6/28/79
SANDIA

SYSTEMS INTERACTION ANALYSIS - SRP TASK

The analysis task of Systems Interaction Methodology Development Program includes a study of the Standard Review Plan (SRP) and supporting documents to determine whether or not the potential systems interactions found in the study are addressed in the licensing review process. The first step in this process is a grouping of potential systems interactions into broad categories. Two purposes are served by this categorization:

1) Large numbers of cut sets involving components are reduced to a lesser number of representative cut sets involving systems.
2) The very specific types of interactions on the component level are redefined in more general terms of the Standard Review Plan.

Table 1 illustrates this process for a branch of one tree (decay heat removal using the secondary coolant systems for loss of offsite power during hot shutdown). In the case shown, actuation and control faults were found to create potential interactions that could lead directly to the top event. The components and systems involved for all literals of the cut sets of concern were determined and grouped as shown. In the example, 12 cut sets were reduced to one larger category; that is, the potential systems interactions of control power or actuation affecting the three trains of auxiliary feedwater. This broader grouping and others like it were used to define the question to be asked about the Standard Review Plan. The results of the SRP task are given below. It is realized that this example is rather elementary (i.e., a fault tree was not needed to realize that all three trains of auxiliary feedwater should not be susceptible to an interaction); however, it is expected that a complete analysis for each fault tree will reveal some much less obvious potentials for interaction.

Standard Review Plan Results

The questions, as defined by the process above, are listed below:

Does the SRP and its supporting documents ensure that:

1) At least two trains of auxiliary feedwater are required?

2) The trains of the auxiliary feedwater are independent in

    a) Motive Power?

    b) Control Power?

    c) Actuation?

    d) Location?

    e) Cooling?

    f) Lubrication?

In review of the SRP and supporting documents, the basic approach was to first review the basic system SRP's which would address the auxiliary feedwater system itself. From an overall system viewpoint this is SRP 10.4.9 and from an electrical standpoint, SRP's 7.3 and 7.4 were reviewed. These further reference other SRPs, Branch Technical Positions, General Design Criteria, Regulatory Guides, and IEEE Standards. These were scanned to determine what additional requirements were imposed by these documents which would impact the questions above. The results of our review is as follows:

1) Are two trains or more of auxiliary feedwater required? A number of general statements were found which would imply a "yes" answer to the above question. Examples are listed below.

From SRP 10.4.9 - The auxiliary feedwater system is reviewed to determine that a single malfunction, a failure of a component or the loss of a cooling source does not reduce the safety-related functional performance capabilities of the system.

Also From SRP 10.4.9 - ... the system shall be capable to withstand a single active failure ...

... portions of the system can be isolated ...

... assure redundancy of components ...

From BTP APCSB10-1 - The piping arrangement should be such that any combination of steam generators can be fed ...

- Sufficient redundancy should exist to withstand a single active component failure.

A few specific references were found to the amount of redundancy required in the auxiliary feedwater system, as a whole:

From BTP APCSB 10-1 - The auxiliary feedwater system should consist of at least two full capacity, independent systems ...

- The system should be able to withstand the rupture of any high energy section of the system, assuming a concurrent single active failure (may imply 3 trains).

From BTP-EICSB-13 - The system must withstand an aux feed pipe break inside containment together with a single electrical failure (active) in the aux feed system or in the onsite system (may imply 3 trains).

Other implications to the requirement of .. or more trains are found in the answers to question 2 discussed below.

2) Are the trains required to be independent in actuation, control power, motive power, location, cooling, and lubrication?

Besides the more general statements already mentioned, the following references provided more detailed information on the areas addressed in question 2:

2a) Motive Power:

From SRP 10.4.9 - Diverse motive power sources should exist.

- AFW pump drive and power supply diversity shall exist.

From BTP APCSB 10-1 - The auxiliary feedwater system should ... include diverse power sources.

- There shall be separate and multiple sources of motive energy.

2b & c) Control and Actuation:

From SRP 7.3 - The adequacy of physical separation criteria for cabling and electrical power equipment is reviewed.

- Make sure control and motive power are from redundant sources.
- Also covers supporting systems essential to ESF operation.

From SRP 7.4 - Covers review for redundancy and single failure susceptibility for the power, logic, and instrumentation of the main system and all supporting systems.

From IEEE 279 - This is probably the best overall document in this area and essentially stresses those requirements to meet single failure, redundancy, and channel independence of safety systems and their supporting systems.

From Reg Guide 1.75 - Includes physical and electrical separation requirements for electric systems.

2d) Location:

From SRP 10.4.9 - There shall be physical separation or shielding to protect from missiles.

- The location and the design of the system, structures, and pump rooms are reviewed to determine that the degree of protection provided (from natural phenomena and missiles) is adequate.

2e & f) Cooling and Lubrication:

No specific references to the auxiliary feed system cooling and lubrication support systems can be found. Statements in other categories above as they apply to the auxiliary feed system support systems can be applied here. SRPs 9.4.5, 9.2.1, and 9.2.2 do cover cooling and ventilation systems in general and will be the subject of other system interaction reviews.

Finally, although other documents such as the General Design Criteria, other Regulatory Guides, etc. make the same requirements as those mentioned above or elaborate on those requirements, none were found which would more specifically answer the questions herein than the statements already given.

Conclusion

Questions 1 and 2a-c are addressed directly in the Standard Review Plan. The potential common mode involving location is only dealt with specifically in reference to missiles and natural phenomena. The potential common modes in 2e and f (cooling and lubrication) are not dealt with specifically in reference to the auxiliary feedwater system. The only SRP statement that would preclude the interactions in 2d-f would be the statement of the single failure criterion, but it is emphasized that the areas of cooling, lubrication, and location are not dealt with specifically in reference to the single failure criterion.

POTENTIAL INTERACTION GROUPING
DHR-SEC-LOP-HS
SINGLES

POTENTIAL SYSTEM INTERACTION	AFWS TRAIN A			AFWS TRAIN B			AFWS TURBINE TRAIN			
	PUMP	MOVs	AOVs	PUMP	MOVs	AOVs	TURBINE	CONTROL VALVES	MOVs	AOVs
ACTUATION and CONTROL	X					X	X			
	X					X		X		
	X					X			X	
	X			X			X			
	X			X				X		
	X			X					X	
			X	X			X			
			X	X				X		
			X	X					X	
			X			X	X			
			X			X		X		
			X			X			X	

SYSTEMS INTERACTIONS

CRITERIA FOR IMPORTANCE

The criteria being used in the systems interaction program to assess the importance of potential systems interaction fall into two categories: those used to identify important systems interactions and those used to rank them.

To identify important systems interactions, the following topics are considered:

A. Unacceptable Core Damage: Unacceptable core damage is the top event of the fault tree. Thus, only systems whose failure would contribute to this top event are included in the trees. <u>Thus the first criterion is: for a potential systems iteraction to be important, it must have the potential for increasing the likelihood of unacceptable core damage</u>.

B. Plant Functions: The loss of any of four major functions could result in unacceptable core damage: reactor shutdown, decay heat removal, protection of the RCS boundary, and LOCA mitigation. The decision was made (by NRC) that the study should be limited to the first three since the latter was being adequately handled in other programs. <u>Thus for a systems interaction to be important in Phase I of this study, it must have the potential for increasing the likelihood of loss of one of the following three functions: reactor shutdown, decay heat removal or protection of the RCS boundary</u>.

C. Cutset Components: The first step of the evaluation is to determine the cutsets associated with each of the three functions. The cutsets identify the combinations of components which, if failed, would lead to loss of a functions. Component failures, or other common causes leading to loss of more than one component in a cutset have a greater potential of increasing the likelihood of loss of a function than an event of equal likelihood which causes loss of only one component in a cutset. Thus, for a systems interaction to be important, it must have the potential for causing failure of two or more components in a cutset.

D. Common Characteristics: The method chosen for identifying potential systems interactions is by identifying common characteristics between components. The common characteristics chosen are ones that could result in systems interactions. There are, of course, many such characteristics. The range of interactions to be treated in Phase I of the program was limited to two categories: physical and spatial. The common physical characteristics were further categorized into lubrication, cooling, control, motive power, and actuation system. Thus, for a systems interaction to be identified as important in Phase I of the program it must originate from a common physical or spatial characteristics.

To rank the important systems interactions, the cutsets will be ordered by the number of failures required. If two or more components in a cutset share a common characteristic, then they will be counted as one failure. Further among those with the same number of failures, those with the largest number of common characteristics will be considered as more important. Then the potential systems interactions represented by common characteristics in cutsets will be identified and ranked based on which ones appear in cutsets with the lowest number of failures.

The above criteria for identifying and ranking potential systems interactions is intended to focus the effort on those areas where potential systems interactions would have the greatest undesirable impact on safety.

SYSTEMS INTERACTIONS

EXPECTED RESULTS

Upon completion of Phase I of the Systems Interaction Program the following will have been accomplished.

A method will have been developed for systematically identifying systems interactions which are important to safety. The method will be applicable to a wide range of interaction types.

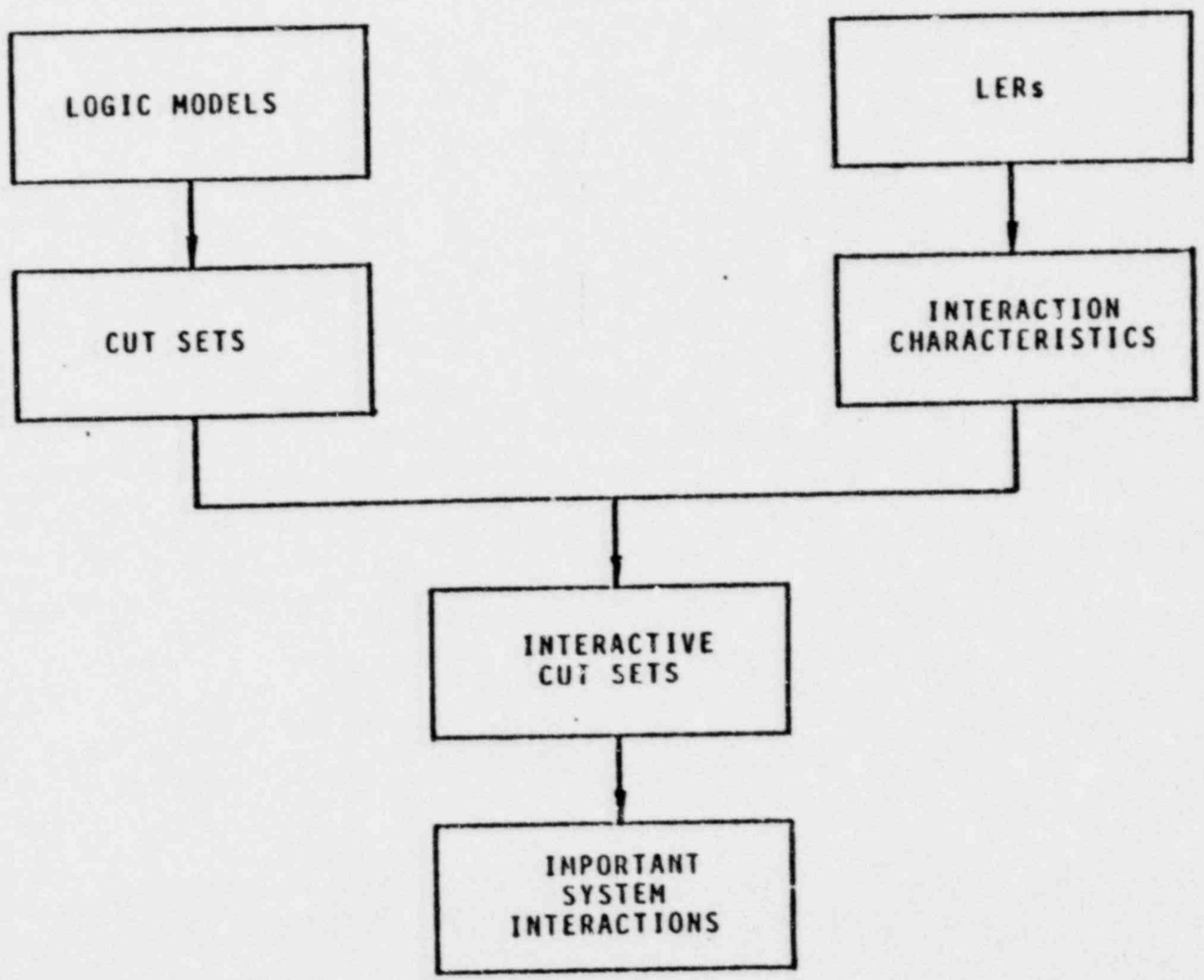
The developed methodology will have been applied to the Watts Bar Pressurized Water Reactor to demonstrate its use. The application to Watts Bar will, however, be limited in scope.

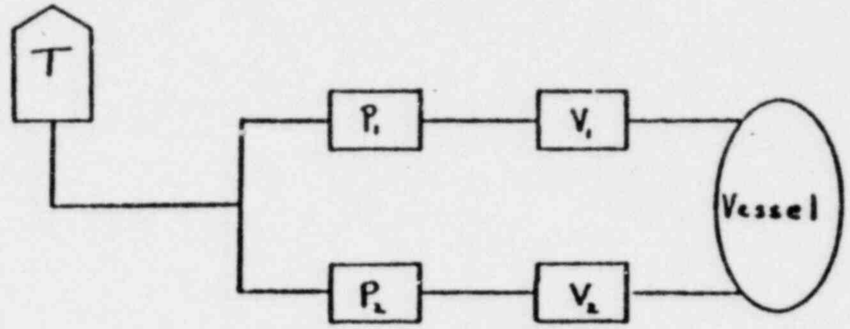
The Standard Review Plan and its supporting documents will have been reviewed to determine if the interactions found to be important in the application of the methodology to Watts Bar are covered in the Plan. Areas not explicitly covered will be delineated.

Systems Interactions

Category	Within Scope	Outside Scope
Plant Type	PWR	BWR
Units Per Site	Single	Multiple
Radioactive Material Sources	Reactor Core	Spent Fuel Pool Radwaste Systems
Plant Functions	Protection of RCS Boundary Reactor Shutdown Decay Heat Removal	LOCA Mitigating Systems All Others
Plant Conditions (N18-2)	Normal Operation Incidents of Moderate Freq.	Infrequent Incidents Limiting Faults
Environmental Conditions (N18-2)	Normal	Flood, Earthquake, Fire, Hurricane, Tornado, Other Abnormal Environments
Interactions	Physical Spatial	Human Manufacture Other

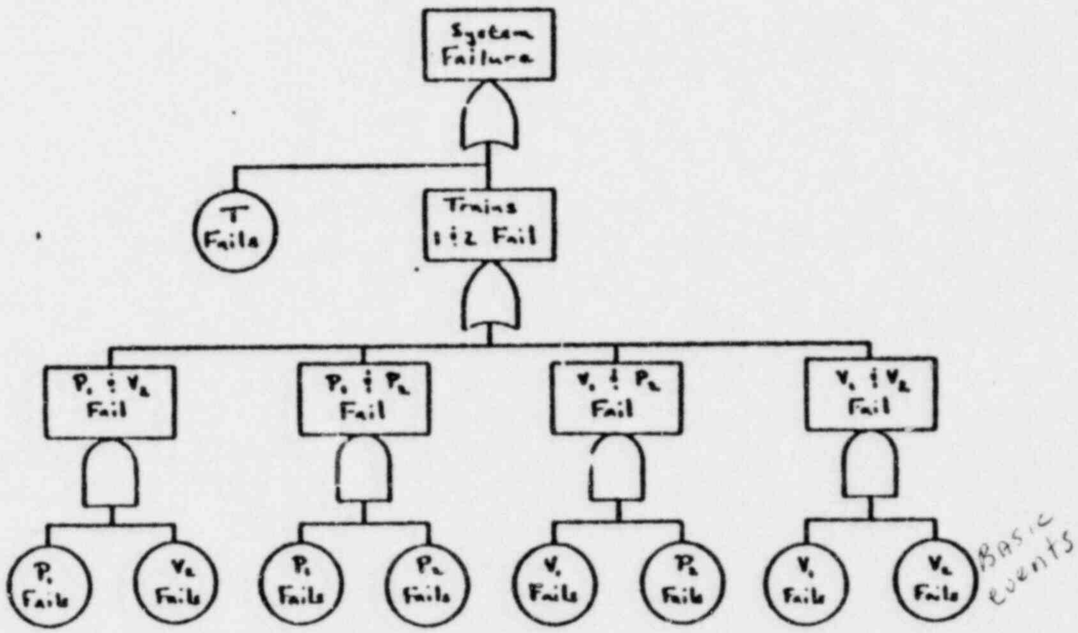
SYSTEMS INTERACTION ANALYSIS - OVERVIEW





SYSTEM

Oxy feed system

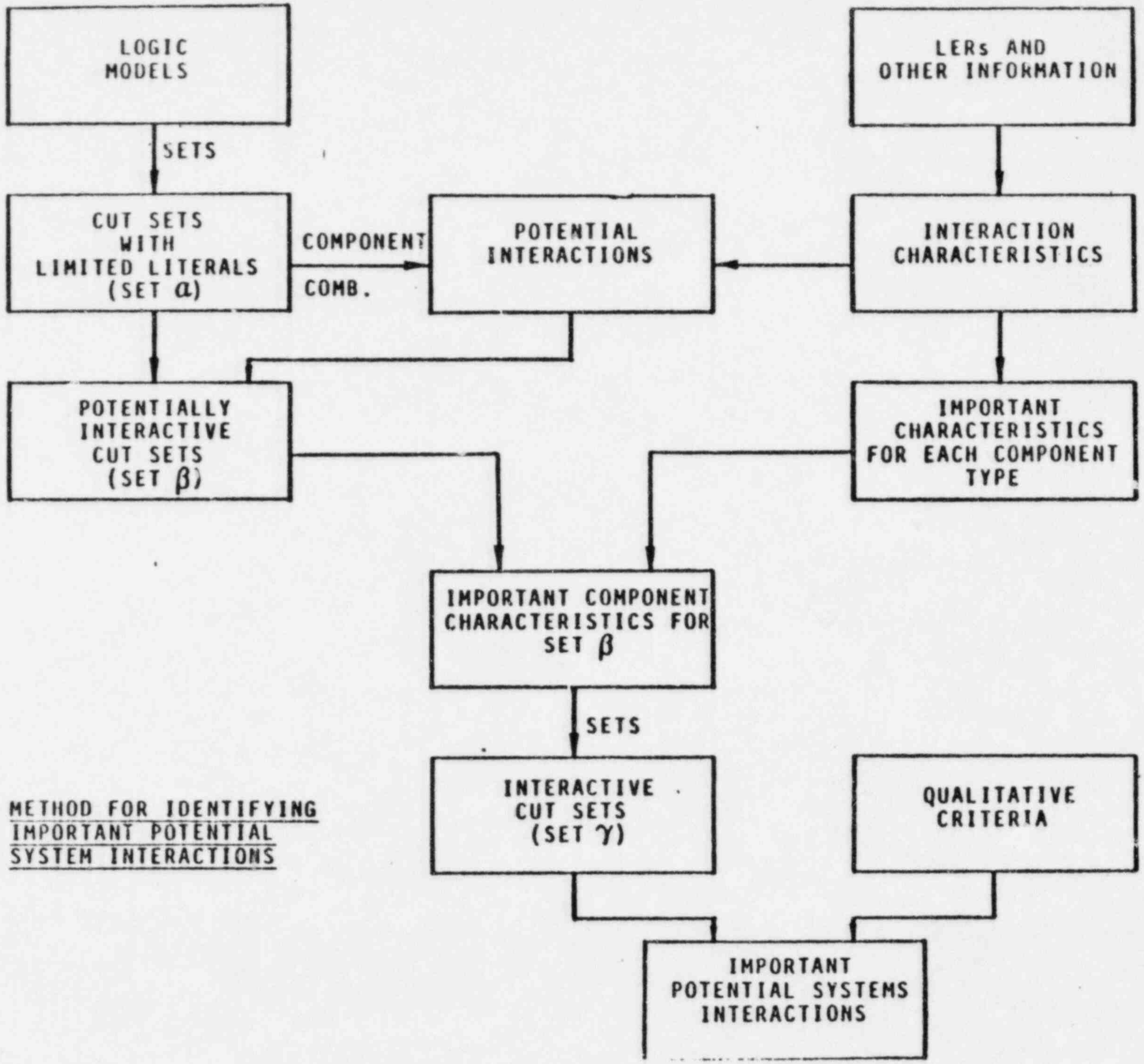


FAULT TREE

System Failure

$$SF = T + P_1 \cdot V_2 + P_1 \cdot P_2 + V_1 \cdot P_2 + V_1 \cdot V_2$$

CUT SETS



METHOD FOR IDENTIFYING IMPORTANT POTENTIAL SYSTEM INTERACTIONS

SAMPLE CUT SETS

2·3

2·4

3·7 ~~2·4·5~~

3·4·5

3·4·6

2·5·6·7

2·5·8·9·10·11·12·13

SET a

INTERACTION CHARACTERISTICS

COMPONENT	LOCATION	POWER	LUBRICATION	OTHERS
2	AUX.	X	X	
3	AUX.	X	X	
4	CONT.			X
5	AUX.	X	X	
6	SITE			
7	TURB.	X		X

POTENTIAL INTERACTIONS: 2-3 3-5

2-5 3-7

2-7 5-7

POTENTIALLY INTERACTIVE CUT SETS

SET α

2·3
2·4
3·7 ~~2·4~~

3·4·5

~~3·4·6~~
3·4·6
2·5·6·7

SET β

2·3
3·7
3·4·5 ~~[illegible]~~

2·5·6·7

operator could shut off 4, so save this item for sensitivity

POTENTIAL INTERACTIONS

2-3	3-5
2-5	3-7
2-7	5-7

COMPONENT CHARACTERISTICS

COMPONENT	LOCATION	POWER SOURCE	LUBRICATION
2	ROOM A	BUS A	SYSTEM Q
3	ROOM A	BUS B	SYSTEM Q
5	ROOM B	BUS B	SYSTEM Q
7	ROOM C	BUS A	

INTERACTIONS: 2-3 (LOCATION, LUBRICATION)
2-7 (POWER SOURCE)
3-5 (POWER, LUBRICATION)

3+7 could interact if have low system voltage on both buses

INTERACTIVE CUT SETS

SET β

2·3
3·7
3·4·5

2·5·6·7

INTERACTIONS

2-3 (2)

2-7 (1)

3-5 (2)

SET γ

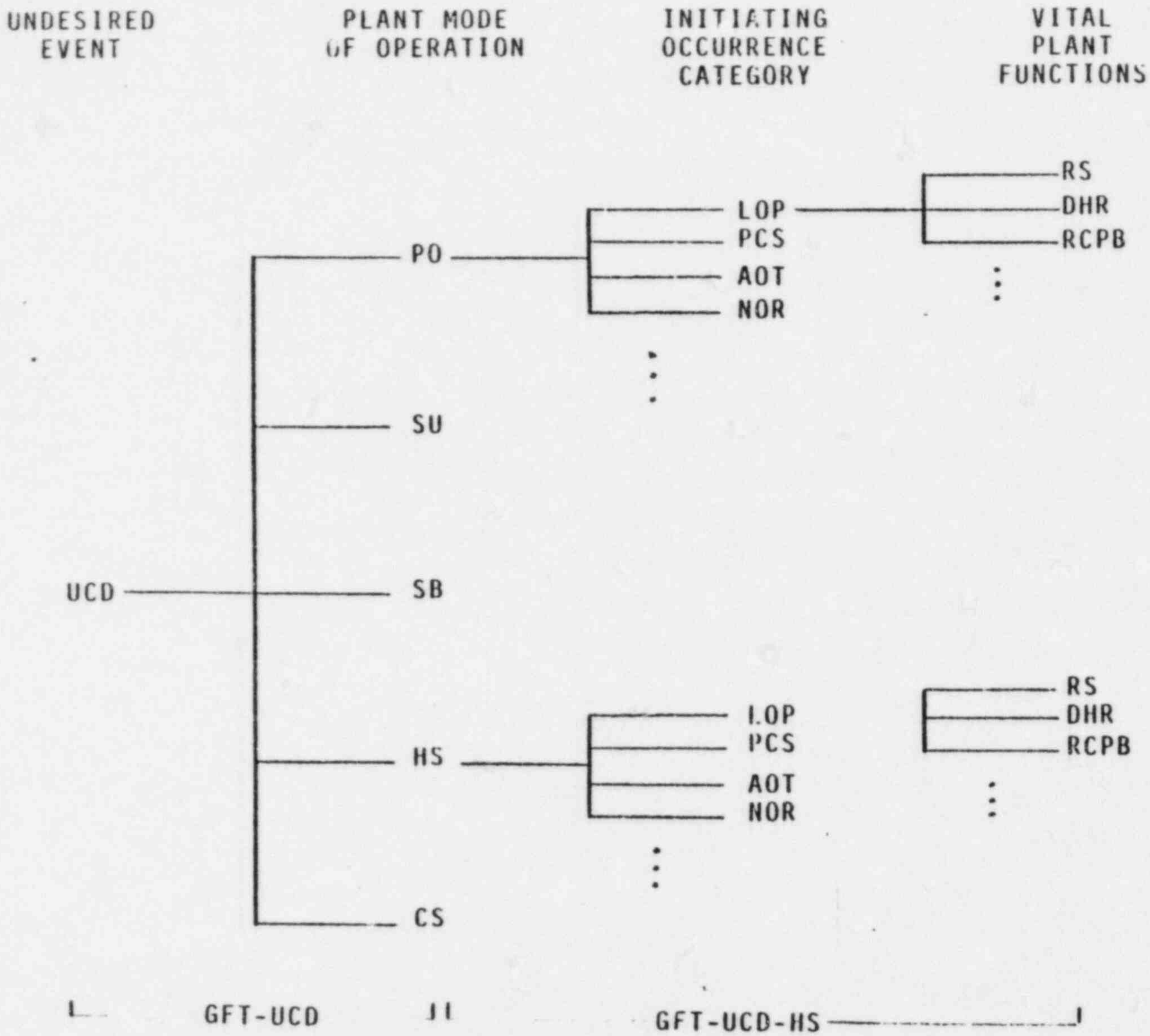
2·3 (1 CAUSE)

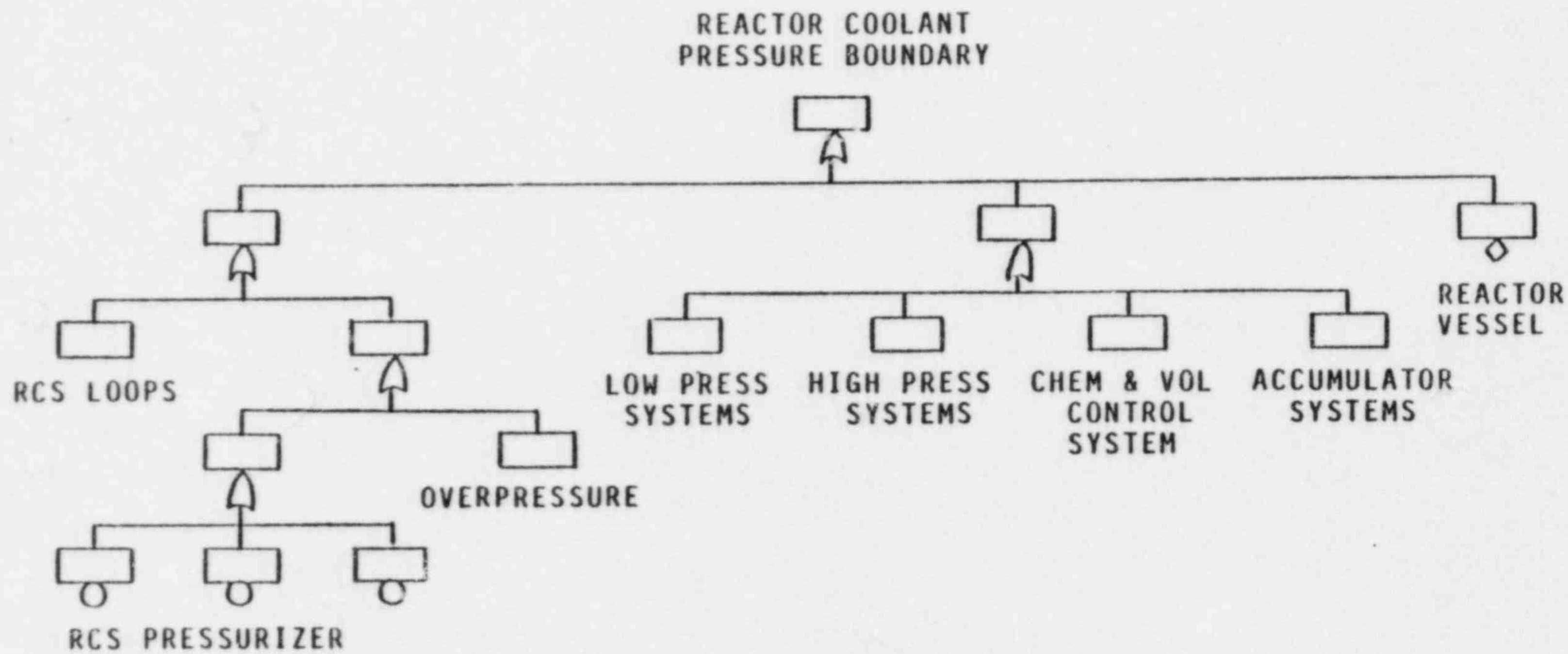
3·4·5 (2 CAUSES)

2·5·6·7 (3 CAUSES)

EXAMPLE QUALITATIVE CRITERIA

- NUMBER OF CAUSES
- RELATIVE FREQUENCY OF TYPES OF INTERACTIONS
- COMPARISON OF SYSTEM INTERACTION FREQUENCY WITH INDEPENDENT COMPONENT FAILURE FREQUENCY


UNDESIRED EVENT
PLANT MODE OF OPERATION
INITIATING OCCURRENCE CATEGORY
VITAL PLANT FUNCTIONS
UCD
PO
SU
SB
HS
CS
LOP
PCS
AOT
NOR
RS
DHR
RCPB
LOP
PCS
AOT
NOR
RS
DHR
RCPB
GFT-UCD
GFT-UCD-HS



REACTOR COOLANT PRESSURE BOUNDARY
RCS LOOPS
OVERPRESSURE
RCS PRESSURIZER
LOW PRESS SYSTEMS
HIGH PRESS SYSTEMS
CHEM & VOL CONTROL SYSTEM
ACCUMULATOR SYSTEMS
REACTOR VESSEL

	POWER OPERATION PO				STARTUP SU				STANDBY SB				HOT SHUTDOWN HS				COLD SHUTDOWN CS				
	LOP	PCS	AOC	NOR	LOP	PCS	AOC	NOR	LOP	PCS	AOC	NOR	LOP	PCS	AOC	NOR	LOP	PCS	AOC	NOR	
RS	3	4	4	5	3	4	4	5	1	2	2	2	1	2	2	2	1	2	2	2	5(3)
DHR	1	2	3	3	1	2	3	3	1	2	3	3	1	2	3	3	1	2	3	3	3(2)
RCPB	3	4	4	4	5	6	6	6	7	8	8	8	1	2	2	2	9	10	10	10	10(2)

FUNCTIONS

RS - REACTOR SUBCRITICALITY

DHR - DECAY HEAT REMOVAL

RCPB - REACTOR COOLANT PRESSURE BOUNDARY

INITIATING EVENTS

LOP - LOSS OF OFFSITE POWER

PCS - LOSS OF POWER CONVERSION SYSTEM CONDENSER

AOT - ALL OTHER CONDITION II OCCURRENCES

NOR - NORMAL SHUTDOWN INCLUDING SOME CONDITION II OCCURRENCES

DESCRIPTION OF SYSTEMS INTERACTIONS

SYSTEMS INTERACTION

A PROCESS WHEREBY ONE SYSTEM ACTS UPON ONE OR MORE OTHER SYSTEMS

SYSTEM DESIGN INTENT

1. INTENDED SYSTEMS INTERACTIONS

   A. ESSENTIAL FOR PERFORMANCE OF IMPORTANT PLANT FUNCTION(S)

   B. INCIDENTAL TO PERFORMANCE OF IMPORTANT PLANT FUNCTION(S)

2. UNINTENDED SYSTEMS INTERACTIONS - ADVERSE TO PERFORMANCE OF IMPORTANT PLANT FUNCTION(S)

UNINTENDED SYSTEMS INTERACTION CHARACTERISTICS

A PROPERTY THAT CLOSELY LINKS TWO OR MORE PLANT COMPONENTS SUCH THAT FAILURE OF THESE COMPONENTS MAY LEAD TO FAILURE OF IMPORTANT PLANT FUNCTION

CAUSE

AN EVENT INITIATING AN UNINTENDED SYSTEMS INTERACTION

UNINTENDED SYSTEMS INTERACTION CHARACTERISTICS COVERED BY PRESENT STUDY

I. COMMON ENERGY SOURCE

   A. COMMON DRIVE SHAFT

   B. COMMON POWER SUPPLY
      (ELECTRICAL, PNEUMATIC, HYDRAULIC, STEAM, ETC.)

II. COMMON LOCATION (COMPONENTS LOCATED IN CLOSE PHYSICAL PROXIMITY)

III. COMMON FLOW PATHS

   A. COMMON HYDRAULIC LOOP

   B. COMMON ELECTRICAL CIRCUIT

IV. COMMON SUPPORT SYSTEM

   A. LIQUID COOLING

   B. LUBRICATION

UNINTENDED SYSTEMS INTERACTION CHARACTERISTICS NOT COVERED BY PRESENT STUDY

I. HUMAN ERROR

A. COMMON MANUFACTURER

B. COMMON INSTALLATION (SAME SUBCONTRACTOR OR WORK CREW)

C. MAINTENANCE

1. INCORRECT MAINTENANCE PROCEDURE

2. INADEQUATELY TRAINED MAINTENANCE PERSONNEL

D. CALIBRATION

1. INCORRECT CALIBRATION PROCEDURE

2. USE OF OUT-OF-CALIBRATION TEST EQUIPMENT

3. VERIFICATION OF TEST EQUIPMENT USING IMPROPER STANDARDS

4. INADEQUATELY TRAINED PERSONNEL

E. TEST PROCEDURE (FAULTY TEST PROCEDURE AFFECTING ALL COMPONENTS NORMALLY TESTED TOGETHER)

F. OPERATOR ERROR (DURING OPERATIONS)

1. OPERATOR DISABLED

2. OPERATOR OVERSTRESSED

3. FAULTY OPERATING PROCEDURE

4. IMPROPER USE OF OPERATING PROCEDURES

5. INADEQUATELY TRAINED OPERATING PERSONNEL

UNINTENDED SYSTEMS INTERACTION CHARACTERISTICS
NOT COVERED BY PRESENT STUDY (CONT.)

II. SIMILAR COMPONENT PARTS

A. COMPONENT PARTS OF SOME TYPE

B. COMPONENT PARTS OF COMMON PRODUCTION RUN

ZION/FLUOR PIONEER LER STUDY

LER DISTRIBUTION (BY OPERATING MODE)

1.	POWER	15
2.	STARTUP	0
3.	HOT SHUTDOWN	3
4.	HOT STANDBY	1
5.	COLD SHUTDOWN	14
	A) SOLID WATER (10)	
	B) STEAM BUBBLE (4)	
6.	REFUELING 2	2
7.	OTHER CONDITIONS	5
8.	UNKNOWN	27
		67

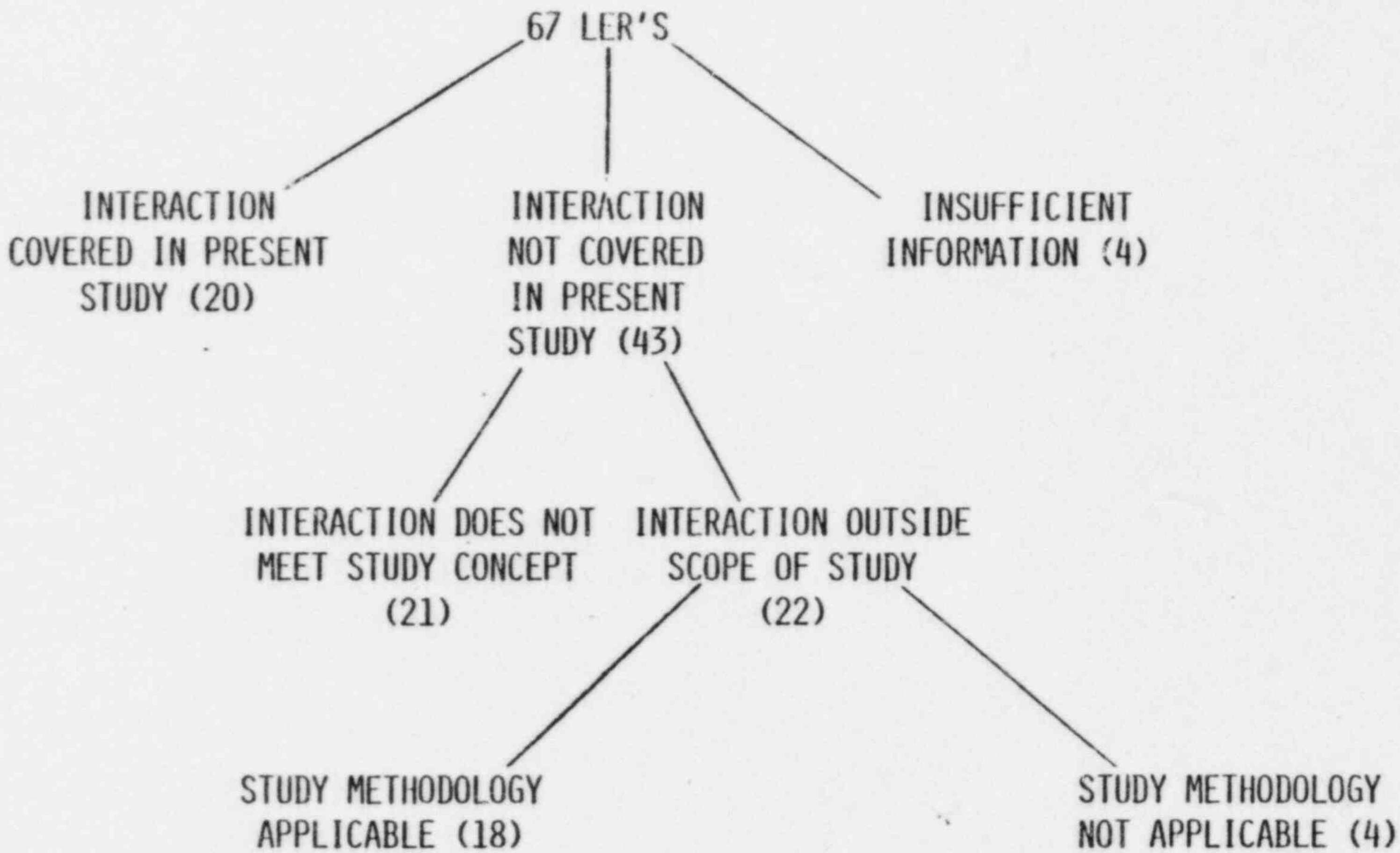
LER DISTRIBUTION (BY INTERACTION CAUSE)

1.	FLOODING OR MOISTURE ACCUMULATION	18
2.	FIRE	6
3.	COMPONENT FAILURES	6
4.	ELECTRICAL BUS FAILURE	6
	A) NOISE (1)	
	B) UNDERVOLTAGE (3)	
	C) LOAD SHEDDING (2)	
5.	HUMAN ERROR	18
	A) DURING MAINTENANCE (4)	
	B) DURING NORMAL OPERATIONS (10)	
	C) DURING COMPONENT INSTALLATION (2)	
	D) DESIGN (2)	

LER DISTRIBUTION (BY INTERACTION CAUSE) (CONT.)

6.	OVERTEMPERATURE	3
7.	MECHANICAL DAMAGE	2
8.	FREEZING	3
9.	UNKNOWN	4
10.	REFUELING (NOT COVERED)	1
		67

LICENSEE EVENT REPORT REVIEW (ZION STUDY)



EXAMPLES OF SYSTEMS INTERACTIONS

TAKEN FROM LER'S

I. COVERED IN PRESENT STUDY

- VALVE PACKING LEAK ON MOV CAUSES MOTOR FAILURE
- SW PUMP SEAL LEAK CAUSES SHORTING OF SW MOTOR OPERATOR
- HPCI STOP VALVE LEAKAGE FLOODS JUNCTION BOX CAUSING LOSS OF TWO BUSSES
- EFFLUENT JETS CAUSE MALFUNCTIONS OF SAFETY/RELIEF VALVES
- HIGH MOISTURE LEVEL CAUSES FAILURE OF DIESEL GENERATOR VOLTAGE REGULATOR

II. NOT COVERED IN PRESENT STUDY

A. INTERACTION DOES NOT MEET STUDY CONCEPT

- OPERATOR ERROR CAUSES RCS OVERPRESSURIZATION WHILE SOLID (STARTING RCP WITH LARGE ΔT BETWEEN RCS AND S/G)

- HPCI VALVE FAILS TO OPEN DUE TO MOISTURE IN CONTROL JUNCTION BOX (SINGLE VALVE FAILURE)

- COMPONENT FAILURE (CIRCUIT BREAKER FOR SAFEGUARDS BUS TRIPS CAUSING LETDOWN VALVE TO CLOSE, RESULTING IN RCS OVERPRESSURIZATION)

B. INTERACTION OUTSIDE OF SCOPE OF STUDY

1. STUDY METHODOLOGY APPLICABLE

   - OPERATOR ERROR CAUSES BORON DILUTION DUE TO UNDETECTED SECONDARY-TO-PRIMARY LEAK

   - DESIGN ERROR - A SINGLE COMPONENT FAILURE IN LPCI SELECTION LOGIC COULD CAUSE FOUR RHR PUMPS TO PUMP TO A BROKEN LINE

2. STUDY METHODOLOGY NOT APPLICABLE

   - PRESSURE VESSEL HEAD DROPS DURING REFUELING

   - WIRING ERROR IN STEAM PRESSURE ΔP CAUSES INCOMPLETE PROTECTION

   - DESIGN ERROR - LOSS OF CERTAIN ESF FEATURES CAUSED BY DIODE FAILURE (DUE TO INSUFFICIENT PRV)