UFRJ - COPPE -
PEN -- 103.

[redacted]

PROGRAMA DE ENGENHARIA NUCLEAR — COPPE/UFRJ

[illegible]

PROGRAMA DE ENGENHARIA NUCLEAR - COPPE/UFRJ
Ilha do Fundão - Centro de Tecnologia - Bl. G S/206
C.P. 68509 - CEP - 21910 - Rio de Janeiro - RJ - Brasil

RELIABILITY ANALYSIS OF ANGRA I SAFETY SYSTEMS

LUIZ FERNANDO S. DE OLIVEIRA, JUAN BAUTISTA SOTO,
CAIO CÉSAR MACIEL, SONIA MARIA ORLANDO GIBELLI,
PAULO VICTOR FLEMING E LUIZ ALBERTO ARRIETA

JUL/80 **PEN/103**

atenção

Apresentado no Simpósio Teuto-Brasileiro sobre Segurança Nuclear, Rio de Janeiro, 16-21 de Junho de 1980.

RELIABILITY ANALYSIS OF ANGRA I SAFETY SYSTEMS

I. Introduction

Although risk methodology and probabilistic analysis have only recently begun to be extensively applied to safety evaluations of large complex systems such as nuclear power plants, several in-depth studies have already been performed, of which the most comprehensive are the Reactor Safety Study-WASH 1400[1] (the so-called "Rasmussen Report") and the recently published German Risk Study[2]. The applications of probabilistic safety analysis are becoming widespread and are currently recognized in the most advanced countries as valuable tools in decision processes pertaining to the licensing, design, and operation of nuclear systems[3,4]. This is particularly true now that after detailed investigations of the TMI-2 accident both the Kemeny Commission[5] and the Rogovin Special Inquiry Group[6] came up with recommendations for an increasing use of probabilistic methods in reactor safety analysis.

Outside the nuclear field risk methodology has also been applied to some important projects of which the most famous one is the "Canvey Island Report"[7] carried out by the U.K. Health and Safety Executive in conjunction with the Safety and Reliability Directorate of U.K.A.E.A.

In Brazil, only very recently (January 1980) a research group was set up at COPPE/UFRJ aimed at studying the applicability of probabilistic methods to nuclear reactor safety[8]. Our group is partly financed by CNEN and benefits from the collaboration of a few people from institutions other than COPPE.

Our initial goal is to perform an extensive reliability analysis of some safety systems of Angra I. For this task we are using the fault tree technique which has been successfully used in most reliability studies of nuclear safety systems performed to date.

The following systems were chosen to be analysed in the first phase of the project: 1) accumulators, 2) low pressure injection and recirculation, 3) high pressure injection and recirculation, 4) containment spray injection and recirculation, 5) auxiliary feedwater, 6) reactor protection, and 7) electrical power supply systems.

In section II of this paper we give a brief description of the fault tree methodology, emphasizing the process steps, its advantages and disadvantages.

Results of a quantitative determination of the unavailability of the accumulator and the containment spray injection systems are presented and analysed in section III. These results are also compared to those reported in WASH-1400. Finally in section IV we summarize our conclusions.

Before closing this brief introduction let us mention that the main objective of our present studies is not to achieve any novel results at this moment, but to develop in our country a group of individuals with ability to formulate and solve more fundamental applications of reliability theory and probabilistic methods in the field of nuclear reactor safety. In this sense, we hope that our present efforts will contribute

to an increasing application of the probabilistic approach in the design, operation, and specially in the licensing procedure of future Brazilian nuclear installations.

II. Reliability Analysis and Pault Tree Methodology

Reliability has been defined as[9]:

> "that characteristic of an item expressed by the probability that it will perform its required function in the desired manner under all the relevant conditions and on the occasions or during the time intervals when it is required so to perform".

For a simple item or one with a high probability of failure (a not very reliable one) it is possible to experimentally estimate its reliability for a certain mission from a frequency argument, that is by relating the number of successful mission completions to the total number of times the item was called upon to perform that function. However, such is not a practical procedure for highly complex technological systems which have extremely small failure probabilities and/or whose failure consequences are too costly or too catastrophic to be allowed to occur.

For a complex system involving a large number of components it is necessary to use the methods and rules of probability to predict system behavior from component behavior, in other words, system reliability from component reliability.

The rules of probability describes also how to numerically express confidence in the predicted outcome. Such is the main objective of reliability analysis. In addition to quantitatively determining the probability of success (or failure) of a system, reliability analysis also provides a valuable means of identifying the critical or "weak" points of the system and of performing sensitivity analyses.

For those systems whose functioning state must be maintained for a considerable period of time the significant probabilistic feature is indeed the unreliability (failure probability) or reliability (probability of success) as previously defined. On the other hand, for standby systems which must function on demand the most important probabilistic parameter is the availability or unavailability of the system.

Availability has been defined as[10]

> "the characteristic of an item expressed by the probability that it will be operational at al randomly selected future instant in time".

In order to quantitatively evaluate any of the above mentioned probabilistic features of a complex system it is necessary to have a logic model relating the system characteristics to those of the components. There are different ways to accomplish this task. In our work we have chosen to use the fault tree methodology which has been successfully applied in the studies previously mentioned[1,2].

Fault Tree Analysis (FTA)

A fault tree (FT) is a deductive logic diagram consisting of a specified and well-defined "undesired event" at the top of the tree and a logic structure beneath it which reveals those various parallel and sequential combinations of component states (possible root causes) that can result in the occurrence of the undesired event (also known as "top event"). In a typical reactor safety analysis, the undesired event is usually a system failure; e.g, "failure of the containment spray injection system to provide sufficient flow to CSIS nozzles given a large LOCA has occurred".

It is extremely important in FTA to properly define the top event. Much time and effort should be dedicated to clearly and precisely defining it, otherwise the whole analysis could be incomplete in accomplishing its final goal.

The symbols used in the construction of a fault tree are shown in Fig. 1.

The rectangle describes the output of a logic gate. Therefore it defines an event that results from the logical operation of two or more events.

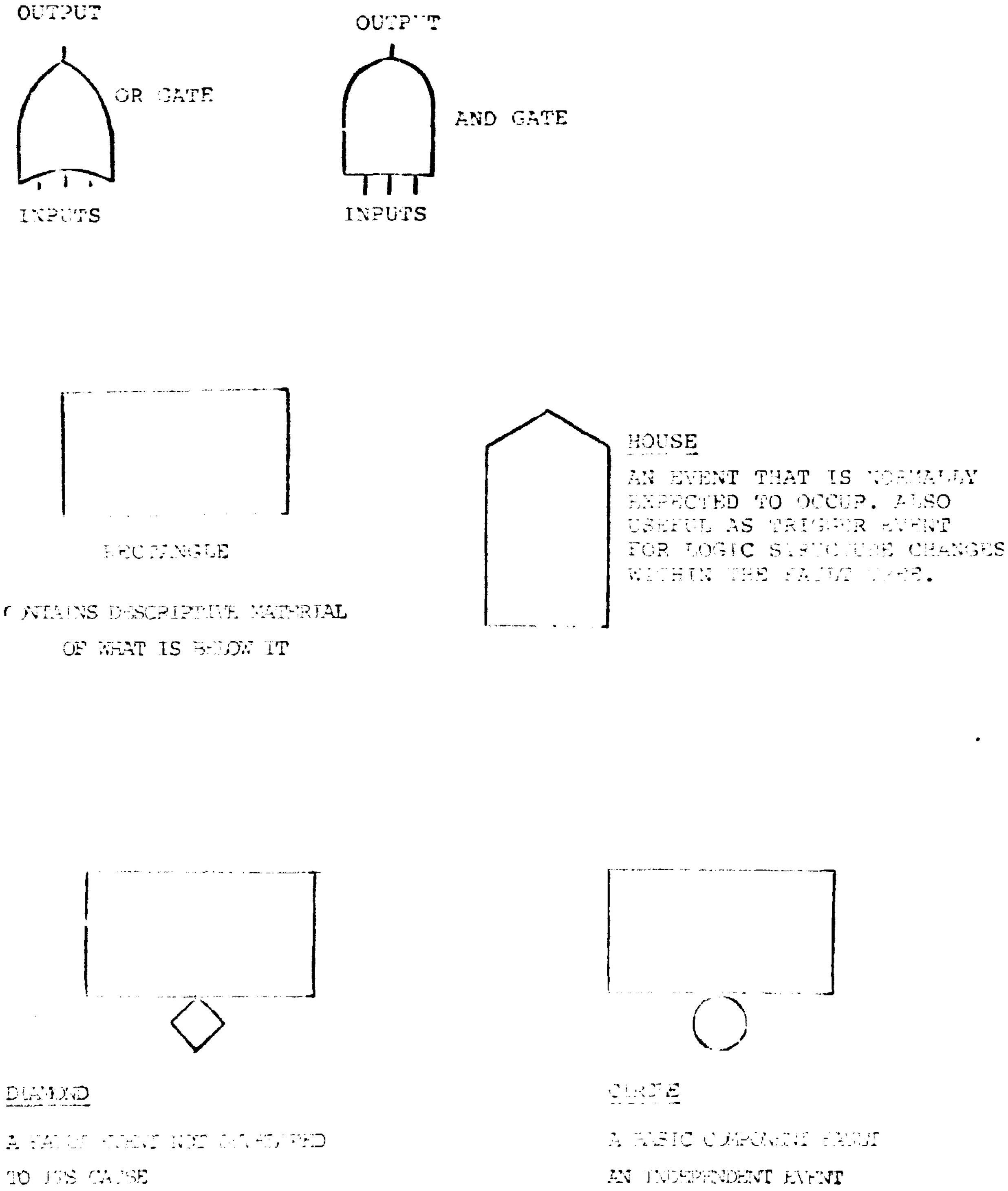


Fig. 1 - Faul Tree Symbols

The circle is used to describe a basic (or primary) failure event. Data regarding frequency and mode of failure can be derived empirically.

The diamond represents an event that is not further developed because of a low probability of occurrence or lack of information, time, or money. It may also be used in cases where another analysis has given sufficient information on the event such that further analysis would be redundant. It is also considered a basic event in the fault tree.

The house defines an event that must occur or is expected to occur because of design and normal operation conditions. Also useful as a trigger event for logic structure changes within the fault tree.

The fundamental logic gates for fault tree construction are the OR gate and the AND gate. The OR gate describes the logical operation that requires the existence of one or more input events to produce the output event. The AND gate describes the logical operation that requires the coexistence of all input events to produce the output event. In Set Theory the OR gate corresponds to the logical union and the AND gate to the logical intersection of the input events.

If two events A and B are inputs to an AND gate the boolean expression for the output event T is:

$$T = A.B, \tag{1}$$

and the corresponding probability expression is

$$P(T) = P(A.B) = P(A).P(B/A) \qquad (2)$$

where (P(B/A) is the probability of occurrence of B given that event A has occurred. If A and B are statistically independent then

$$P(B/A) = P(B)$$

and Eq. (2) becomes

$$P(T) = P(A).P(B) \qquad (3)$$

Substituting the AND gate by an OR gate, the boolean expression of the output event T becomes

$$T = A + B \qquad (4)$$

and the corresponding probability expression can be written:

$$P(T) = P(A) + P(B) - P(A.B) \qquad (5)$$

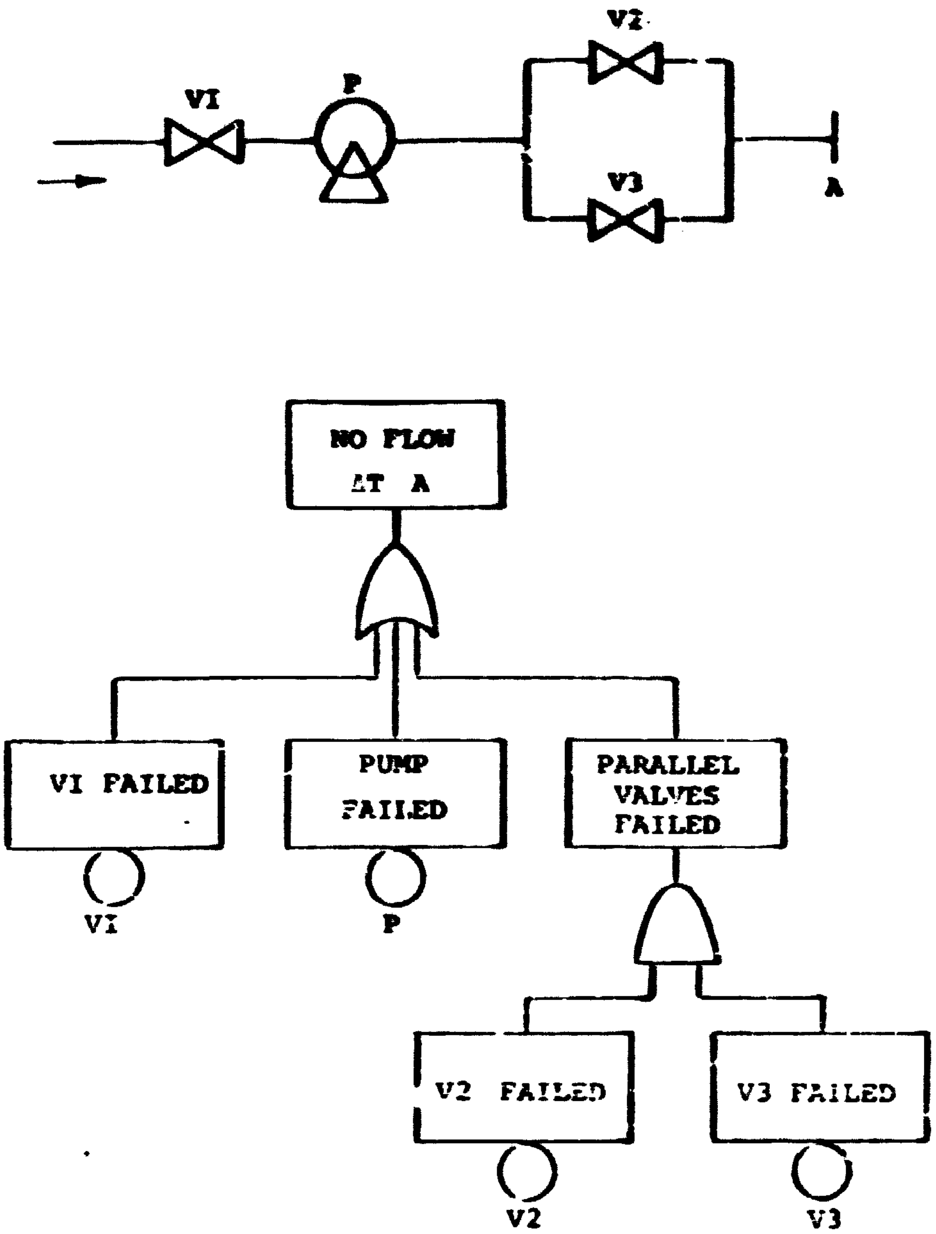
If A and B are statistically independent

$$P(T) = P(A) + P(B) - P(A) . P(B) \qquad (6)$$

The above equations can be readily extended to encompass any number of input events.

Fig. 2 shows an example of a simple fault tree and the associated boolean and probabilistic expressions.

In general three main steps are necessary to the performance of a fault tree analysis on a system: 1) a thorough understanding of the system, 2) construction and evaluation of the fault tree, and 3) analysis of the results.



BOOLEAN EXPRESSION:

$$TOP = V1 + P + (V2.V3)$$

PROBABILISTIC EXPRESSION:

$$P(TOP) = 1 - (1 - P(V1)) (1 - P(P)) (1 - P(V2).P(V3))$$

Fig. 2 - Fault Tree Illustration

The first step requires a complete and detailed understanding of the function, controls and operating and failure modes of the system, besides its interface with other systems and its T&M procedures.

As previously mentioned, the fault tree is constructed using the symbols in Fig. 1, according to a deductive process that tries to identify all causes of each event on the tree, starting with the top event and stoping when each branch ends in a basic (circle) or an undeveloped event (diamond). After the tree has been constructed, the probability of the top event can be calculated by substituting available data for the basic events in a probabilistic expression. Computer codes are generally used to calculate the top event probability when the tree involves a large number of logic gates and basic events.

After constructing and evaluating the fault tree, a great deal of information concerning the system can be developed. For example, the contributions from various types of failures such as hardware, test and maintenance, or common-mode, can be determined. Sensitivity analysis can also be performed to determine, for example, the system's response to variations in the reliability value of a particular component type or of a certain human error. Thus, a sensitivity analysis coupled with an analysis of the relative reliability importance of the components will improve our understanding of the "weak points" in the system and provide essential informations for cost-benefit analyses of potential system improvements, if such improvements are being considered.

It has been said many times that the main problem of applying FTA to nuclear systems is the lack of proper reliability data. Indeed this had been a major concern among fault tree analysts in the nuclear field and data collection has received a lot of attention in the past five years. On the other hand, WASH-1400 has shown that many conclusions reached by reliability techniques are relatively insensitive to possible errors in assignment of failure rates. This is because nuclear safety systems are generally so redundant and complex that the accuracy of reliability estimates is determined more by assumptions in modeling the system than by the data used. Thus, when considering complex systems with many backups or redundancies, an error of 10 (sometimes even 100) in an assigned failure rate will rarely dominate the overall probability of failure (remember we are talking about failure rates in the 10^{-6} to 10^{-9}/hr range).

Moreover, uncertainties in the data can be brought into the analysis by assuming failure and repair rate distributions instead of single point values. The data uncertainties are propagated through the tree logical expressions, and a distribution is obtained for the top event probability, for which confidence levels are then assigned.

The treatment of common-mode failures[2] (CMFs) is another issue that has attracted a great deal of attention from safety analysts in general and fault tree analysts in particular. A CMF is an event that causes two or more channels of a redundancy system to fail in the same category or failure mode. Although the appearance of a CMF can eliminate any degree of redundancy in a system, it has been recognized that the probability of CMFs can be reduced by using physically separated redundant components, different types of equipment, having more than one operator to review personnel actions and by employing other forms of diversities. Different ways of handling the quantification of the probability of occurrence of CMFs have been devised. So far we have been using the same method as used in WASH-1400[12] but we are planning to switch to a more modern approach in the near future. We will return to this discussion in the section IV.

III. Application to Angra-I Safety Systems

In this section we concentrate on the discussion of some preliminary qualitative and quantitative results obtained for the accumulator (ACC) and containment spray injection systems (CSIS). These two systems were the first to be analysed because they are the simplest among those already mentioned in the introduction of this work.

Accumulator System

A simplified diagram of the ACC system of Angra I is shown in Fig. 3. This is a subsystem of the emergency core cooling system (ECCS). It consists of a large tank containing borated water, some valves, instrumentation and associated piping. The borated water in the tank is pressurized with nitrogen gas (N_2), and the ACC discharge lines are connected to the cold legs of the reactor coolant system (RCS). When pressure in the cold legs drops below 750 psig as a result of a loss of

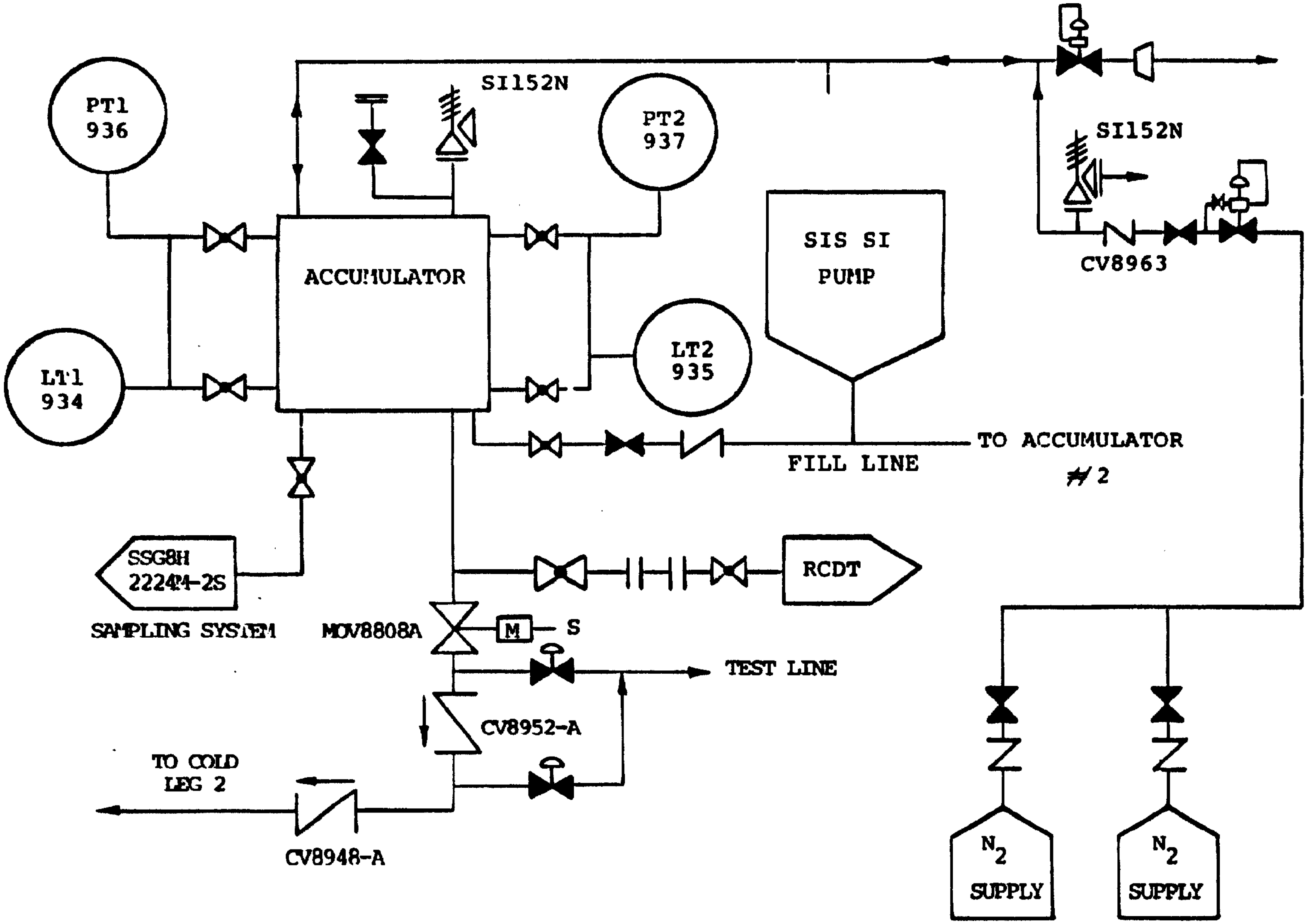


Fig. 3 - Simplified Diagram of Angra I ACC system

coolant accident (LOCA) the accumulators discharge borated water into the reactor vessel. The ACC system is considered to be a passive system because mechanical operation of the check valves (see Fig. 3) is the only requirement for its discharging. Therefore, a pressure differential between the water in the tank and that in the RCS is the only condition for the operation of the ACC system, dispensing any electric control signal or operator action.

A quantitative evaluation of the unavailability of the accumulator system was performed for the case of a postulated large cold leg LOCA. Angra I has two accumulators, one for each cold leg. Since the contents of one accumulator is lost out the break in case of a LOCA in the corresponding cold leg, only the contents of one accumulator is (necessarily) enough to keep the core cooled during the initial phase of the accident. Therefore, success for accumulator discharge to the RCS requires a successful discharge of 1 out of 1 accumulator. A detailed fault tree was constructed, taking into consideration the same kind of basic faults considered in WASH-1400[1]. Because many events have negligible unavailability values, this tree was reduced and reformulated to consider only those events with significant unavailabilities. The reduced tree (shown in Fig. 4) was evaluated with the SAMPLE code, a Monte Carlo simulation code also used in WASH-1400[1], assuming the unavailabilities of the basic events to be log-normally distributed. The data used here was taken from Ref. 1. The median and 90% confidence upper and lower values for the unavailability of the ACC system of Angra I as obtained from the Monte Carlo simulation are, respectively,

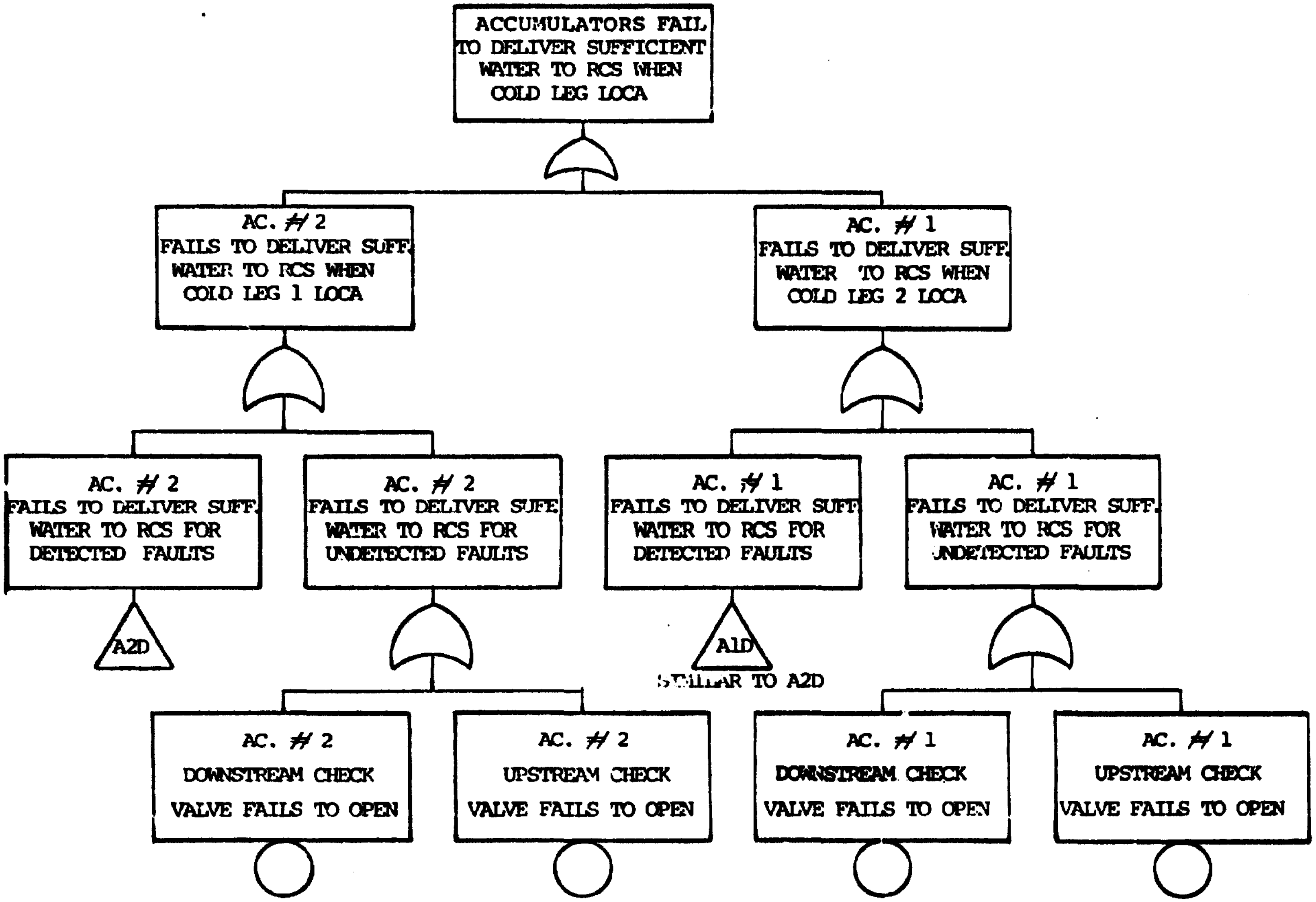

ACCUMULATORS FAIL TO DELIVER SUFFICIENT WATER TO RCS WHEN COLD LEG LOCA
AC. # 2 FAILS TO DELIVER SUFF. WATER TO RCS WHEN COLD LEG 1 LOCA
AC. # 1 FAILS TO DELIVER SUFF. WATER TO RCS WHEN COLD LEG 2 LOCA
AC. # 2 FAILS TO DELIVER SUFF. WATER TO RCS FOR DETECTED FAULTS
AC. # 2 FAILS TO DELIVER SUFF. WATER TO RCS FOR UNDETECTED FAULTS
AC. # 1 FAILS TO DELIVER SUFF. WATER TO RCS FOR DETECTED FAULTS
AC. # 1 FAILS TO DELIVER SUFF. WATER TO RCS FOR UNDETECTED FAULTS
A2D
A1D
SIMILAR TO A2D
AC. # 2 DOWNSTREAM CHECK VALVE FAILS TO OPEN
AC. # 2 UPSTREAM CHECK VALVE FAILS TO OPEN
AC. # 1 DOWNSTREAM CHECK VALVE FAILS TO OPEN
AC. # 1 UPSTREAM CHECK VALVE FAILS TO OPEN

Fig. 4 - Angra I Accumulator Reduced Faul Tree

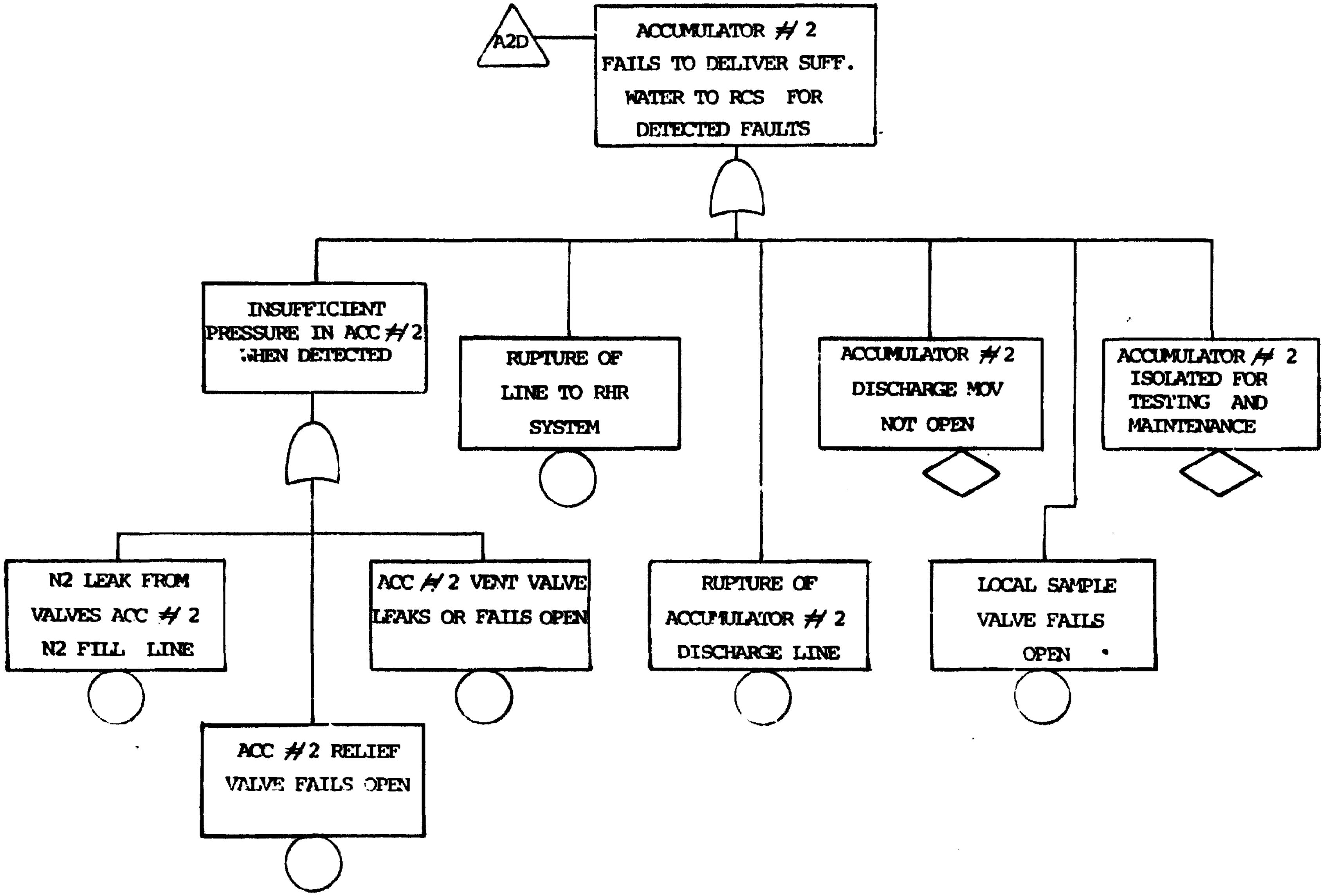

A2D
ACCUMULATOR # 2 FAILS TO DELIVER SUFF. WATER TO RCS FOR DETECTED FAULTS
INSUFFICIENT PRESSURE IN ACC # 2 WHEN DETECTED
RUPTURE OF LINE TO RHR SYSTEM
ACCUMULATOR # 2 DISCHARGE MOV NOT OPEN
ACCUMULATOR # 2 ISOLATED FOR TESTING AND MAINTENANCE
N2 LEAK FROM VALVES ACC # 2 N2 FILL LINE
ACC # 2 VENT VALVE LEAKS OR FAILS OPEN
RUPTURE OF ACCUMULATOR # 2 DISCHARGE LINE
LOCAL SAMPLE VALVE FAILS OPEN
ACC # 2 RELIEF VALVE FAILS OPEN

Fig. 4 - (Cont.) - Angra I Accumulator Reduced Faul Tree

$Q_{median} = 5.0 \times 10^{-4}$
$Q_{upper} = 7.9 \times 10^{-4}$
$Q_{lower} = 3.2 \times 10^{-4}$

These values are approximately a factor of two lower than those obtained for the ACC system of the typical PWR reported in WASH-1400[1]. This is not surprising at all, given the close similarity between the two systems and that the same methods and data base were used in both calculations.

An importance analysis of the component failures involved in the fault tree has shown that failure (to open) of the two check values in the interface between the ACC system and the reactor coolant system (see Fig. 4) is the main contributor to system unavailability. This tells us that if we were to look for possible ways to improve the availability of the ACC system, we should start by closely studying the referred valves. As an example of what could be done, let us suppose we substitute each one of those check valves ($q = 1.0 \times 10^{-4}$ each) by two similar ones in a parallel arrangement ($q_{arrang.} = 10^{-4} \times \times 10^{-4} = 1.0 \times 10^{-8}$). Then a simple calculation shows that this modification results in a factor of four decrease in the unavailability of the ACC system[13].

Containment Spray Injection System

The containment spray injection system (CSIS) of Angra I is designed to perform two functions:

1) reduction of temperature and pressure inside the containment after a loss of coolant accident or a rupture of a main steam or feedwater pipe in the containment;

2) removal of fission product from the containment atmosphere following a LOCA.

This latter function is accomplished by the inclusion of a chemical additive subsystem which injects sodium hydroxide into the spray water at an optimum value for fission product removal from the post-LOCA containment atmosphere.

In this paper we restrict ourselses to the analysis of the first function mentioned above. This means that the chemical additive subsystem is not considered here.

A simplified diagram of the CSIS is shown in Fig. 5. It consists of two separate 100 percent capacity trains, each one consisting of one pump, spray ring headers nozzles, valves and associated piping. Both trains draw water from the refueling water storage tank (RWST) during the initial phase of the accident, the injection phase, and the containment spray injection system is required to function only until the water supply in the RWST is exhausted.

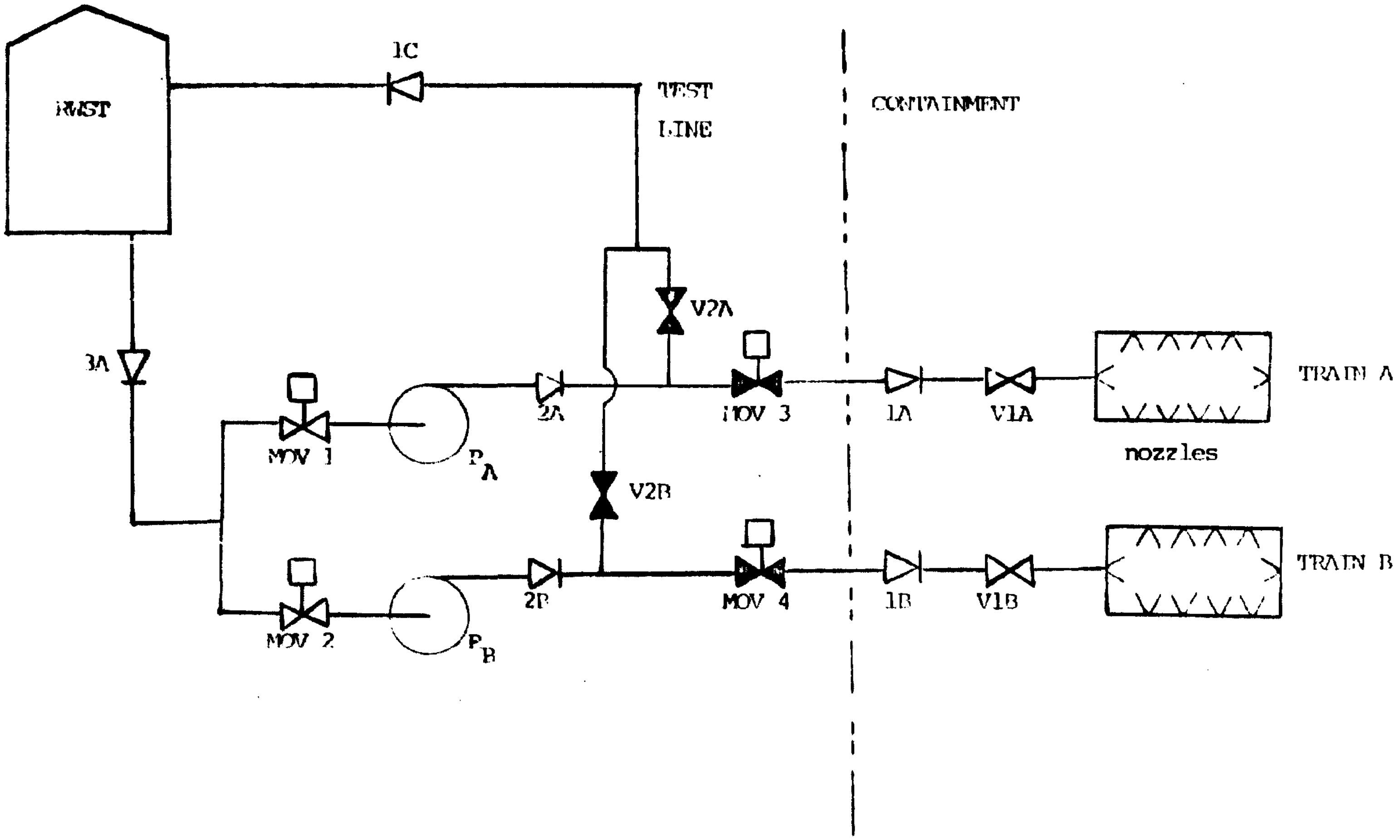


Fig. 5 - Simplified Diagram of Angra I CSI System

Similary to what was done for the ACC system, a detailed fault tree was constructed to investigate the failure of the CSIS (unavailability) to deliver sufficient fluid flow to nozzles in the containment in case of a LOCA. This tree was further reduced to account only for those events with significant unavailabilities. The reduced tree (shown in Fig. 6) was also evaluated with the SAMPLE code, again assuming the unavailabilities of the basic events to follow a log-normal distribution, and employing data from Ref. 1. The median and 90% confidence upper and lower values for the unavailability of the CSIS of Angra I are, respectively,

$$Q_{median} = 2.96 \times 10^{-3}$$
$$Q_{upper} = 9.74 \times 10^{-3}$$
$$Q_{lower} = 1.06 \times 10^{-3}$$

These values are again of the same order of magnitude as the corresponding ones presented in WASH-1400, a fact that is not surprising for the same reasons given for the ACC system. Nevertheless, a few interesting differences exist between the CSIS of Angra I and that of the typical PWR of WASH-1400. These differences are currently being explored and will be reported in the future.

The largest contribution to the CSIS unavailability values presented above comes from common-mode failures. Following WASH-1400, this contribution was calculated assuming possible coupled human errors in the calibration of several sensors of the engineered safety features actuation system and during the periodic tests of the CSIS spray subsystems.

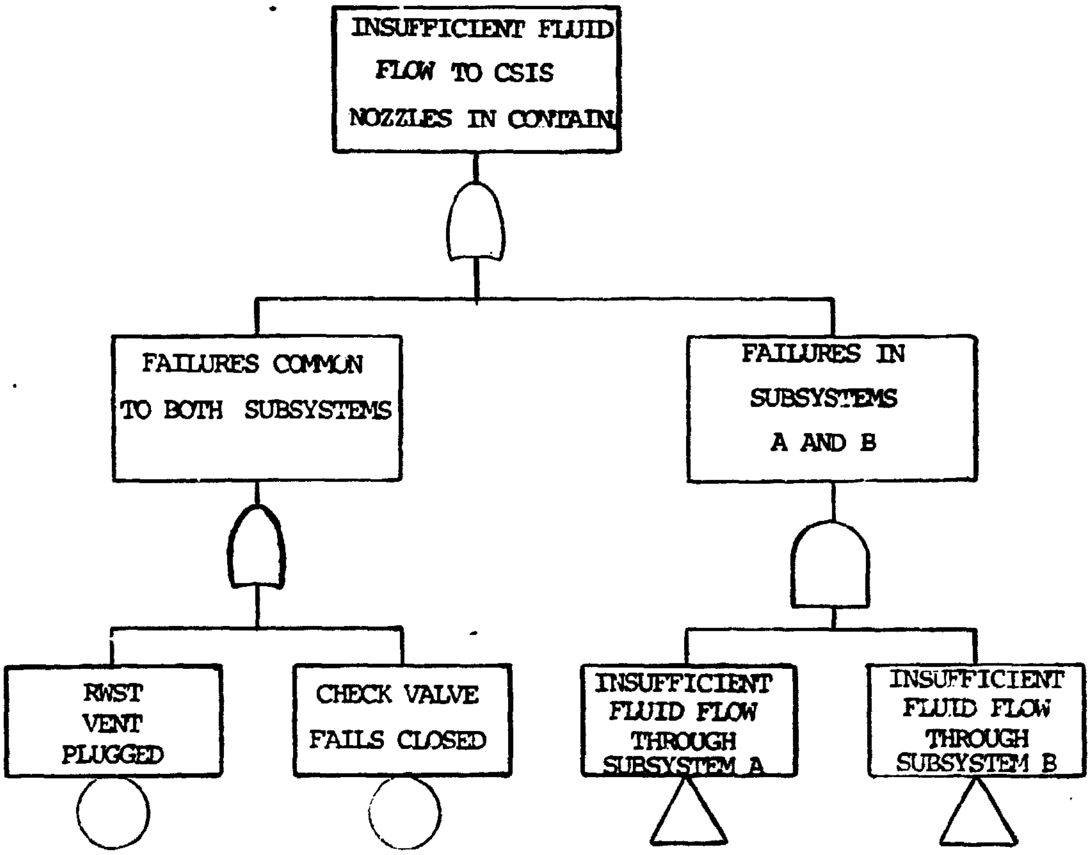

INSUFFICIENT FLUID FLOW TO CSIS NOZZLES IN CONTAIN
FAILURES COMMON TO BOTH SUBSYSTEMS
FAILURES IN SUBSYSTEMS A AND B
RWST VENT PLUGGED
CHECK VALVE FAILS CLOSED
INSUFFICIENT FLUID FLOW THROUGH SUBSYSTEM A
INSUFFICIENT FLUID FLOW THROUGH SUBSYSTEM B

Fig. 6 - Angra I Containment Spray Injection Fault Tree

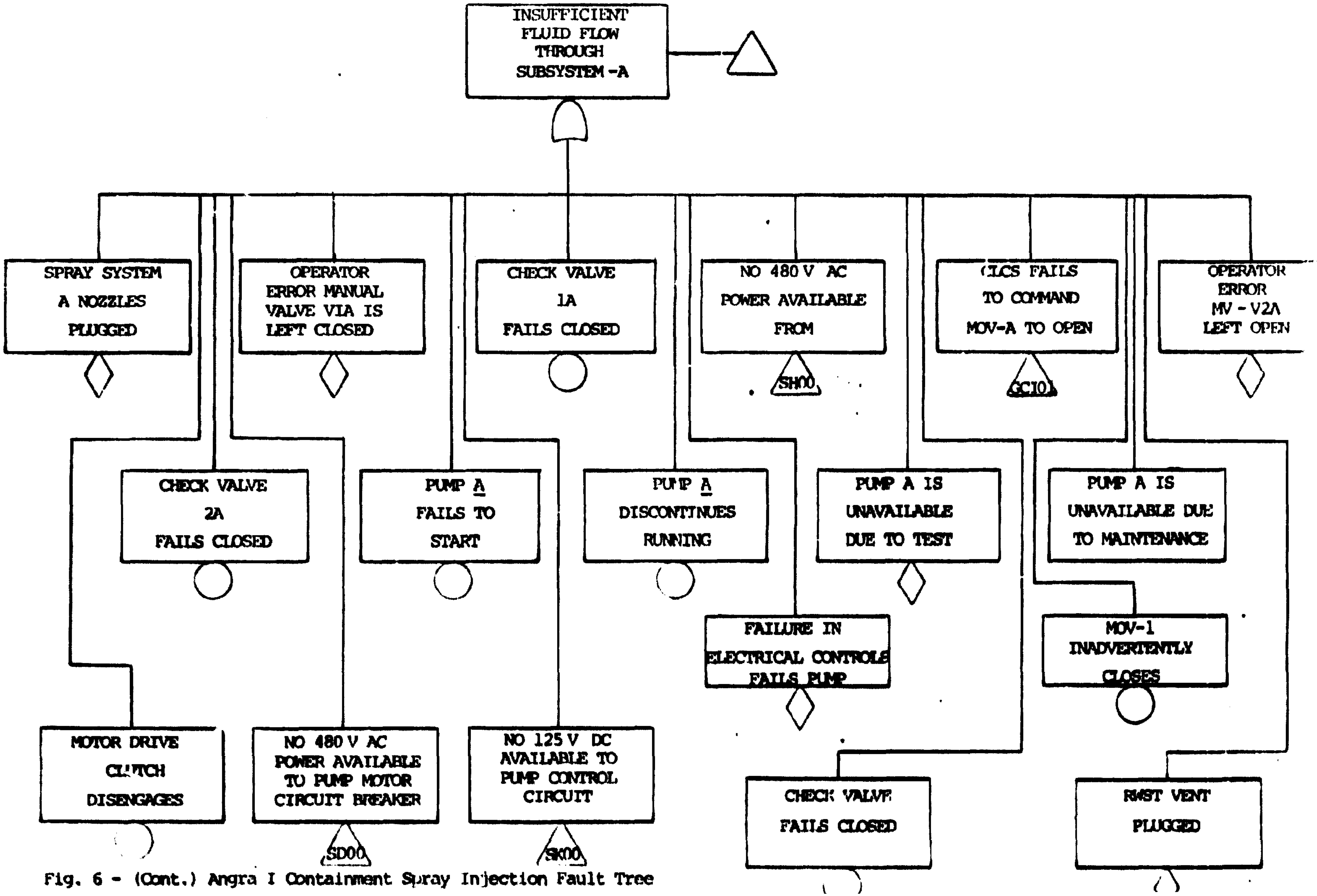

INSUFFICIENT FLUID FLOW THROUGH SUBSYSTEM -A
SPRAY SYSTEM A NOZZLES PLUGGED
OPERATOR ERROR MANUAL VALVE VIA IS LEFT CLOSED
CHECK VALVE 1A FAILS CLOSED
NO 480 V AC POWER AVAILABLE FROM
SH00
CICS FAILS TO COMMAND MOV-A TO OPEN
GC10
OPERATOR ERROR MV - V2A LEFT OPEN
CHECK VALVE 2A FAILS CLOSED
PUMP A FAILS TO START
PUMP A DISCONTINUES RUNNING
PUMP A IS UNAVAILABLE DUE TO TEST
PUMP A IS UNAVAILABLE DUE TO MAINTENANCE
FAILURE IN ELECTRICAL CONTROLS FAILS PUMP
MOV-1 INADVERTENTLY CLOSES
MOTOR DRIVE CLUTCH DISENGAGES
NO 480 V AC POWER AVAILABLE TO PUMP MOTOR CIRCUIT BREAKER
SD00
NO 125 V DC AVAILABLE TO PUMP CONTROL CIRCUIT
SK00
CHECK VALVE FAILS CLOSED
RWST VENT PLUGGED

Fig. 6 - (Cont.) Angra I Containment Spray Injection Fault Tree

IV. Conclusions

In view of the ever increasing complexity of modern technological systems and of the large number of persons who may be affected by a single accident, maintaining the safety and reliability of such systems have become a critical issue in the most advanced technological societies.

For the case of nuclear power generation, although the deterministic safety analysis approach (adopted since the beginning of the nuclear industry regulation) has proven to be capable of insuring a very good safety record, it has been recognized that probabilistic safety analysis will play a significant role in the near future. Right now it is being used in the licensing procedure of some countries only as a means of providing information of a supplementary nature.

In this paper we have briefly described the fault tree methodology used to perform both qualitative and quantitative reliability analysis of a complex system involving a large number of components. We have applied the methodology to calculate the unavailability values of the accumulator and of the containment spray injection systems of Angra I for the hypothetical case of a large LOCA. The values obtained for both systems were shown to be comparable to the corresponding ones reported in WASH-1400, a fact which was expected from the beginning given the similarity between the respective systems and that the same method and data base were used in both calculations.

Up to now we have been calculating the contributions of common-mode failures and T&M procedures to the unavailabilities of the systems in the same way as done in WASH-1400, that is, by incorporating those contributions in an ad-hoc fashion after the hardware fault tree is quantitatively evaluated. It has been shown elsewhere[14] that the use of a NOT gate (besides the more traditional OR and AND gates) allows the incorporation of common-mode and T&M contributions in the analysis in a more natural way. It is our intention to switch to this approach in the near future.

NOTES AND REFERENCES

1. "Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", WASH-1400 (NUREG 75/104) October 1975.

2. "Deutsche Risikostudie Kernkraftwerke, Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko", BMFT, 1979.

3. Proceedings of the ANS/ENS Topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety, Newport Beach, CA U.S.A., May 8-10, 1978.

4. For a review of recent applications see
   A. Birkhofer, "Recent Status of Development and Practical Application of Risk Analysis in the Nuclear Field", paper presented at this meeting.

5. "Report of the President's Commission on the Accident at Three Mile Island", October 1979.

6. Rogovin Report, Inside NRC, February 11, 1980, p. 10.

7. "CANVEY: An Investigation of potential Hazards from Operations in the Canvey Island/Thurruck Area", Health and Safety Executive, Her Majesty's Stationery Office, London, 1978.

8. The work of our group evolved from the initial studies carried out by Dr. Luiz A. Arrieta at CNEN. As far as we know, the only previous work in this field in our country was that of Dr. Hukai and collaborators at IPEN. See:

   a) Paulo Roberto Borba, "Cálculo das Probabilidades de Falha de Suprimento de Energia Elētrica aos Barramentos de Classe 1E da Usina Nuclear de Angra I", M.S. Thesis, IEA, 1978.

b) Ting Yang, "Um Modelo para Avaliação da Confiabilidade do Sistema de Suprimento de Energia Elētrica aos Barramentos de Segurança 1A3 e 1A4 de Angra I", M.S. Thesis, IEA, 1978.

9. A. E. Green and A. J. Bourne, "Reliability Technology", John Wiley & Sons, 1972, p. 25.

10. IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems, ANSI/IEEE Std 352-1975, p.7.

11. I.A. Watson and G.T. Edwards, "Common-Mode Failures in Redundancy Systems", Nuc. Tech. 46 (1979) 183.

12. Ref. 1, Appendix III.

13. For further details on the analysis of the ACC system see: Caio César Maciel, "Estudo da Confiabilidade do Sistema de Acumuladores de Angra I", M.S. Thesis, COPPE/UFRJ, 1980.

14. "Generalized Fault Tree Analysis for Reactor Safety", EPRI 217-2-2, June 1975.