analyst must make the choice between the two alternatives.

To illustrate the potential applicability of the Marshall-Olkin specialization, consider an arrangement of three sensors, any two of which must provide a signal to activate an alarm. If the sensors are of similar design and are exposed to the same environment, one may make the assumption that the common-cause failure rates depend only on the number of failed sensors, not the specific ones. This forms the basis of the homogeneous model. Generally, the sensors will be subject to the same common failures, although small design or environmental variations may alter the failure thresholds from sensor to sensor. Thus, each would fail at a different rate due to common-cause, a situation for which the binomial-rate case is appropriate. If the sensors are identical in design, probably from the same manufacturer, and are exposed equally to the environment, each would have the same failure tendency due to common-cause. Thus, the common-cause failure rates would be the same whether two or three sensors fail, a situation for which the constant-rate case is appropriate.

REFERENCES

1. "Description of the Systems Interaction Program for Seismically-Induced Events, Diablo Canyon Units 1&2," Revision 2, Dockets 50-275/323; Pacific Gas & Electric Co. (7/80).

2. Lambert, H., "Systems Safety Analysis and Fault Tree Analysis", UCID-16238; LLL (10/73).

3. Recht, J., "Systems Safety Analysis: Failure Mode and Effect"; National Safety News (2/66), p. 24.

4. Jordan, W., "Failure Modes, Effects and Criticality Analyses"; Annals of Assurance Sciences, from "Proceedings - 1972 Annual Reliability and Maintainability Symposium"; (1/72), p. 30.

5. Reactor Safety Study: An Assessment of Accident Risks in Commercial Nuclear Power Plants, WASH-1400, USNRC (10/75)*

6. Smith, T., et. al., "A Risk-Based Fault Tree Analysis Method for Identification, Preliminary Evaluation, and Screening of Potential Accident Release Sequences in Nuclear Fuel Cycle Operations", BNWL-1959; Battelle Northwest (1/76)

7. "Reliability Manual for Liquid Metal Fast Breeder Reactors", SRD-75-064; General Electric Co. (12/78)

8. Burdick, G., et. al., "The Implementation of Phased Mission Techniques to Nuclear Systems Analysis". Part of "Methods for Reliability and Safety Engineering", MAP #0015; Aerojet Nuclear Corp., Idaho Falls, (6/75)

9. Nielsen, D., "The Cause-Consequence Diagram Method as a Basis for Quantitative Reliability Analysis". Presented at the ENEA/CREST Meeting on Applicability of Quantitative Reliability Analysis of Complex Systems and Nuclear Plants in Its Relation to Safety, Munich (5/71)

10. "Methods for Reliability and Safety Engineering", MAP #0015; Aerojet Nuclear Co., Idaho Falls, (6/75)

11. Gateley, W., et. al., "GO-A Computer Program for the Reliability Analysis of Complex Systems", KN-67-704; Kaman Sciences Corp., Colorado Springs (4/68)

12. Shooman, M., Probabilistic Reliability: An Engineering Approach; McGraw-Hill Book Co., Inc., New York (1968)

13. Papazoglou, I. and E. Gyftopoulos, "Markov Processes for Reliability Analyses of Large Systems", IEEE Transactions on Reliability, R-26, 3 (8/77)

14. Gokcek, O., et. al., "Markov Analyses of Nuclear Plant Failure Dependencies". Part of "Proceedings of the Annual Reliability and Maintainability Symposium", ISSN 0149-144X, Washington, D.C. (1/79)

15. Fussell, J. et. al., "A Collection of Methods for Reliability and Safety Engineering", ANCR-1273; Aerojet Nuclear Co. (4/76)

16. Cate, C., "A Method for Quantitative Evaluation of Common-Cause Failures in System Reliability Analysis", M.S. Thesis; University of Tennessee, Knoxville (8/77)

17. Rasmuson, D. et. al., "COMCAN II-A - A Computer Program for Automated Common-Cause Failure Analysis", TREE-1361; EG&G Idaho (5/79)

18. Boyd, G. et. al., "Final Report, Phase I, Systems Interaction Methodology Applications Program," NUREG/CR-1321; Sandia Laboratories (12/79)**

19. Cate, C. and J. Fussell, "BACFIRE - A Computer Code for Common-Cause Failure Analysis"; University of Tennessee, Knoxville (2/77)

20. Worrell, R. and D. Stack, "Common-Cause Analysis Using SETS", SAND-77-1832; Sandia Labs (12/77)

21. Colombo, A. and G. Volta, "Logic-Probabilistic Approaches for Nuclear Safety Assessment," EURATOM Joint Research Center Report; Ispra, Italy (10/74)

22. Fleming, K. et. al., "AIPA Risk Assessment Methodology". Part of "HTGR Accident Initiation and Progression Analysis Status Report", Vol. II, GA-A13617; General Atomics (10/75)

23. Vesely, W., "Estimating Common-Cause Failure Probabilities in Reliability and Risk Analysis: Marshall-Olkin Specializations", International Conference on Nuclear Systems Reliability Engineering and Risk Assessment, Gatlinburg, Tennessee (6/77)

24. Marshall, A. and I. Olkin, "A Multivariate Exponential Distribution," JASA 62 (1967)

25. Bertucio, R. C., Large LMFBR Shutdown Heat Removal System Reliability Trade-off Study, WARD-SR-3045-7; Westinghouse Electric Corp., Madison, Pennsylvania, 1978.

26. Rasmuson, D. et. al., "Common-Cause Failure Analysis Techniques: A Review and Comparative Evaluation", TREE-1349, EG&G Idaho (9/79)

27. Browns Ferry Nuclear Plant, Units 1, 2, and 3. Final Safety Analysis Report, DOCKET-50259; Tennessee Valley Authority, Chattanooga (9/70)

*Available free upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

**Available for purchase from the NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission, Washington, DC 20555, and the National Technical Information Service, Springfield, VA 22161.

APPENDIX B

BROWNS FERRY 3 PARTIAL FAILURE-TO-SCRAM: SYSTEMS INTERACTION ANALYSIS

The purpose of this exercise is to demonstrate the use of the proposed methodology for analyzing systems interactions by applying it to a specific example - the Browns Ferry 3 (BF3) partial failure-to-scram (6/28/80). The event is documented in other sources;[1,2] the description will not be reproduced here. The purpose of this analysis is demonstrative; it is not intended to be complete.

The proposed methodology advocates an approach from a success viewpoint. The steps in this approach are outlined in Table B-1 . The starting point is each plant safety function analyzed during each applicable plant mode. These are developed through the system, subsystem, and major component levels, which are subsequently developed through the levels of the support systems, subsystems, and major components. Throughout this development, the analyst seeks to identify systems interactions that are possible through:

1. Sequential operation, such as the requirement that systems for Core Heat Removal operate successfully during Hot Shutdown to permit the operation of others during Cold Shutdown (by lowering the primary coolant temperature to an appropriate level).
2. Component sharing, such as the LPCI/RHR pumps being used for both the LPCI and RHR systems in a BWR.

TABLE B-1.
SYSTEMS INTERACTION ANALYSIS - SUCCESS APPROACH

- For each safety function during a specific plant mode:
  - Determine system success paths
  - Identify subsystems & major components
  - Define support systems, subsystems, & major components
  - Determine systems interactions that are possible through:
    - Sequential operation of systems, subsystems, or components
    - Sharing of a subsystem or component by two or more systems
    - Support systems, subsystems, or components common to two or more systems
    - Common links among subsystems or components in two or more systems

3. Common support, such as electric power (AC and/or DC) to nearly all nuclear plant systems.
4. Common links, such as components in separate systems with electric power cables whose physical proximity could subject them to failure from a single event (such as a fire). Table B-2 lists these common links[3] and specifies elements of the review process which would lead to their identification.

The various plant safety functions are identified in Table B-3 . While it must be remembered that all of these require analysis in an overall systems interaction assessment, for the purpose of this exercise only Reactor Control has been analyzed (this being the safety function associated with the BF3 incident). The various plant operating modes[3] are listed in Table B-4 . Again, in an overall assessment each mode must be considered for each safety function. However, for the BF3 incident, only the transition from Power Operation to Hot Shutdown has been considered (for Reactor Control).

Referring back to Table B-1 , note that the safety function and the plant mode have been identified. The next step requires the determination of the system success paths. These are given in Table B-5 . Note that there are two success paths for maintaining Reactor Control during the transition from Power Operation to Hot Shutdown. The Control Rod Scram (CRS) system (at high reactor pressure) alone or the Standby Liquid Control (SLC) system, coupled with isolation of the Reactor Water Cleanup (RWC) system, leads to Reactor Control success during the transition. Also listed in Table B-5 are the major components and their required redundancies for the systems in each success path. To help visualize the systems, and to

TABLE B-2
REGULATORY REVIEW OF COMMON LINKING CHARACTERISTICS

Common Links	Review Element
• Physical	Systems Analysis
• Electrical	
• Mechanical	
• Hydraulic	
• Pneumatic	
• Spatial	Plant Walk-Through
• Thermal	
• Fluid	
• Mechanical	
• Radiation	
• Inherent	Systems Analysis
• Common Manufacturer	
• Similar Technology	
• Equal Aging or Wear	
• Shared Components	
• Human	Review of Plant Procedures & Technical Specifications
• Dynamic	
• Latent	

TABLE B-3
SAFETY FUNCTIONS

Safety Function	Purpose
• Reactor Control *	Maintain desired power level and shutdown reactor when required.
• Reactor Coolant System Inventory Control	Maintain a suitable coolant medium around the core.
• Reactor Coolant System Pressure Control	Maintain the coolant in the proper state.
• Core Heat Removal	Transfer heat from the core to the coolant.
• Reactor Coolant System Heat Removal	Remove heat from the primary system.
• Containment Isolation	Maintain containment integrity to prevent radiation releases.
• Containment Temperature and Pressure Control	Avoid potential damage to containment and vital equipment.
• Combustible Gas Control	Remove and/or redistribute hydrogen to avoid potentially damaging reactions.
• Maintenance of Vital Auxiliaries	Maintain operability of systems needed to support safety systems.
• Indirect Radioactivity Release Control	Contain miscellaneous stored radioactivity to protect the public and the environment.

* Applicable to Brown's Ferry 3 Incident

TABLE B-4. PLANT MODES

- Startup
- Power Operation*
- Hot Standby
- Hot Shutdown*
- Cold Shutdown
- Refueling

*Applicable to Browns Ferry 3 Incident.
(Transition from Power Operation to Hot Shutdown)

TABLE B-5

SUCCESS PATH WITH REQUIRED SYSTEMS & MAJOR COMPONENTS

FOR REACTOR CONTROL DURING TRANSITION FROM POWER OPERATION

TO HOT SHUTDOWN

Path #	Systems	Major Components
1	Control Rod Scram (High Pressure)*	183/185 Hydraulic Control Units, each requiring: 1/1 Diaphragm-Operated Scram Inlet Valve 1/1 Diaphragm-Operated Scram Exhaust Valve 1/1 Ball-Check (Shuttle) Valve 2/2 Three-way Solenoid Scram Pilot Valves or 2/2 Pairs of Three-way Solenoid Backup Scram Pilot Valves (1/2 required per pair) 2/2 Pairs of Scram Discharge Volumes & Diaphragm-Operated SDV Vent Valves 1/1 Scram Instrument Volume 1/1 Diaphragm-Operated SIV Drain Valve
2	Standby Liquid Control	1/1 Tank 1/2 Positive-Displacement Pumps 1/2 Explosive Valves
	Reactor Water Cleanup (Isolation only)	1/2 Motor-Operated Isolation Valves

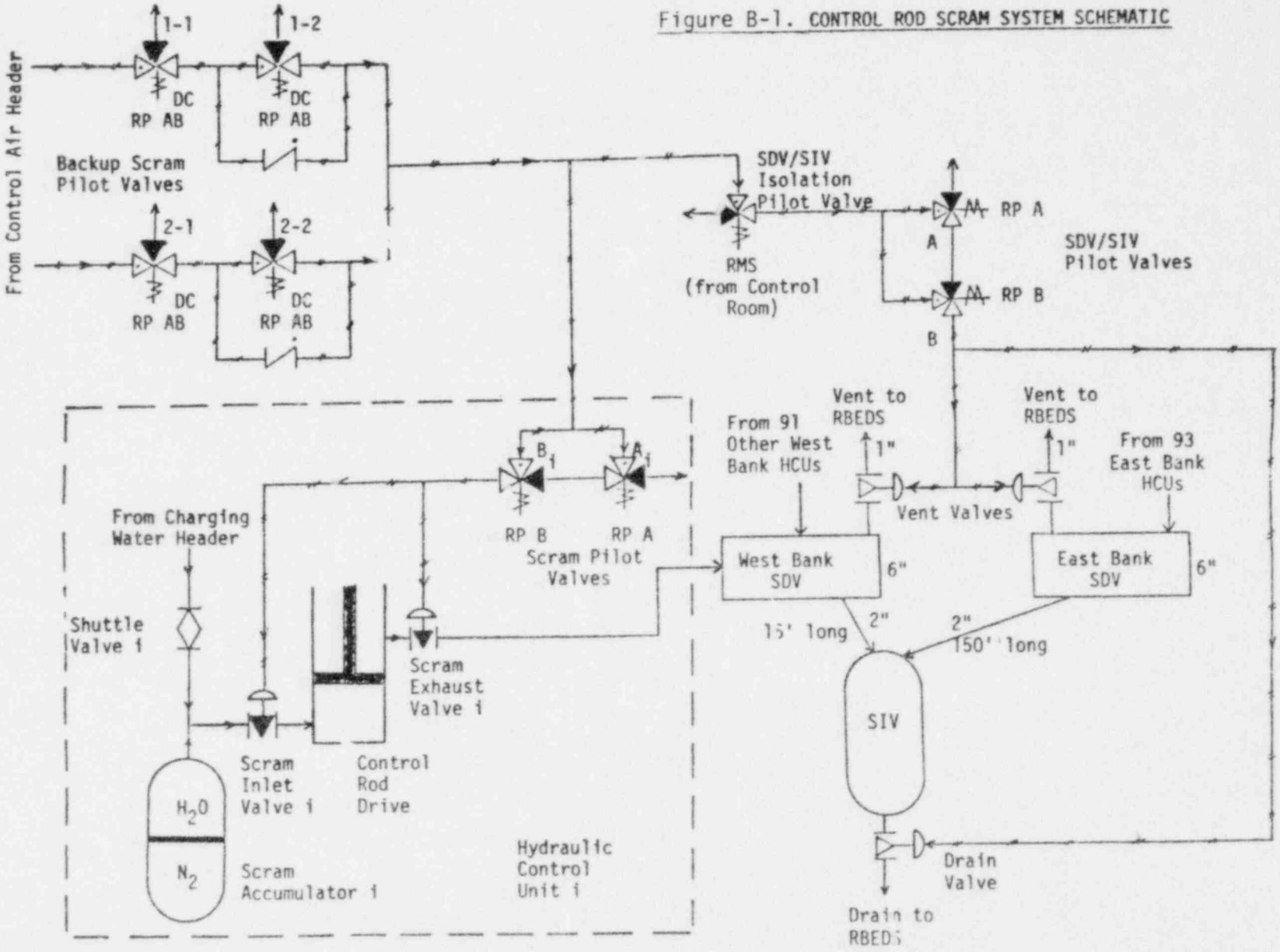
*Scram Accumulators not required at reactor operating pressure (applicable to Brown's Ferry 3 incident)

establish the nomenclature used in specifying their components, schematics of the CRS, SLC and RWC (isolation only) systems are provided in Figures B-1 and B-2 .

Having identified the major components of the main systems required for the plant safety function in the operating mode of interest, the support systems, subsystems, and major components required by these primary systems (usually through their components) are determined. The results for the BF3 example are summarized in Table B-6 . Note that there are several levels of support systems, especially with regard to electric power. Component locations, when available, have been included on the Table as an indication of the type of information needed to identify potential systems interactions due to common links (spatial, in this example). A secondary goal of this exercise is to determine the amount of information typically available from a Final Safety Analysis Report (FSAR); the information in Table B-6 reflects that available from the BF3 FSAR[4]. A plant walk-through could be used to supply additional information.

In order to procedurally determine potential systems interactions, the information in Table B-6 is developed into an overall success tree for the safety function in the plant mode of interest. The results for the BF3 example are summarized in Figures B-3 through B-12 . Note that these Figures are grouped by the level of development of the overall success tree for Reactor Control during the transition from Power Operation to Hot Shutdown as follows:

Figure B-1. CONTROL ROD SCRAM SYSTEM SCHEMATIC



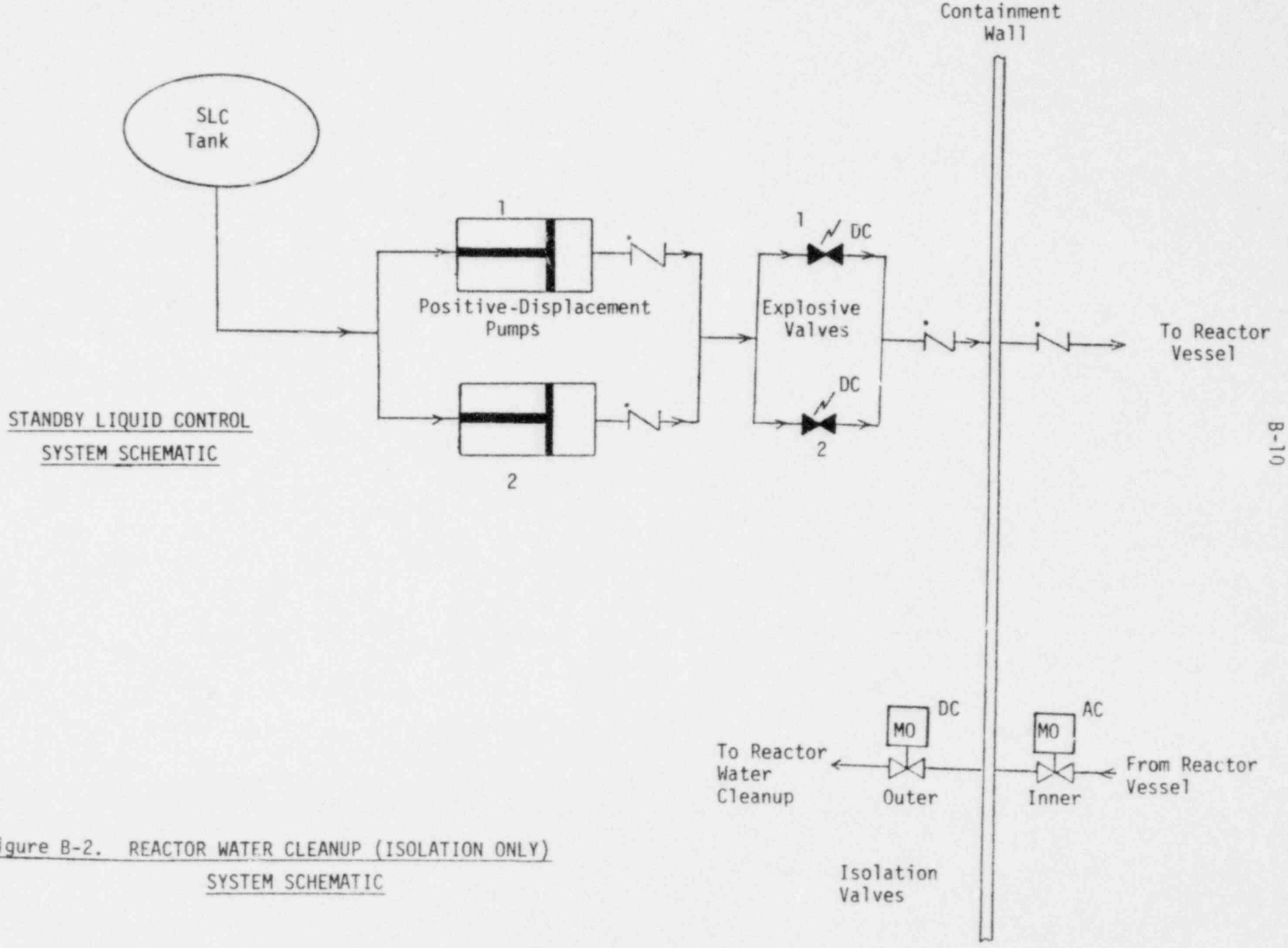


Figure B-2. REACTOR WATER CLEANUP (ISOLATION ONLY)
SYSTEM SCHEMATIC

SYSTEM	MAJOR COMPONENTS	LOCATION*			MAIN SUPPORTS
		BLDG.	ELEV.	COORD.	
Standby Liquid Control	Standby Liquid Control Tank	Unit 3 Reactor Bldg.	639	QP/$R_{19}R_{20}$	None
	Positive-Displacement Pump 1				AC Power from 480v AC Shutdown Board 3A
	Positive-Displacement Pump 2				AC Power from 480 v AC Shutdown Board 3B
	Explosive Valve 1				DC Power from 250v DC Battery Board 2 or 3
	Explosive Valve 2				
Reactor Water Cleanup (Isolation Only)	DC Motor-Operated Isolation Valve (Outside drywell)				
	AC Motor-Operated Isolation Valve (inside drywell)		Inside Drywell		AC Power from 480 v AC Reactor MOV Board 3A
Control Rod Scram (High Pressure)	185 Control Rods & Drives				185 Hydraulic Control Units (HCUs)
	185 HCUs (93-East Bank 92-West Bank)		565	SQ/ $R_{15}R_{16}$(West) $R_{20}R_{21}$(East)	See individual components
For each HCU	Diaphragm-Operated Scram Inlet Valve 1				Three-way Solenoid Scram Pilot Valves A & B
	Diaphragm-Operated Scram Exhaust Valve 1				Control Air (opens upon loss)
	Three-way Solenoid Scram Pilot Valve A				RP Trip-Logic Channel A
	Three-way Solenoid Scram Pilot Valve B				RP Trip-Logic Channel B

TABLE B-6.

SYSTEM	MAJOR COMPONENTS	LOCATION*			MAIN SUPPORTS	
		BLDG.	ELEV.	COORD.		
Control Rod Scram (High Pressure)	Ball-Check Shuttle Valve 1 (For ea. HCU)	Unit 3 Reactor Bldg.	Inside Drywell		None	
	Three-way Solenoid Backup Scram Pilot Valve 1-1				RP Close-Logic Channels A & B	DC Power from 250v DC Battery Board 1, 2, or 3
	Three-way Solenoid Backup Scram Pilot Valve 1-2					
	Three-way Solenoid Backup Scram Pilot Valve 2-1					
	Three-way Solenoid Backup Scram Pilot Vavle 2-2					
	West Bank Scram Discharge Volume (SDV)				Ventilation through Reactor Bldg. Equipment Drain Sump (RBEDS)	
	East Bank SDV					
	Scram Instrument Volume (SIV)				None	
	2" Drain Line from West Bank SDV to SIV (15' long)					
	2" Drain Line from East Bank SDV to SIV (15C' long)					
	Drain Line from SIV to RBEDS					
	1" Vent Line from West Bank SDV to RBEDS					

TABLE B-6 (cont)

SYSTEM	MAJOR COMPONENTS	LOCATION *			MAIN SUPPORTS	
		BLDG.	ELEV.	COORD.		
Control Rod Scram (High Pressure)	1" Vent Line from East Bank SDV to RBEDS	Unit 3 Reactor Bldg.			None	
	Diaphragm-Operated West Bank SDV Vent Valve				Three-way Solenoid SDV/SIV Pilot Valves A & B or Three-way Solenoid SDV/SIV Isolation Pilot Valve	Control Air (closes upon los_,
	Diaphragm-Operated East Bank SDV Vent Valve					
	Diaphragm-Operated SIV Drain Valve					
	Three-way Solenoid SDV/SIV Pilot Valve A				RP Trip-Logic Channel A	
	Three-way Solenoid SDV/SIV Pilot Valve B				RP Trip-Logic Channel B	
	Three-way Solenoid SDV/SIV Isolation Pilot Valve				Remote Manual Signal from Control Room	
Reactor Protection	Trip-Logic Channel A				Fail-safe upon loss of AC power	
	Trip-Logic Channel B					
	Close-Logic Channel A					
	Close-Logic Channel B					
Reactor Building Equipment Drain Sump (Ventilation only)	RBEDS Exhaust Fan 1	Unit 3 Reactor Bldg.			AC Power from 480v AC Reactor Bldg. Vent Board 3A.	
	RBEDS Exhaust Fan 2				AC Power from 480v AC Reactor Bldg. Vent Board 3B	
Control Air	Air Compressor A	Turbine Bldg.	565	MJ/T_1T_2	AC Power from 480v AC Shutdown Board 1A	
	Air Compressor B				AC Power from 480v AC Shutdown Board 2A	
	Air Compressor C				AC Power from 480v AC Common Board 1	

TABLE B-6 (cont)

SYSTEM	MAJOR COMPONENTS	LOCATION*			MAIN SUPPORTS	
		BLDG.	ELEV.	COORD.		
Control Air	Air Compressor D	Turbine Bldg	565	MJ/T_1T_2	AC Power from 480v AC Common Board 2	
250v DC	250v DC Battery Board 1	Unit 1 Reac. Bldg.	593	PN/$R_{3.5}R_4$	DC Power from 250v DC Battery 1	or Battery Charger 1, 2, 3 or Spare
	250v DC Battery Board 2	Unit 2 Reac. Bldg.		PN/$R_{9.5}R_{10}$	DC Power from 250v DC Battery 2	
	250v DC Battery Board 3	Unit 3 Reac. Bldg.		PN/$R_{18}R_{18.5}$	DC Power from 250v DC Battery 3	
	250v DC Battery Charger 1				AC Power from 480v AC Shutdown Board 1A	or Common Board 1
	250v DC Battery Charger 2				AC Power from 480v AC Shutdown Board 2A	
	250v DC Battery Charger 3				AC Power from 480v AC Shutdown Board 3A	
	250v DC Spare Battery Charger				AC Power from 480v AC Shutdown Board 2B	
	250v DC Battery 1	Unit 1 Reac. Bldg.	593	PN/$R_{2.5}R_{3.5}$	None	
	250v DC Battery 2	Unit 2 Reac. Bldg.		PN/$R_{10}R_{11}$		
	250v DC Battery 3	Unit 3 Reac. Bldg.		PN/$R_{18.5}R_{19.5}$		
AC Reactor Bldg. Vent (Unit 3 only)	480v AC Reactor Bldg. Vent Board 3A		734	QN/$R_{18}R_{19}$	AC Power from 480v AC Common Board 3 or Unit Board 3A	
	480v AC Reactor Bldg. Vent Board 3B		565	UT/$R_{19}R_{20}$		
AC Reactor MOV (Unit 3, Board 3A only)	480v AC Reactor MOV Board 3A		621	RP/$R_{20}R_{21}$	AC Power from 480v AC Shutdown Board 3A or 3B	DC Power from 250v DC Battery Board 2 or 3

TABLE B-6 (cont)

SYSTEM	MAJOR COMPONENTS	LOCATION*			MAIN SUPPORTS
		BLDG.	ELEV.	COORD.	
AC Common (excluding 4.16kv AC Common Start Board 2)	480v AC Common Board 1	Turbine Bldg.	586	KJ/T_6T_7	AC Power from 4160/480v AC Common Transformer 1A or 1B
	480v AC Common Board 2		604	CB/T_6T_8	AC Power from 4160/480v AC Common Transformer 2A or 2B
	480V AC Common Board 3		586	$HG/T_{11}T_{12}$	AC Power from 4160/480v AC Common Transformer 3A or 3B
	4160/480v AC Common Transformer EA		604	$CB/T_{12}T_{13}$	AC Power from 4.16kV AC Common Board A

TABLE 8-6 (cont)

*From reference 4, Figures 1.6-1 through 1.6-21

SYSTEM	MAJOR COMPONENTS	LOCATION*			MAIN SUPPORTS	
		BLDG.	ELEV.	COORD.		
AC Common	4160/480v AC Common Transformer 1A	Turbine Bldg.	586	KJ/T_6T_7	AC Power from 4.16kV AC Common Board A	
	4160/480v AC Common Transformer 2A		604	CB/T_7T_8		
	4160/480v AC Common Transformer 3A		586	HG/$T_{11}T_{12}$		
	4160/480v AC Common Transformer 1B			KJ/T_6T_7	AC Power from 4.16kV AC Common Board B	
	4160/480v AC Common Transformer 2B		604	CB/T_6T_7		
	4160/480v AC Common Transformer 3B		586	HG/$T_{11}T_{12}$		
	4.16kv AC Common Board A		604	CB/T_1T_2	AC Power from 20.7/4.16kv AC Unit Station Service Transformer 1	or 4.16 kV AC Common Start Board 1
	4.15kv AC Common Board B			CB/$T_{10}T_{11}$	AC Power from 20.7/4.16kv AC Unit Station Service Transformer 2	
	4.16 kV AC Common Start Board 1			BA/T_1T_2	AC Power from 161/4.16kV AC Common Station Service Transformer A or B	
	161/4.16 kv AC Common Station Service Transformer A	Switchyard			AC Power from 161 kv AC Athens or Trinity Off-site Power Supply	
	161/4.16 kv AC Common Station Service Transformer B					
	161 kv AC Athens Off-Site Power Supply				AC Off-Site Power Grid	
	161 kv AC Trinity Off-Site Power Supply					

TABLE B-6 (cont)

SYSTEM	MAJOR COMPONENTS	LOCATION*			MAIN SUPPORTS	
		Bldg	Elev.	Coord		
AC Shutdown (excluding 480v AC Shutdown Board 1B)	480v AC Shutdown Board 1A	Unit 1 Reactor Bldg	621	TS/$R_1R_{1.5}$	AC Power from 4160/480v AC Shutdown Transformer 1A or 1E	DC Power from 250v DC Battery 1,2 or 3
	480v AC Shutdown Board 2A	Unit 2 Reactor Bldg		TS/$R_{13}R_{13.5}$	AC Power from 4160/480v AC Shutdown Transformer 2A or 2E	
	480v AC Shutdown Board 2B			TS/$R_{13.5}R_{14}$	AC Power from 4160/480v AC Shutdown Transformer 2B	
	480v AC Shutdown Board 3A	Unit 3 Reactor Bldg		SR/$R_{20}R_{20.5}$	AC Power from 4160/480v AC Shutdown Transformer 3A or 3E	
	480v AC Shutdown Board 3B			SR/$R_{20.5}R_{21}$	AC Power from 4160/480v AC Shutdown Transformer 3B	
	4160/480v AC Shutdown Transformer 3B				AC Power from 4.16 kV AC Shutdown Board A	
	4160/480v AC Shutdown Transformer 1A	Unit 1 Reactor Bldg		SR/$R_1R_{1.5}$		
	4160/480v AC Shutdown Transformer 1E		639	SR/R_1R_2	AC Power from 4.16 kV AC Shutdown Board B	
	4160/480v AC Shutdown Transformer 2A	Unit 2 Reactor Bldg	621	SR/$R_{13}R_{13.5}$		
	4160/480v AC Shutdown Transformer 2E		639	SR/$R_{13}R_{14}$	AC Power from 4.16 kV AC Shutdown Board C	
	4160/480v AC Shutdown Transformer 3A	Unit 3 Reactor Bldg	621	SR/$R_{20}R_{20.5}$		
	4160/480v AC Shutdown Transformer 3E		639	SR/$R_{20}R_{21}$	AC Power from 4.16 kV AC Shutdown Board D	
	4160/480v AC Shutdown Transformer 2B	Unit 2 Reactor Bldg	621	SR/$R_{13.5}R_{14}$		

TABLE B-6 (cont)

SYSTEM	MAJOR COMPONENTS	LOCATION*			MAIN SUPPORTS		
		Bldg	Elev.	Coord			
AC Shutdown (excluding 480v AC Shutdown Board 1B)	4.16 kV AC Diesel Generator A	Diesel Generator	565	Room A	Not resolved		
	4.16 kV AC Diesel Generator B			Room B			
	4.16 kV AC Diesel Generator C			Room C			
	4.16 kV AC Diesel Generator D			Room D			
	4.16 kV AC Shutdown Board A	Unit 1 Reactor Bldg	621	SP/R_1R_2	AC Power from 4.16 kV AC Diesel Generator A	or Shutdown Bus 1 or 2	DC Power from 250v DC Battery 1,2, or 3
	4.16 kV AC Shutdown Board B		593		AC Power from 4.16 kV AC Diesel Generator B		
	4.16 kV AC Shutdown Board C	Unit 2 Reactor Bldg	621	$SP/R_{13}R_{14}$	AC Power from 4.16 kV AC Diesel Generator C		
	4.16 kV AC Shutdown Board D		593		AC Power from 4.16 kV AC Diesel Generator D		
	4.16 kV AC Shutdown Bus 1				AC Power from 4.16 kV AC Unit Boards 1A, 2B, or 3A		
	4.16 kV AC Shutdown Bus 2				AC Power from 4.16 kV AC Unit Boards, 1B, 2A, or 3B		
AC Unit (including only 480v AC Unit Board 3A from among all 480V AC Unit Boards; excluding 4.16 kV AC Unit Boards 1C,2C, &3C)	480V AC Unit Board 3A	Turbine Bldg	586	$DC/T_{11}T_{12}$	AC Power from 4160/480v AC Unit Transformer 3A or Common Transformer EA		
	4160/480v AC Unit Transformer 3A				AC Power from 4.16 kV AC Unit Board 3A		
	4.16 kV AC Unit Board 1A		604	CB/T_1T_2	AC Power from 20.7/4.16 kV AC Unit Station Service Transformer 1	or 4.16 kV AC Common Start Board 1	
	4.16 kV AC Unit Board 1B		586				

TABLE B-6 (cont)

TABLE B-6 (cont)

SYSTEM	MAJOR COMPONENTS	LOCATION*			MAIN SUPPORTS
		Bldg	Elev	Coord	
AC Unit (Including only 480v AC Unit Board 3A from among all 480V AC Unit Boards; excluding 4.16 kV AC Unit Boards 1C,2C &3C)	4.16 kV AC Unit Board 2A	Turbine Bldg	604	CB/$T_{10}T_{11}$	AC Power from 20.7/4.16 kV AC Unit Station Service Transformer 2 or 4.16 kV AC Common Start Board 1
	4.16 kV AC Unit Board 2B		586		
	4.16 kV AC Unit Board 3A		604	CB/$T_{16}T_{17}$	AC Power from 20.7/4.16 kV AC Unit Station Service Transformer 3 or 4.16 kV AC Common Start Board 1
	4.16 kV AC Unit Board 3B		586		
	20.7/4.16 kV AC Unit Station Service Transformer 1	Switchyard			AC Power from 22 kV AC Main Generator 1 or 500/20.7 kV AC Main Transformer 1
	20.7/4.16 kV AC Unit Station Service Transformer 2				AC Power from 22 kV AC Main Generator 2 or 500/20.7 kV AC Main Transformer 2
	20.7/4.16 kV AC Unit Station Service Transformer 3				AC Power from 22 kV AC Main Generator 3 or 500/20.7 kV AC Main Transformer 3
	22 kV AC Main Generator 1	Turbine Bldg	621	DB/$T_{2.5}T_{3.5}$	Not Resolved
	22 kV AC Main Generator 2			DB/$T_{8.5}T_{9.5}$	
	22 kV AC Main Generator 3			DB/$T_{14.5}T_{15.5}$	
	500/20.7 kV AC Main Transformer 1	Switchyard			AC Power from 500 kV AC Off-Site Power Supply
	500/20.7 kV AC Main Transformer 2				
	500/20.7 kV AC Main Transformer 3				
	500 kV AC Off-Site Power Supply				AC Off-Site Power Grid

Figure B-3 - TOP of Overall Safety Function Success Tree

Figure B-4 - Standby Liquid Control

Figure B-5 - Control Rod Scram

Figure B-6 - Reactor Building Equipment Drain Sump (Ventilation Only) and Control Air

Figure B-7 - 250v DC

Figure B-8 - AC Reactor Building Ventilation

Figure B-9 - AC Unit

Figure B-10 - AC Common

Figure B-11 - AC Reactor Motor-Operated Valve

Figure B-12 - AC Shutdown

Table B-7 presents a key to the symbols used for basic success events on the trees.

The use of success trees instead of the more common fault trees at this stage of the analysis reflects analyst preference. They complement one another; each is readily convertible to the other form. The use of success trees in no way precludes that of fault trees. In fact, they serve as a logical starting point for the subsequent development of detailed fault trees. However, at this point in the analysis the concern lies with identifying potential areas for systems interaction as a prelude to more detailed analysis of the important ones. The success tree approach can accomplish this without the need to specify the various failure modes for components. By dealing with basic success rather than basic failure events, some complexity is deferred until later.

Initially, the overall success tree is resolved to a level necessary for identifying the potential causes of inadequate drainage of the east bank scram

Table B-7. Key to Success Tree Symbols

Components

A = 4.16kV AC Board/Bus
Q = 480v AC Board
B = 250v DC Battery
C = RP Logic Channel
D = 250v DC Battery Board
F = Fan
G = Multi-kV AC Generator
H = 250v DC Battery Charger
K = Multi-kV AC Off-Site Power Supply
L = Drain/Vent Pipeline
M = Manual Signal
P = Pump
Q = Air Compressor
T = > 4.16kV AC Transformer
T = < 4.16 kV AC Transformer
V = Valve
W = Reactor Water

Systems

B = RBEDS (Reactor Bldg. Equipment Drain Sump)
C = CRS (Control Rod Scram)
D = 250v DC
H = AC Shutdown
M = AC Reactor MOV (Motor-Operated Valve)
N = AC Common
P = RP (Reactor Protection)
Q = Control Air
S = SLC (Standby Liquid Control)
U = AC Unit
V = AC Reactor Bldg. Vent
W = RWC (Reactor Water Cleanup)

Notation Scheme

Component Type (F = Fan) → F

B ← System (B = RBEDS)

1 ← Identifier (if necessary)

This represents RBEDS Exhaust Fan #1 (operable).

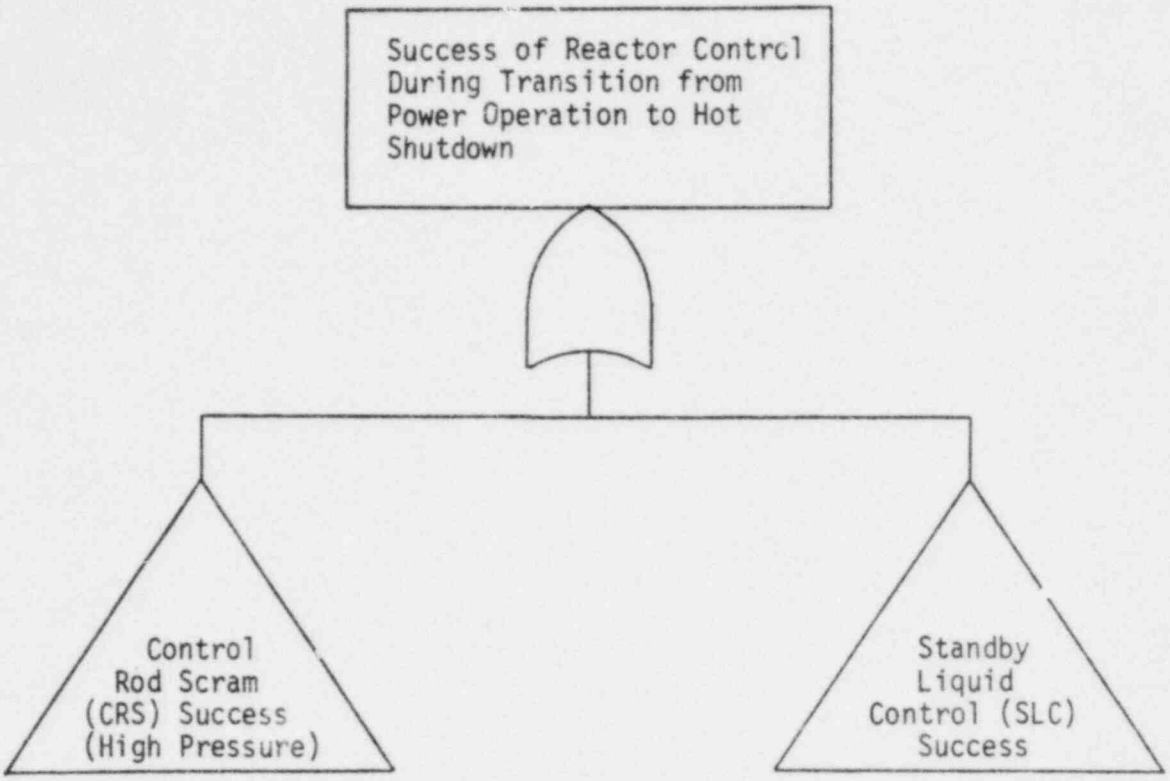


FIGURE B-3
TOP OF SUCCESS TREE FOR REACTOR CONTROL DURING TRANSITION FROM POWER OPERATION TO HOT SHUTDOWN

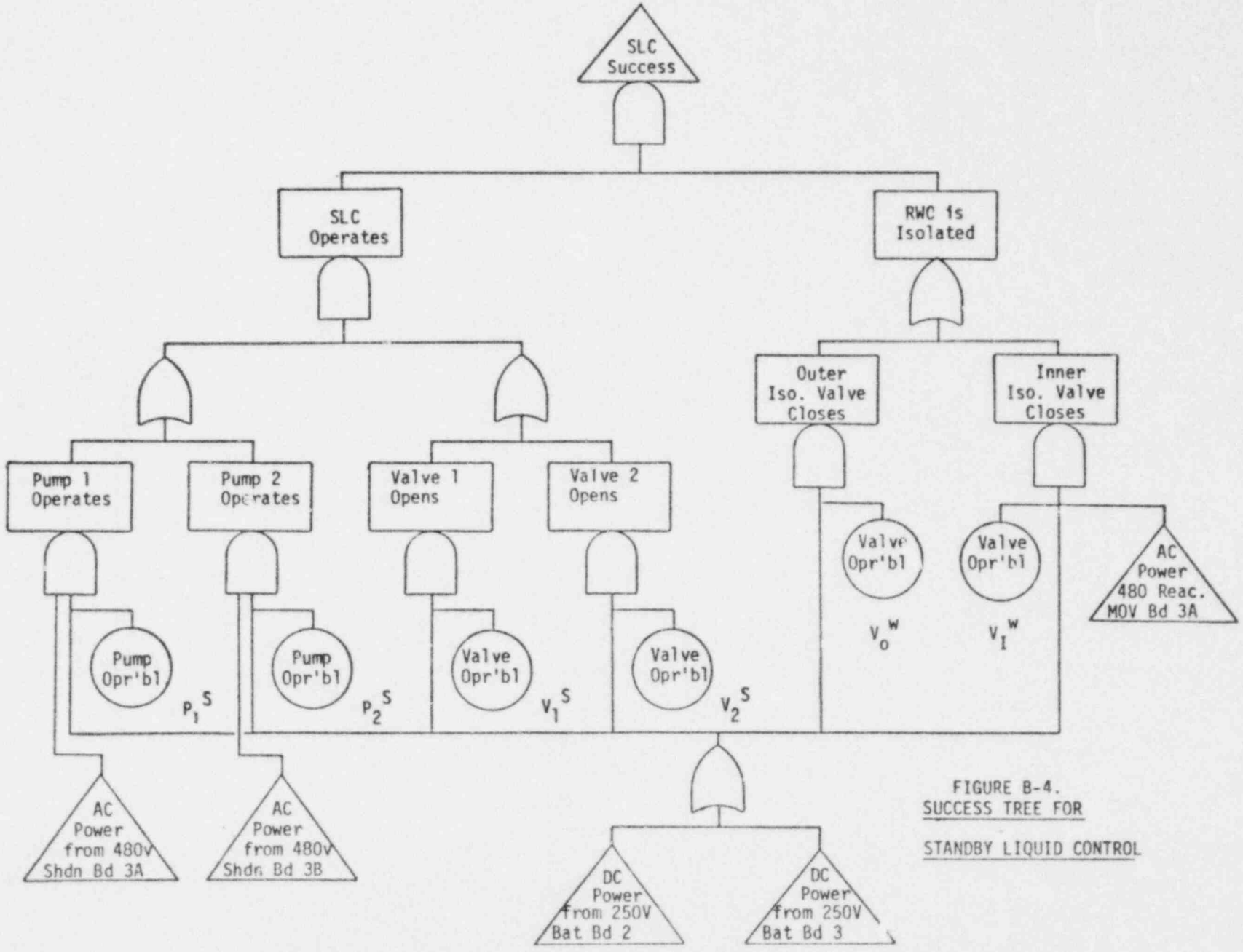


FIGURE B-4.
SUCCESS TREE FOR

STANDBY LIQUID CONTROL

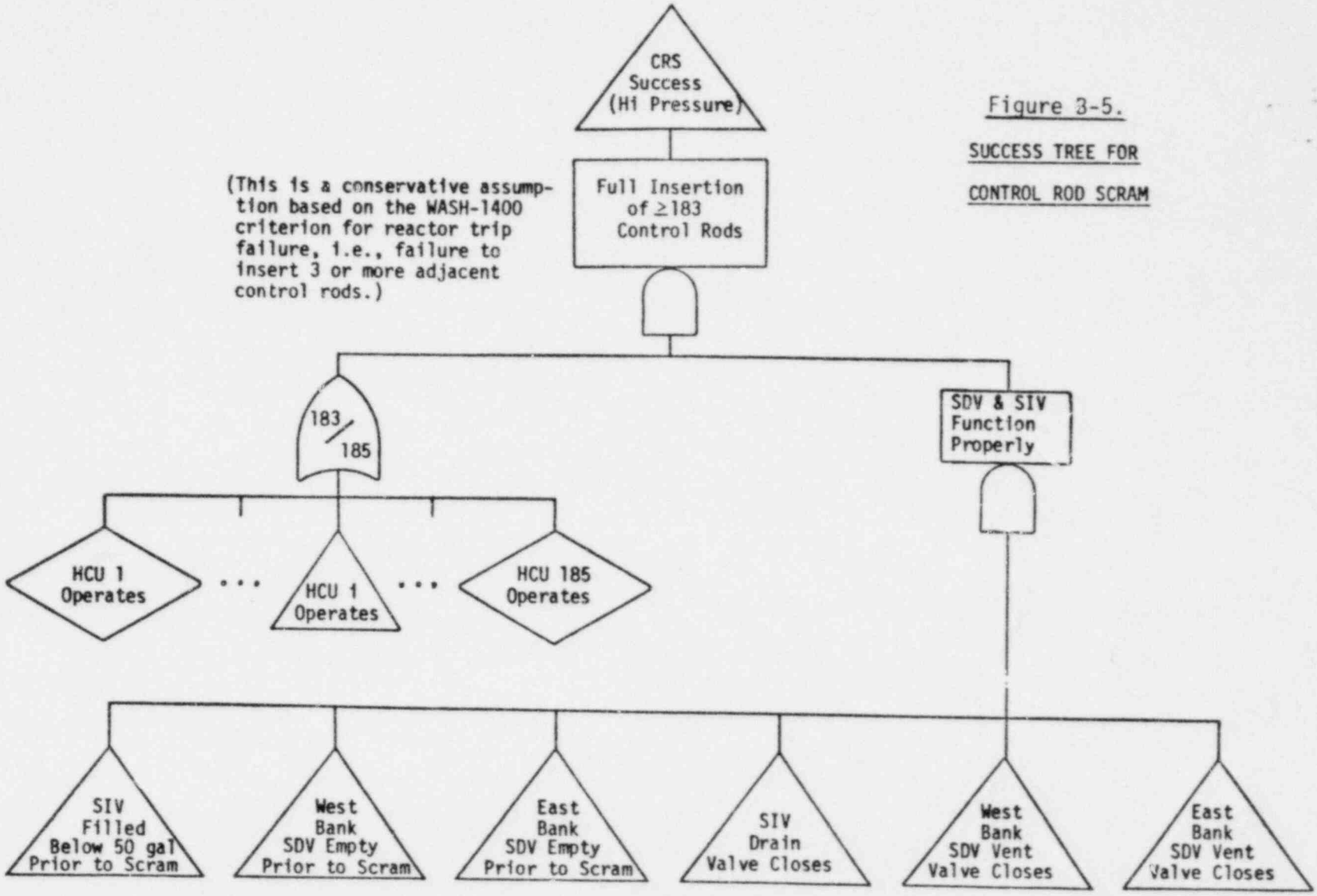


Figure 3-5.

SUCCESS TREE FOR

CONTROL ROD SCRAM

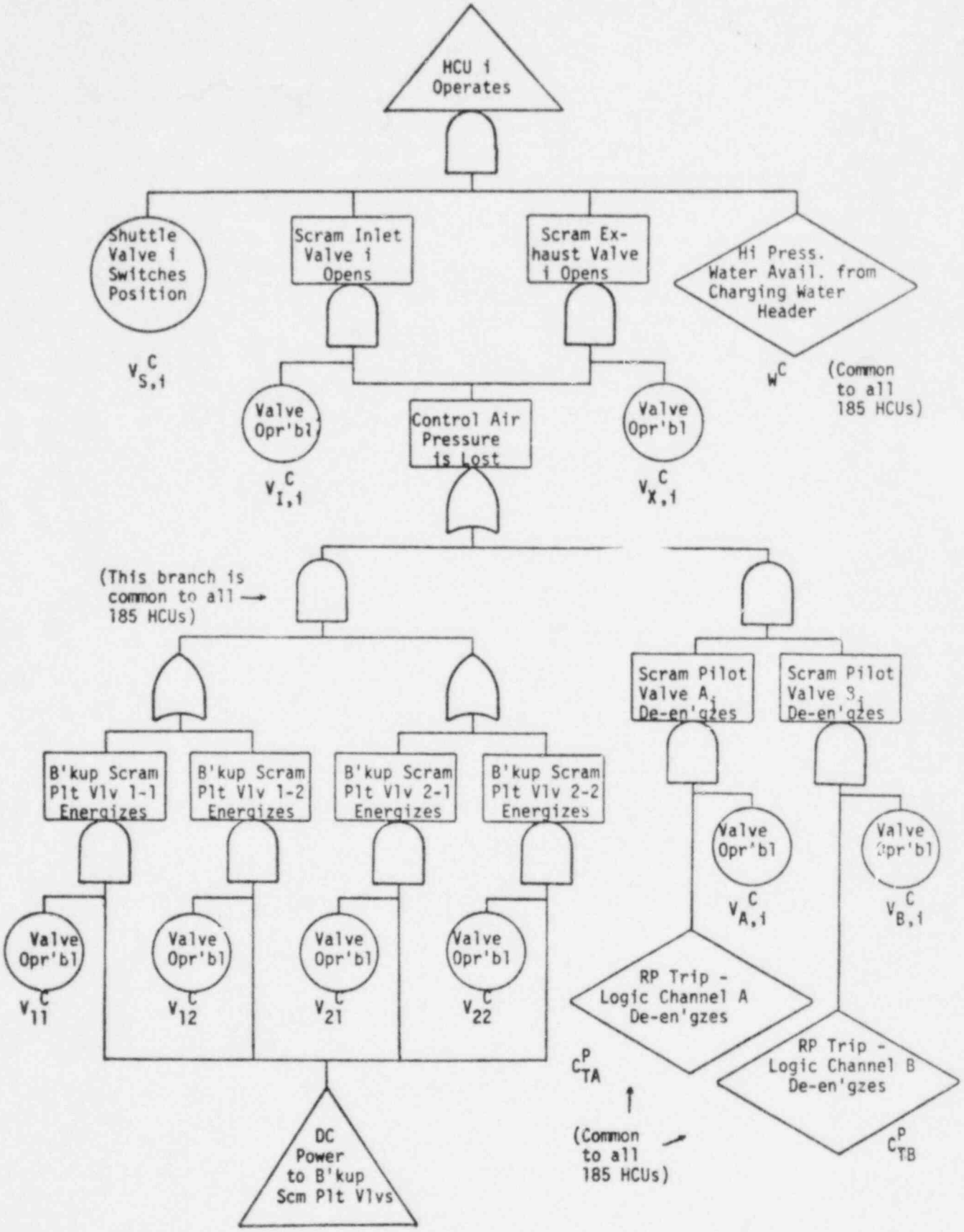
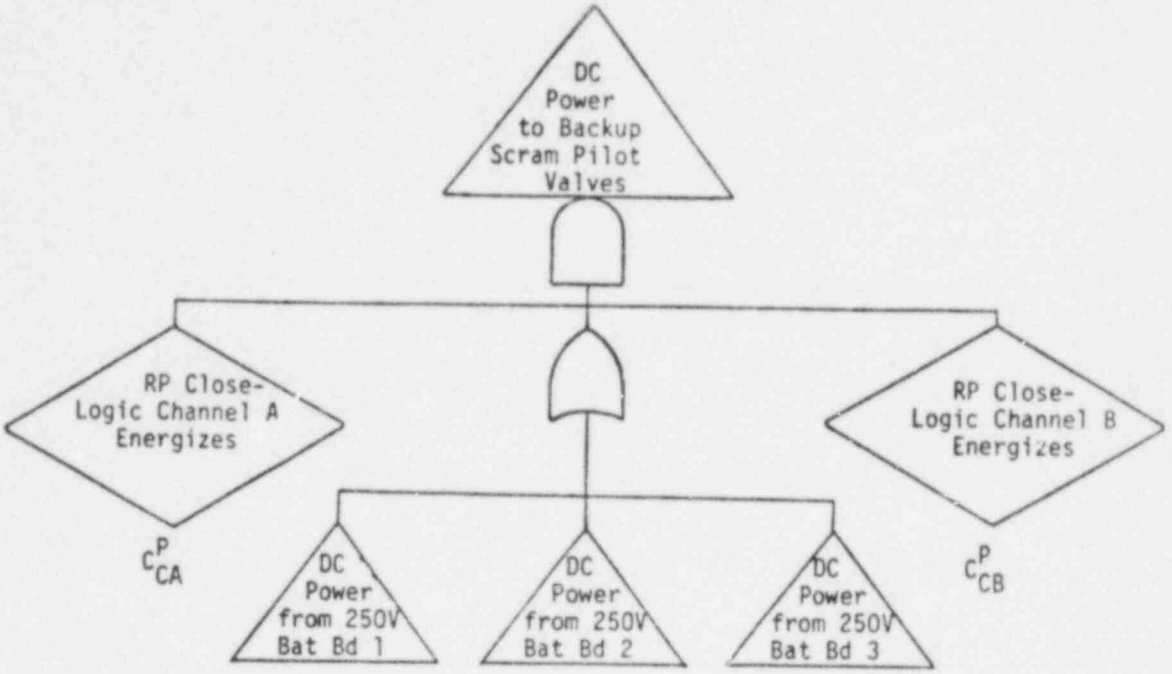


Figure B-5 (cont)



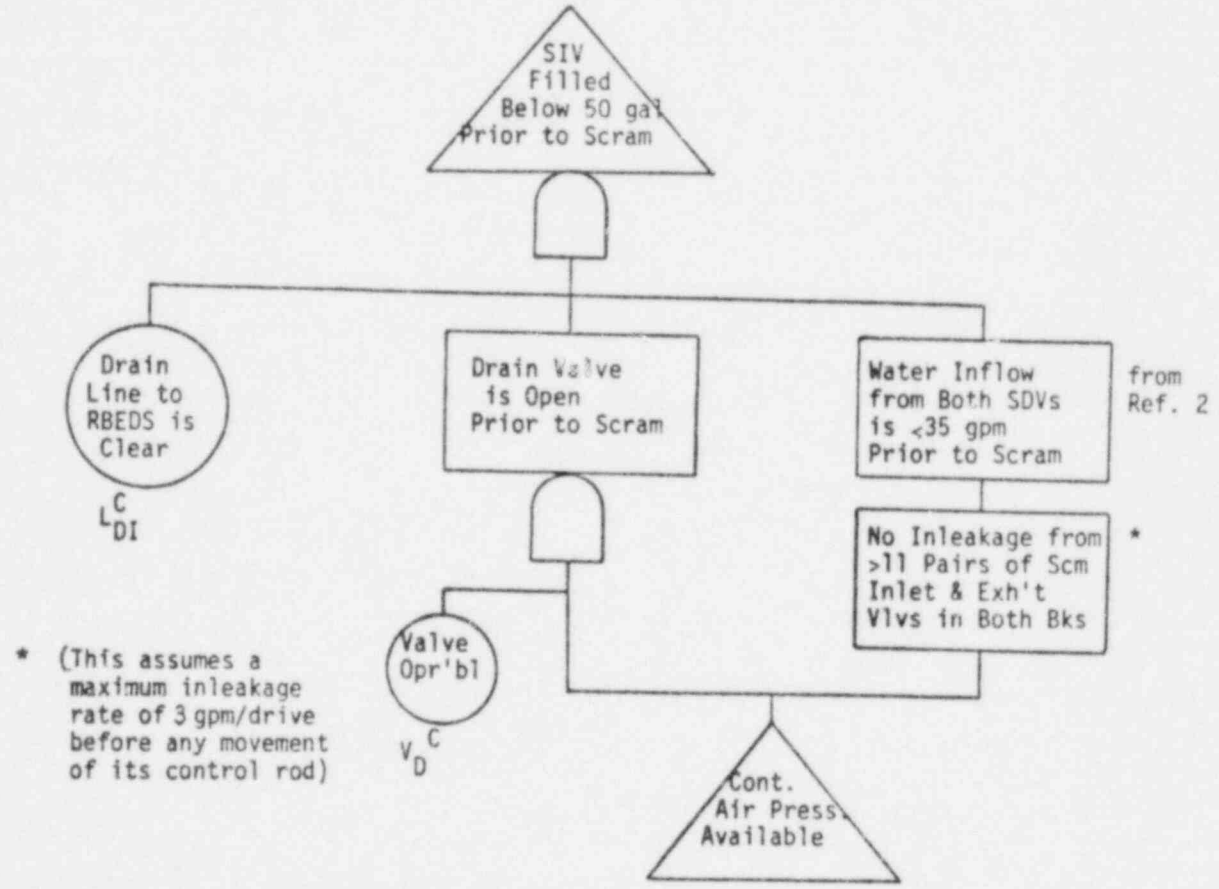


Figure B-5 (cont)

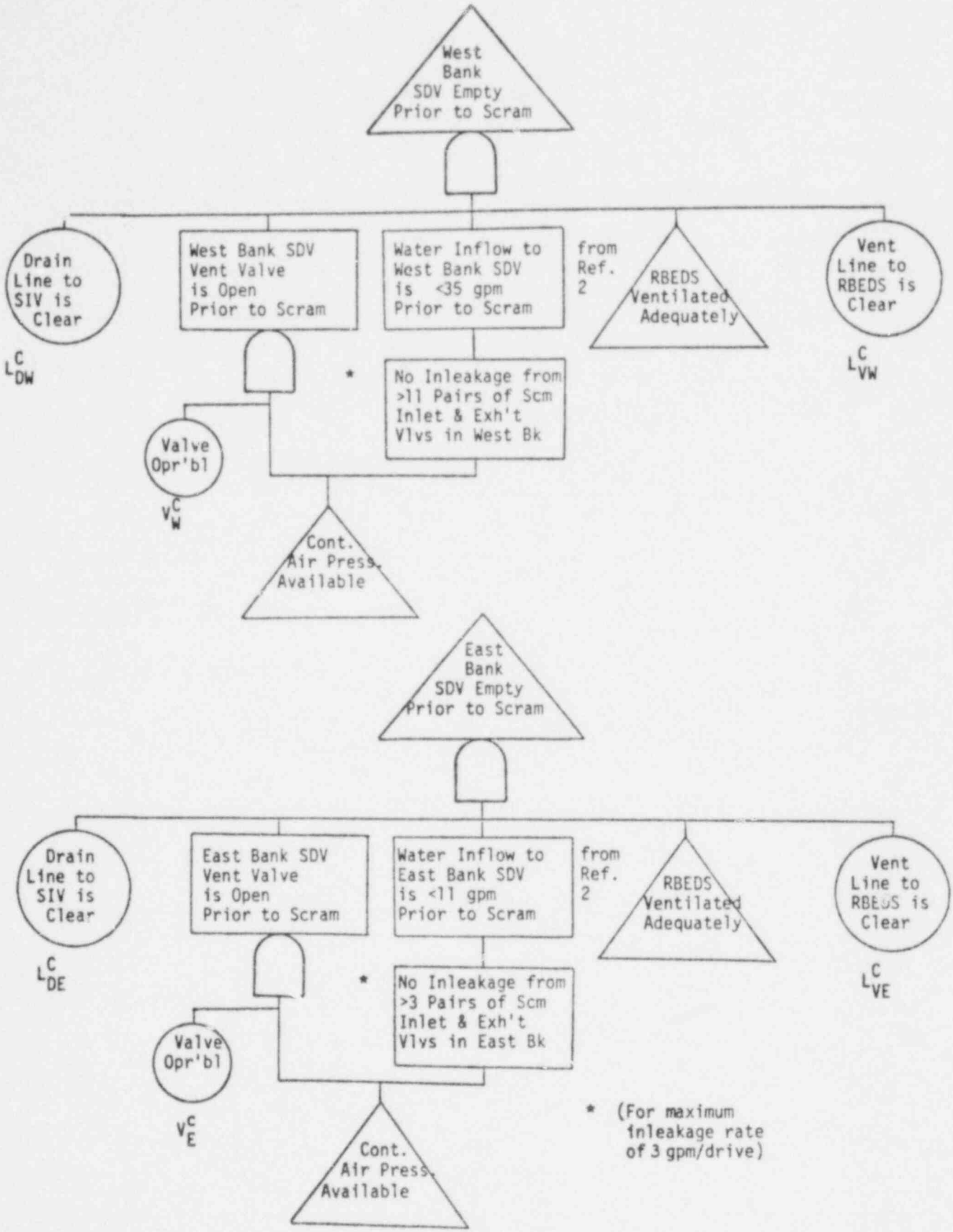


Figure B-5 (cont)

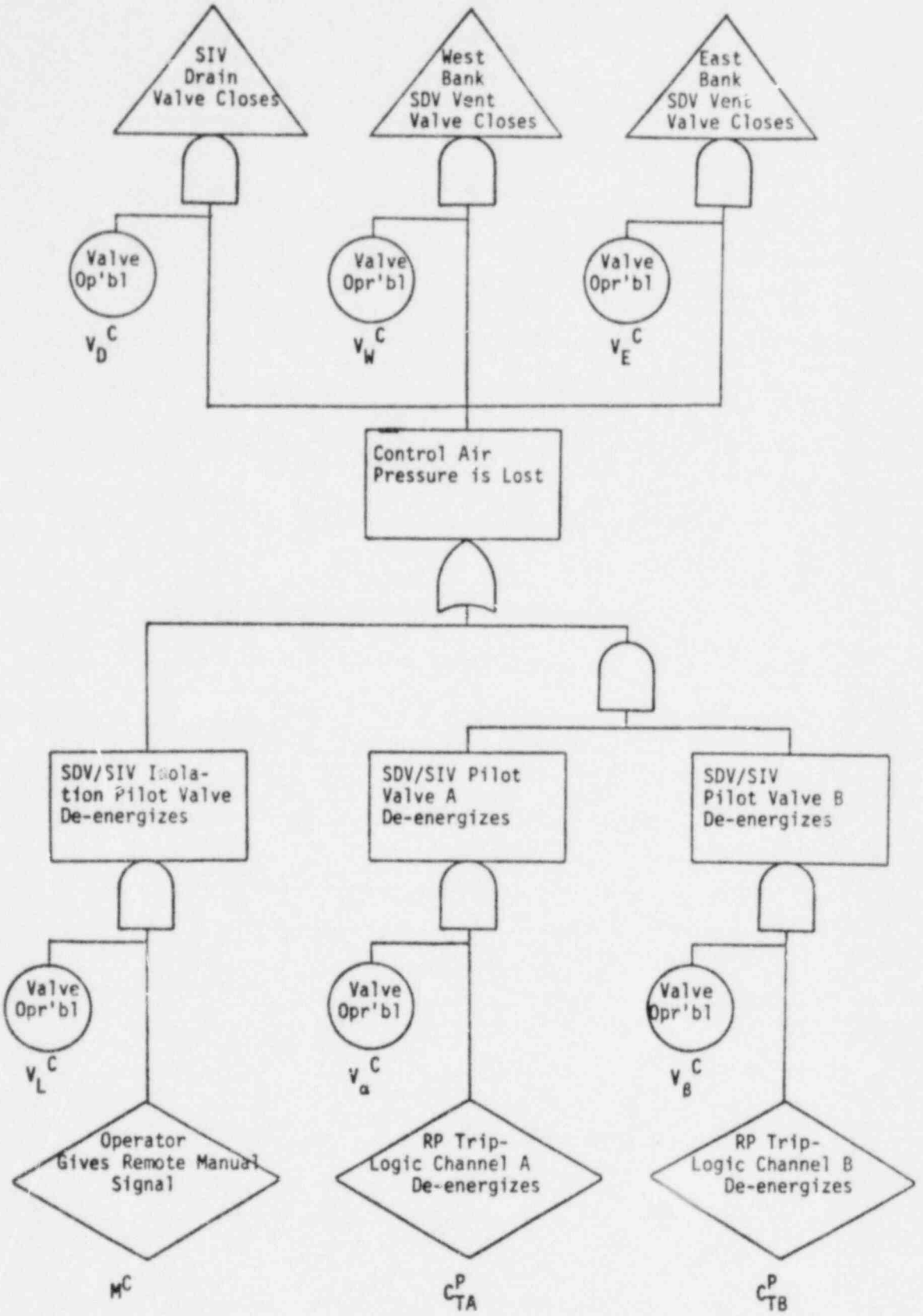


Figure B-5 (cont)

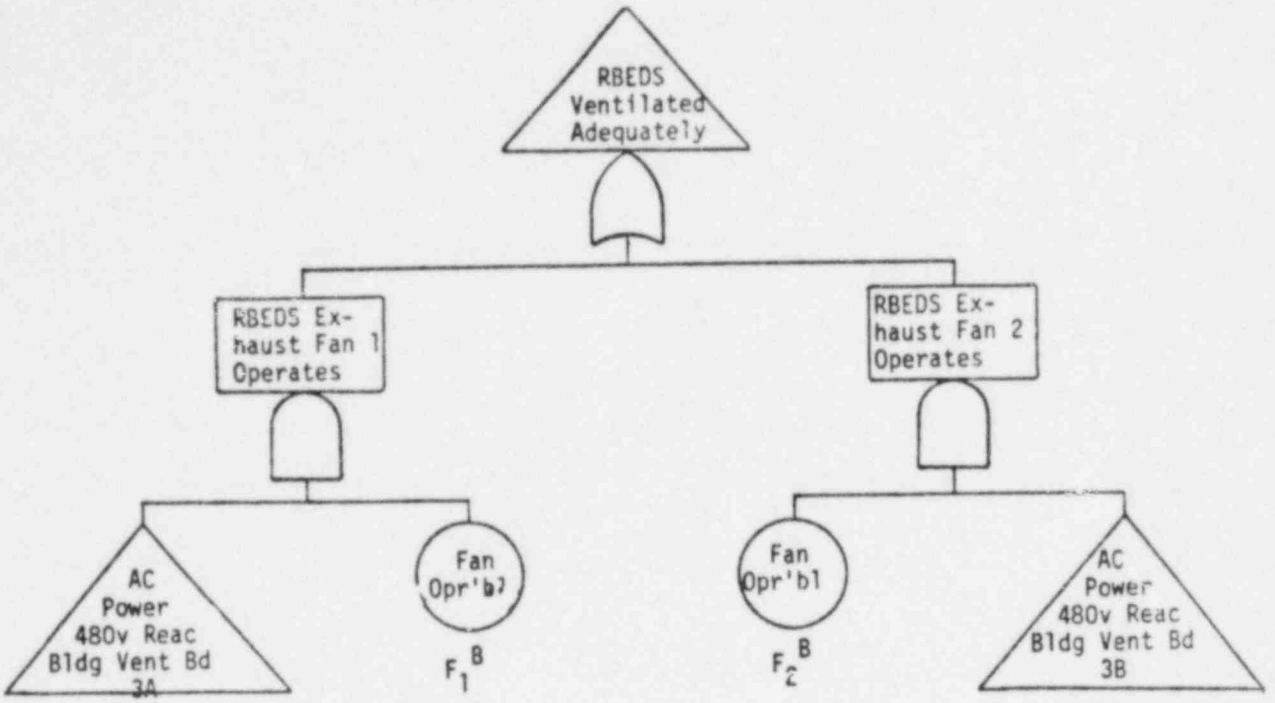
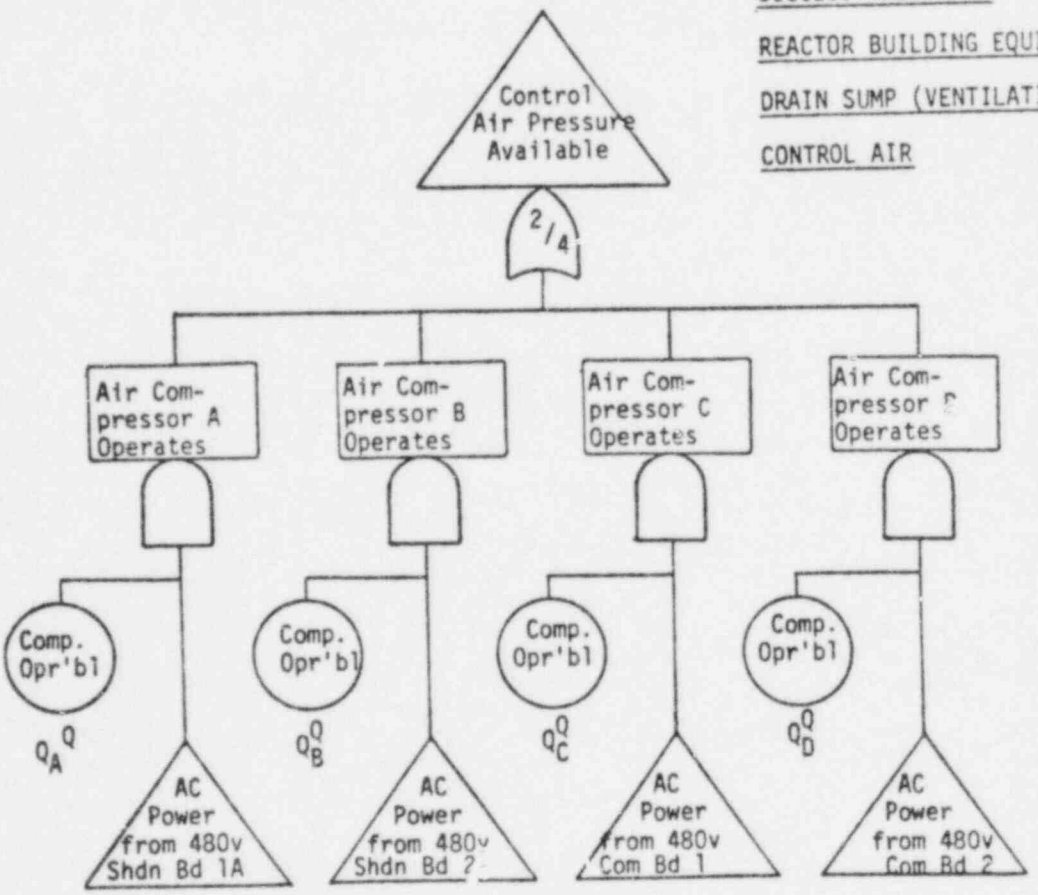


Figure B-6.
SUCCESS TREES FOR
REACTOR BUILDING EQUIPMENT
DRAIN SUMP (VENTILATION) &
CONTROL AIR



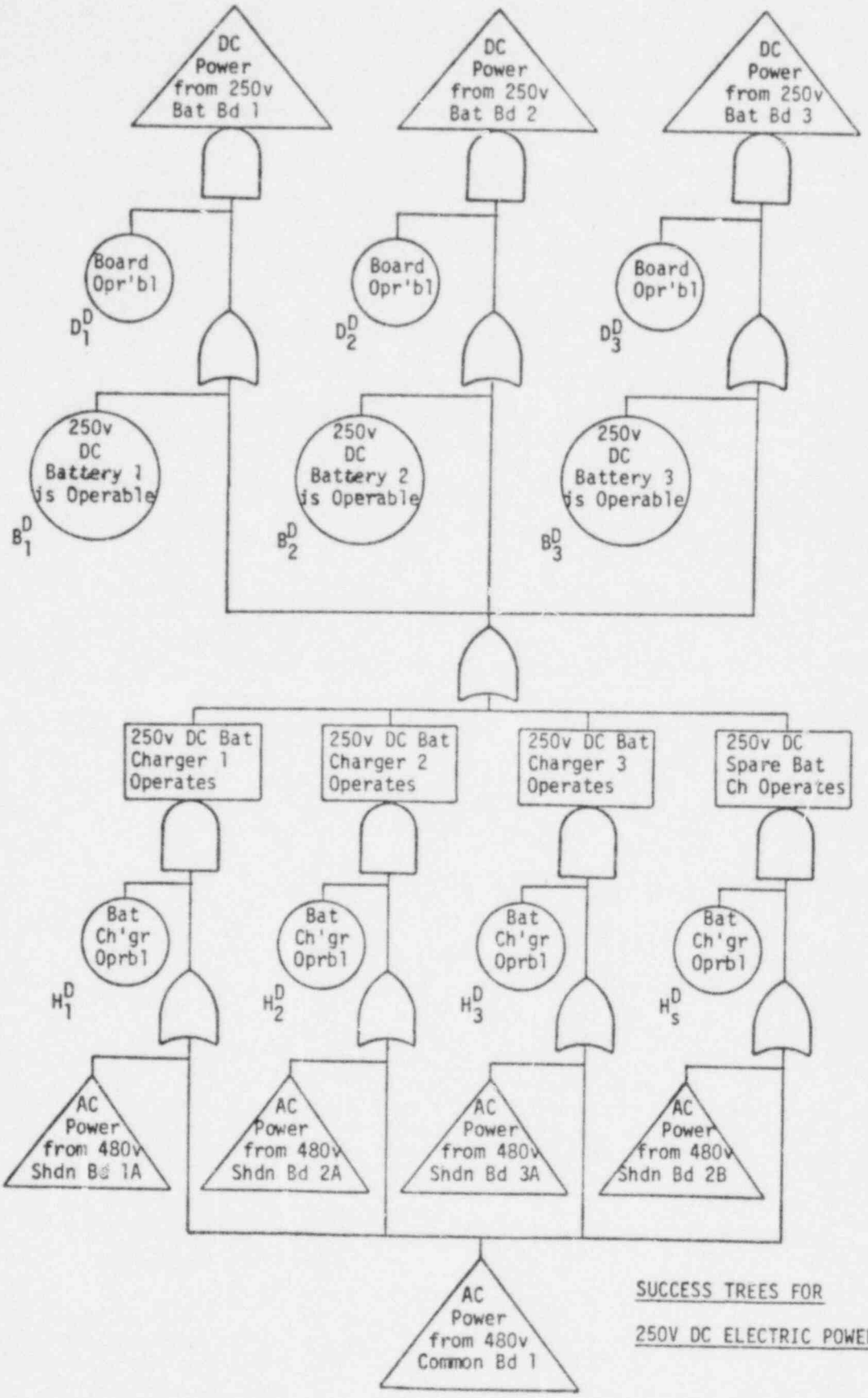

DC Power from 250v Bat Bd 1
DC Power from 250v Bat Bd 2
DC Power from 250v Bat Bd 3
Board Opr'bl
D_1^D
Board Opr'bl
D_2^D
Board Opr'bl
D_3^D
250v DC Battery 1 is Operable
B_1^D
250v DC Battery 2 is Operable
B_2^D
250v DC Battery 3 is Operable
B_3^D
250v DC Bat Charger 1 Operates
250v DC Bat Charger 2 Operates
250v DC Bat Charger 3 Operates
250v DC Spare Bat Ch Operates
Bat Ch'gr Oprbl
H_1^D
Bat Ch'gr Oprbl
H_2^D
Bat Ch'gr Oprbl
H_3^D
Bat Ch'gr Oprbl
H_s^D
AC Power from 480v Shdn Bd 1A
AC Power from 480v Shdn Bd 2A
AC Power from 480v Shdn Bd 3A
AC Power from 480v Shdn Bd 2B
AC Power from 480v Common Bd 1
SUCCESS TREES FOR
250V DC ELECTRIC POWER

Figure B-7.

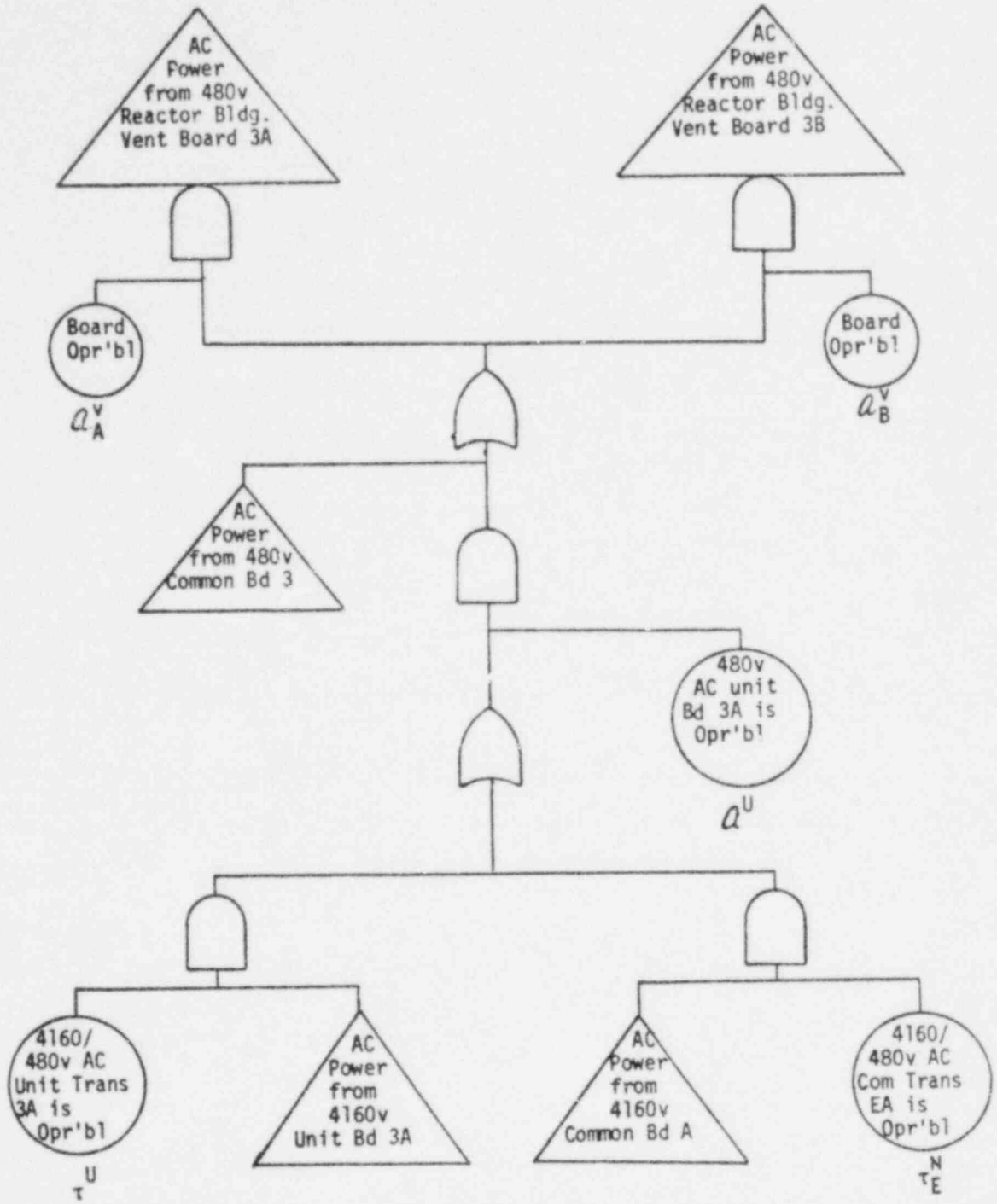


FIGURE B-8.

SUCCESS TREES FOR AC REACTOR BUILDING VENTILATION ELECTRIC POWER

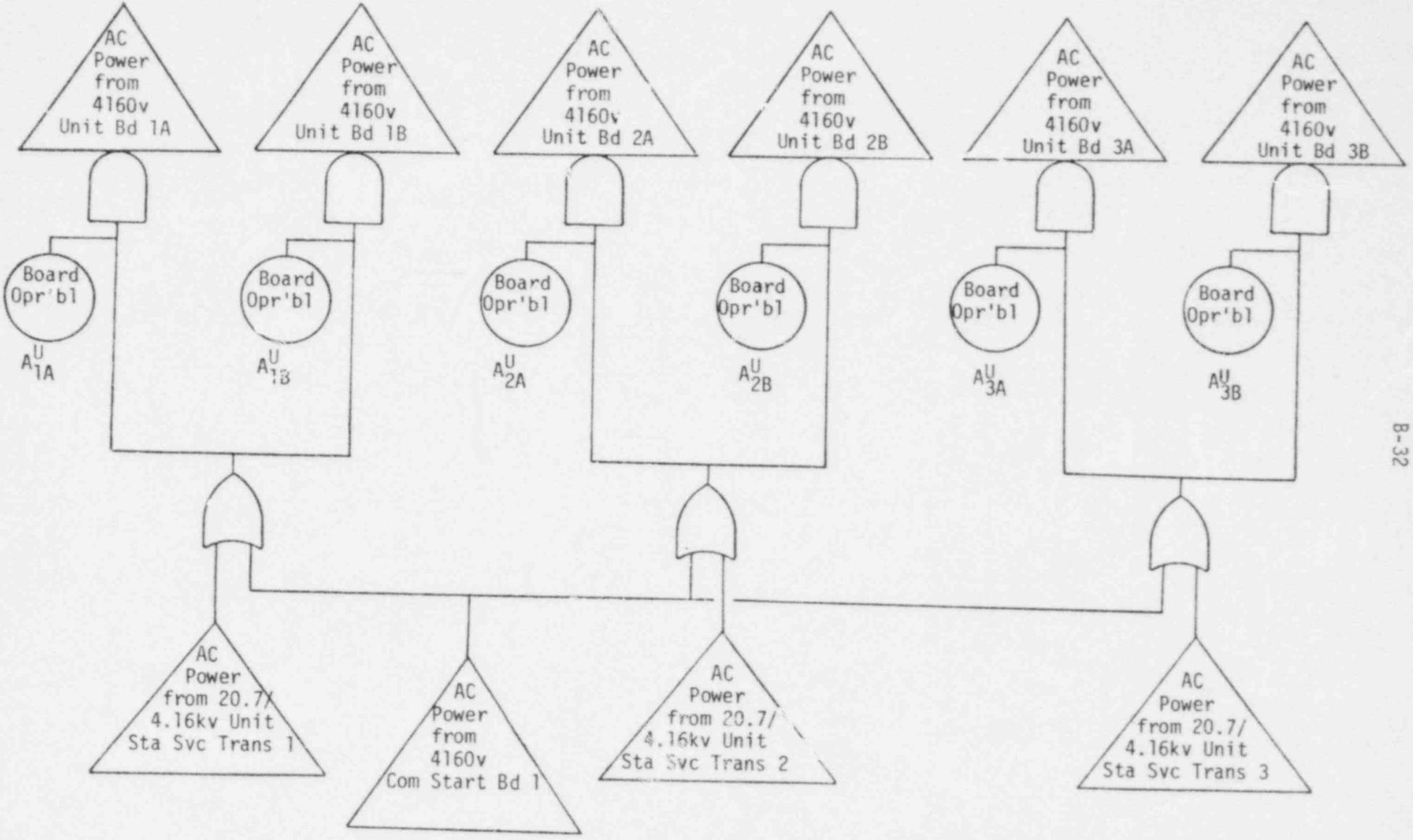


FIGURE B-9.

SUCCESS TREES FOR AC UNIT ELECTRIC POWER

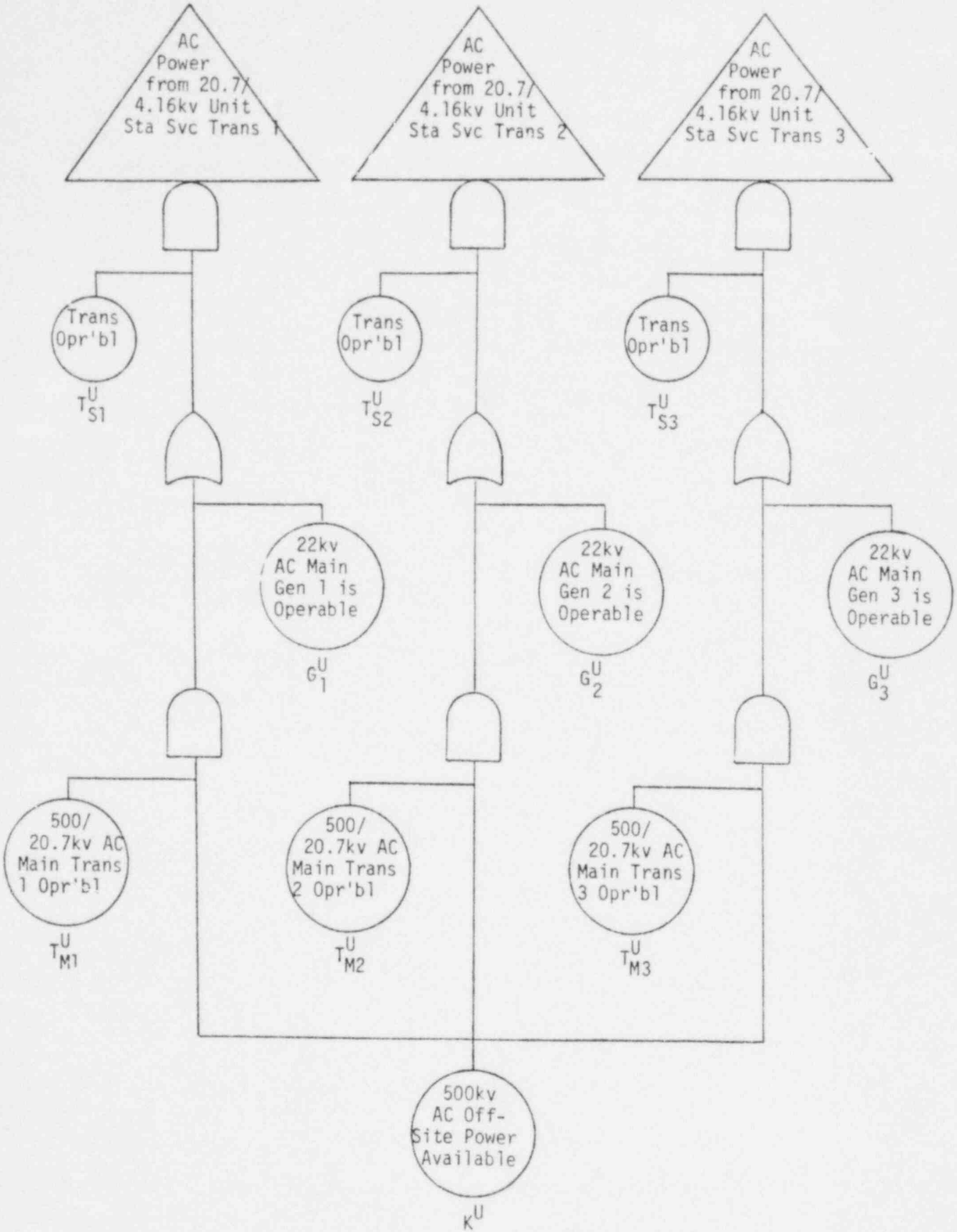


FIGURE B-9 (cont)

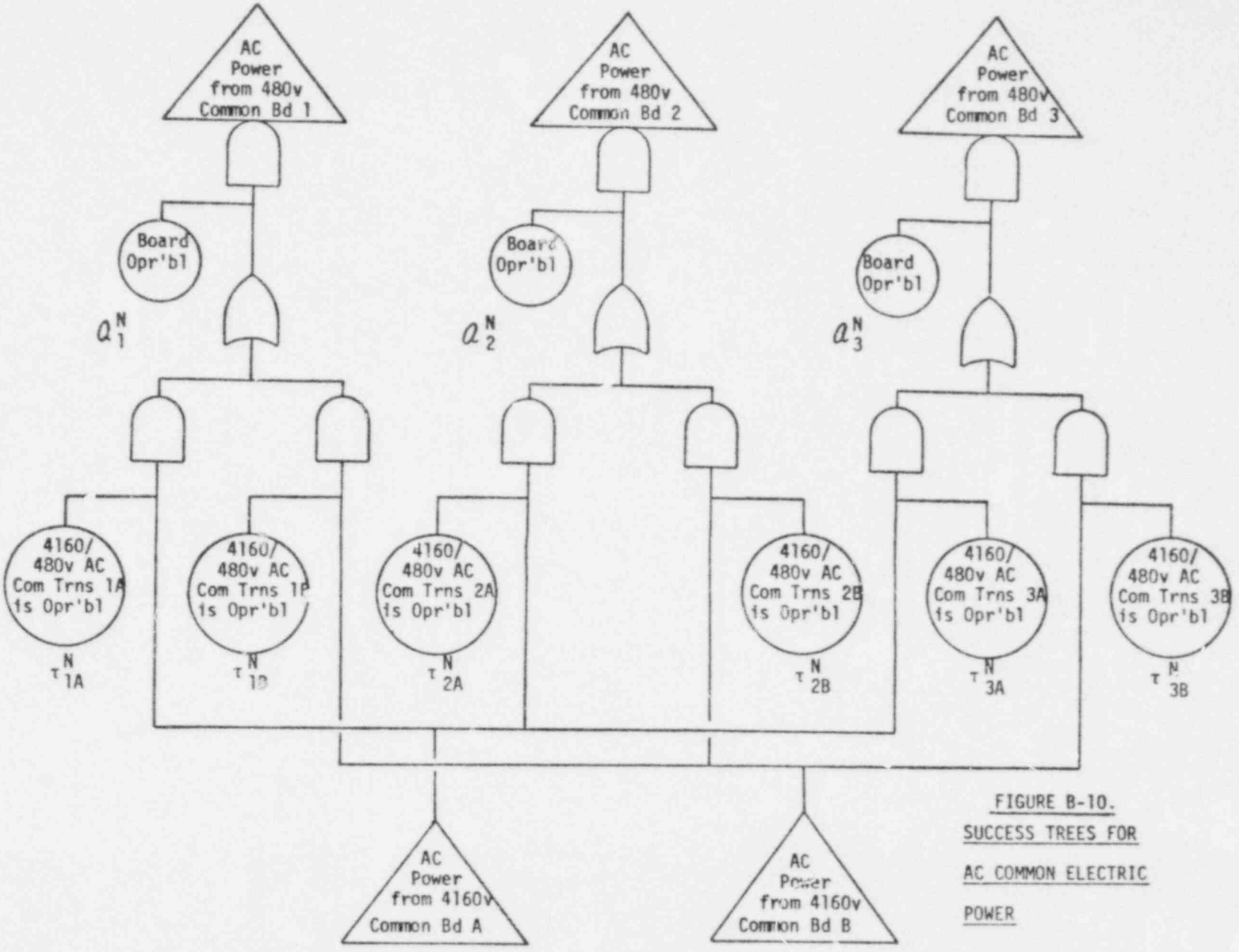


FIGURE B-10.
SUCCESS TREES FOR
AC COMMON ELECTRIC
POWER

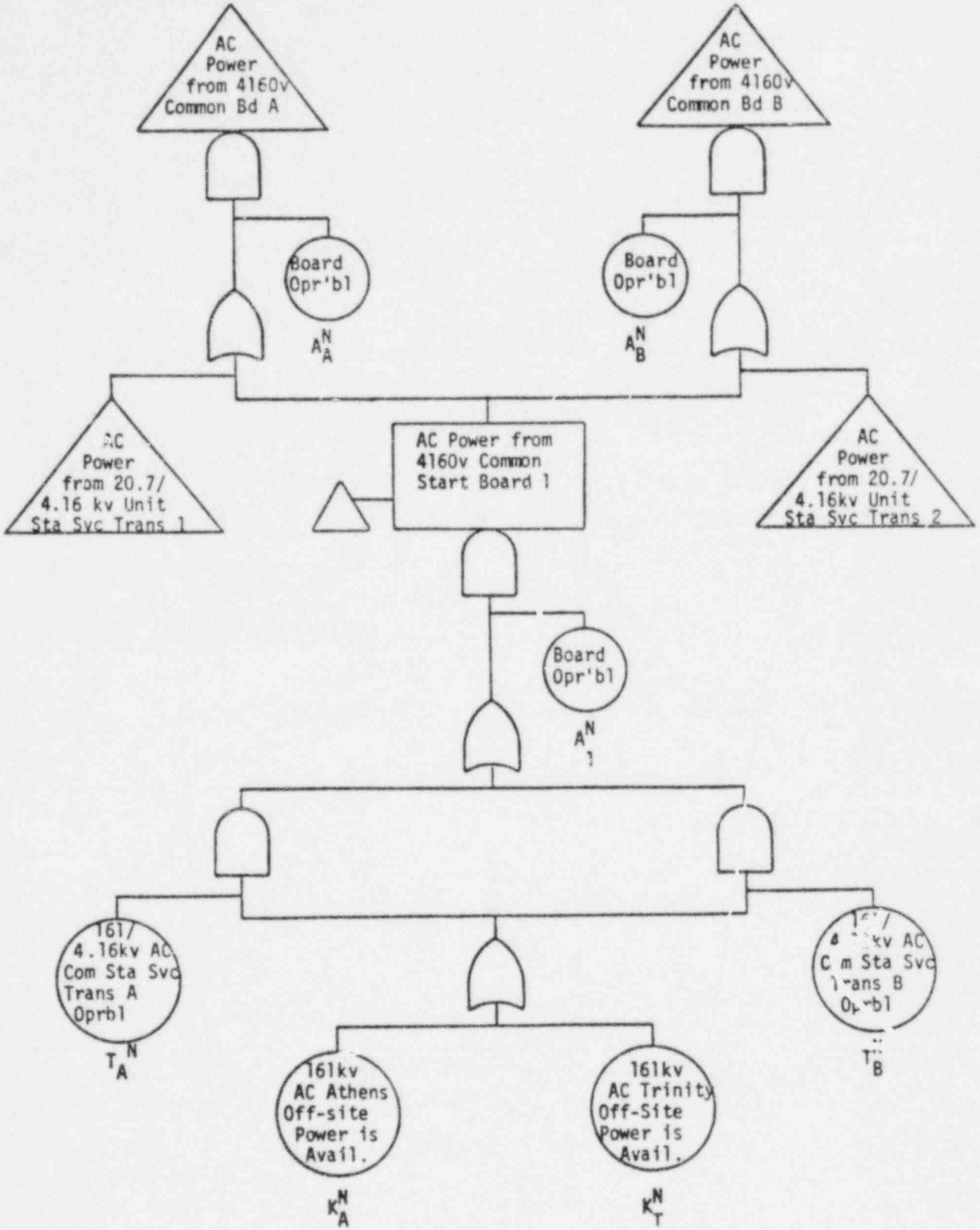


Figure B-10 (cont)

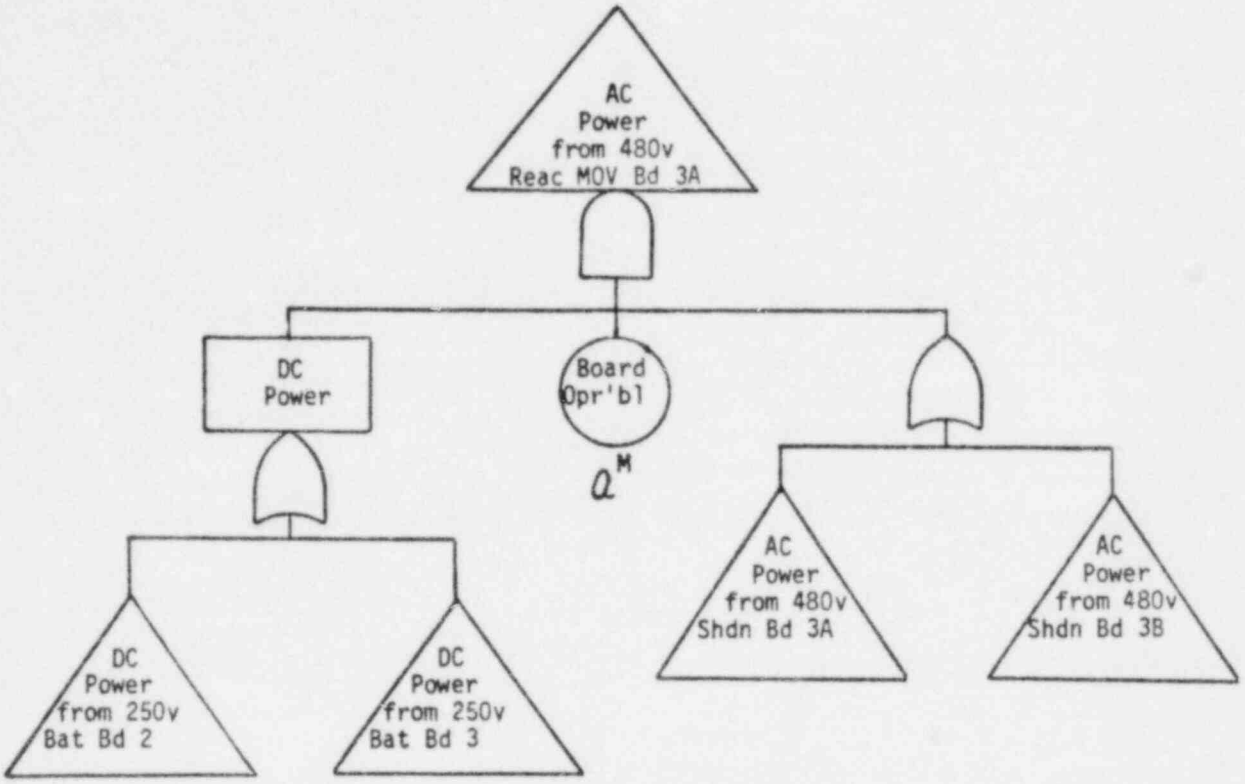


FIGURE B-11.

SUCCESS TREE FOR AC REACTOR MOTOR-OPERATED VALVE ELECTRIC POWER

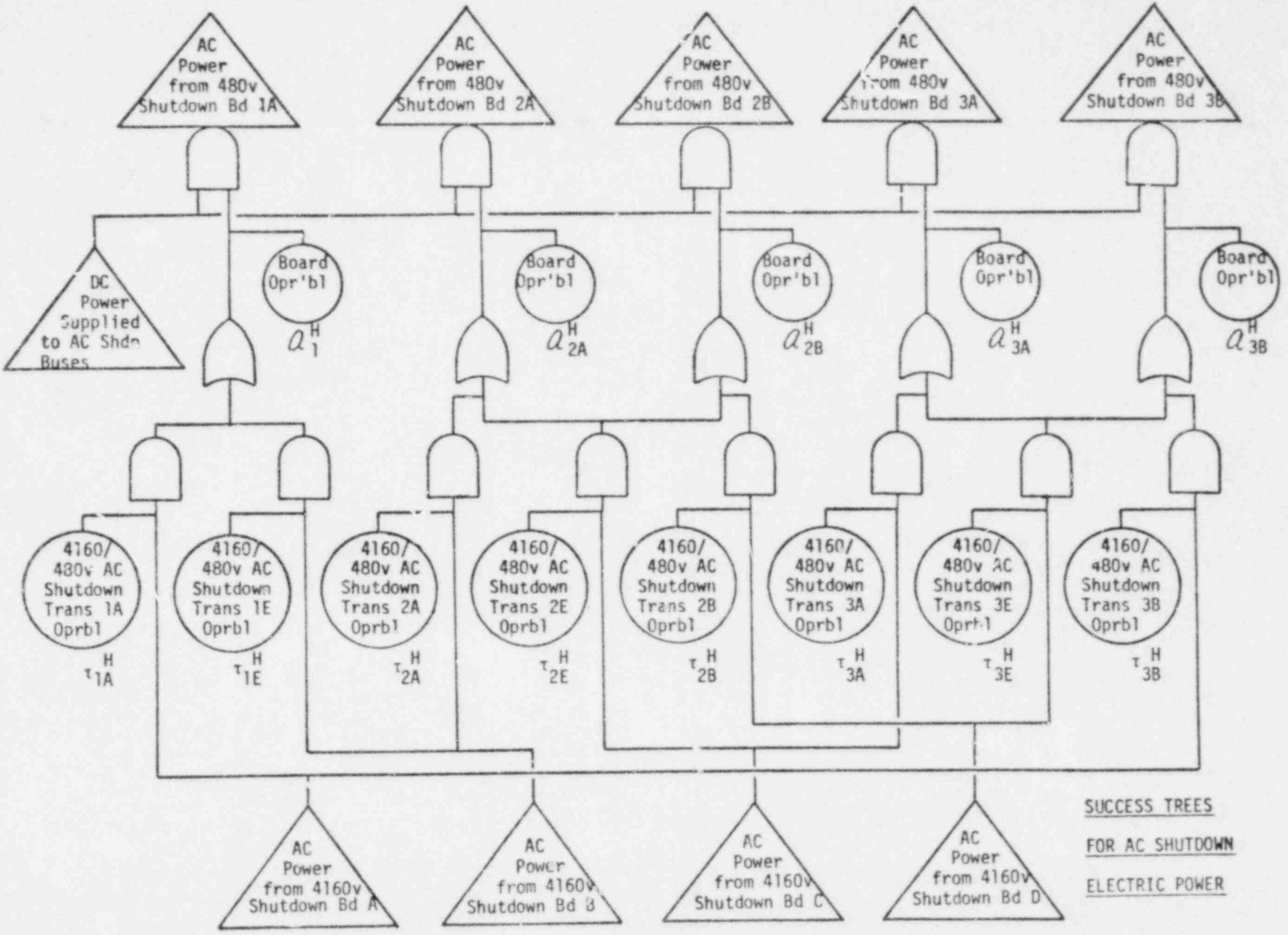

AC Power from 480v Shutdown Bd 1A
AC Power from 480v Shutdown Bd 2A
AC Power from 480v Shutdown Bd 2B
AC Power from 480v Shutdown Bd 3A
AC Power from 480v Shutdown Bd 3B
DC Power Supplied to AC Shdn Buses
Board Opr'bl
a^H_1
Board Opr'bl
a^H_{2A}
Board Opr'bl
a^H_{2B}
Board Opr'bl
a^H_{3A}
Board Opr'bl
a^H_{3B}
4160/ 480v AC Shutdown Trans 1A Oprbl
τ^H_{1A}
4160/ 480v AC Shutdown Trans 1E Oprbl
τ^H_{1E}
4160/ 480v AC Shutdown Trans 2A Oprbl
τ^H_{2A}
4160/ 480v AC Shutdown Trans 2E Oprbl
τ^H_{2E}
4160/ 480v AC Shutdown Trans 2B Oprbl
τ^H_{2B}
4160/ 480v AC Shutdown Trans 3A Oprbl
τ^H_{3A}
4160/ 480v AC Shutdown Trans 3E Oprbl
τ^H_{3E}
4160/ 480v AC Shutdown Trans 3B Oprbl
τ^H_{3B}
AC Power from 4160v Shutdown Bd A
AC Power from 4160v Shutdown Bd B
AC Power from 4160v Shutdown Bd C
AC Power from 4160v Shutdown Bd D
SUCCESS TREES
FOR AC SHUTDOWN
ELECTRIC POWER

Figure B-12

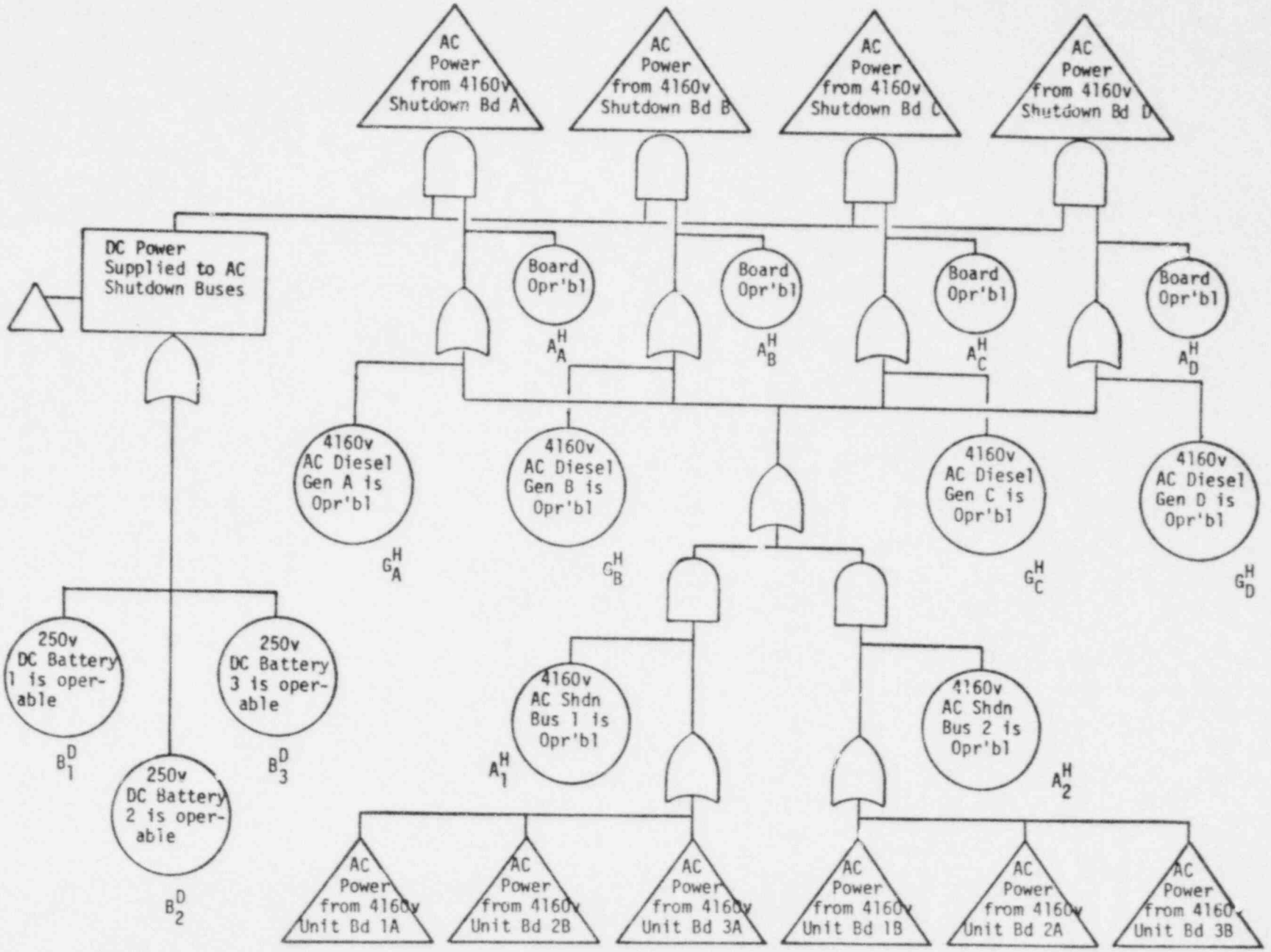


Figure B-12 (cont)

discharge volume (SDV) responsible for the BF3 partial failure-to-scram. One such contributor, the length of the drain line from the east bank SDV to the scram instrument volume (SIV), does not represent a systems interaction, but rather a component deficiency within a system (CRS). Others, such as inadequate ventilation of the SDV as provided by the exhaust fans of the Reactor Building Equipment Drain Sump (RBEDS) through each SDV vent line and, also, the slow opening of the scram inlet and exhaust valves (causing inleakage to the SDVs) due to slow loss of control air pressure (as identified by Michelson[5]), represent potential systems interactions. Note that these two each involve interaction between a safety (CRS) and a non-safety (RBEDS or Control Air) system. These interactions have been identified on the success trees for the east and west bank SDVs being empty prior to scram (see Figure B-5). Should the analyst's goal be merely to identify the interactions related to the BF3 incident, he could stop here.

At this point, it seems worthwhile to observe that the success tree itself does not necessarily identify these interactions, particularly for this incident. Without previous knowledge,[1,2,5] it is questionable whether such subtle interactions as these involving RBEDS ventilation and control air pressure availability would be identified by the analyst in the process of developing the success tree. However, what the success (or fault) tree does provide is a logical framework within which the analyst is led to consider many possible interaction mechanisms, hopefully resulting in his identification of the more subtle ones.

Note that an event such as slow loss of control air pressure represents a partial failure with consequences distincly different from those of a rapid loss[5] (a total failure). Neither success nor fault trees are especially

adaptable to modelling partial failures (or partial successes). On the overall success tree used in this BF3 exercise, this issue has been circumvented by considering the availability of control air pressure to presume no loss of pressure (not even a slow loss). However, the analyst must still recognize the possibility of a slow loss.

Since the primary goal of this exercise is to demonstrate the use of the proposed systems interaction methodology, the overall success tree has been resolved to levels beyond those needed just for identifying the interactions leading to the BF3 incident. Both RBEDS ventilation and control air pressure availability have been developed in Figure B-6 . Further, both the DC and AC electric power supplies to all systems and components needed for success of Reactor Control during the Power Operation to Hot Shutdown transition have been developed in Figures B-7 through B-12.

In an overall systems interaction analysis, the support systems must be developed in order to identify potential interactions at their level. Such systems provide common auxiliary support to numerous plant systems, and these represent potential "pathways" for systems interactions. Again, the degree of detail shown on the tree in this exercise is indicative of the type and amount of information readily available from an FSAR. Only major components (such as electrical boards, buses, and transformers) have been included. Remembering that this example represents only one plant mode of a single safety function, one should appreciate the amount of detail needed in an overall analysis.

The potential systems interactions can be identified from success trees in various ways. If the trees are relatively simple, inspection may

be sufficient. However, for more complex trees, a more rigorous scheme involving Boolean equations or their equivalents becomes practical. Suppose that success of event A requires success of event B or event C (an OR situation); the Boolean success equation becomes $A = B + C$. For failure of event A, failure of both events B and C is necessary (an AND situation); the Boolean failure equation becomes $\bar{A} = \bar{B} \cdot \bar{C}$ (where a bar indicates failure). The success of event A may be represented by a success tree with an OR gate having success events B and C as inputs. The failure of event A can be shown as a fault tree with an AND gate having failure events B and C as inputs. The two are complementary.

The pair of failure events $\bar{B}$ and $\bar{C}$ is known as a "minimal cut set" (see Section A.2.1), sufficient for failure of TOP event A. The determination of minimal cut sets is one means of identifying systems interactions. Note that not all minimal cut sets represent failures due to systems interactions. Some may correspond to hardware failures of components within a single system, while others refer to unrelated failures of components in different systems. However, some may represent related failures between systems, usually through their components; these are characteristic of systems interactions.

Consider the example in this exercise. Minimal cut sets are most readily found from fault trees; thus, the overall success tree (see Figures B-3 through B-12) for Reactor Control during the Power Operation to Hot Shutdown transition has been transformed into its equivalent fault tree (see corresponding Figures B-13 through B-22). For demonstration purposes, the computer program MFAULT[6] has been used to find the minimal cut sets for failure of SLC. This has been selected as the TOP event rather than

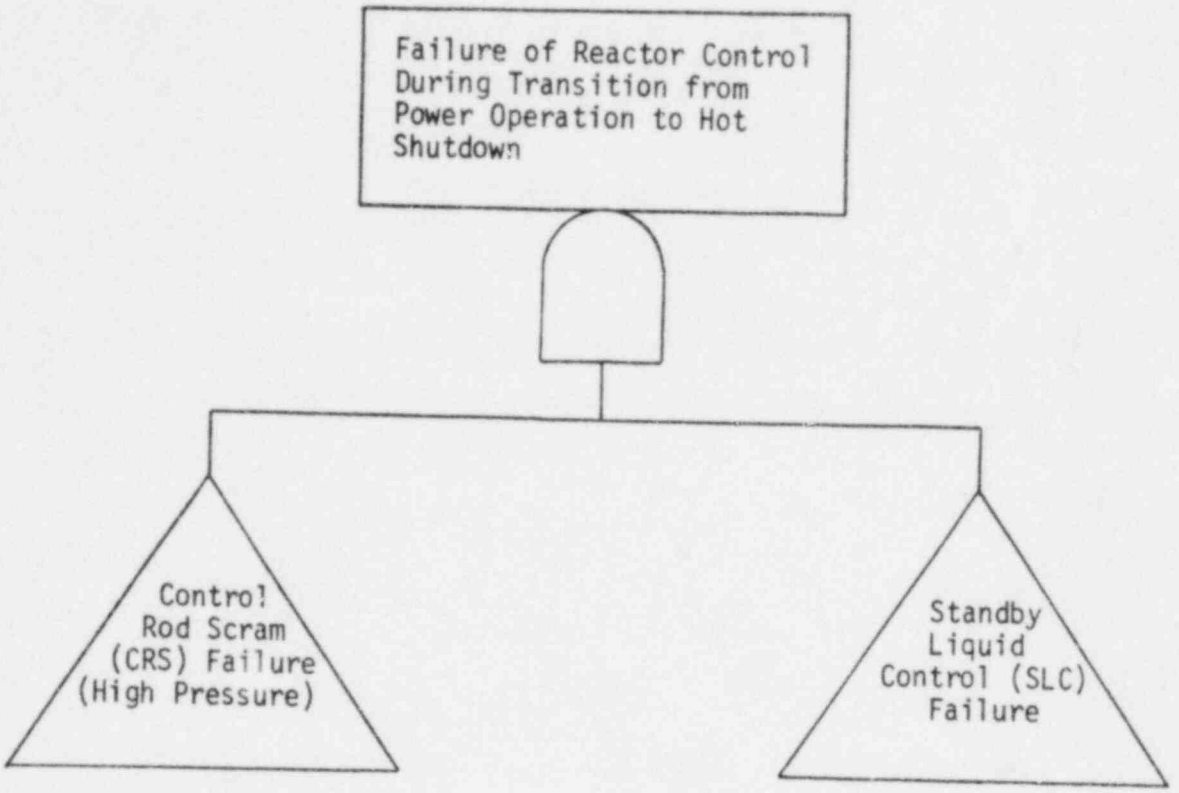


FIGURE B-13.
TOP OF FAULT TREE FOR REACTOR CONTROL DURING TRANSITION FROM POWER OPERATION TO HOT SHUTDOWN

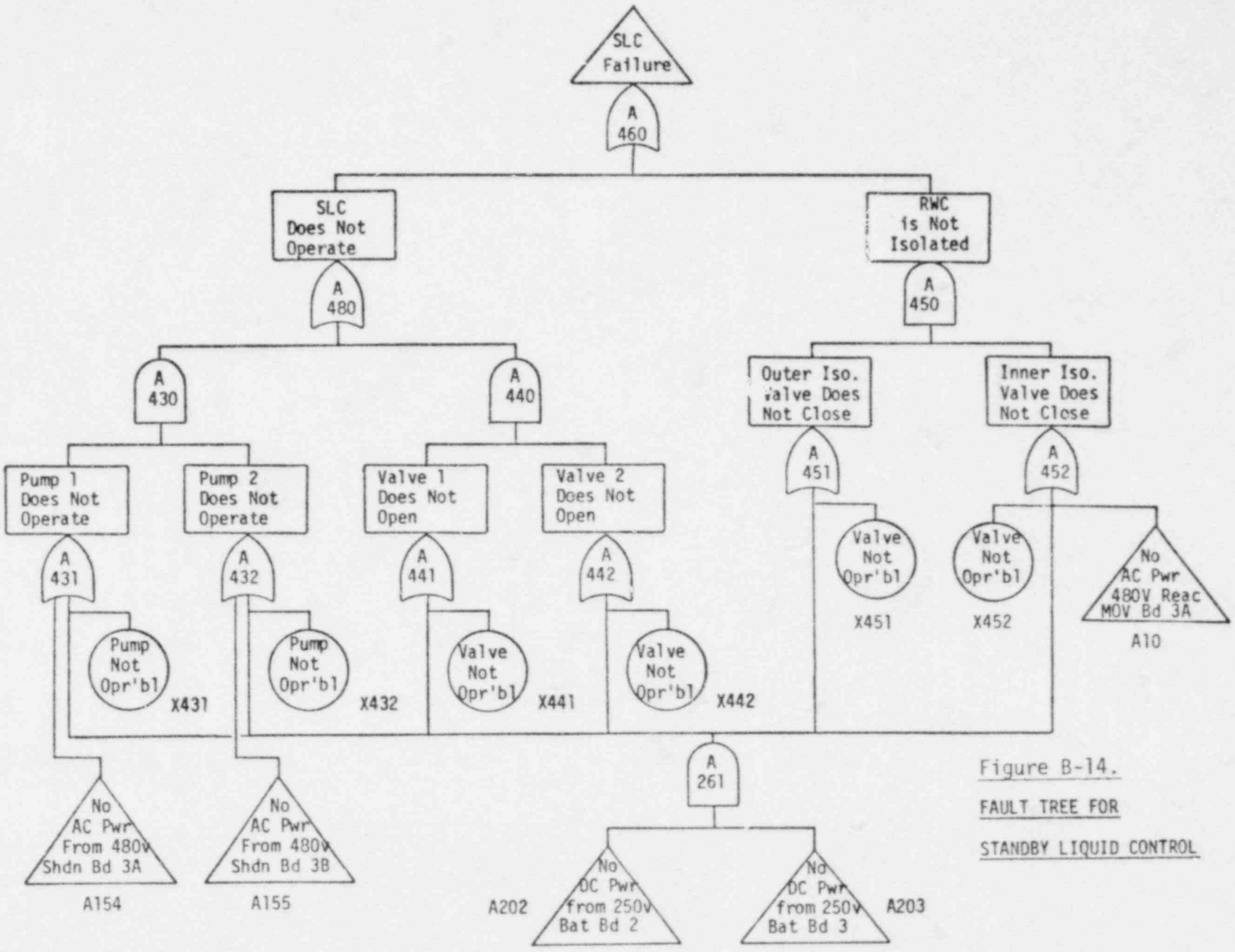


Figure B-14.

FAULT TREE FOR

STANDBY LIQUID CONTROL

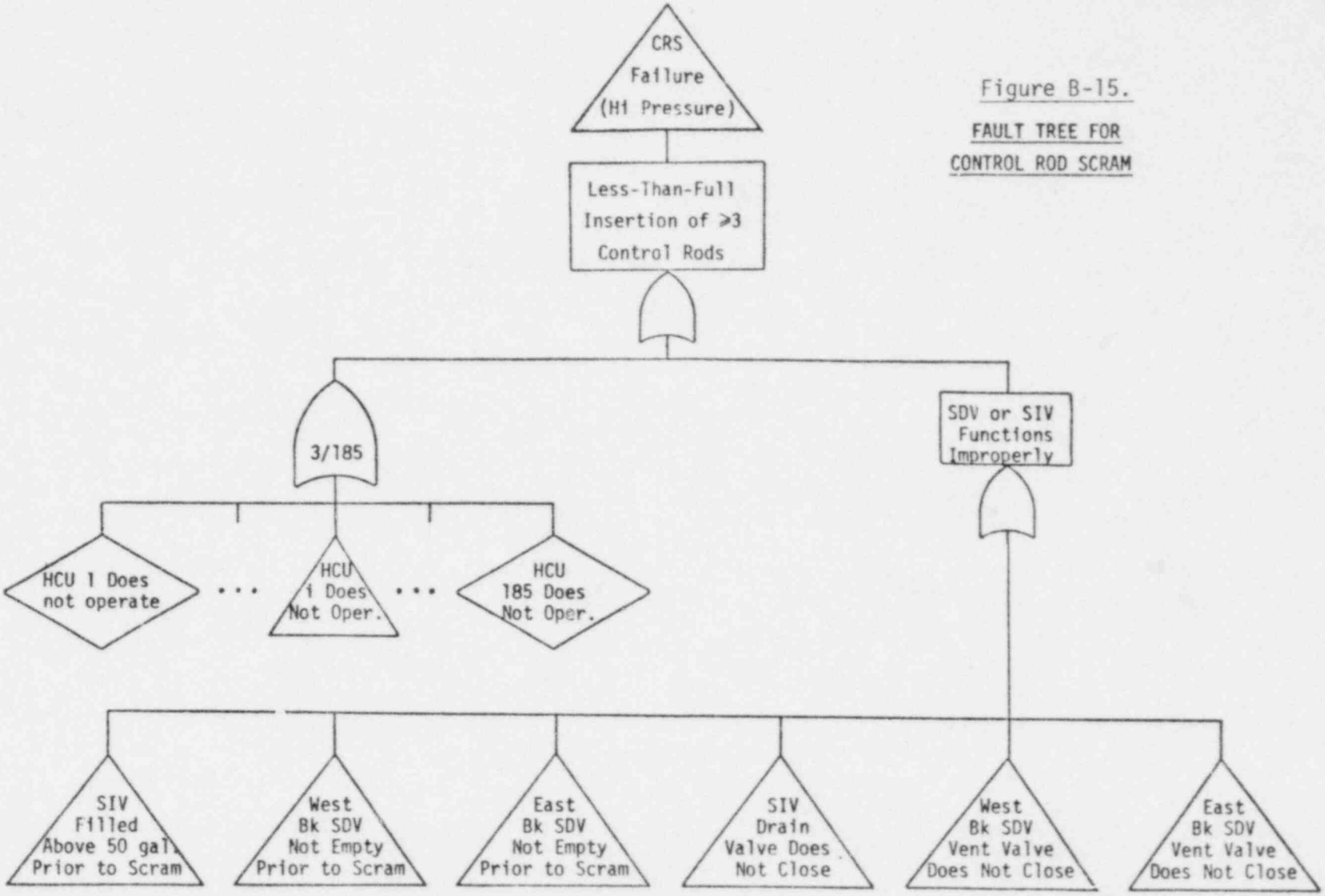


Figure B-15.

FAULT TREE FOR
CONTROL ROD SCRAM

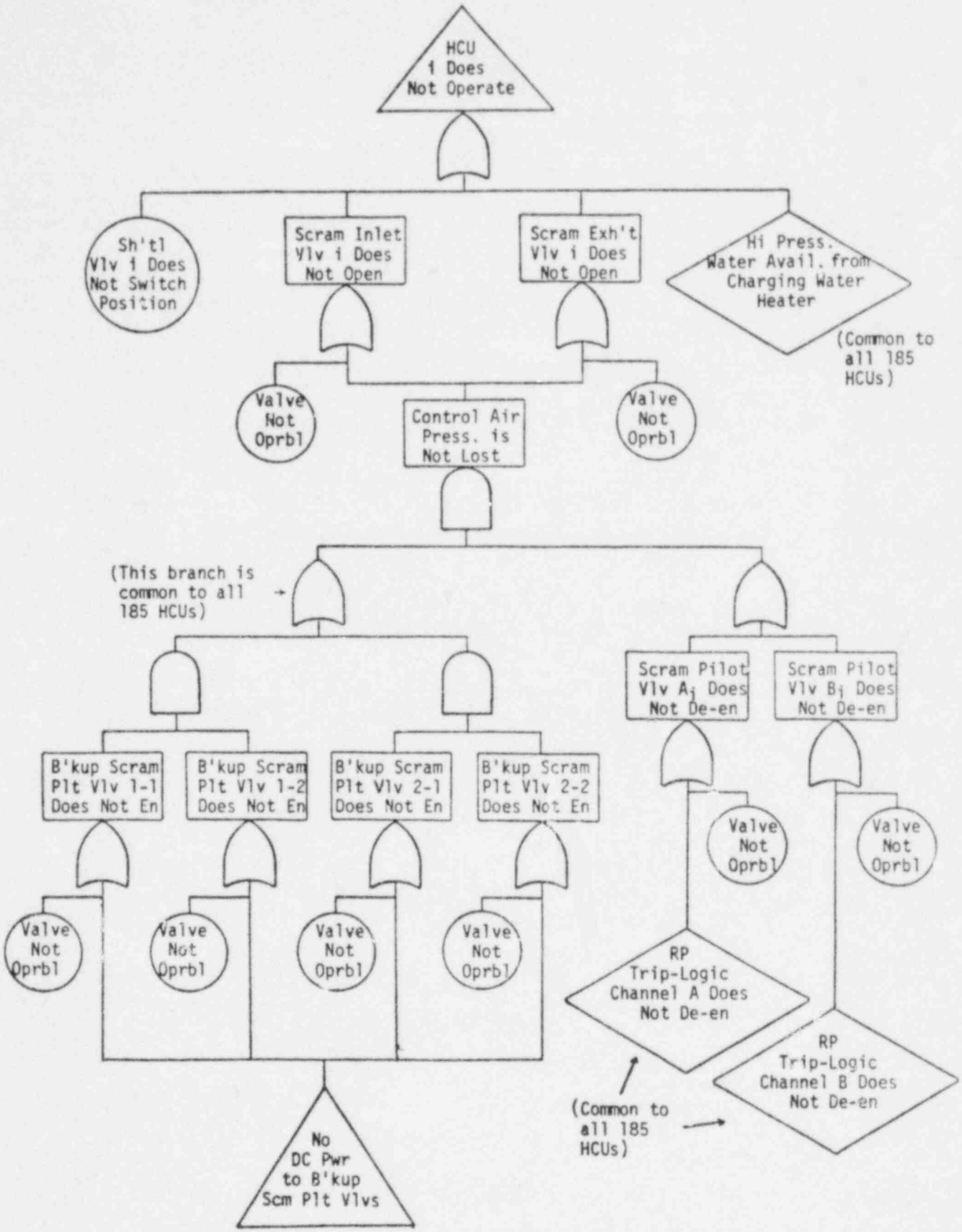
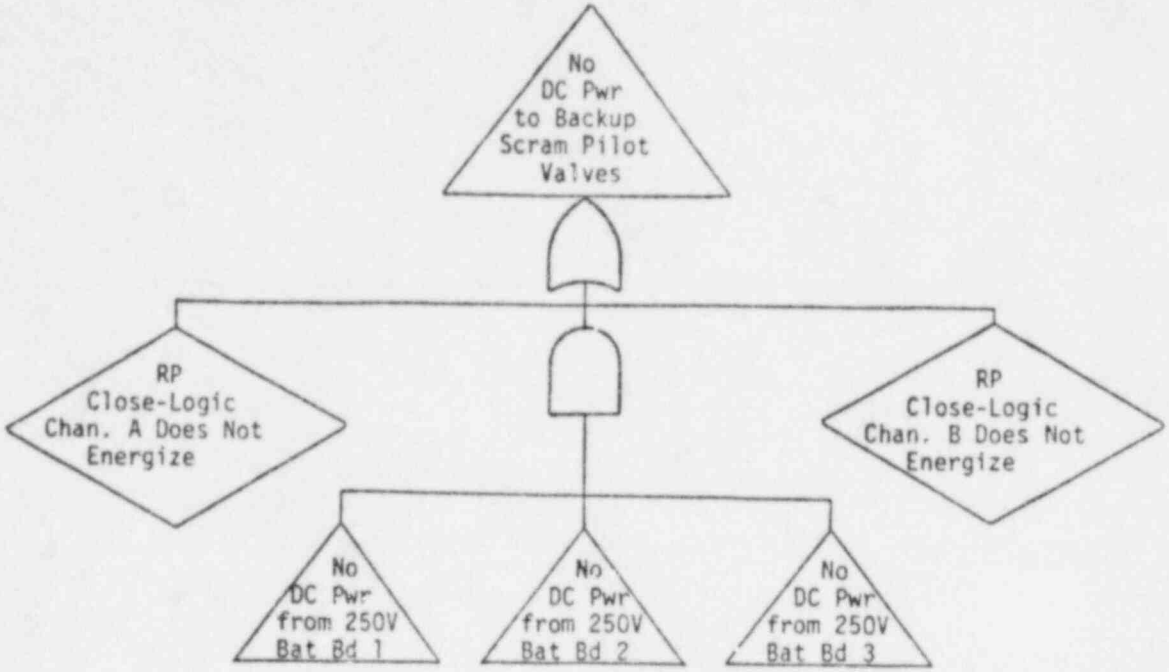


Figure B-15 (cont)



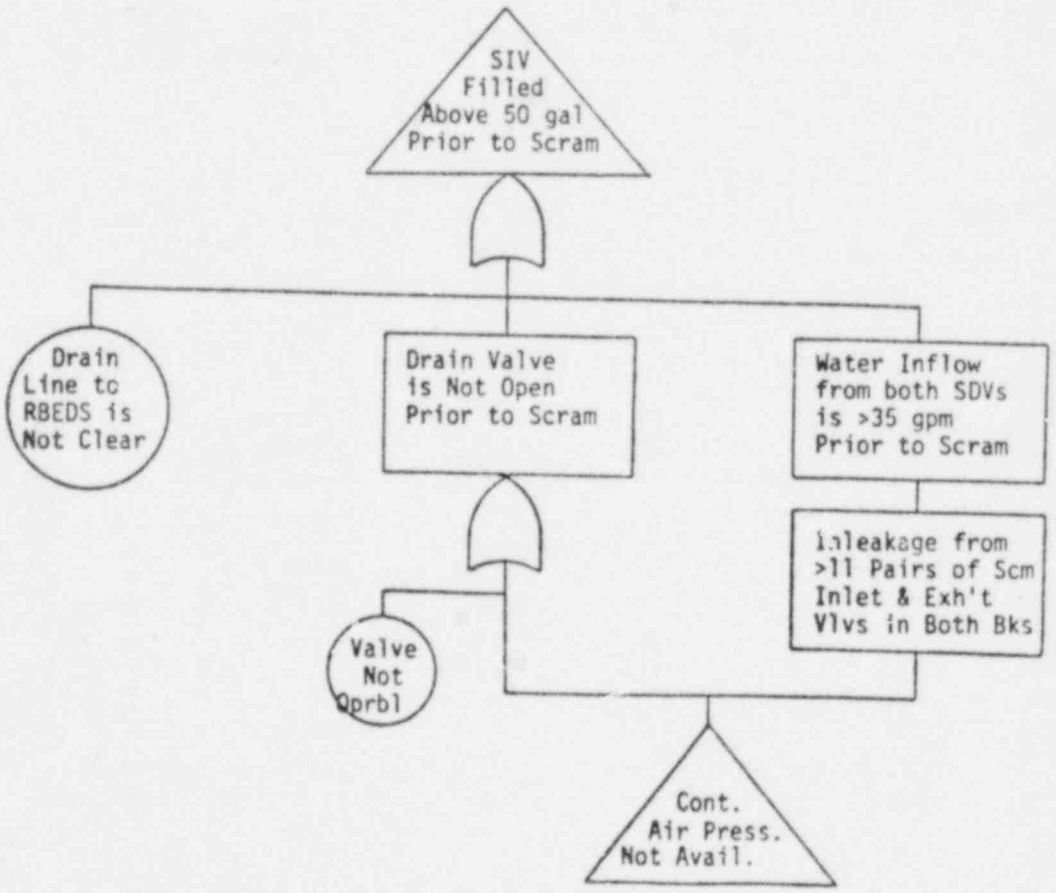


Figure B-15 (cont)

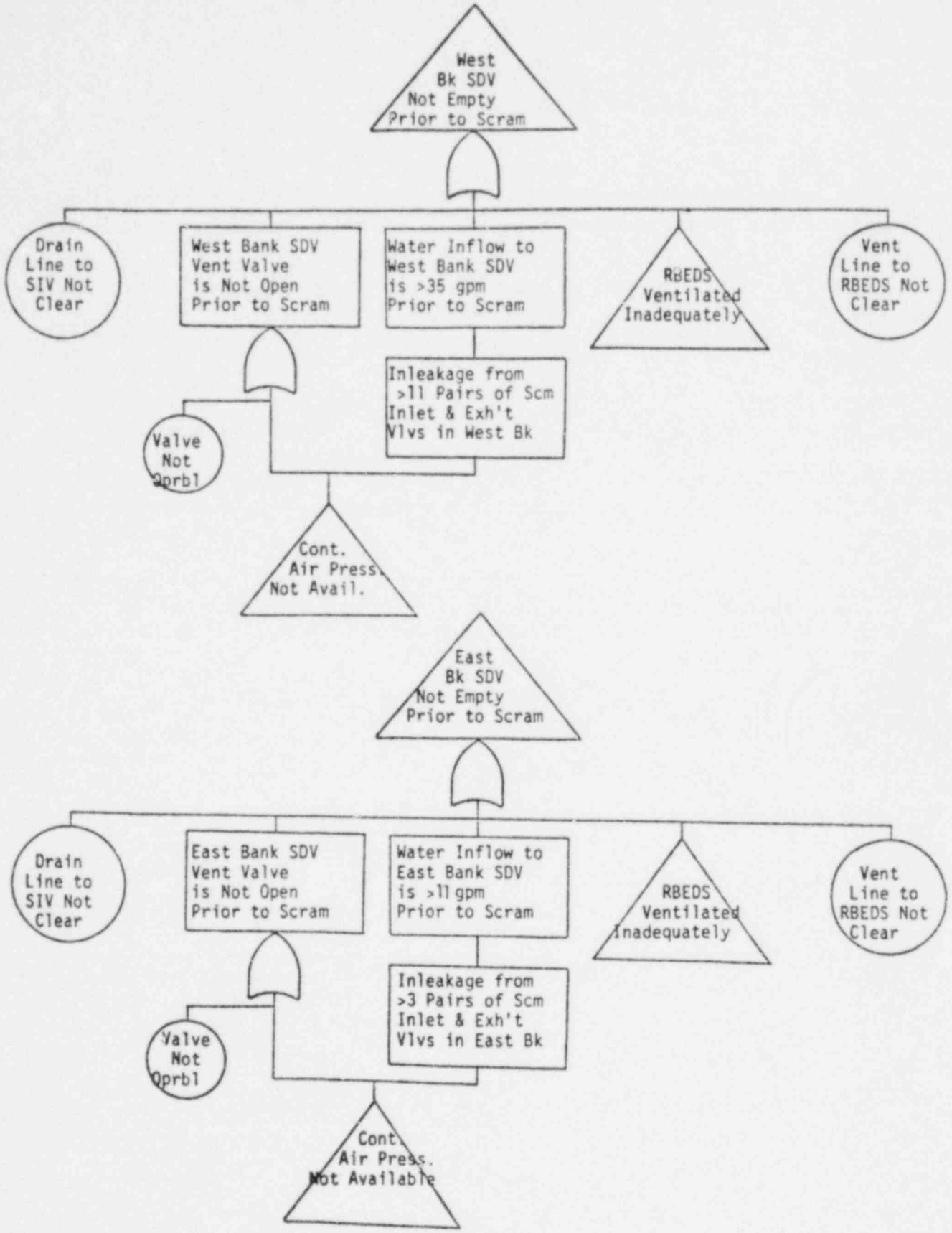


Figure B-15 (cont)

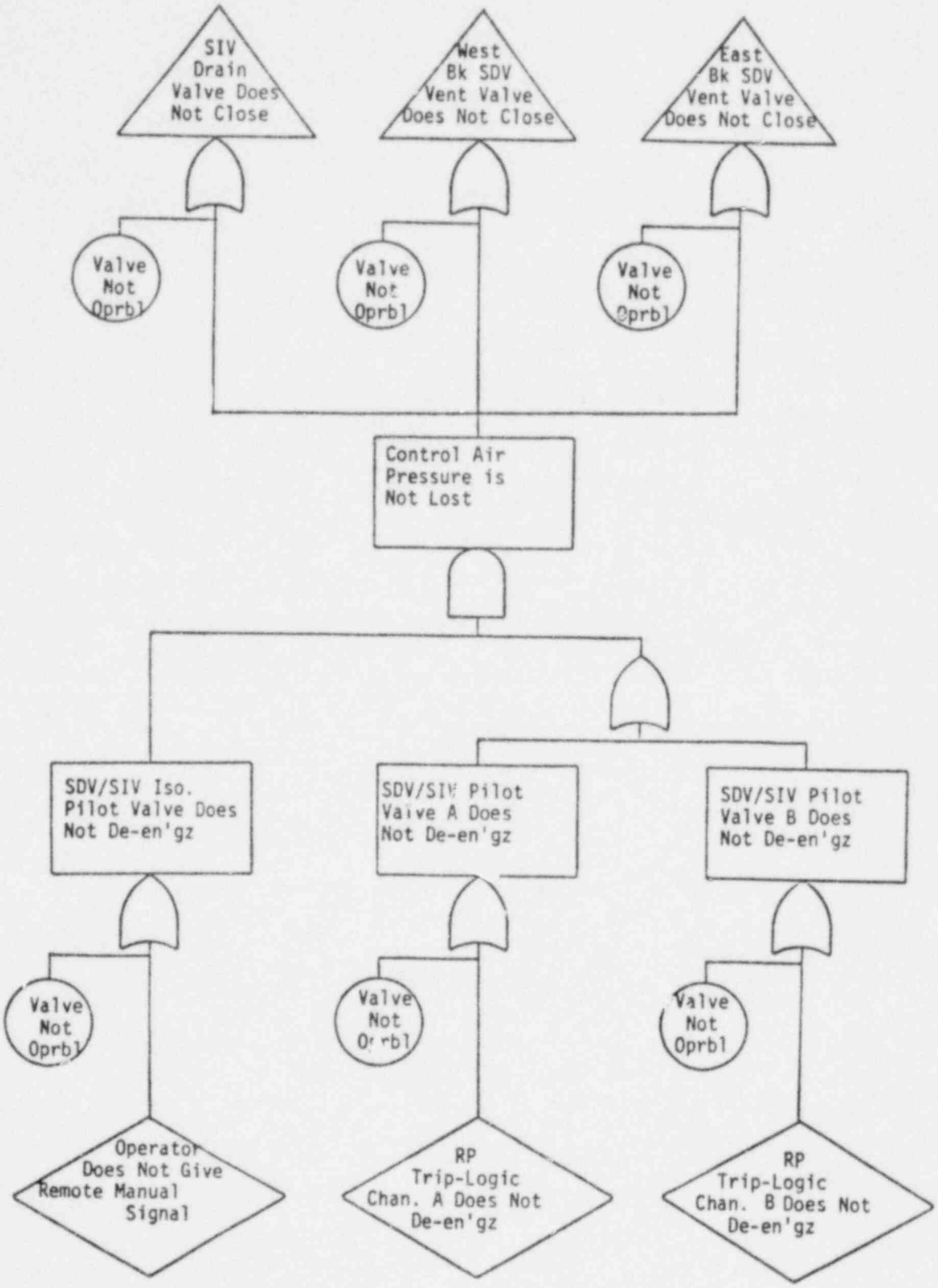


Figure B-15 (cont)

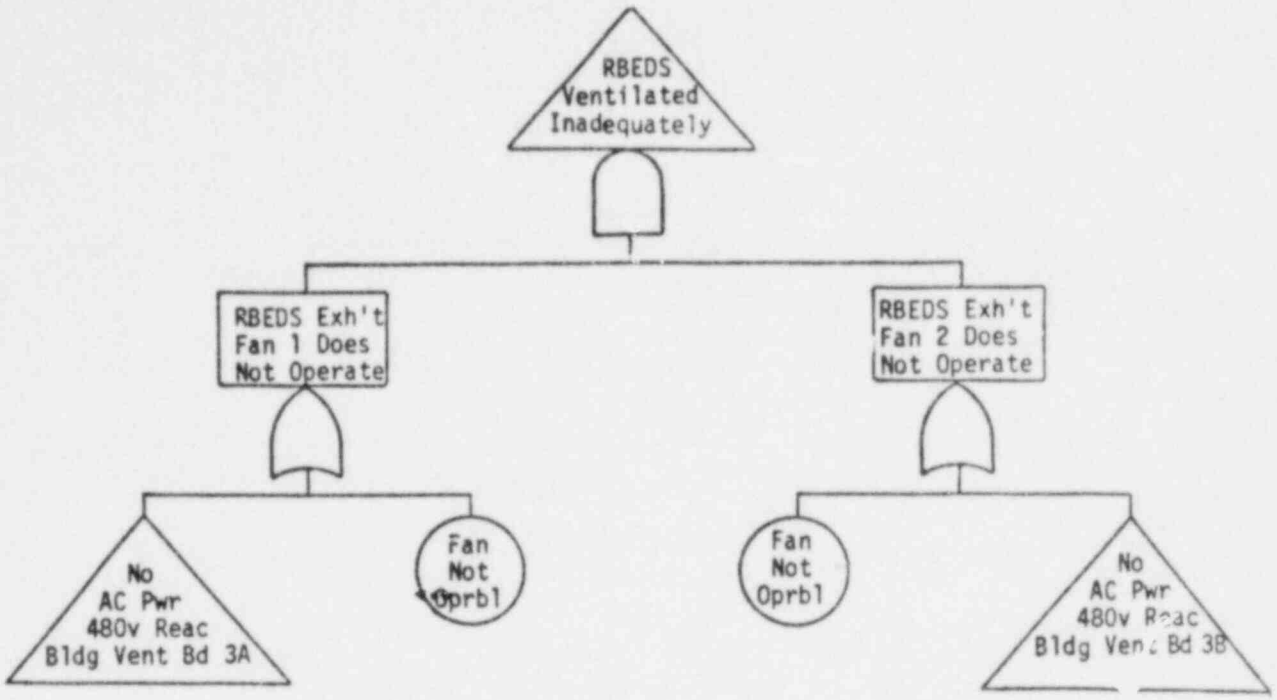
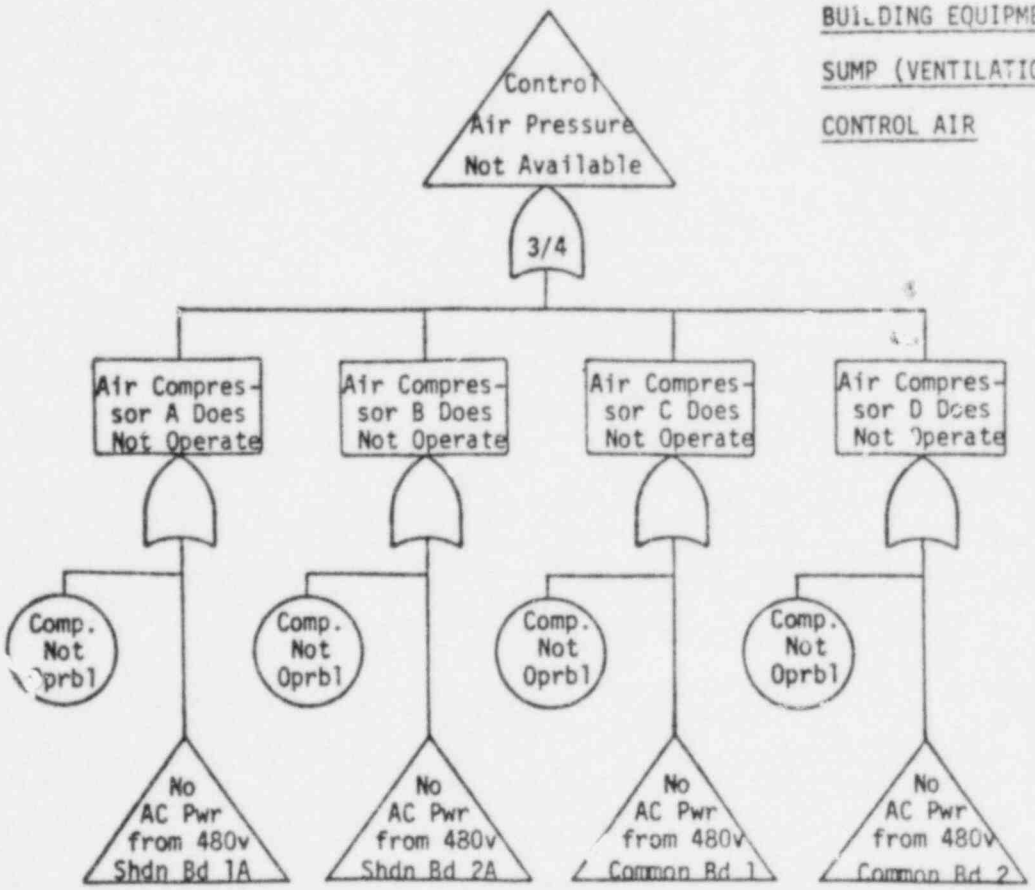


Figure B-16. FAULT TREES FOR REACTOR BUILDING EQUIPMENT DRAIN SUMP (VENTILATION) & CONTROL AIR



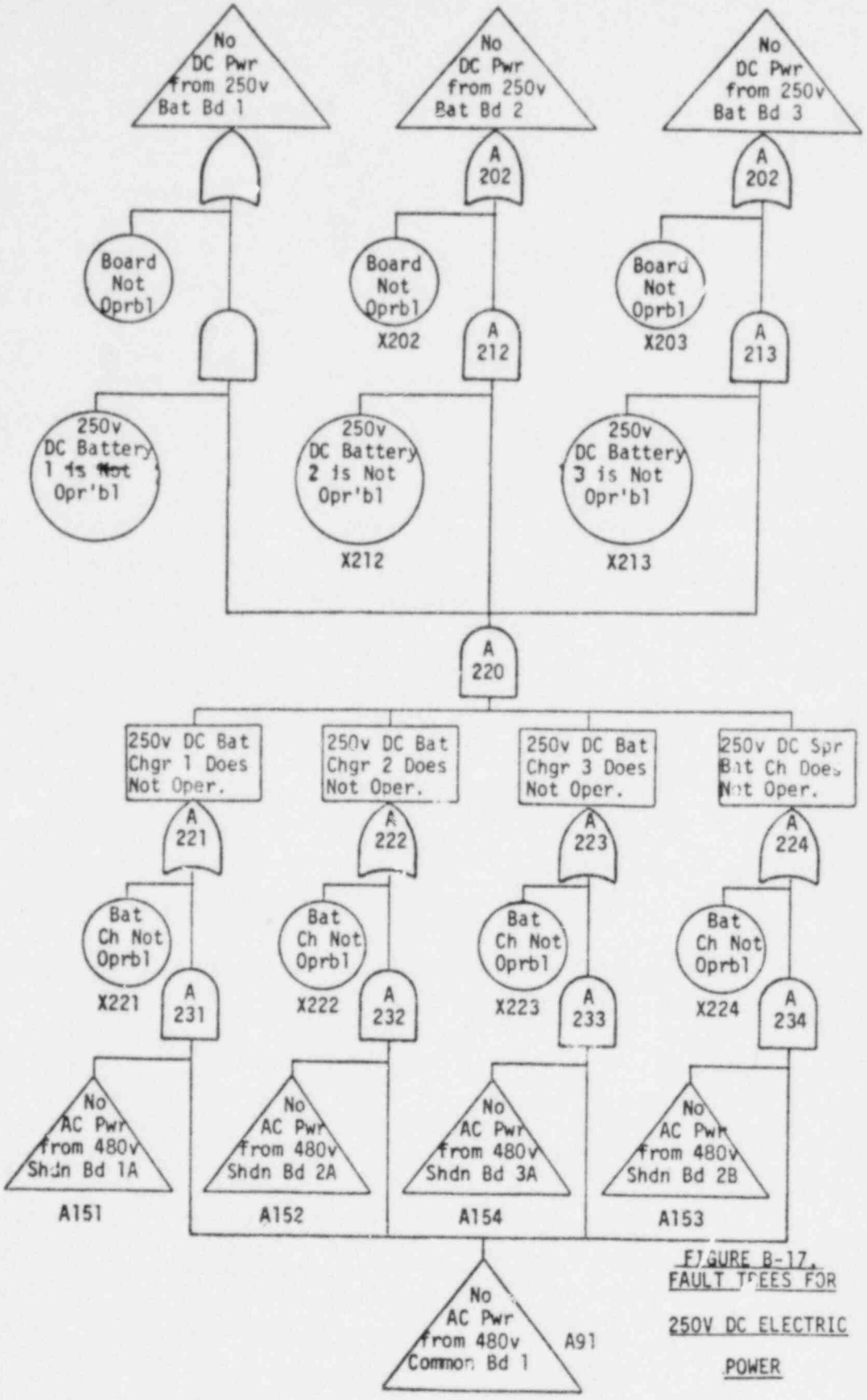


FIGURE B-17. FAULT TREES FOR 250V DC ELECTRIC POWER

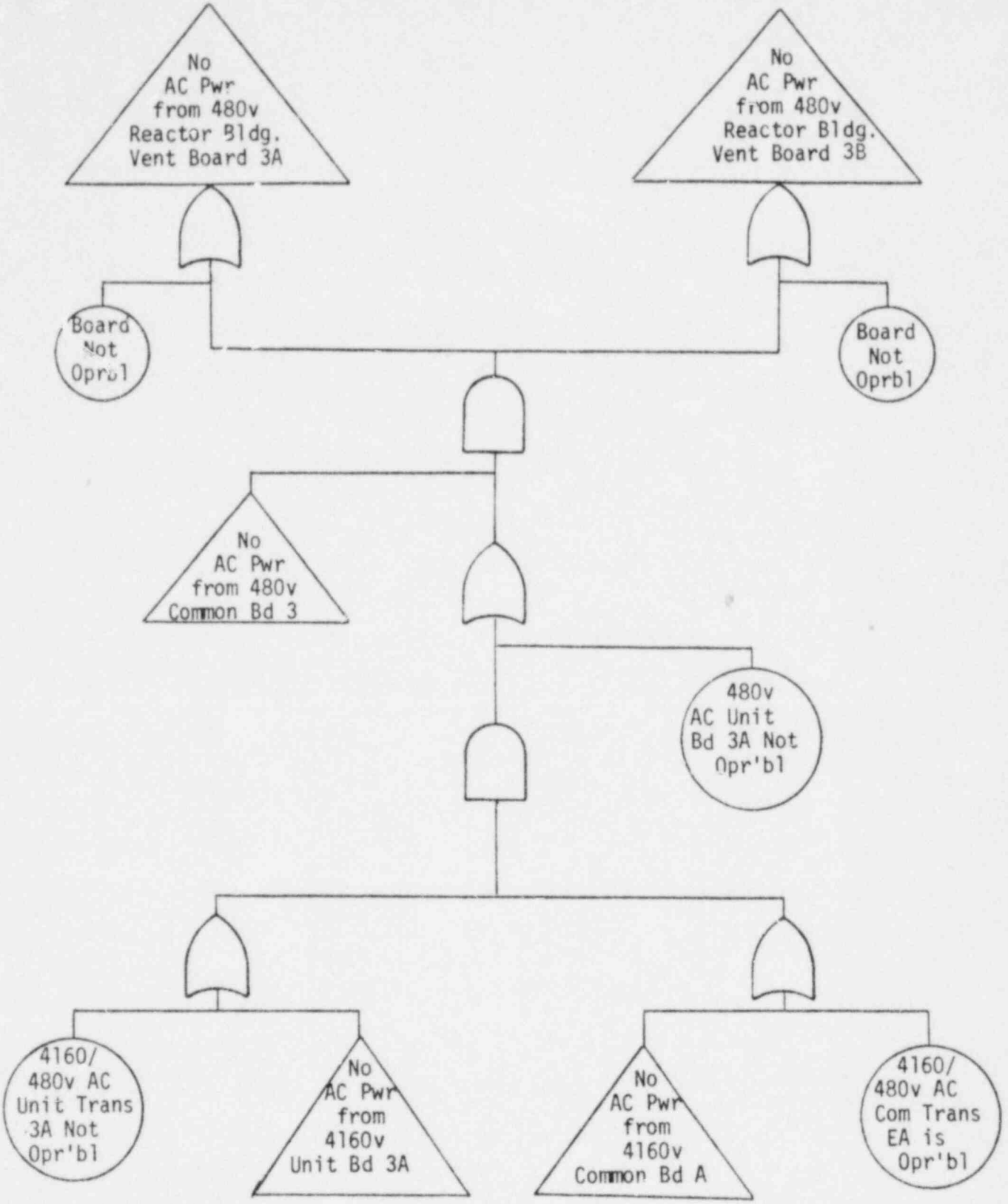


FIGURE B-18.

FAULT TREES FOR AC REACTOR BUILDING VENTILATION ELECTRIC POWER

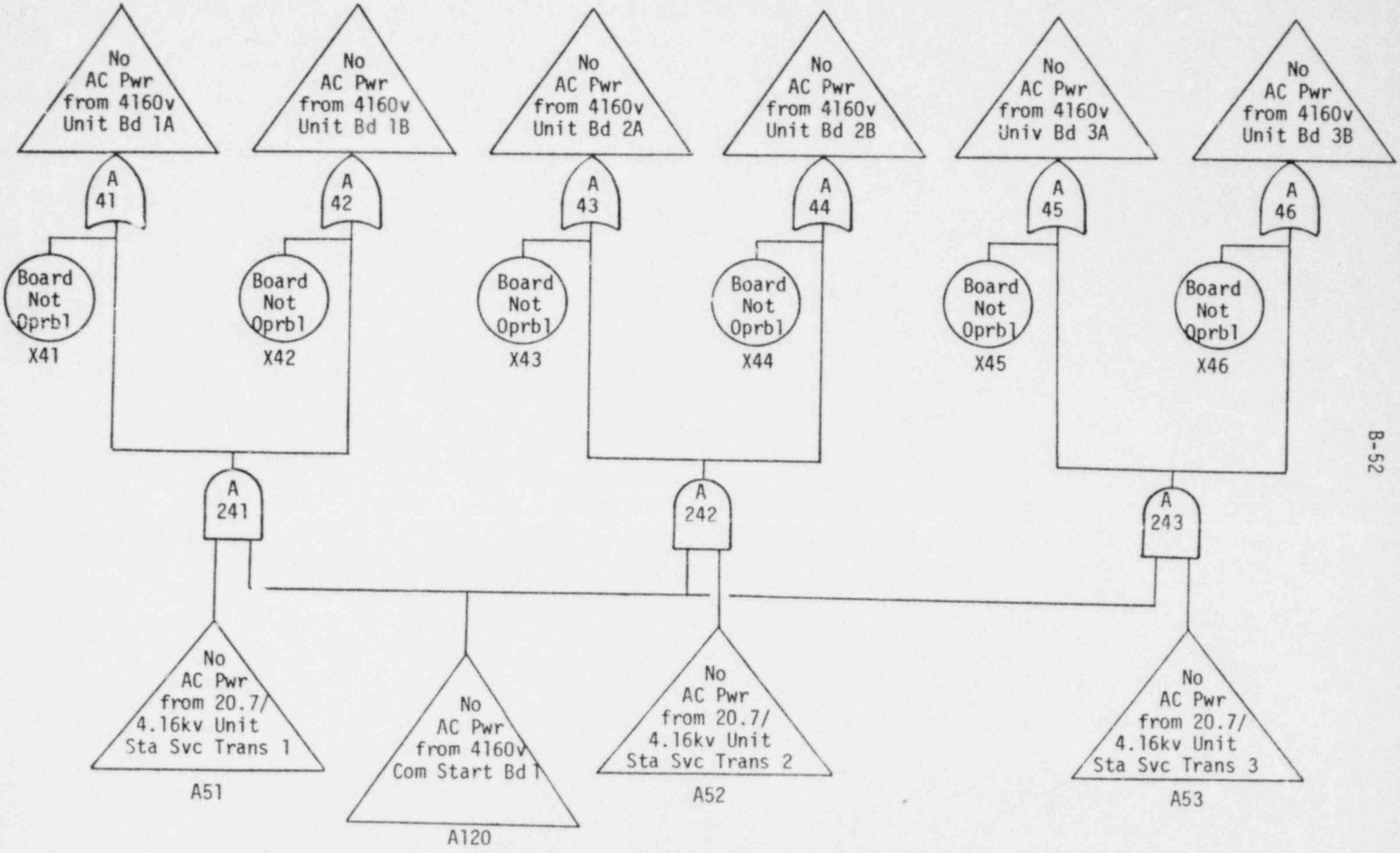


FIGURE B-19.

FAULT TREES FOR AC UNIT ELECTRIC POWER

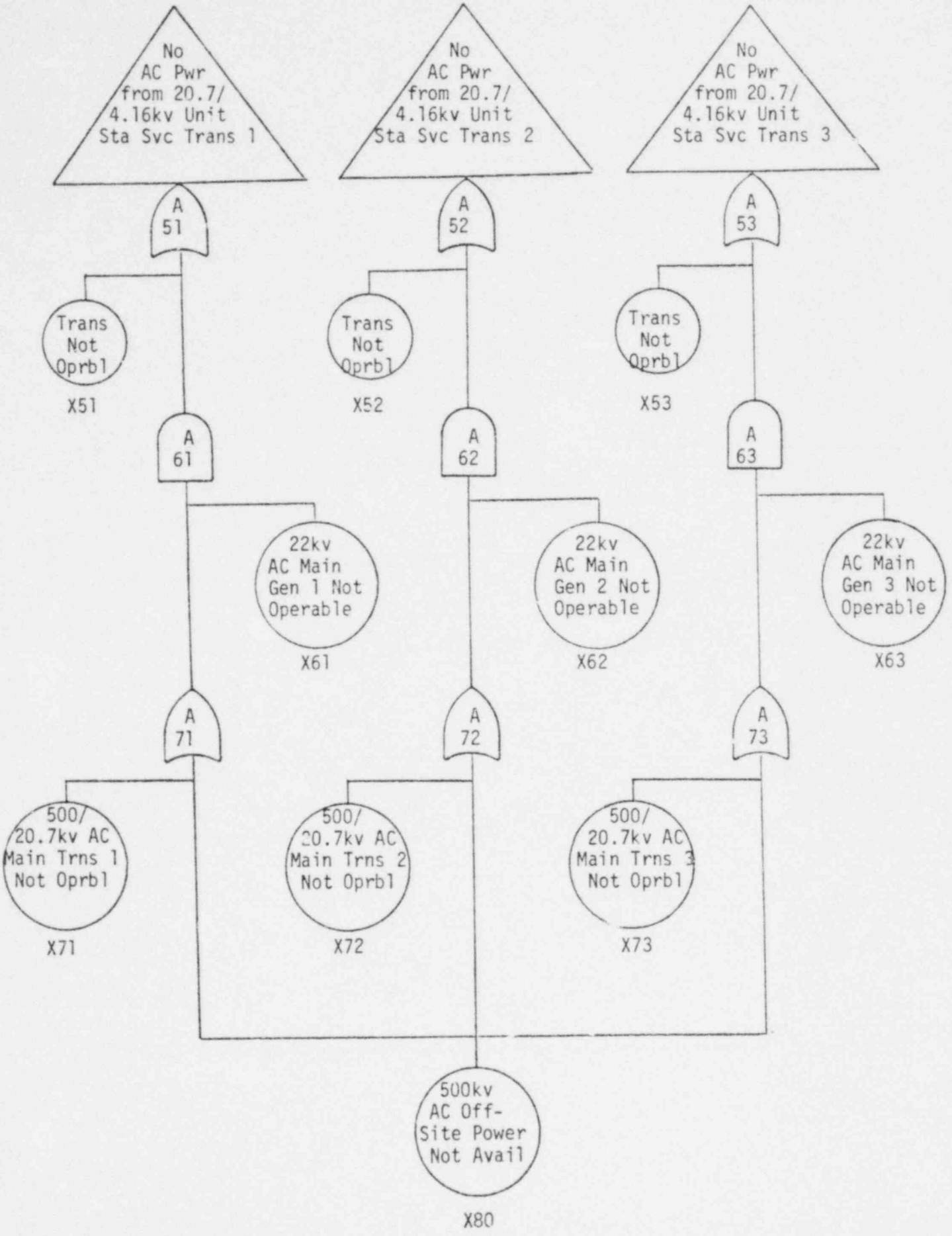


FIGURE B-19 (cont)

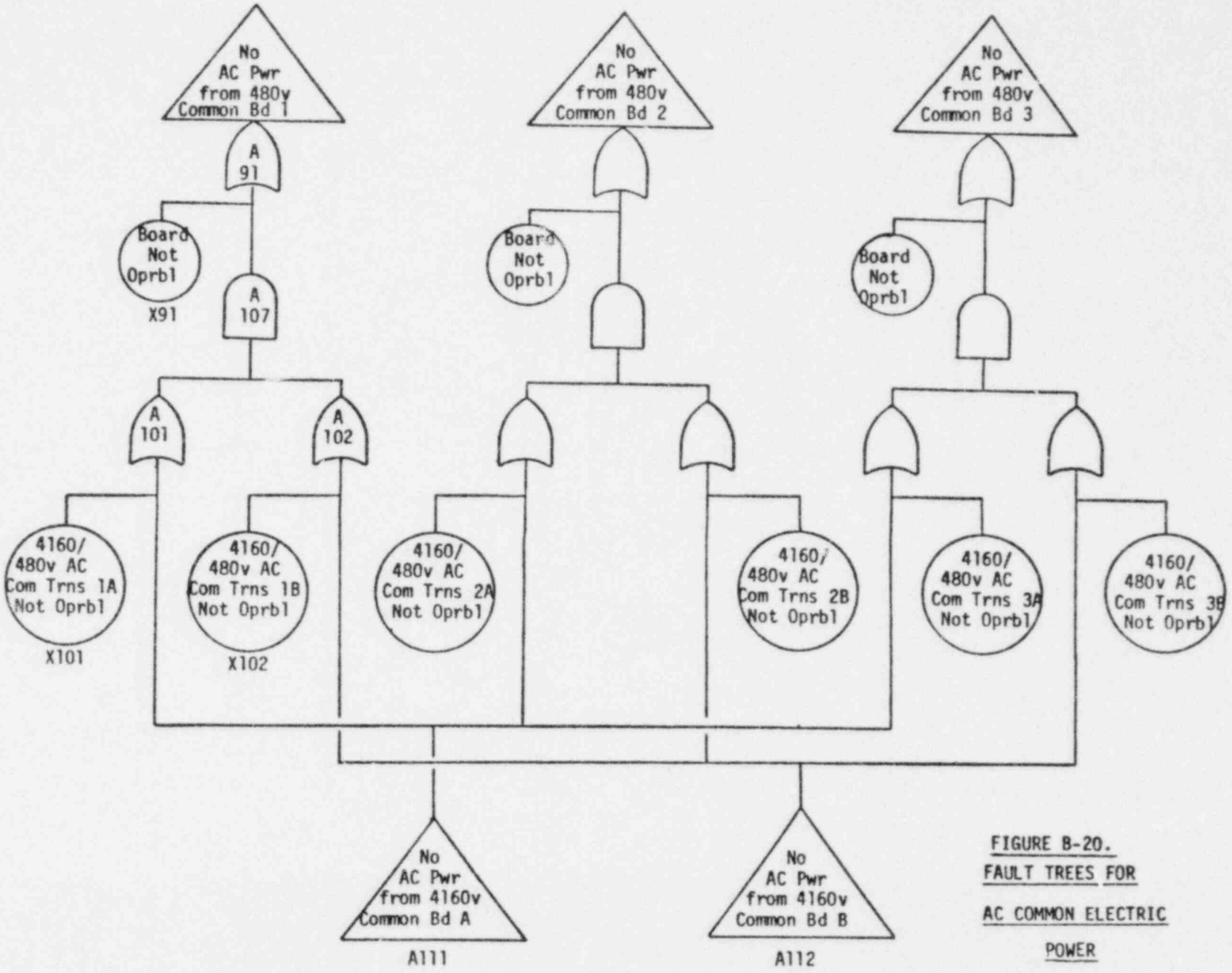


FIGURE B-20.
FAULT TREES FOR
AC COMMON ELECTRIC
POWER

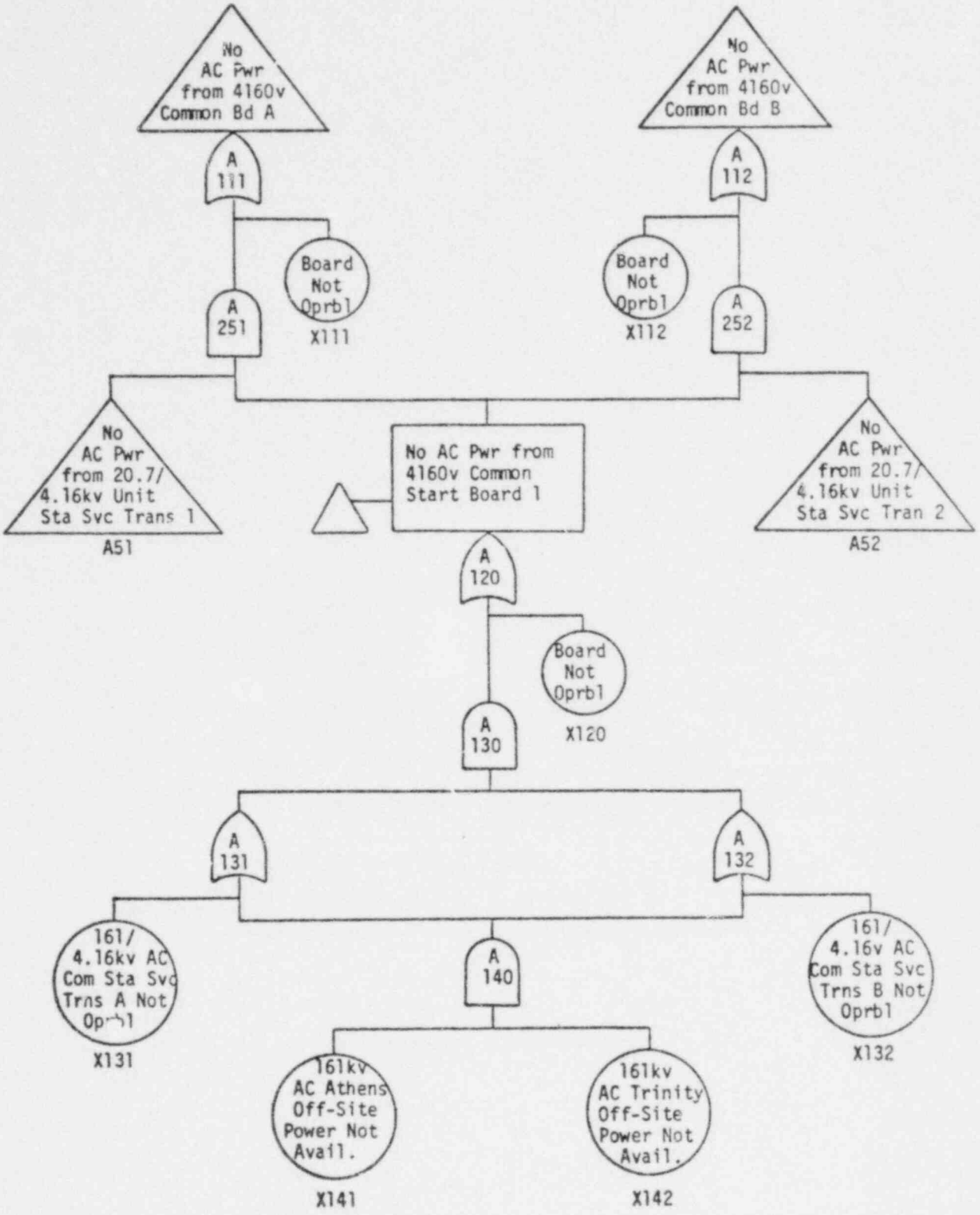


Figure B-20 (cont)

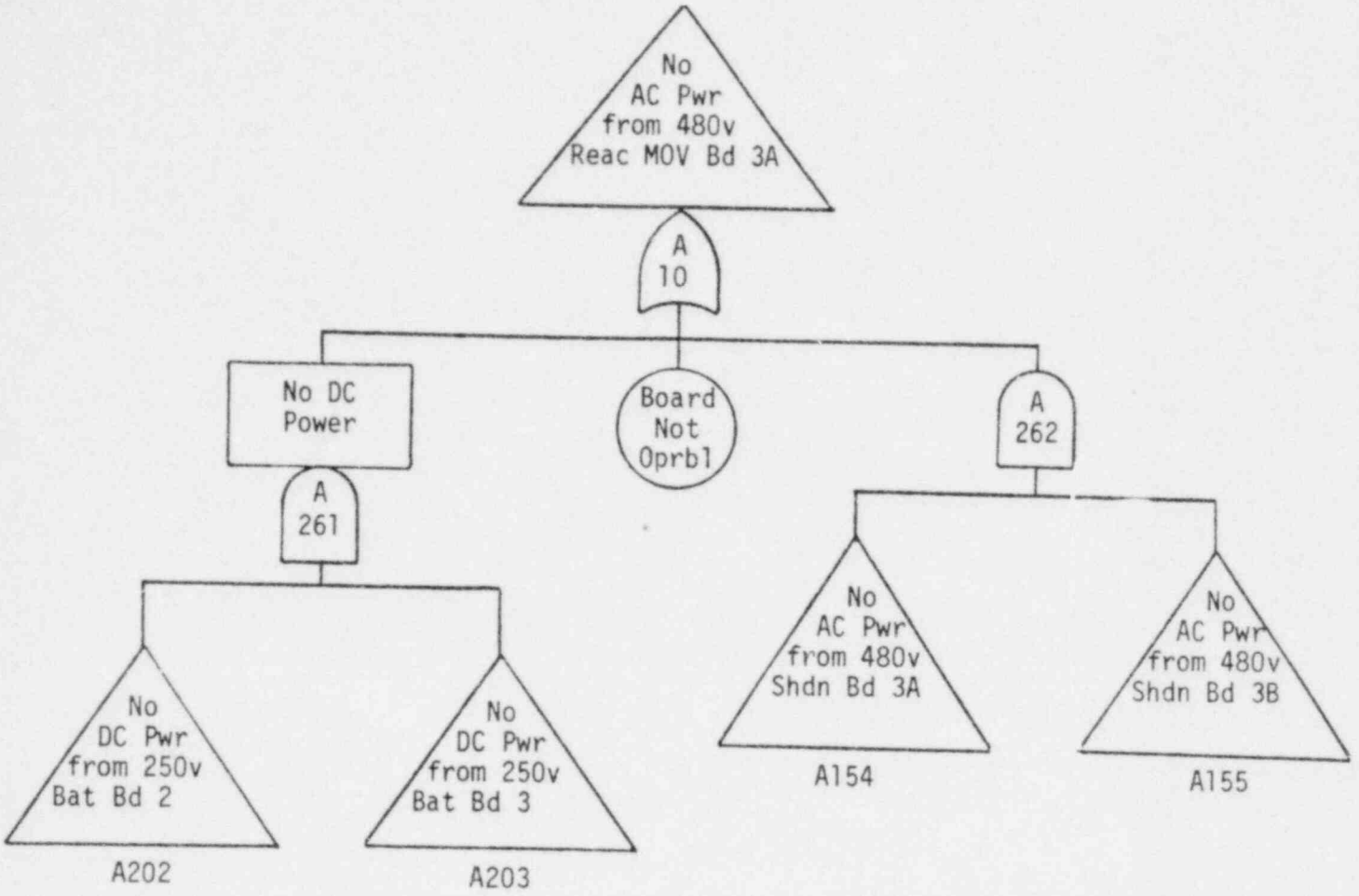


FIGURE B-21.

FAULT TREE FOR AC REACTOR MOTOR-OPERATED VALVE ELECTRIC POWER

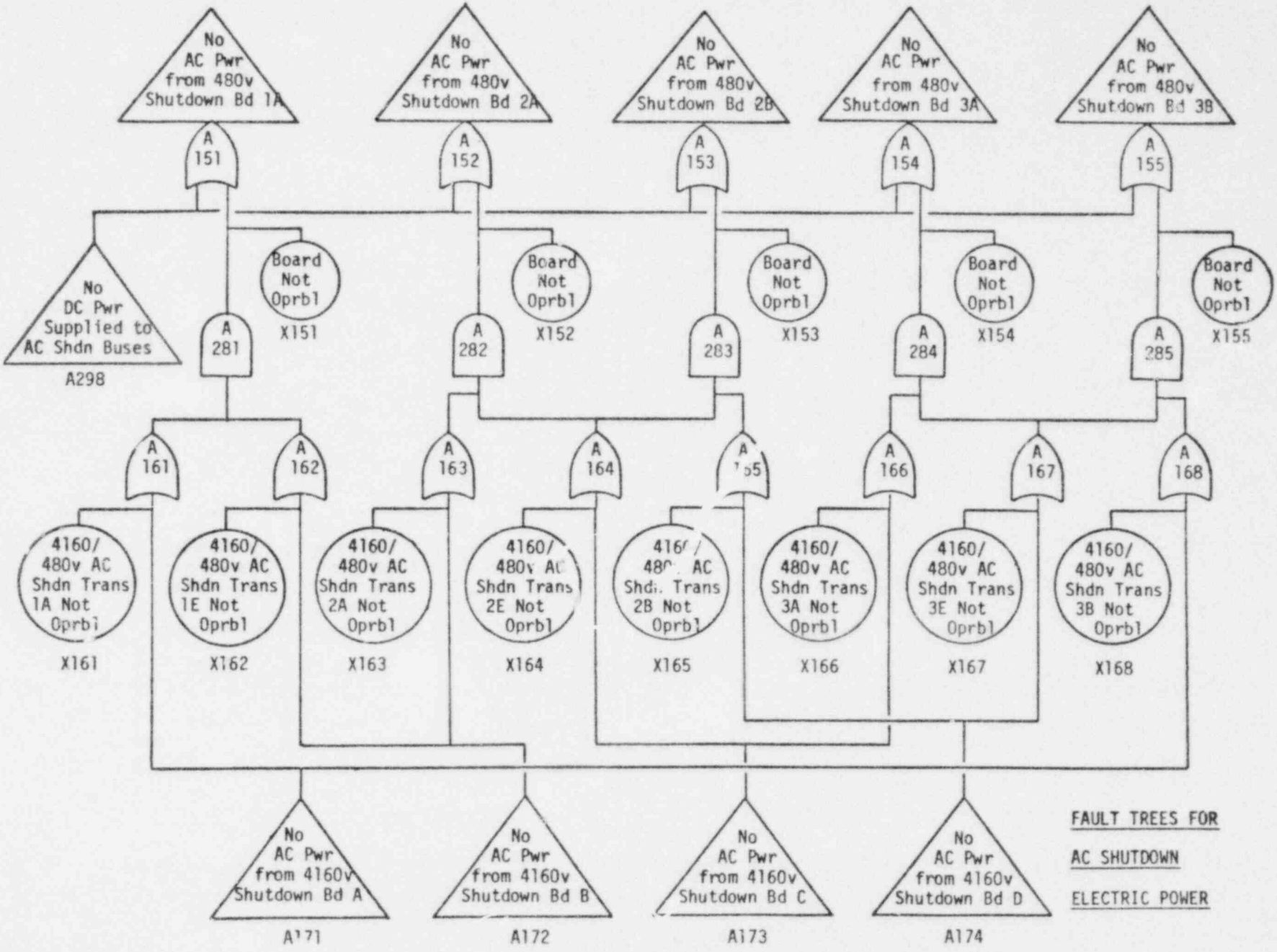

No AC Pwr from 480v Shutdown Bd 1A
No AC Pwr from 480v Shutdown Bd 2A
No AC Pwr from 480v Shutdown Bd 2B
No AC Pwr from 480v Shutdown Bd 3A
No AC Pwr from 480v Shutdown Bd 3B
A 151
A 152
A 153
A 154
A 155
No DC Pwr Supplied to AC Shdn Buses
A298
Board Not Oprbl
X151
Board Not Oprbl
X152
Board Not Oprbl
X153
Board Not Oprbl
X154
Board Not Oprbl
X155
A 281
A 282
A 283
A 284
A 285
A 161
A 162
A 163
A 164
A 166
A 167
A 168
4160/ 480v AC Shdn Trans 1A Not Oprbl
X161
4160/ 480v AC Shdn Trans 1E Not Oprbl
X162
4160/ 480v AC Shdn Trans 2A Not Oprbl
X163
4160/ 480v AC Shdn Trans 2E Not Oprbl
X164
4160/ 480v AC Shdn Trans 2B Not Oprbl
X165
4160/ 480v AC Shdn Trans 3A Not Oprbl
X166
4160/ 480v AC Shdn Trans 3E Not Oprbl
X167
4160/ 480v AC Shdn Trans 3B Not Oprbl
X168
No AC Pwr from 4160v Shutdown Bd A
A171
No AC Pwr from 4160v Shutdown Bd B
A172
No AC Pwr from 4160v Shutdown Bd C
A173
No AC Pwr from 4160v Shutdown Bd D
A174
FAULT TREES FOR
AC SHUTDOWN
ELECTRIC POWER

Figure B-22.

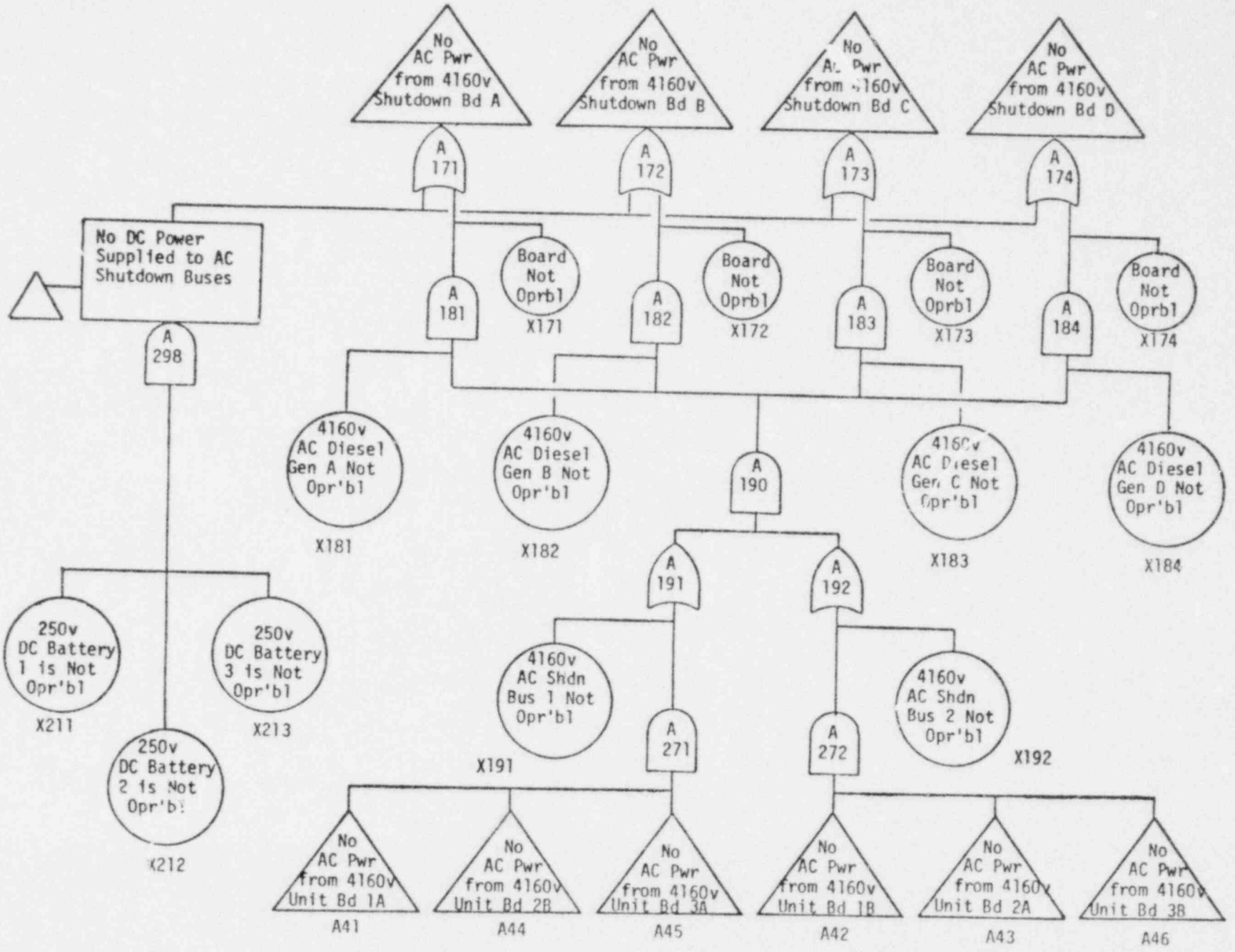


Figure B-22 (cont)

failure of Reactor Control or failure of CRS to minimize computer time. The gates and the component failures contributing to failure of SLC must be input to MFAULT. These have been designated on the overall fault tree with letters (A for gates and X for basic events) and numbers. The TOP event, failure of SLC, is gate A460 (see Figure B-14). The minimal cut sets are listed in Table B-8 .

Note that a minimal cut set such as (X441,X442) does not represent a systems interaction, but rather only a pair of random hardware failures (explosive valves 1 and 2) within SLC itself. However, a minimal cut set such as (X202,X203) represents failures in a support system (battery boards 2 and 3 of 250v DC) which fail essential components of the main system (SLC), in turn failing the TOP event. A systems interaction between 250v DC power and SLC is possible. Further, should more detailed resolution of events X202 and X203 indicate some common link between them (such as the proximity of each board's electrical cables at some location), a single, common-cause failure event (such as a fire) could manifest the systems interaction. Resolution of such minimal cut sets is necessary to uncover these types of subtle interactions.

Although beyond the scope of this exercise, the next step would be to examine these minimal cut sets representing potential systems interactions. Common links among each set's basic events would be determined, possibly converting some with multiple elements into single-element ones. Eventually, as many systems interactions as possible from the analysis will have been found. These may be quite numerous for an overall plant analysis. Rather than examine all of them in detail, it is sufficient to examine only the more important ones.

TABLE B-8.

MINIMAL CUT SETS FOR FAILURE OF STANDBY LIQUID CONTROL

1-Element

None

2-Element

X441	X442
X202	X203
X431	X432
X154	X432
X155	X431
X154	X155
X451	X452
X10	X451

3-Element

X211	X212	X213
X166	X167	X432
X167	X173	X432
X166	X174	X432
X173	X174	X432
X155	X166	X167
X155	X167	X17[illegible]
X155	X166	X174
X155	X173	X174
X167	X168	X431
X154	X167	X168
X166	X167	X168
X167	X168	X173
X168	X174	X431
X154	X168	X174
X166	X168	X174
X168	X173	X174
X167	X171	X431
X154	X167	X171
X166	X167	X171
X167	X171	X173
X171	X174	X431
X154	X171	X174
X166	X171	X174
X171	X173	X174

4-Element

None

5-Element

X167	X183	X191	X192	X432
X174	X183	X191	X192	X432
X166	X184	X191	X192	X432
X173	X184	X191	X192	X432
X183	X184	X191	X192	X432
X155	X167	X183	X191	X192
X155	X174	X183	X191	X192
X155	X166	X184	X191	X192
X155	X173	X184	X191	X192
X155	X183	X184	X191	X192
X167	X168	X183	X191	X192
X168	X174	X183	X191	X192
X167	X171	X183	X191	X192
X171	X174	X183	X191	X192
X168	X184	X191	X192	X431
X154	X168	X184	X191	X192
X166	X168	X184	X191	X192
X168	X173	X184	X191	X192
X168	X183	X184	X191	X192
X171	X184	X191	X192	X431
X154	X171	X184	X191	X192
X166	X171	X184	X191	X192
X171	X173	X184	X191	X192
X171	X183	X181	X191	X192
X167	X181	X191	X192	X431
X154	X167	X181	X191	X192
X166	X167	X181	X191	X192
X167	X173	X181	X191	X192
X167	X181	X183	X191	X192
X174	X181	X191	X192	X431
X154	X174	X181	X191	X192
X166	X174	X181	X191	X192
X173	X174	X181	X191	X192
X174	X181	X183	X191	X192
X181	X184	X191	X192	X431
X154	X181	X184	X191	X192
X166	X181	X184	X191	X192
X173	X181	X184	X191	X192
X181	X183	X184	X191	X192

Resolution of this criterion of importance remains to be determined. It implies some method for screening among the various candidates, the method depending upon the criterion. Screening based on the risk associated with each interaction would be optimal, but this necessitates calculation of both the probability and the consequence of each interaction, an extremely involved procedure. Screening solely on probability is somewhat simpler but this method can lead to overlooking low probability interactions with severe consequences. Weighting factor techniques are simpler still, but they may be too arbitrary to permit accurate screening. Further research is needed in this area of screening, which is essential to keeping an overall systems interaction assessment tractable.

REFERENCES

1. LER 80-024/01T-1, Access #8008040161; USNRC (6/28/80) *

2. Rubin, S. and G. Lanik, "Report on the Browns Ferry 3 Partial Failure to Scram Event on June 28, 1980"; USNRC (7/30/80) *

3. Boyd, G. et. al., "Final Report, Phase I, Systems Interaction Methodology Applications Program", NUREG/CR-1321; Sandia Labs (12/79) **

4. Browns Ferry Nuclear Plant, Units 1, 2 & 3. Final Safety Analysis Report, Docket-50259; TVA, Chattanooga (9/70)

5. Michelson, C., "Potential for Unacceptable Interaction Between the Control Rod Drive System and Non-Essential Control Air System at the Browns Ferry Nuclear Plant"; memorandum to H. Denton, USNRC (8/18/80) *

6. Pelto, P. and W. Purcell, "MFAULT: A Computer Program for Analyzing Fault Trees", BNWL-2145; PNL (11/77)

*Available in the NRC Public Document Room for inspection and copying for a fee.

**Available for purchase from the NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission, Washington, DC 20555, and the National Technical Information Service, Springfield, VA 22161.

APPENDIX C

CRYSTAL RIVER 3 LOCA EVENT: SYSTEMS INTERACTION ANALYSIS

The binary matrix/digraph method has been applied to the Crystal River Unit 3 LOCA event of February 26, 1980. The systems interaction in this event involved, among other things, the dependence of the steam generator feedwater supply, the pressurizer PORV controller, and a major part of the control room displays on a single non-nuclear instrumentation (NNI) power supply. The purpose of this exercise is to illustrate the application of the method and the manner in which systems interactions can be identified by its use. This analysis is, of course, after-the-fact, but is presented as if the event had not occurred, i.e., the failures that initiated and contributed to the event are not assumed a priori.

The scope of the analysis is as follows:

1) The analysis is assumed to be one part of a larger task to analyze the entire RCS Heat Removal function.
2) It is directed to the part of that function involving the Steam and Power Conversion system.
3) It is focused on the Controls and Instrumentation pertinent to the Steam and Power Conversion System.

The general approach taken here is (1) the analysis is broken down into tasks defined by the basic safety functions, (2) the functions are broken down into the systems that provide and serve them, and (3) the systems are anlayzed on a quasi-disciplinary basis. In this example, controls and instrumentation are of particular interest. Similar analyses would be performed for motive power, cooling, lubrication, physical location, and other potential linking characteristics.

The steps in the procedure are:

1. Through a review of plant descriptions and drawings, i.e., an operational survey, identify all pertinent subsystems and major components, and their support systems of interest. (In this example, the support systems include control signals, instrument signals, and associated power sources.)

2. Evaluate the system and its connections to identify systems interaction candidates.
3. Screen candidates to identify valid systems interactions.
4. Analyze systems interactions to determine their importance.

Figure C.1 is the schematic used as the basis for the analysis. The system is presented in a considerably simplified form for the purposes of the example. Many important features of the system (such as the heat removal path through the steam header safety valves) have been omitted because they played no role in the event. For the same reason, only a few of the control and instrumentation connections are shown.

The binary dependency matrix for the system is shown in Figure C.2; nomenclature is defined in Table C.1. (The binary matrix and its associated digraph are described in Appendix A.) It is important to point out that the matrix entries include not only components, but also subsystems and functions. The entry PC (power conversion function), for example, represents the steam generator and all the components associated with the transfer of heat from the primary to the secondary coolant systems. This feature of the matrix illustrates one of the major advantages of this approach: the level of detail required is determined by the scope of the analysis, and particular components are included only as they are identified as being important or of interest.

The digraph obtained by processing the matrix is shown in Figure C.3, and indicates a strong dependence of the system's heat removal function (CHR and THR) on the non-nuclear instrumentation power supply (NNIX). At this point, however, the power supply has been identified only as a candidate. Further analysis is required to establish that a valid systems interaction exists.

The form of the matrix output suggests the use of FMEA to determine the nature of the indicated dependencies; that is, the digraph points directly to the potentially important failure and the components and functions which would be affected by the failure. The results of such an analysis are summarized in Table C.2. The single failure of the power supply would, at least, degrade the RCS Heat Removal function, and thus, qualifies as a valid systems interaction.

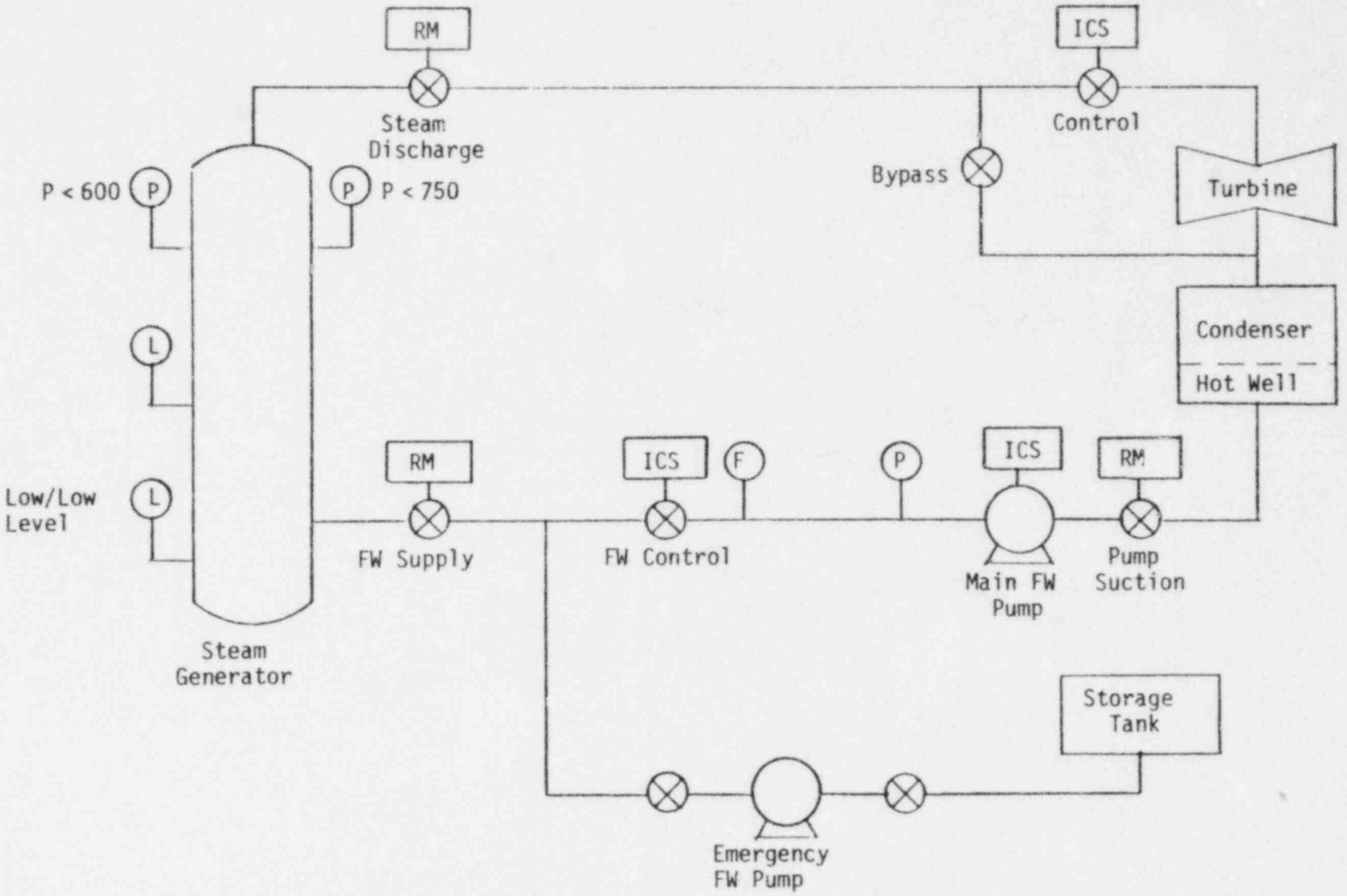


Figure C.1 Schematic of the Simplified Steam and Power Conversion System

	CHR	TBPV	PC	MFWF	CHW	MFP	MFCV	MFSV	ICS	FWSV	MSDV	RM	THR	TCV	SGP1	SGL	MFFT	SGP2	NNIX	SGLL	EFP	AFWF	CST	MFPT
CHR	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TBPV	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PC	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0
MFWF	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CHW	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MFP	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MFCV	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MFSV	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
ICS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0
FWSV	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
MSDV	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
RM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0
THR	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
TCV	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SGP1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
SGL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
MFFT	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
SGP2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NNIX	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SGLL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
EFP	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	1	0	0	0	0
AFWF	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1
CST	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MFPT	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure C.2 Binary Matrix of the Dependencies in the Simplified Steam and Power Conversion System

Table C.1 Digraph Nomenclature

NNIX	NON-NUCLEAR INSTRUMENTATION "X" POWER SUPPLY
SGP1	STEAM GENERATOR PRESSURE SWITCH (600 PSI)
SGL	STEAM GENERATOR LEVEL INSTRUMENT
SGLL	STEAM GENERATOR LOW/LOW LEVEL INSTRUMENT
ICS	INTEGRATED CONTROL SYSTEM
MFCV	MAIN FEEDWATER CONTROL VALVE
MFP	MAIN FEEDWATER PUMP
TCV	TURBINE CONTROL VALVE
MFWF	MAIN FEEDWATER FLOW
CHW	CONDENSER HOTWELL
PC	STEAM GENERATOR POWER CONVERSION FUNCTION
MFPT	MAIN FEEDWATER PRESSURE INSTRUMENT
AFWF	AUXILIARY FEEDWATER FLOW
CST	CONDENSATE STORAGE TANK
RM	RUPTURE MATRIX
FWSV	FEEDWATER SUPPLY VALVE
MSDV	MAIN STEAM DISCHARGE VALVE
MFSV	MAIN FEEDWATER PUMP SUCTION VALVE
TBPV	TURBINE BYPASS VALVE
CHR	CONDENSER HEAT REMOVAL
THR	TURBINE HEAT REMOVAL
SGP2	STEAM GENERATORE PRESSURE SWITCH (750 PSI)
MFFT	MAIN FEEDWATER FLOW INSTRUMENT
EFP	EMERGENCY FEEDWATER PUMP

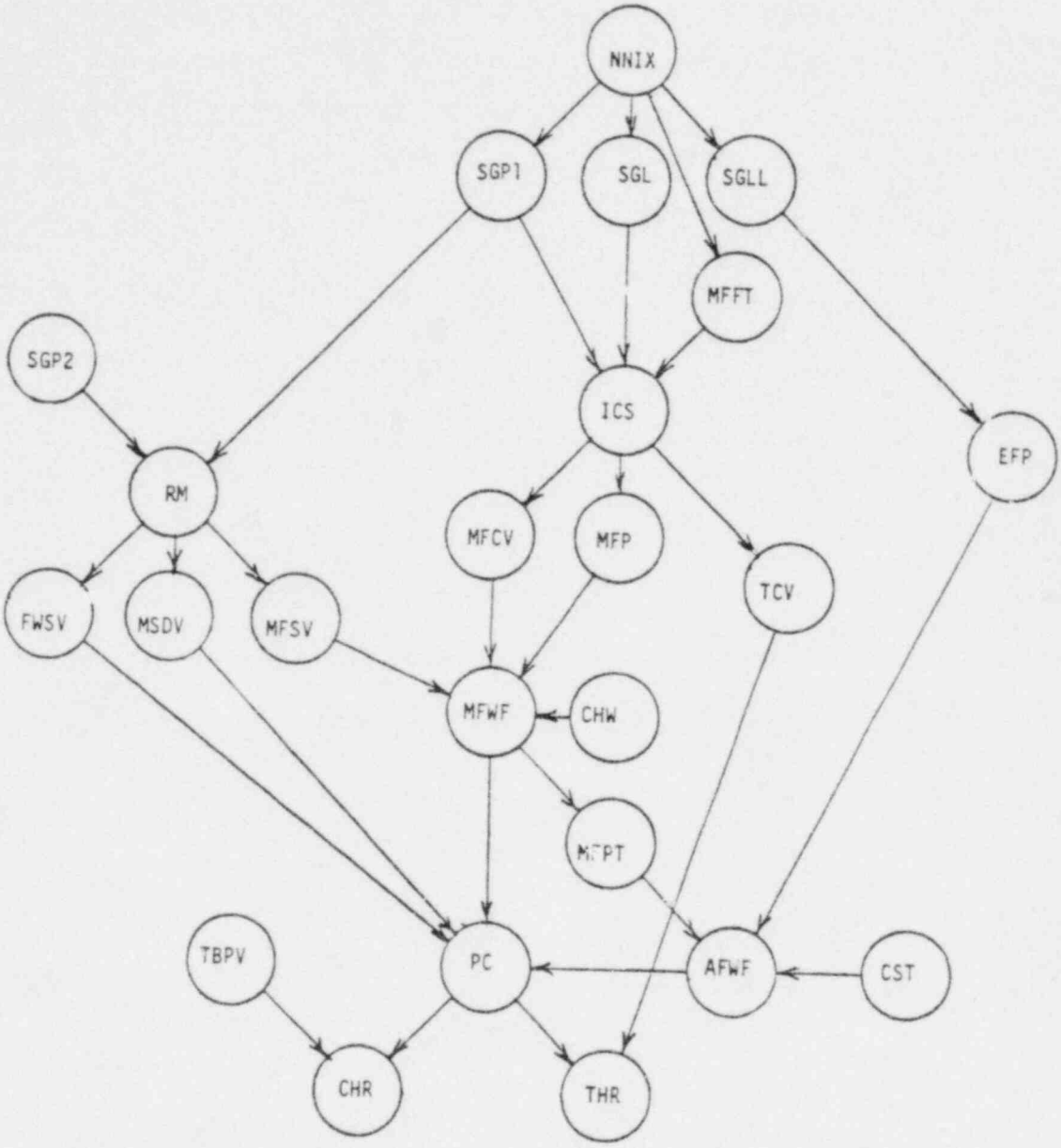


Figure C.3 Digraph of Dependencies in the Simplified Steam and Power Conversion System

Table C.2 Summary of FMEA of NNI-X Failure

Instrument	Effect of Failure
Main feedwater flow	Feedwater control valves fail to 50% open
Feedwater Temperature	A. Increase reactor power B. Reduce feedwater pump speed
Steam Generator Level	Reduce feedwater pump spped
Steam Generator Pressure	A. Reduce feedwater pump speed B. Actuate rupture matrix
Turbine inlet temperature	Open turbine control valves
Steam generator low/low pressure	Disable emergency feedwater pump auto-start

The procedural steps of identification (operational survey), screening (binary matrix and digraph), and evaluation (FMEA) have been illustrated. The determination of the importance of the systems interaction remains. The basis for the ultimate determination of importance is not addressed here. Regardless of the basis, however, a knowledge of the full extent of the influence of a systems interaction is necessary to make the determination. This requirement raises the question: how can this methodology be applied to ascertain that all interactions are identified?

Two approaches to inter-system analysis appear to be reasonable. By the first approach (as it would be applied in this exercise), once the NNI power supply has been identified as a systems interaction candidate, the analysis would proceed by tracing the distribution of this power to other systems. The dependence of the PORV controller and control room displays would be identified, and FMEA performed on them would reveal the extent of the effects of the interconnections.

By the second approach, analyses similar to the one illustrated here would be performed on each of the other Vital Safety functions. Integration of the results of these analyses would show the linkages of the NNI power supply to and its failure effects on: the RCS Heat Removal (steam generator feedwater), the RCS Pressure Control (PORV controller), and Vital Support (control room displays) functions.

APPENDIX D

REVIEW OF OPERATING EXPERIENCES

Following are summaries of operating experiences judged to have some element of systems interaction involved. In some cases, systems interaction played a minor role and in others it is only suggested; all are included to serve as examples of the types of interactions that should be considered in systems interaction analysis. These summaries are based on, and in some cases inferred from, descriptions of events reported in Licensee Event Reports.

A. Degradation of Core and RCS Heat Removal Functions: RC Pumps made inoperable by a minor steam leak.

Fault:

Minor steam leak

Consequences:

(1) Steam condensation caused a short on a solenoid terminal board.
(2) Solenoid failure caused isolation of the return line for Component Cooling Water to the RC Pumps.
(3) RC Pumps tripped on the loss of cooling water.

Hazard:

RC Pumps' operability dependent on the physical proximity of a potential steam source and an unprotected terminal board.

B. Degradation of Core and RCS Heat Removal Functions: RC Pumps (and turbine) damaged by low voltage condition on a DC bus.

Fault:

Batteries discharged by failure of operator to terminate a pump test.

Consequences:

(1) Failure of several electrical circuits due to low voltage.
(2) Loss of cooling for the RC Pump shafts (turbine bearing lubrication was also lost due to circuit failure.)
(3) RC Pumps (and turbine) damaged.

Hazard:

RC Pump operation dependent on an auxiliary system which was not protected against low voltage.

Comment:

The reactor tripped as a result of this occurrence; whether the trip was caused by the low DC voltage, RC pump damage or turbine damage was not reported. However, the low voltage condition had caused the pump and turbine damage prior to the reactor trip.

C. Degradation of the RCS Heat Removal Function: Steam Generator feedwater flow blocked by the loss of an instrumentation power supply.

Fault:

A Non-Nuclear Instrumentation (NNI) power supply failed due to an operator-caused short circuit.

Consequences: Power supply failure caused

(1) Feedwater flow reduction due to invalid signal inputs to the Integrated Control System (ICS).
(2) Steam Generator isolation due to instrumentation failure.
(3) Loss of control room indicators needed for manual control.

Hazards:

(1) Secondary heat removal dependent on a single power supply.
(2) ICS unprotected against invalid signal inputs.
(3) Control room indicators dependent on a single power supply whose failure causes plant conditions which require these indicators for manual control.

Comment:

This occurrence is one of three cited in this section which were initiated by a short circuit associated with an indicator lamp.

D. Degradation of RCS Heat Removal and Pressure Control Functions: Steam Generator feedwater flow blocked, and PORV opened and sealed open by the loss of an instrumentation power supply.

Fault:

A Non-Nuclear Instrumentation (NNI) power supply failed due to a short circuit, possibly operator-caused.

Consequences: Power supply failure caused:

(1) Feedwater flow reduction due to invalid signal inputs to the ICS.
(2) Steam generator isolation due to instrumentation failure.
(3) PORV opening and sealing open due to controller failure.
(4) Loss of control room indicators needed for manual control.

Hazards:

(1) Secondary heat removal dependent on a single power supply.
(2) ICS unprotected against invalid signal inputs.
(3) PORV controller unprotected against power supply failure.
(4) Control room indicators dependent on a single power supply whose failure causes plant conditions which require these indicators for manual control.

E. Loss of a Vital Support Function: Emergency electric power system disabled by a DC bus switching error.

Fault:

DC bus disconnected by an operator switching error.

Consequences:

(1) Loss of control power to AC transfer contactors.
(2) Loss of capability to isolate the generator and transfer AC loads.
(3) Loss of capability to shed loads from the emergency bus.
(4) Loss of DC bus alarms.

Hazards:

(1) Switching configuration and plant procedures that allow the isolation of a DC bus.
(2) DC bus monitored by alarms that are powered by the bus.

F. Challenge to the Reactor Control Function: Unplanned power increase caused by an electric bus short circuit.

Fault:

Bus short-circuited during replacement of an indicator lamp.

Consequences:

(1) Trip of motor control center due to short on feed breaker bus.
(2) Feedwater heaters isolated by motor control center trip.
(3) Reactor power increased due to decrease in feedwater temperature.

Hazard:

Motor control center operability dependent on a bus that is unprotected against a short in an indicator lamp.

G. Degradation of a Vital Support Function: Emergency diesel generator would not run because of water-contaminated fuel.

Faults:

(1) Rainwater accumulated in the access area of the fuel supply tank.

(2) Water contamination was not detected.

Consequences:

(1) Water-contaminated fuel was transferred to the diesel generators day tank.

(2) The diesel generator started on demand but failed to run because of contaminated fuel.

Hazards:

(1) Emergency electric power source dependent on a fuel supply that is susceptible to water contamination because of the physical arrangement of components.

(2) Fuel supply protected against water contamination by an ineffective water detector.

H. Degradation of a Vital Support Function: Emergency diesel generator disabled by a control power short circuit.

Fault:

Control circuit disabled by a short in the circuit's pilot light.

Consequences:

(1) Control circuit fuse blown by the pilot light short.
(2) Diesel generator disabled by the loss of the control circuit.

Hazard:

Emergency power source dependent on a control circuit that is unprotected against pilot light short circuits.

I. Loss of Vital Support Function: Emergency power to Engineered Safety features lost by improper undervoltage setpoint.

Fault:

Undervoltage setpoints were raised to assure isolation from the grid and to prevent motor controller fuses from blowing on low grid voltage.

Consequences:

(1) A normal motor starting load isolated the unit from the grid because of the higher setpoints.
(2) The emergency power bus could not accept starting loads of Engineered Safeguards Equipment because of the higher setpoints.

Hazard:

Improper setpoint settings caused isolation from the grid and prevented load transfers to the emergency bus, which were required because of the isolation.

J. Degradation of the Reactor Control Function: Boron addition system disabled by fire damage.

Fault:

Fire caused by insufficient ventilation.

Consequences:

(1) Electrical cables were damaged by the fire.
(2) Principal boron addition system was disabled because of the cable damage.

Hazard:

Boration system availability dependent on an area ventilation system.

K. Degradation of Reactor Coolant Inventory Control Function: Loss of HPCI or RCIC system isolated by inadvertent isolation.

Fault:

Air ventilation system fails in an area containing HPCI or RCIC steam lines.

Consequences:

(1) Steam-line break instrumentation senses temperature rise.
(2) Instrumentation isolates HPCI or RCIC.

Hazard:

HPCI or RCIC isolation instrumentation unprotected against temperature increases not caused by steam-line break.

*U.S. GOVERNMENT PRINTING OFFICE: 1981-0-341-742/603

NRC FORM 335 (7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)
NUREG/CR-1896
BMI-2073

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)
Review of Systems Interaction Methodologies

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
P. Cybulskis, R.S. Denning, R. Gallucci,
P. Pelto, A.M. Plummer, R.D. Widrig

5. DATE REPORT COMPLETED
MONTH: December | YEAR: 1980

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Battelle, Columbus Laboratories
505 King Avenue
Columbus, Ohio 43201

DATE REPORT ISSUED
MONTH: January | YEAR: 1981

6. (Leave blank)

8. (Leave blank)

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

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.
FIN B2335

13. TYPE OF REPORT
Technical Report

PERIOD COVERED (Inclusive dates)
July 1, 1980 to December 31, 1980

15. SUPPLEMENTARY NOTES

14. (Leave blank)

16. ABSTRACT (200 words or less)

The results of a study of methodologies with possible applications to systems interaction analysis are presented. A definition of systems interaction is developed and various methodologies and their applicability to systems interaction analysis are discussed and compared. The recommended approach is based on the concept of principal safety functions and employs logic models to identify and evaluate systems interactions candidates. The approach is applied to actual operating incidents to demonstrate its capabilities.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

systems interaction
systems analysis
fault trees

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS (This report)
Unclassified

21. NO. OF PAGES

20. SECURITY CLASS (This page)
Unclassified

22. PRICE
$

NRC FORM 335 (7-77)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555