MARYLAND

TECHNICAL
RESEARCH
REPORT

SRC TR 87-115-r1

Probabilistic Risk Assessment: A Look At the Role of Artificial Intelligence

by

J. Wang and M. Modarres

SYSTEMS RESEARCH CENTER

UNIVERSITY OF MARYLAND

COLLEGE PARK, MARYLAND 20742

PROBABILISTIC RISK ASSESSMENT: A LOOK AT THE ROLE OF ARTIFICIAL INTELLIGENCE

J. WANG
M. MODARRES*

Department of Chemical And Nuclear Engineering
The University of Maryland
College Park, MD 20742

R.N.M. HUNT

Baltimore Gas And Electric
Calvert Cliffs Nuclear Power Plant
Lusby, MD 20657

Submitted for Publication to
Nuclear Engineering and Design Journal, June 1987

*To whom correspondence should be sent

PROBABILISTIC RISK ASSESSMENT: A LOOK AT THE ROLE OF ARTIFICIAL INTELLIGENCE

J. WANG

M. MODARRES

Department of Chemical And Nuclear Engineering
The University of Maryland, College Park, MD 20742

R.N.M. HUNT

Baltimore Gas And Electric
Calvert Cliffs Nuclear Power Plant, Lusby, MD 20657

ABSTRACT

A review of traditional Probabilistic Risk Assessment (PRA) methods used in the nuclear power industry is presented. The shortcomings of the current PRA methods are pointed out. A method of performing a PRA is proposed and is computerized. The role of artificial intelligence in developing and performing the proposed PRA approach is discussed. The proposed PRA approach is verified by comparing its results to previously performed PRAs. The comparisons have supported the adequacy and completeness of the results of the proposed model. A discussion of how the proposed method can be used as an expert system to verify plant status following loss of plant hardware is also presented.

PROBABILISTIC RISK ASSESSMENT: A LOOK AT THE ROLE OF ARTIFICIAL INTELLIGENCE

J. WANG

M. MODARRES

Department of Chemical And Nuclear Engineering

The University of Maryland, College Park, MD 20742

R. N. M. HUNT

Baltimore Gas And Electric

Calvert Cliffs Nuclear Power Plant

Lusby, MD 20657

1- INTRODUCTION

Today's complex industrial facilities, typified by the nuclear power industry, often contain an enormous inventory of hazardous material, which have the potential to impact many people as a result of major releases from the process. Fortunately, due to their inherently safe design, there are few accidents. Therefore, it is not possible to evaluate the risk from major accidents as easily as may be done for those of a more common nature, such as highway safety. In recent years, to overcome this difficulty, sophisticated methods of accident risk analysis have been developed and applied to these industries. Nuclear, chemical and aerospace industries are amongst those

pioneering the development and use of these methods.

The assessment of risk for industrial installations attempts to achieve five general objectives. These objectives are:

1- To identify accidental initiating events and event sequences which have significant importance to overall risk.

2- To provide a quantitative measure of the expected frequency of occurrence of these important initiating events and sequences.

3- To perform a realistic evaluation of the potential consequences which result from the individual important event sequences.

4- To quantitatively assess the overall risk to both the equipments of the facilities and those persons in and around those facilities.

5- To provide a framework upon which decisions regarding design and operation of the installation can be made to optimize its performance.

In this paper, we will briefly discuss the development of risk analysis methods in the nuclear industry and their shortcomings. We will focus on the risk analysis objectives listed above, with the exception that little will be said about consequences, i.e. objective 3. Finally, we will discuss a technique which aims to utilize artificial intelligence at remedying some of these shortcomings.

2- BACKGROUND

Although the application of formalized probabilistic risk analysis (PRA) techniques to nuclear plants is a relatively new development, the practice of risk assessment on a broader scale is not [1]. In an attempt to improve the accuracy of risk assessments, three basic approaches have been used. These are: worst-case, actuarial-case, and analytical approaches [2]. Results from analyses using the first two approaches have typically been poor, whereas the latter approach has been quite successful.

The worst case approach identifies the most pessimistic set of sequences of events and their respective consequences, with no attempt made to assess likelihood or credibility of such events. This approach is exemplified in a U.S. Government study entitled " Theoretical Possibilities and Consequences of Major Accidents In Large Nuclear Power Plants", otherwise known as WASH-740 [3]. In this study, subjective estimates of the likelihood of the identified worst-case scenarios were made using an expert judgement method. Because of an inability to account for the realistic accident sequences, the results of the analysis were not considered credible.

The actuarial approach has been used in a limited number of applications in an attempt to assess risk. This approach is based on the use of broad, actual statistical data, from which an attempt is made to infer the future occurrences of important accident sequences. The accident sequence precursor study [4], is a recent application of such an actuarial approach. Due to the paucity of statistically significant data, the use of this method for nuclear risk analyses has not been wide spread. On the other hand in industries such as insurance and banking wherein the supply of data is adequate, the actuarial approach has been widely used.

The analytical approach has been used successfully since it was first employed in the landmark Reactor Safety study which is often referred to as WASH-1400 [5]. This study described and delineated the various initiating events and sequences of events which could lead to a significant radioactivity release from a nuclear plant. Health and economic effects of such radioactive releases were evaluated, as were the likelihoods of occurrence of such events. From these data, a quantitative assessment of overall risk, and the sources of individual contributions were generated.

The WASH-1400 study contributed significantly to the state-of-the-art application of risk analysis methods in the nuclear industry. It established the fault tree/event tree method as both a serviceable and credible method for evaluating plants, and for identifying risk-significant accident sequences. As a by product it also provided a comprehensive failure data base for quantifying the likelihood of plant hardware and human failures.

In an effort to extend and refine the techniques used in the WASH-1400, the Nuclear Regulatory Commission (NRC) initiated a program called the Reactor Safety Study Methodology Application (RSSMAP)

[6-10]. The principal objectives of this program were to identify the risk dominating accident sequences for a broader spectrum of nuclear reactors, using information and insights gained from WASH-1400 to determined whether analyses of other plants could be performed without such a large expenditure of resources for determining their individual risk profiles.

The accident at the Three Mile Island (TMI) in March of 1979, sparked an even greater interest in PRA and its role for enhancement of nuclear plant safety. For that reason the NRC initiated the Interim Reliability Evaluation Program (IREP) [11-14] whose aim was to to identify those nuclear plant accident sequences which dominate the risk to public health and safety. Other NRC plans with regard to IREP were to formalize and better disseminate PRA knowledge, both within the NRC and throughout the nuclear industry. This and several other PRA based NRC supported studies [15-20] that followed the IREP studies in large measure were successful.

In addition to these major NRC-sponsored PRA programs, a number of industry supported PRA efforts were performed [20-25]. These privately funded studies were generally designed to answer specific safety issues. As such, they were often quite different in their scope and methods. Most significant amongst the utility industry initiated programs was the Industry Degraded Core Rulemaking program (IDCOR) [26].

The IDCOR objective was one of development of a comprehensive, integrated, well-documented, and technically sound position on the issues related to severe nuclear accidents. The IDCOR methodology was then applied to a representative set of four nuclear plants. To answer the question of whether it would be possible to extrapolate the results of these six plants to other nuclear plants, the individual plant evaluation (IPE) method was developed and applied to eight other plants to confirm that individual plant responses are similar to, or bounded by those of the reference plants[27-30].

3- PRA METHODS: PROBLEMS AND RATIONAL FOR IMPROVEMENTS

To achieve the general objectives of risk analysis as outlined in section 1, two basic approaches have been used in model-based PRAs:

Small Event Tree Large Fault Tree Approach

A single detailed model, or set of related models, which combine all plant components, systems, and phenomenological relationships is developed and solved in its entirety to determine important accident sequences and calculate both their probability and consequential societal risks. In this process an event tree is constructed for each significant initiating event (i.e., LOCAs ...etc.) to model the behavior of the primary mitigating or direct core protection systems (often known as front-line systems). A fault tree is constructed to model the possible failure mechanisms which disable each front-line system including the system's inter and intra-dependencies which reflect the basic plant reliability structure. The event trees and their associated front-line fault trees are then combined into a massive logic model which is then solved using sophisticated codes such as SETS [31]. This process sometimes referred to as " small event tree-large fault tree" approach and has been the basis for all NRC supported PRA studies.

Large Event Tree Small Fault Tree Approach

A plant model which has the minimum detail required to provide an adequate description of plant systems and their interdependences is developed and solved . Here, the analyst develops two sets of event trees; one set describing the behavior of front-line systems with regard to each important initiating event (similar to the previously described approach), the second describing the behavior of the support systems or dependent events. Fault trees are then developed to model conditional failure behavior of each front-line and support systems. Finally, the model is solved by using either hand calculation [32], or simple fault tree analysis computer codes. In this approach, since the event trees contain only independent events , the event probabilities can be processed directly within the event trees to provide the overall frequency for each accident sequence. The event probabilities are directly and independently computed from front-line and support system failure probabilities. Since these systems do not include dependent system failures, the fault trees are relatively small. This approach has been the basis of most of the industry sponsored PRAs including the IDCOR study, and is often referred to as " large event tree small fault tree approach".

Diagrammatic displays of these two approaches are shown in Figures 1 and 2 . Each of these approaches can give comparable results, but their usefulness is vastly different when examined within the context of the objectives of a risk analysis described earlier. Both of these approaches satisfy the objectives of identifying and quantifying the dominant accident sequences, but, each is extremely resource intensive and the underlying analytical process is rather difficult to understand and need not to use a standard format. A second and perhaps more profound problem lies with their inability to effectively achieve the objective of providing a framework for utilizing the plant risk analysis in routine nuclear plant design and operational activities.

Furthermore, within the the environment of an operating power plant, the plant owner's goal is not only one of being able to easily identify risk contributing event sequences, but to also understand how these risks changes as a result of various postulated or observed change in the plant character. It is within the context of these types of abilities and needs, that a method which takes advantage of modern artificial intelligence techniques and languages has been developed and is further discussed in this paper.

4- REQUIREMENTS FOR A SUCCESSFUL PRA

In the previous section we pointed out that there are two major shortcomings with current PRAs:

1. They are difficult to understand and perform, and their development is resource intensive.

2. Frequently, when a PRA is completed, it is difficult to easily and effectively use it in routine plant operation or design activities.

It is within the context of these difficulties, which can be attributed primarily to the complexity of plant configurations and accident scenarios, that there is a need for substantial PRA expertise. Modern A.I. based approaches promise to remedy the situation. The questions we must ask ourselves are, first, "how can human intensive activities in PRAs such as event tree and fault tree construction, operator recovery considerations, failure data gathering and treatment activities, and accident sequence likelihood quantification be improved?", and second, "how can the final PRA model be routinely used in plant activities for plant status verification, maintenance impacts, procedure writing and modification, and plant safety issue evaluation and resolution?". Finally we must ask, "how can the developed models be modified to reflect continuous plant configuration changes?".

Review of current PRA approaches and A.I. techniques which·potentially can answer these questions, has led to the following conclusions :

1- The "large event tree small fault tree" approach, due to its modularity and independent way of treating the plant systems, provides an ideal means for introducing expert systems into the PRA process.

2- The required hierarchical knowledge-base, upon which an expert systems program can be used to simplify development of the support system event tree and the front-line event trees sequences, can be constructed using a Master Plant Logic Diagram (MPLD) similar to that shown and discussed in section 5.

3- An A.I. based approach can be used to easily determine the probability of events (or system failure probabilities) described by the developed event trees. This approach is discussed in section 6.

4- A control mechanism must be in place to perform all requisite activities within the overall PRA process namely, numerical calculations, accident sequence screening, and operator recovery actions. A diagrammatic representation of these activities is shown in Figure 2.

5- The PRA risk model can be added to the knowledge-base of the expert system to allow an engineer to interactively explore the answers to questions such as : what happens if components or systems X,Y... are failed or taken out of service? The expert system can be structured to provide a list of affected plant systems, procedures, etc. and, be able to promptly calculate the conditional probabilities of various core damage or dominant accident sequences.

6- The program must be able to easily accommodate an update of the knowledge-base, if plant configurational or physical changes occur.

Steps 4-6 are further discussed in section 7.

Within the following sections of this paper, brief description of the MPLD knowledge base, the development of the expert system, case studies, potential uses ,and future directions are provided.

5- THE KNOWLEDGE BASE: PRESENTATION OF THE MASTER PLANT LOGIC DIAGRAM (MPLD)

In order to provide a knowledge base for the A.I. program, a single visual display of the plant reliability structure is developed. Called the MPLD, this diagram easily shows all the interrelationships amongst initiating events , front-line systems, and support (dependent) systems.

The success oriented MPLD is generated by first determining the functional requirements which must be satisfied if a core damage event is to be prevented, and then by identifying the front-line systems which have the capability to support the functional requirements.

The relationships between initiating events and front-line system requirements are logically described in terms of functional success criteria, whereby each required function is satisfied if either:

(1) no transient is present, or

(2) system hardware is available.

In essence, the upper part of the model describes the information normally displayed in the front-line system event trees. The systems themselves are further divided into trains or subsystems which are logically related by their success criteria. The hierarchy of the model is further displayed by the support system matrix. This is developed from an interfacing systems Failure Mode and Effects Analysis (FMEA)[33]. For each front-line system trains (or subsystems), an analysis of the effects of failures from all the combinations of support systems (their trains or subsystems) are established and explicitly shown, and is followed by an analogous process to establish interrelationships between different support systems.

The hierarchical nature of the model is important because it is possible to select any element within the MPLD and differentiate between local hardware fault and dependent system faults. This will be very important when the MPLD is used to develop and quantify the support and front-line system event trees. Since the hardware within each dependent system is totally independent from that of other systems, the dependence relationship is shown in the MPLD only.

For example, consider the MPLD in Figure 3. In this diagram there are two front-line systems F1 and F2 (each of which performs its required function using one of its two trains). Among the three support systems S1, S2, and S3, S1 has two trains of which only one is required to achieve success. The dependencies between various systems, trains, and initiating events are explicitly shown by ● .

The support system event tree and the front-line event trees are developed from the MPLD shown in Figure 3. The support system event tree sequences (often referred to as end-states) are obtained from examination of all possible failure combinations of support systems in the MPLD. For example, failure of S3 leads directly to failure of S2 and F2-1, which in turn results in failure of F1-1 and F2-2. From this, one can infer that the end-state which cause failure of S3 is F1-1, F2. The reader should be aware that the MPLD diagram is oriented within "success space" and thus both F2-1 and F2-2 must fail before F2 fails. The list of all the possible end-states obtained from the MPLD is shown in Table 1. Table 1 in essence shows all the possible sequences from the corresponding support system event tree, and their associated effect on the front-line systems.

In developing Table 1, it was assumed that all the failure probabilities of support systems (Sl-l, Sl-2, S2, S3) was .1, and that all the failure probabilities of trains (Fl-l, Fl-2, F2-l, F2-2) was .01. Since many end-states are identical, i.e., their front-line system impact is the same, they can be merged into more compact form as shown in Table 2. From the MPLD, it can be inferred that the front-line event tree for this situation should have the generic form shown in Figure 4.

The probability of occurrence each "damage state" (i.e., the end-state of the front-line system event tree) for initiator A, and for each possible end-state can be calculated by using the data shown in Table 2 and Fig 4. For example, following the occurrence of initiating event A with a hypothetical frequency of l/year, if S3 is unavailable (i.e. Fl-l, and F2 are unavailable but Fl-2 is available), then, the sequence probabilities can be easily determined to be those shown in Fig 5. Furthermore, if recovery action are to be included in the sequence, non-recovery probabilities should be incorporated. If we assume the probability of non-recovery of each support system to be 1.0 (i.e. support system is not recoverable), and for each front-line system train to be .1, then the sequence probabilities are calculated to be those shown in Figure 5.

Credit for recovery action can not be directly attributed to Fl-l and F2 because their failure result from the failure of support systems. recovery can only occur if the support systems themselves are recoverable. This same operation must be repeated for each end states listed in Table 2.

In the specific cases where front-line event sequences result from an initiating event (e.g., a transient induced LOCA), the respective front-line event tree must also be incorporated into the quantification process.

Since we have demonstrated that, the MPLD can serve as the knowledge-base for performing the evaluation process explained above, it only remains to be shown that development of a control strategy is necessary to allow the whole process to be automatically performed by a computer. The question as to how one can easily determine the independent system , or train probabilities still remains, but the solution is presented in section 6.

6.DETERMINATION OF SYSTEM FAILURE PROBABILITIES- THE AI APPROACH

Following development of the MPLD, the failure probability for each support system, front-line system, or their respective trains is determined. Traditionally, these probabilities are found from fault tree analysis but current AI technology can eliminate the need for fault tree development by allowing estimation of the failure probability for each system directly from the P&ID or simplified system block diagrams. The use of block diagrams offers an opportunity to substantially reduce the problem of evaluating the system's reliability. A comparison of these two possible approaches are shown in Figure 6.

To better understand the proposed approach, consider the block diagram shown in Figure 7. This diagram includes:

(1) Branches - BA, CA etc.

(2) Branch points - A, B, C etc.

(3) Blocks - X1, X2 etc.

To model the actual P&ID in a simple form,block diagram method is used. In which each block represents a collection of hardware (valves, pumps, heat exchangers, etc.) A branch represents a flow path , control, or power line, thus must have direction. The branch point is the connection tee, cross, etc.

To represent the diagram in an AI format, each block can be represented as a node (frame), which has basic defined attributes such as:

(1) name or type of the block (e.g., pump, heat exchanger, etc.),

(2) operating position of the block (e.g., normally open, operating, closed, standby, energized ... etc.). and,

(3) name of other blocks, directly connected to this block.

Representation of the block diagram in AI format requires that each of the branch points be identified, i.e., for the block diagram of Figure 7, branch points A,B,C,D must be entered.

To ensure correct model structure, since the branch points are not directly connected to each other, it is necessary for the user to identify the interconnecting branches DB, BA, DC, BC, and CA and the starting and ending point(s). For example, end branching point (where system delivers its flow, ... etc.) A; start point D. It is also necessary to know the direction of the flow in each branch. If no direction is defined, the branch by default can be assumed to be available in both directions.

The following describes the program upon format, and shows how the list of blocks in each branch is defined. For example, the list AB(X4, X5) indicates the presence of blocks (X4, X5) in branch AB. Since the analyst must also indicate the success criteria or logic for the block diagram, the following format is used:

(1) (OR BA CA) to indicate that either branch BA or CA needs to work for success.

(2) (AND DB DC) to indicate that both branches DB and DC must work for success.

To this point, all available information (factual knowledge) for evaluating the block diagram has been entered, so a set of inference rules (perceptual knowledge) must be defined to use this factual knowledge through the use of a standard control strategy (inference engine) to infer which success paths are available, and thus calculate the probability of their failure. Rules for block diagram analysis are generic in nature, and apply to all typical block diagrams. Examples of these rules are:

If X is a block, and X is in stand-by operating position, then obtain the probability for " Failure of X to work when demanded?" and " Failure to operate following a demand?"

If X is a block, and X is in a normally closed operating position, then obtain the probability for "Failure of X to open?" and " Failure of X to stay open after it is opened?"

This set of rules is used until the probability of failure for every blocks is obtained either from a generic data base or provided by the user, at which time the success path (in Boolean refered to as path sets) determination inference rules are implemented. The generic inference rules used for this purpose are as follows:

Rule A: If flow from point X to Y and from Y to Z exist, then flow from X to Z exists.

Rule B: If flow from point X to Y exists, and X = start point Y = end point, then XY is a flow path.

Rule C: If XY is a flow path and XY includes all success criteria then XY is a success path.

Rule D: If XY is a flow path but XY does not guarantee inclusion of all success criteria, then other path(s) which when combined with XY makes it a success path are identified, and combined with XY.

Rule E: If XY is a success path and XY is a subset of another success path ZT, then ZT is not a minimal success path and should be eliminated.

Rule F: If all blocks (or components) in a minimal success path works then, the success path is an operational success path.

By applying rules A-F to the example shown in Figure 7 the following is inferred:

Rule A and Rule B: path DBA exists.
path DBCA exists.
path DCA exists.
path DCBA exists.

Rule C: No success path.

Rule D: From combining DBA and DCA a success path is generated.
From combining DBA and DCBA a success path is generated.
From combining DBCA and DCA a success path is generated.
From combining DBCA and DCBA a success path is generated.

Rule E: The success path made by combining DBCA and DCBA is a non-minimal path since it contains the success path made by combining DBA and DCBA and it should be eliminated.

Rule F: Since all blocks X1 through X7 work, then the following three operational success paths exist:

(X1) (X4 X5) (X2) (X6 X7).
(X1) (X4 X5) (X2) (X3).
(X2) (X6 X7) (X1) (X3).

Knowing this, it is easy to calculate the probabilities of success for each available path. For example, if the unavailability is the same for each block and is equal to .01, then for the fourth success path shown above, the success probability is: (.99) (.99 .99) (.99) (.99) = .95.

To calculate the total system success probability, a summation is made of the contributions from each operational success path. However, success paths are highly dependent (i.e., they have elements in common), so to minimize the dependencies among the generated minimal operational success paths the method of Sum of Disjoint Products (SDP) is used [34]. In this approach, if n success paths SP1,SP2,...,SPn exist then

$$\begin{aligned}\Pr(SP1 \text{ OR } SP2 \text{ OR } \ldots \text{ OR } SPn) = {} & \Pr(SP1) + \Pr(\overline{SP1} \text{ AND } SP2) + \ldots \\ & + \Pr(\overline{SP1} \text{ AND } \overline{SP2} \text{ AND } \ldots \text{ AND } SPn), \quad (1)\end{aligned}$$

where OR ,and AND are Boolean union and intersection operators, respectively. Since each system has a small number of success paths, the numerical solutions using equation (1) are much simpler than those of the traditional cut-set approach. If desired, it is possible to find the Boolean complement of the success path, in order to obtain all of the minimal cut-sets.

7- DEVELOPMENT OF PRA-EXPERT COMPUTER PROGRAM

The simple MPLD structure, and the rule-based method for developing success paths and system failure probabilities are amenable to applications of artificial intelligence. For example an expert system has been developed, to perform the PRA process automatically. This expert system program contains:

1- A front-end symbolic menu driven routine for easily entering all necessary factual knowledge, such as an MPLD, a simplified P&ID or block diagram of the front-line and support systems that appear on the MPLD, plant specific failure data, maintenance and surveillance data.

2- A routine which monitors the process for generating all feasible plant end-states (i.e., support system event tree sequences), and sequences which result in a plant damage (i.e., front-line event tree sequences) as detailed in section 5.

3- A forward-chaining control strategy [35] which automatically recognizes and confirms all simplified P&IDs or block diagrams, and generates all possible success paths which meet the stated success criteria. These success paths are used in the final strategy,which implements the calculation of probabilities for each individual operational success path, and uses the available data to assess the total system failure probability.

4- A routine which combines the results of 2 and 3 above, and calculates the frequency of occurrence for each plant damage state, in addition to the total frequency of damage which result from all causes. This routine has the inherent capability to describe each dominant accident sequence in simple natural language, so that the analyst can consider for incorporation of possible operator recovery action probabilities.

5- A control strategy which makes the expert system useful for answering questions such as : " what happens if one of the Salt Water System pumps are taken out of service or fails...?". The system will quickly list all affected plant systems and the corresponding terms of change in the expected total core melt frequency or the individual system probabilities. Future plant design or configuration changes can be easily incorporated using the user friendly input routine and conveniently and automatically repeat the PRA. This capability makes the PRA-Expert a valuable tool for many safety related activities (outlined in section 9).

PRA-Expert is currently modelled for the LMI Lambda computer (LMI Lisp Machine) using Zetalisp(a dialect of lisp language). With the recent introduction of Golden Lisp's GCLISP-286 [36], it will be possible to develop a comparable version of PRA-Expert for use on an IBM personal computer (AT series), so PRA-Expert will become more accessible and easier to implement. Development of the IBM-AT version of the PRA-EXPERT is currently underway at the University of Maryland Center for Reliability Engineering (CRE).

8- APPLICATIONS OF THE PRA-EXPERT

In order to demonstrate the effectiveness and accuracy of the program several application tests were performed. In this section we will briefly discuss one of such applications. The Baltimore Gas and Electric Company's Calvert Cliffs Nuclear Power Plant units have been analyzed in several PRA studies [7, 11, 27], hence providing an excellent opportunity for testing the PRA-EXPERT program. For this purpose, a preliminary MPLD structure for Calvert Cliffs Unit 1 was developed and carefully reviewed for accuracy. This diagram is presented in Figure 8. The results were compared with the most recent PRA study, IDCOR-IPE [27], by using similar component failure probability data. It is found that the PRA-EXPERT output contains the same dominant accident sequences, sequence frequencies, and system failure probabilities as the IDCOR-IPE. Some minor differences between the numerical results obtained are attributed to round-off values used in IDCOR-IPE hand calculation. Table 3 presents a partial comparison of these results.

The major advantage of using the PRA-EXPERT in this application exercise is found to be its effectiveness to perform the PRA study quickly and accurately. FOR example, the performance of the whole PRA study in this case took about two person-months; one person-month of which is attributed to the development of the MPLD structure, and one-person month is attributed to data collection and running the PRA-EXPERT. This is less than one-third of the efforts used to obtain similar results through one of the conventional approaches. Existence of many useful information obtained from Calvert Cliff PRA studies facilitated the application of the PRA-EXPERT program. However, performance of the same type of study for a plant without an existing PRA study can still be performed much faster than the tradition PRA approaches, and through less experienced staff. The PRA-EXPERT program is also used in several occasions as an expert system to infer the qualitative consequences (plant systems affected), and quantitative consequences (changes in system failure probabilities and core melt frequencies) of failing certain plant hardware.

The consequences provided by the PRA-EXPERT in all cases, were determined to be accurate - through careful reviews. The PRA-EXPERT program demonstrated that it could provide an analyst with the ability to quickly perform a variety of other PRA related studies when actual or proposed physical and operational configuration changes occurs within the plant. In the next section we will elaborate on several potential uses of the PRA-EXPERT program.

9- UTILIZATION OF PRA-EXPERT AS A DYNAMIC PLANT MODEL

The use of PRA techniques in the routine decision making process of a nuclear power plant requires that the analytical methods be capable of both providing results in a timely manner and be usable by non-PRA specialists. Current techniques tend to be less than adequate in both regards, whereas the AI based methods have the potential for providing the means for achieving both requirements. When the AI plant analysis models (MPLD), and probability data are fully developed and entered into PRA-EXPERT, it will be possible to quickly evaluate all proposed changes to plant configuration and quickly assess their worth. This could provide the facility with a powerful capability for immediately assessing risk benefit ratios for all postulated changes. Having this ability could allow the methods to be incorporated directly into the prioritization and justification process for plant improvements.

The ability to update the plant model through a natural language interface, and calculate conditional plant risk in a timely manner, could allow extrapolation of the capabilities of this technology to one which could perform the functions of a plant status monitor. When integrated with normal plant operations, it should be possible a priori to establish the risk significance of various proposed equipment realignments to ensure that within the flexibility allowed by various operational and maintenance constraints, the plant could always be maintained in a configuration which assures minimum risk. This same process could also provide protection from inadvertent violation of plant technical specifications and minimize the frequency and duration with which the plant would have to enter a state in which it is constrained by a Limiting Condition for Operation (LCO).

An important potential attribute of the modelling techniques which utilizes AI as their solution tool, may be that data collection and evaluation could be done on-line to provide a measure of the instantaneous plant risk. If this risk measure was integrated over a stated period of time, the average value could be used to provide a very high level indicator of nuclear plant performance. Presumably, routine operational configuration changes within the plant could be used to update the model in real time, if an interface were created to directly interact with the plant data acquisition system and plant operational configuration management system. Having such an interface could, conceptually, lead to the use of the program output as a "risk meter".

10- CONCLUSIONS

Artificial Intelligence methods and specifically the expert system approach are important tools which have the potential to remedy the many shortcomings of PRA technique. PRA-EXPERT can effectively help users to build a PRA model, and utilize the model as the knowledge-base of an expert system for future safety analyses. PRA-EXPERT has been tested with a high degree of success.

Acknowledgement

The authors wish to acknowledge the support of the University of Maryland's System Research Center, the Baltimore Gas and Electric Company, and the National Science Foundation.

REFERENCE

[1] Probabilistic Risk Assessment Course Documentation volume 1: PRA Fundamentals, U.S. Nuclear Regulatory Commission NUREG/CR-4350/1067 1985, August.

[2] Theoretical Possibilities and Consequences of Major Accidents In Large Nuclear Power Plants, U.S. Atomic Energy Commission, NUREG-740, 1956.

[3] Precursors to Potential Severe Core Damage Accidents : 1985 A Status Report, U.S. Nuclear Regulatory Commission, 1986, December.

[4] Reactor Safety Study - WASH-1400, U.S. Nuclear Regulatory Commission, NUREG- 75/014, 1975, October.

[5] Reactor Safety Study Methodology Application Program : Oconee # 3 PWR Power Plant, U.S. Nuclear Regulatory Commission, NUREG/CR-1659. 1981, May.

[6] Reactor Safety Study Methodology Application Program : Sequoyah # 1 PWR Power Plant, U.S. Nuclear Regulatory Commission, NUREG/CR- 1659, 1981, April.

[7] Reactor Safety Study Methodology Application Program : Calvert Cliffs # 2 PWR Power Plant, U.S. Nuclear Regulatory Commission, NUREG/CR- 1659, 1982, May.

[8] Reactor Safety Study Methodology Application Program : Grand Gulf BWR Power Plant, U.S. Nuclear Regulatory Commission, NUREG/CR- 1659, 1982, August.

[9] Interim Reliability Evaluation Program: Analysis of Millstone Point Unit 1 Nuclear Power Plant, U.S. Nuclear Regulatory Commission, NUREG/CR- 3085, 1983,February.

[10] Interim Reliability Evaluation Program: Analysis of Browns Ferry Unit 1 Nuclear Power Plant, U.S. Nuclear Regulatory Commission, NUREG/CR- 2802 1982 July.

[11] Interim Reliability Evaluation Program: Analysis of Calvert Cliffs Unit 1 Nuclear Power Plant, U.S. Nuclear Regulatory Commission, NUREG/CR- 3511, 1984, August.

[12] Interim Reliability Evaluation Program: Analysis of Crystal River-3, Unit 1 Nuclear Power Plant, U.S. Nuclear Regulatory Commission, NUREG/CR- 2515, 1981, December.

[13] Anticipated Transients Without Scram For Light Water Reactors, U.S. Nuclear Regulatory Commission, NUREG - 0640, 1978, December.

[14] Reliability of Emergency AC Power Systems at Nuclear Power Plants, U.S. Nuclear Regulatory Commission, NUREG/CR- 2989, 1983, July.

[15] Generic Evaluation of Small Break Loss-of-Coolant Accident Behavior, U.S. Nuclear Regulatory Commission, NUREG - 0565, 1980, January.

[16] Station Blackout Accidents in LWRs, U.S. Nuclear Regulatory Commission, NUREG/CR- 3226, 1985.

[17] A Probabilistic Safety Analysis of D.C. Power Supply Requirements for Nuclear Power Plants, U.S. Nuclear Regulatory Commission, NUREG - 0666, 1981, April.

[18] Reliability Analysis of Containment Isolation System, U.S. Nuclear Regulatory Commission, NUREG/CR- 4220, 1985, June.

[19] A Prioritization of Generic Safety Issues, U.S. Nuclear Regulatory Commission, NUREG - 0933, 1984, July.

[20] Reactor Risk Reference Document, U.S. Nuclear Regulatory Commission, NUREG - 1150, 1987, February.

[21] Zion Probabilistic Safety Study, Commonwealth Edison Company of Chicago, 1981, September.

[22] Millstone Unit 3 Probabilistic Safety Study, Northeast Utilities, 1983, August.

[23] Seabrook Probabilistic Safety Study, Pickard, Lowe, and Garrick, 1985.

[24] Indian Point Probabilistic Safety Study, Power Authority of State of New York, and Consolidated Edison, 1982.

[25] Limerick Probabilistic Safety Study, Philadelphia Power Company, 1984.

[26] IDCOR Technical Summary Report - Nuclear Power Plant Response to Severe Accidents, Technology for Energy Corp., 1984, November.

[27] Calvert Cliffs IPE Study, Baltimore Gas and Electric Company, 1987, July.

[28] Grand Gulf Power Station IPE Study, Mississippi Power and Light Company, 1987, July.

[29] Shorhm Nuclear Power Station IPE Study, Long Island Lighting Company, 1987, July.

[30] Oconee Nuclear Power Station, Duke Power Company, 1987, July.

[31] R.B. Worrel, Sets Reference Manual, U.S. Nuclear Regulatory Commission, NUREG/CR- 4213, 1985, May.

[32] Hunt, R.N.M. and M. Modarres, Performing a Plant Specific PRA by Hand - A Practical Reality, 14th-Inter-RAM-Conference, Toronto, 1987, May.

[33] Procedure for Performing A Failure-Mode-and-Effect-Analysis for Shipboard Equipment, U.S. Department of Defense, MIL-STD-1629 (SHIP), 1974, November.

[34] Locks, M.O., Recent Developments in Computing of System-Reliability IEEE Transactions on Reliability, 5, 1985 December.

[35] Waterman D., A Guide to Expert Systems, Addison Wesely, 1986.

[36] Golden Common Lisp 286, GCLISP-286, Gold Hill Computers, Incorporated, Cambridge, MA, 1986, October.

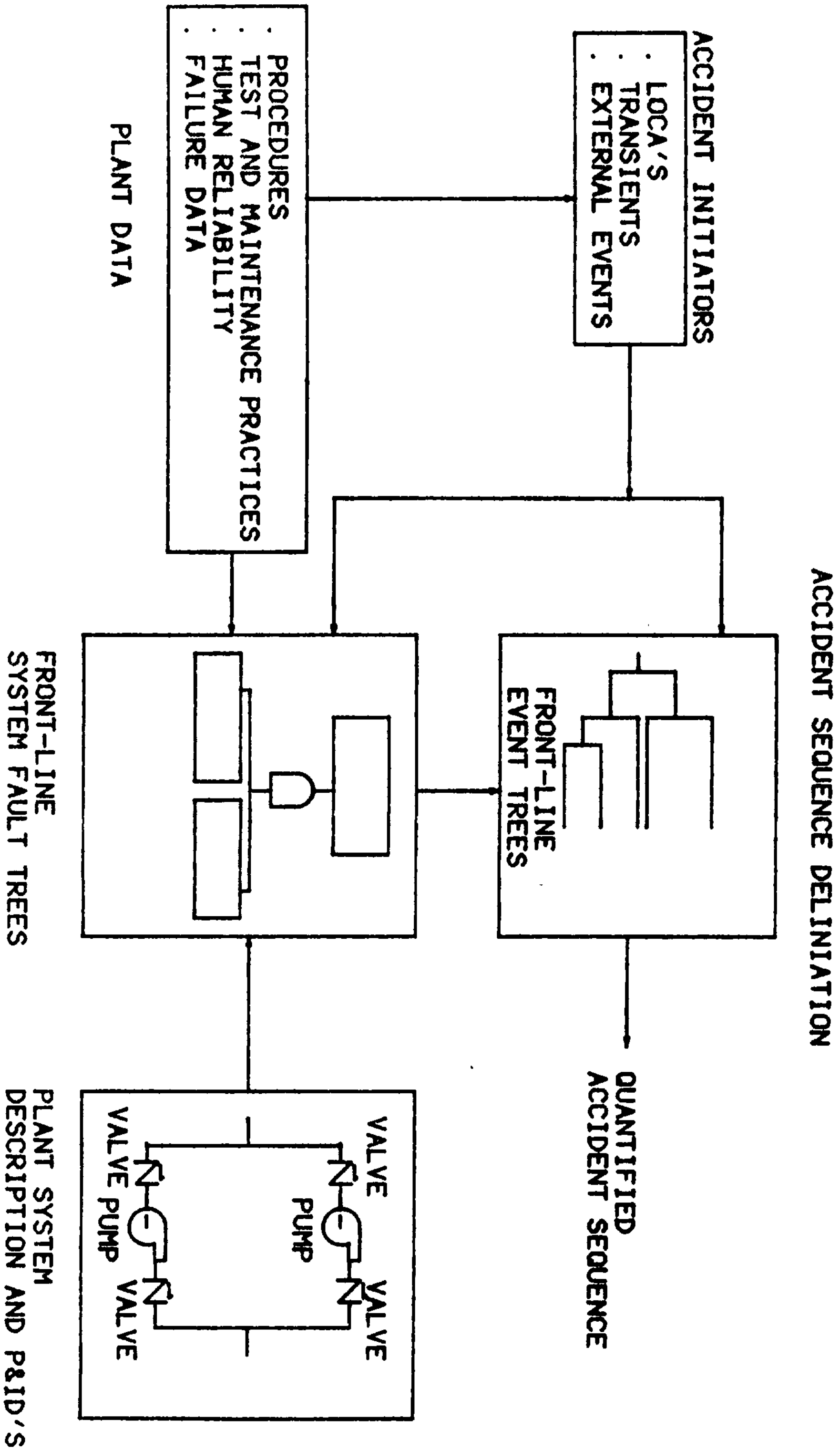


Figure 1: SMALL EVENT TREE LARGE FAULT TREE APPROACH

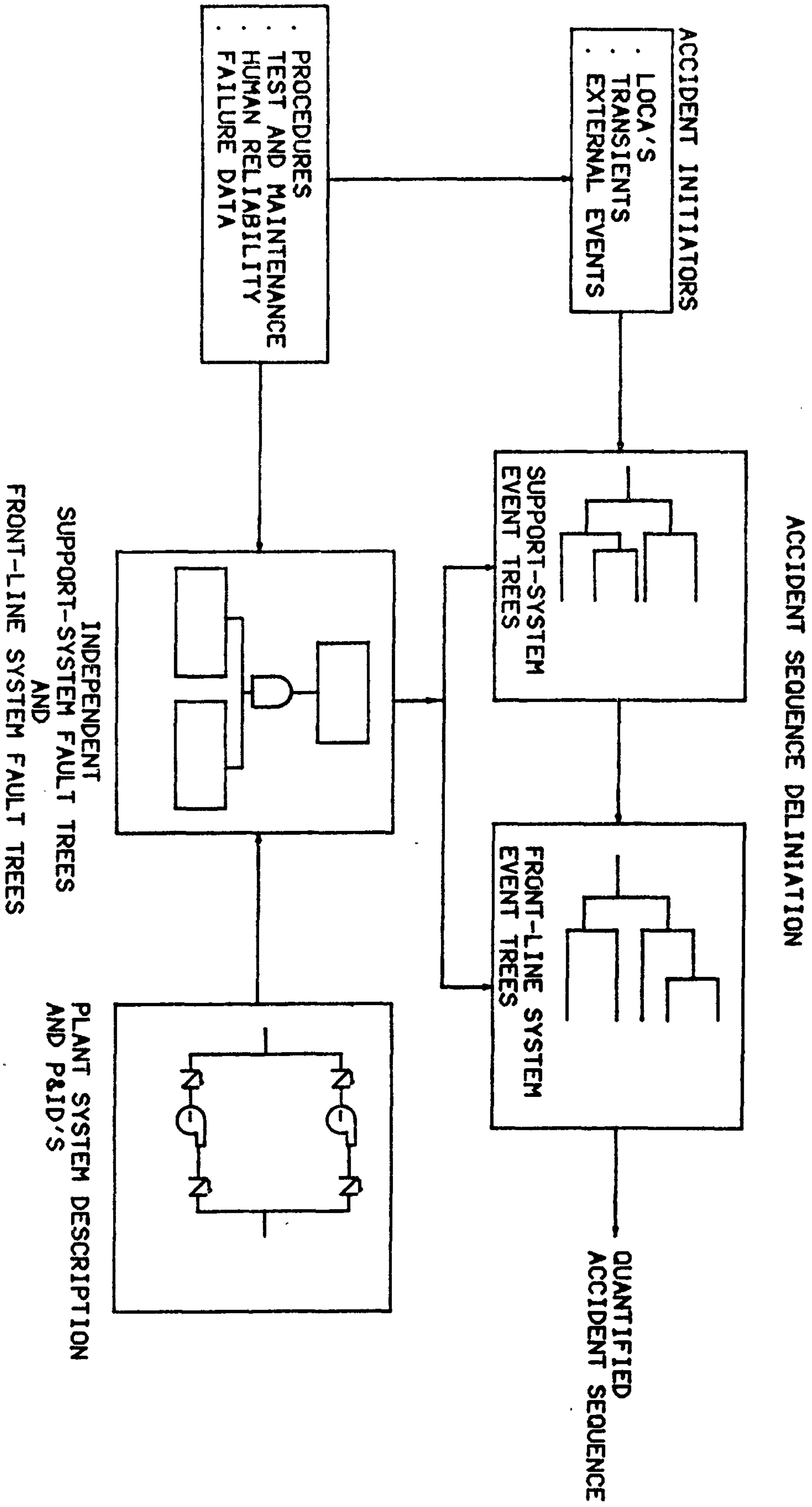

ACCIDENT INITIATORS
. LOCA'S
. TRANSIENTS
. EXTERNAL EVENTS
. PROCEDURES
. TEST AND MAINTENANCE
. HUMAN RELIABILITY
. FAILURE DATA
ACCIDENT SEQUENCE DELINIATION
SUPPORT-SYSTEM EVENT TREES
FRONT-LINE SYSTEM EVENT TREES
QUANTIFIED ACCIDENT SEQUENCE
INDEPENDENT SUPPORT-SYSTEM FAULT TREES AND FRONT-LINE SYSTEM FAULT TREES
PLANT SYSTEM DESCRIPTION AND P&ID'S

Figure 2: LARGE EVENT TREE SMALL FAULT TREE APPROACH

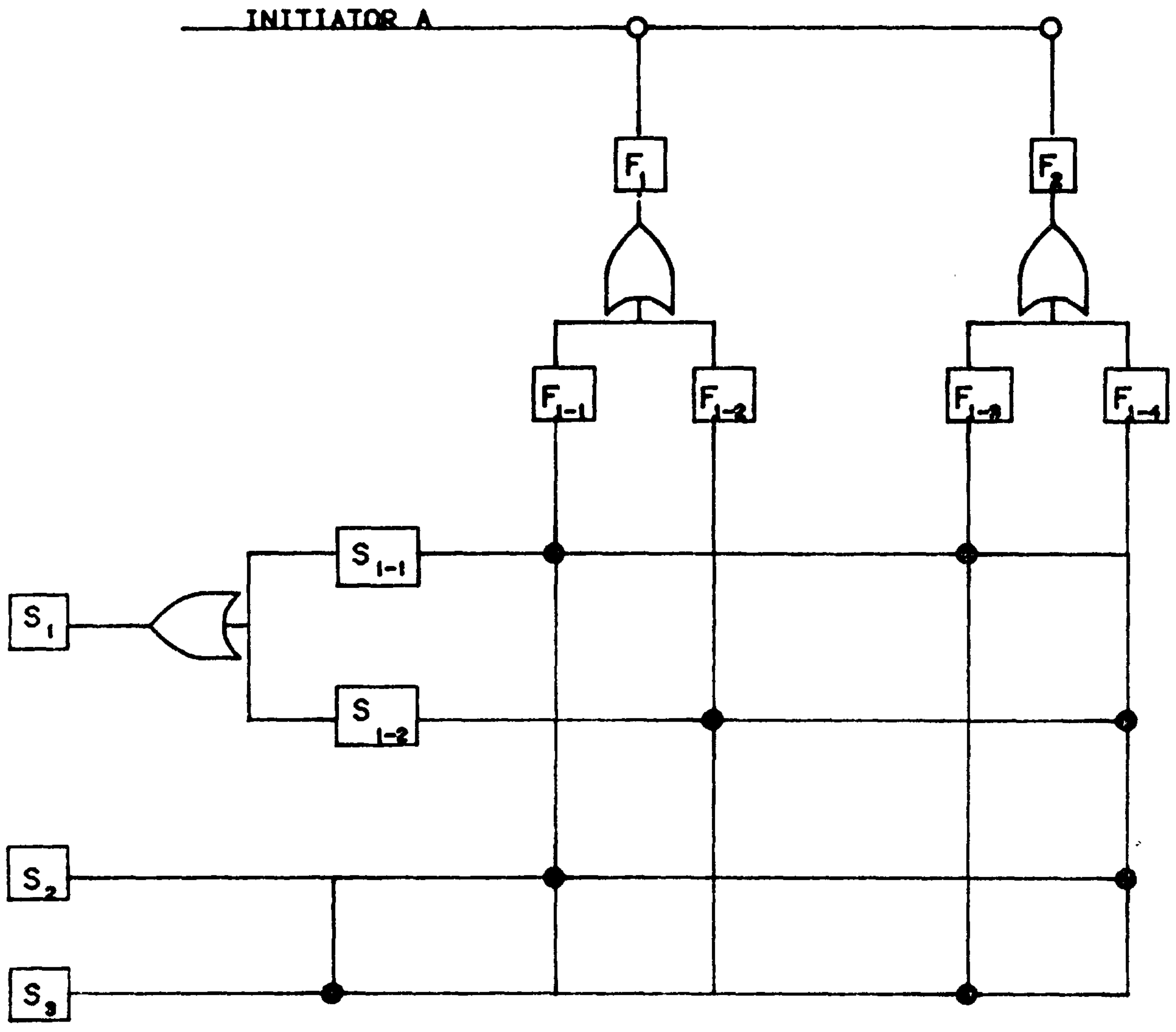


Figure 3: THE EXAMPLE OF MPLD

Failed Support systems	Prob.	End-State Unavail. Front-line
S_{1-1}	0.1	F_{1-1}, F_{2-1}
S_{1-2}	0.1	F_{1-2}, F_{2-2}
S_2	0.1	F_{1-1}, F_{2-2}
S_3	0.1	F_{1-1}, F_2
S_{1-1}, S_{1-2}	0.01	F_1, F_2
S_{1-1}, S_2	0.01	F_{1-1}, F_2
S_{1-1}, S_3	0.01	F_{1-1}, F_2
S_{1-2}, S_2	0.01	F_1, F_{2-2}
S_{1-2}, S_3	0.01	F_1, F_2
S_2, S_3	0.01	F_{1-1}, F_2
S_{1-1}, S_{1-2}, S_2	0.001	F_1, F_2
S_{1-1}, S_{1-2}, S_3	0.001	F_1, F_2

Table 1: SUPPORT SYSTEM END STATES

Reduced End State	Prob.
F_{1-1}, F_{2-1}	0.1
F_{1-2}, F_{2-2}	0.1
F_{1-1}, F_{2-2}	0.1
F_{1-1}, F_2	0.13
F_1, F_2	0.022
F_1, F_{2-2}	0.01

Table 2: REDUCED END STATES

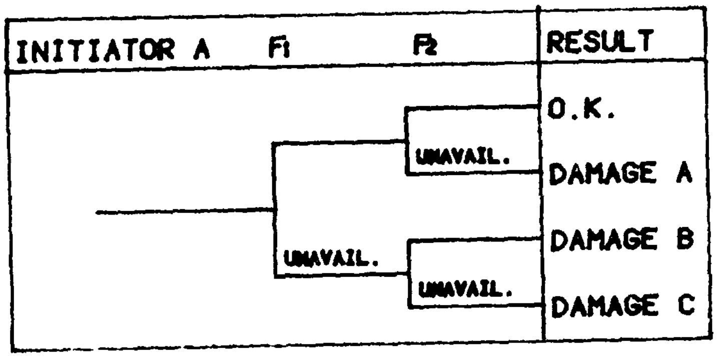


FIGURE 4: A GENERIC FRONT-LINE EVENT TREE

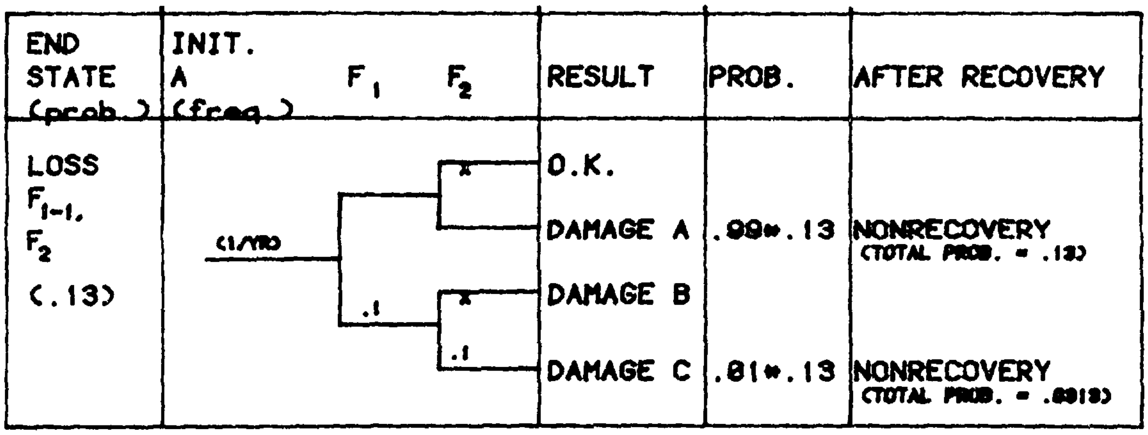
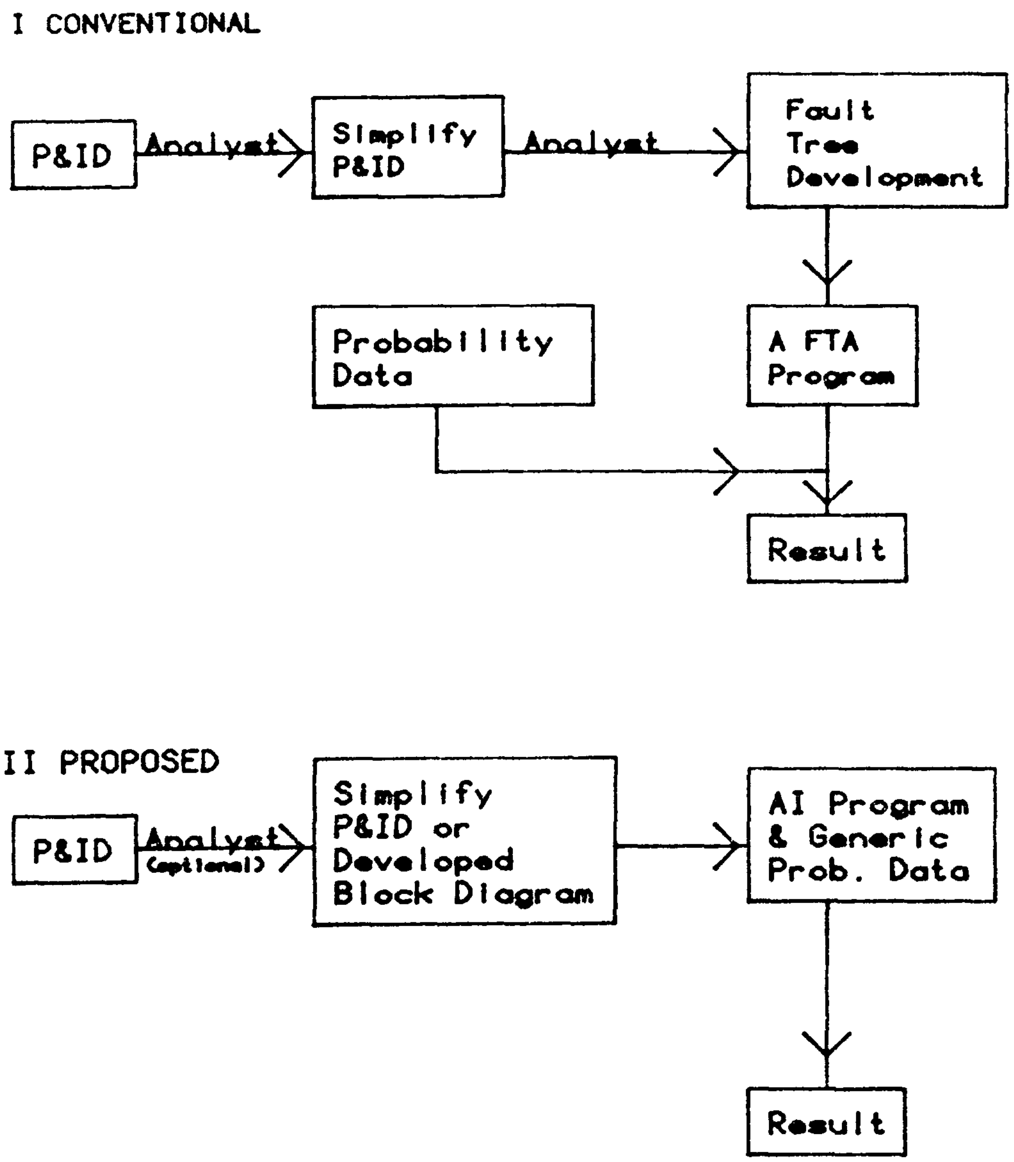


Figure 5: FRONT-LINE EVENT TREE
FOR S3 UNAVAILABLE



I CONVENTIONAL

II PROPOSED

Figure 6: SUMMARY OF THE SYSTEM PROBABILITY DETERMINATION PROCESS

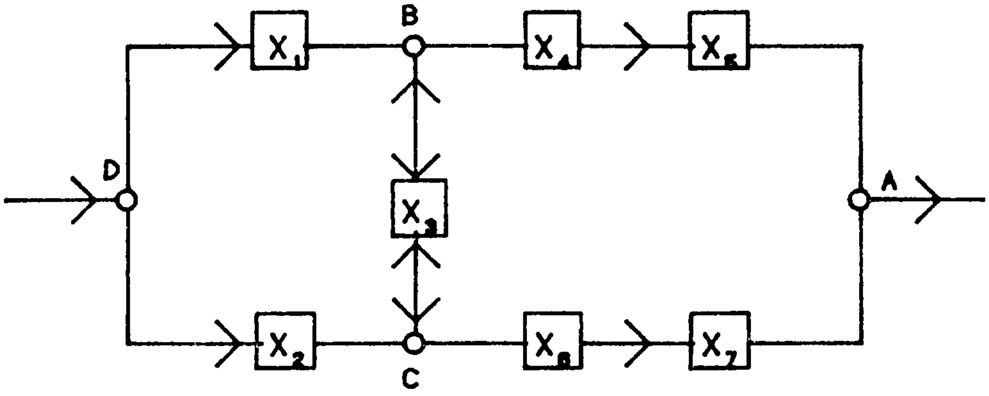


Figure 7: THE BLOCK DIAGRAM

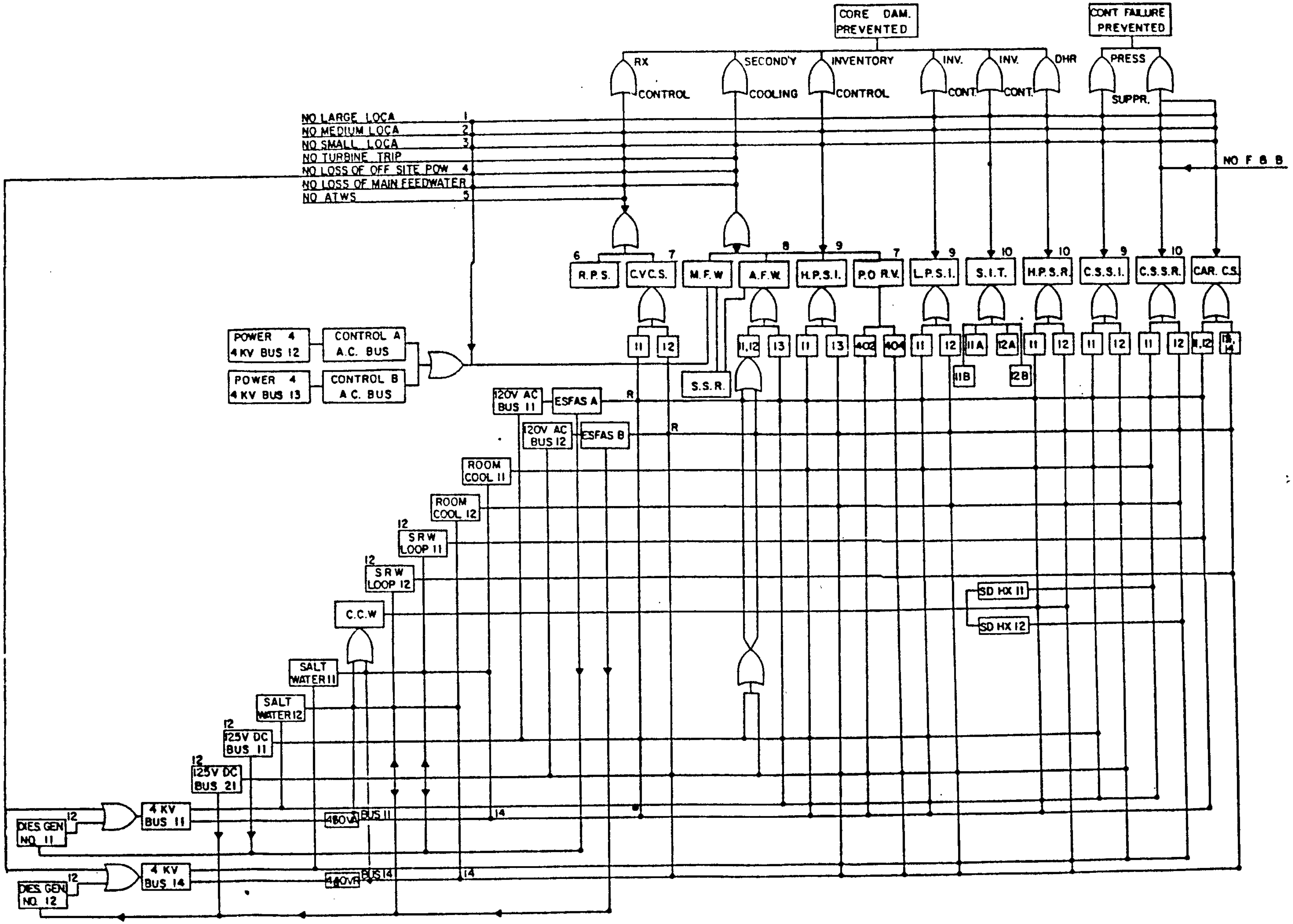


Figure 8: Master Plant Logic Diagram

SHORTHAND	DESCRIPTION
AFW	Auxiliary FeedWater system
ATWS	Anticipated Transient Without Scram
CARCS	Containment Air Recirculation and Cooling System
CCW	Component Cooling Water system
CONT	CONTainment
CSSI	Containment Spray System in Injection mode
CSSR	Containment Spray System in Recirculation mode
CVCS	Chemical and Volume Control System
DHR	Direct Heat Remover
DIES. GEN	DIESel GENerator
ESFAS	Engineered Safety Features Actuation System
F&B	Feed and Bleed
HPSI	High Pressure Safety Injection
HPSR	High Pressure Safety Recirculation
INV CONT	INVentory CONTrol
LOCA	Loss-Of-Coolant Accident
LPSI	Low Pressure Safety Injection
MFW	Main FeedWater system
PORV	Power Operated Relief Valves
PRESS SUPPR	PRESSure SUPPResion
RPS	Reactor Protection System
RX	Reactor
SD HX	ShutDown Heat Exchanger
SIT	Safety Injection Tanks system
SSR	Secondary System Relief

Figure 8: Continued

INITIATING EVENT	END STATE PROB.		THE REDUCE END STATES THAT CAUSE THIS CORE MELT	CORE MELT PROB.	
	HAND	PRA-EXPERT		HAND	PRA-EXPERT
LOSS OF OFFSITE POWER FREQ. = .13	5.3E-2	5.3E-2	1-2-11-X-11-1	2.2E-5	2.2E-5
	2.2E-1	2.2E-1	2-0-22-X-22-2	1.7E-5	1.6E-5
	1.8E-2	1.8E-2	0-0-11-0-11-0	3.0E-6	3.0E-6
	1.8E-2	1.8E-2	0-0-22-0-22-0		
	.67	.67	0-0-00-0-00-0	1.7E-6	1.6E-6

Table 3: COMPARISON OF IDCOR-IPE HAND CALCULATION WITH PRA-EXPERT PROGRAM (PARTIAL)

* indicate the status of front-line system (CVCS)-(AFW)-(HPSI/LPSI)(CSSI)-(PORV)-(HPSR)(CSSR)-(CARCS); 0 for available, 1 for loss train 1, 2 for loss train 2 x for train 1 & 2 unavailable e.g., 1-2-11-x-11-1 indicates AFW lost train 2, PORV lost all trains, other front-line systems lost train 1.