PROBABILISTIC SAFETY ASSESSMENT (PSA) FOR A FEEDWATER SYSTEM IN PRESSURIZED WATER REACTOR

Mohamed K. Shaat*, A.M. Metwally and M. Nagy**

* Reactors Department, Nuclear Research Center,
Atomic Energy Engineering Department,
** Nuclear Engineering Department,
Faculty of Engineering, Alexandria University
Alexandria, Egypt

ABSTRACT

The total failure probability of A typical feedwater system is evaluated. The overall success and failure combinations are determined through the construction of event tree model. The fault tree model, is constructed to describe how the combination of basic events could result in overall system failure. The fault tree is solved using the International Atomic Energy suite of computer codes PSAPACK.

Using the application of probabilistic safety assessment in decisions on risk management, the improvement of system reliability is discussed through adding two trains of essential plant sequencing equipment.

INTRODUCTION

Several nuclear accidents such those occurred at three Mill Island and Chernobyl Have led to a rapid expansion of the use of probabilistic Safety Assessment (PSA) techniques all over the world. the reactor Safety Study (WASH-1400) is considered as one of valuable publications in demonstrating the safety of power stations.

Several PSA methods are used to evaluate the safety and reliability of complex systems, especially in the nuclear industry[2].

The development of the event trees and fault trees[3] that are necessary to perform PSA studies of complex systems requires a considerable effort, and an in-depth understanding of the systems design and operation.

Recent developments in PSA have demonstrated many applications in safety decisions related to design, licensing and operation [4]. such applications provide invaluable suggestions in eliminating weaknesses, which may led to major accidents.

In this paper, the reliability of a typical feedwater system will be analyzed. The overall success and failure combinations are determined through the construction of event tree model. The fault tree model is constructed to describe how the combination of basic events could result in overall system failure. The fault tree is solved using the International Atomic Energy Agency (IAEA) suite of computer codes PSAPACK (5). The results are analysed using the application PAS decisions rules in risk management.

SYSTEM DESCRIPTION

The typical feedwater system shown in Figure (1) is a three pump standby system, normally not running, but required to supply feedwater when demanded by the "system demand signal" shown. The system preferentially starts the main feed pump 1. In the event of failure to start this pump, the standby pump 2 is automatically started. Both these pump are electrically driven from 3.3 Kv supplies. In the event of failure of both these pump the diesel driven reserve pump 3 is manually started from the central control room (CCR). Two storage tanks are used to supply water to the pump and hence to the boilers. The main water storage tank (MWST) is the preferred source of water and supplies the main and standby pumps 1&2. Following a detected failure of this supply, the supply from the reserve water storage tank (RWST) is automatically available to all three pumps.

Figure (1) illustrates the various electrical power supplies (3.3 KV) and electrical instrumentation supplies (110 V) used. Overall sequence control for the system is provided by the Essential Plant sequencing Equipment (EPSE) with local controllers for opening the RWST discharge control valve and for starting the diesel driving the reserve pump 3.

EVENT TREE ANALYSIS (ETA)

The purpose of the event tree construction is to define

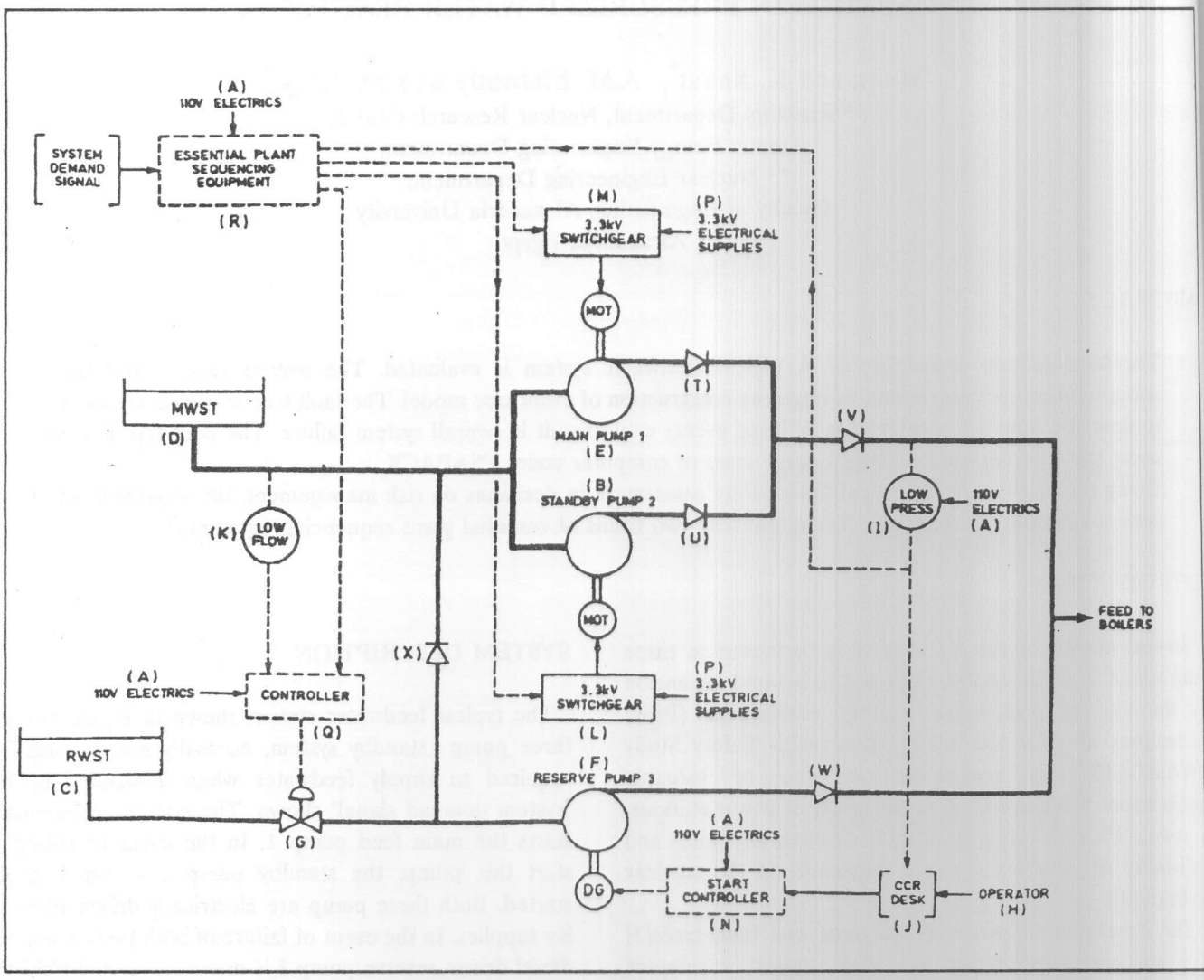

Figure 1. A Typical Feedwater System.

the overall system success and failure states in terms of the states of main system components.

The only components to be considered in the ETA area:

Essential Plant Sequencing (R),
MWST (D),
Main Pimp (E),
Standby Pump (B),
RWST (C),
and Diesel Pump (F),

Figures (2). and (3) represent the functional event tree and the event tree for the feedwater system described in Figure (1). As shown from Figure (3). The failure states of the feedwater system can be described by Boolean algebra as:

$$\underset{(4)}{R\bar{D}\bar{E}\bar{B}\bar{C}F} + \underset{(5)}{RD\bar{E}\bar{B}\bar{C}} + \underset{(7)}{R\bar{D}\bar{E}\bar{C}} + \underset{(5)}{RD\bar{E}\bar{B}\bar{C}} +$$

$$\underset{(11)}{R\bar{D}\bar{E}\bar{B}\bar{C}F} + \underset{(12)}{RD\bar{E}\bar{B}\bar{C}} + \underset{(13)}{\bar{R}}$$

$$= R[\bar{D}\bar{C}\bar{E}\bar{B}F + \bar{D}\bar{C}\bar{E}\bar{B} + \bar{D}\bar{C}\bar{E} + \bar{D}\bar{C}\bar{E}\bar{B}$$

$$+ \bar{D}\bar{C}\bar{E}\bar{B}F + \bar{D}\,\bar{C}\bar{E}\bar{B}] + R$$

$$= R\,\bar{D}\bar{C}\bar{E}\bar{B}F + R\bar{D}\bar{C}[E + \bar{E}B + \bar{E}\bar{B}] + R\bar{D}\bar{C}\bar{E}\bar{B}$$

$$+ R\bar{D}\bar{C}\bar{E}\bar{B}F + \bar{R}$$

$$= R\,\bar{D}\bar{C}\bar{E}\bar{B}F + R\bar{D}\bar{C} + R\bar{D}\bar{C}\bar{E}\bar{B} + R\bar{D}\bar{C}\bar{E}\bar{B}F + \bar{R}.$$

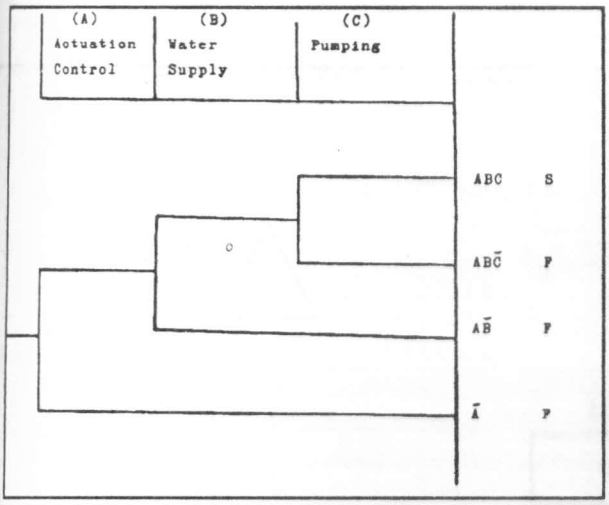

Figure 2. Functional Event Tree.

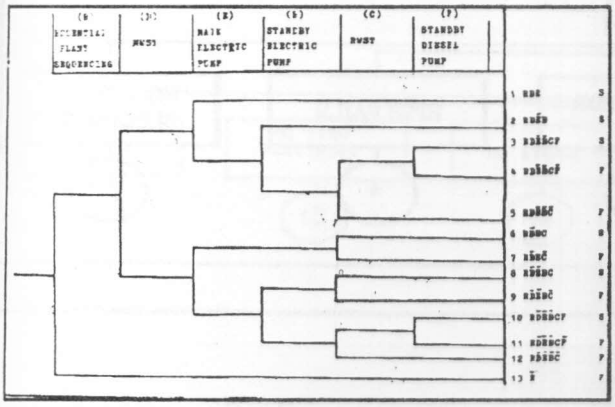

Figure 3. Event tree analysis.

FAULT TREE ANALYSIS (FTA)

Fault tree analysis for the feedwater system shown in Figure (1) can be constructed under the following simplifying assumptions:

(1) The assessment is to be limited to calculating the probability of failing to establish a specified feedwater flow. Probabilities of overfeeding are not be considered.
(2) The specified minimum feedwater flow is that supplied from one feedwater storage tank and provided by one running pump.
(3) Partial failures are not to be considered.
(4) Common cause failures are not to be modelled.
(5) Human factors contributions are not to be included except for the one manual action shown in Figure (1), and denoted by (H).
(6) Support systems are only to be modelled to the extent shown in Figure(1).

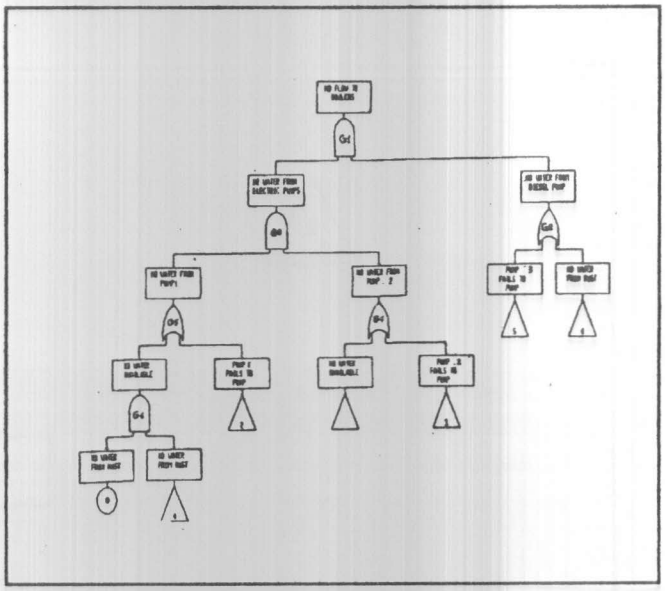

Figure 4. The fault tree analysis (Sheet 1).

(7) Passive failures, such as pipe failures, are not to be modelled.
(8) Certain failure effects are to be excluded, i.e. non return valve failures pipe blockages or breaks spurious trips and spurious signals effects, such as hazards.
(9) Real failure probability data for some items are only available as a failure probability per demand. The failure probabilities of failure on system demand.

The complete fault tree analysis for the feedwater system is constructed as shown in Figure (4). From this figure we notice that the failure states identified in the event tree should be cross checked for consistency.

RESULTS USING PSAPACK PROGRAM

The fault threes are solved using the IAEA suite of computer codes PSAPACKE. The date to be used in this solution are drive from a database in PSAPACK (5) and are shown in Table (1).

The results of the fault tree analysis are:

1. Overall system failure probability = 9.5447×10^{-4}
2. Number of cut-stes derived = 49
3. Dominant cut-sets-1st order = 2
   2 nd order = 15
   3 rd order = 32
4. Most significant plant item = EPSE

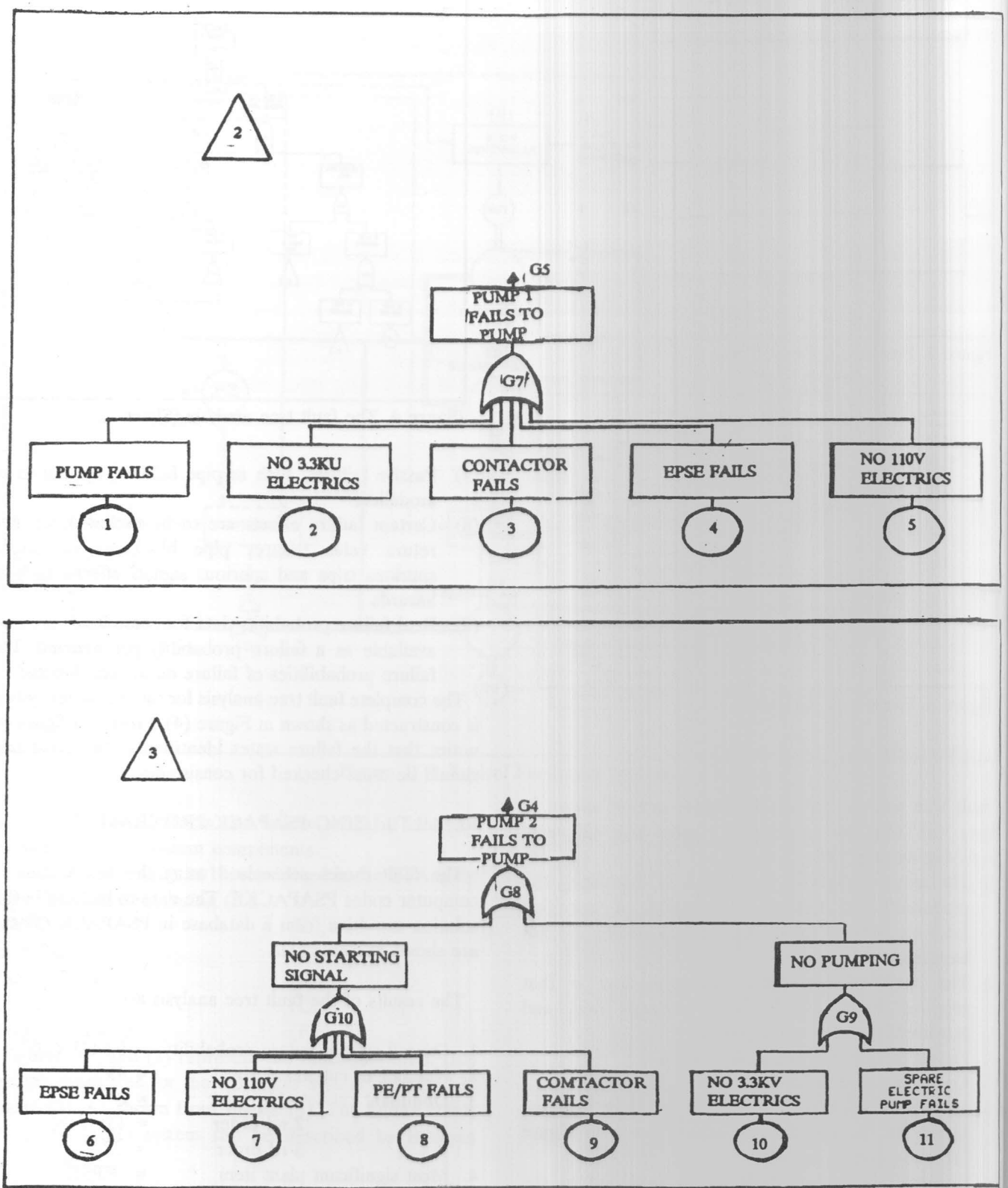

Figure 4. Continued (sheet 2).

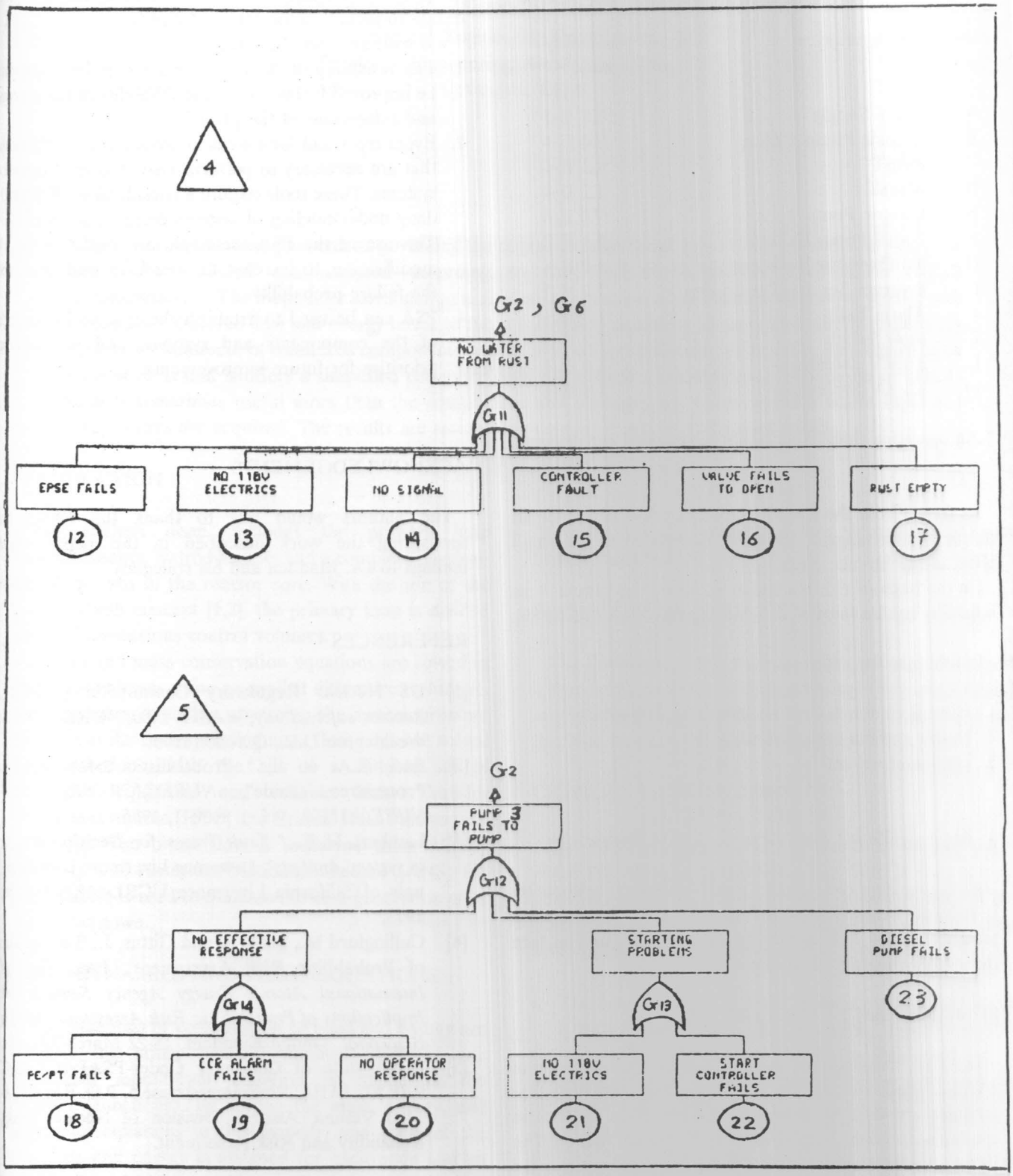

Figure 4. Continned (sheet 3).

Table 1 . Failure Probabilities Used for the Fault Tree Analysis

Item Code	Item Description	Failure probability per demand*
A	110 V Supply	1.8 E-5
B	Electric Pump Failure	7.0 E-4
C	PWST	1.2 E-4
D	MWST	1.2 E-4
E	Electric Pump 2 Failure	7.0 E-4
F	Diesel Pump Failure	3.1 E-2
H	No Operator Response	1.0 E-4
I	Pressure Sensor/Transmitter	5.9 E-3
J	Alarm Fails	1.7 E-3
K	Flow Switch	2.2 E-3
L	3.3 KV Switchgear	1.6 E-3
M	3.3 KV Switchgear	1.6 E-3

* An operating time of 12 hours is assumed per demand.

As shown from the results, the large effect of the EPSE on the system failure probability compared to the small effect of the human error.

On the basis of risk management issue, the system = m reliability can be improved by adding two trains of EPSE.

In this case the results are:

1. Overall system failure probability= 4.37×10^{-5}
2. Number of cut-sets derived = 49
3. Dominant cut-set-1st order = 2
   2 nd order = 15
   3 rd order = 32
4. Most significant plant item = 110 V electric.

As shown from the results, the system failure probability is reduced from 9.544×10^{-4} to 4.37×10^{-5} due t system modification by adding two trains of EPSE, and in turn the system reliability is improved.

SUMMARY AND CONCLUSIONS

The PSA technique are used to analyze the operation of a typical feedwater system. The event tree and fault tree modules are used to describe how the plant failures in combination could results in overall system failure. The IAEA-Computer Codes PASPACK are used to solve the fault tree and obtained the total failure probability of the system.

The system reliability can be improved by modifying the design to include more trains of EPSE.

We conclude this study that:

1. The reliability of the overall nuclear power plant can be improved by improving the reliability of the systems and subsystems of the plant.
2. Event trees and fault trees analysis are powerful tools that are necessary to perform PSA studies of complex systems. These tools require a considerable effort, and deep understanding of systems design and operation.
3. The use of the PSA technique are useful to system modification, to increase the reliability and to reduce the failure probability.
4. PSA can be used to establish the relative importance of the components and systems, and in assigning priorities for future improvements.

ACKNOWLEDGEMENTS

The authors would like to thank the CEGE for sponsoring the work described in this paper. Greet feelings to Dr. Madden and his collegues.

REFERENCES

[1] US Nuclear Regulatory Commission (USNRC), *Reactor safety Study*, WASH- 1400, NUREC-75/014, Weshington D.C., October 1975.

[2] Bari, R.A. et al; " Probabilistic Safety Analysis Procedures Guide", *NUREC/CR-2815, BNL-NUREC-51559*, vol. 1, Rev. 1, 1985.

[3] Lambert, H. E., " *Fault Treees for Decision Making in system Analysis*", Lawernce Livermore Laboratory, univ. of California, Livermore, UCRL-51829, October 1975.

[4] Cullingford M., Shah, S. and Gittus, J., "Implications of Probabilitic Risk Assessment", Proceedings of *International Atomic Energy Agency Seminor on Implications of Probabilistic Risk Assessment Held in Blackpool*, United Kingdom, 18-22 March 1985.

[5] IAEA suite of Computer Codes-PSAPACK (INT 9/0630), IAEA, Wagramerstrasse 5, P.O. Box 100, A-1400 Veinna, Austria, Division of Nuclear Safety, Reliability and Risk Assesment.