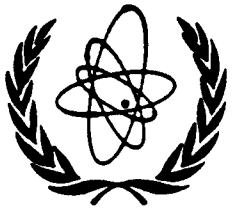
SAFETY ENGINEERING SERVICE CENTRE
SP2 F4



INTERNATIONAL ATOMIC ENERGY AGENCY

INTERNATIONAL SYMPOSIUM ON SAFETY CODES AND GUIDES (NUSS) IN THE LIGHT OF CURRENT SAFETY ISSUES

Vienna, Austria, 29 October – 2 November 1984

IAEA-SM-275/15

H. SHAPIRO

# PROBABILISTIC ASSESSMENT METHODS AS A TOOL FOR DEVELOPING NATIONS TO MAKE SAFETY DECISIONS

by

P. Gumley, Safety Assessment, AECL

S.V. Inamdar, Safety Concepts, AECL

ATOMIC ENERGY OF CANADA LIMITED
CANDU Operations
Sheridan Park Research Community
Mississauga, Ontario, Canada
L5K 1B2

This is a preprint of a paper intended for presentation at a scientific meeting. Because of the provisional nature of its content and since changes of substance or detail may have to be made before publication, the preprint is made available on the understanding that it will not be cited in the literature or in any way be reproduced in its present form. The views expressed and the statements made remain the responsibility of the named author(s); the views do not necessarily reflect those of the government of the designating Member State(s) or of the designating organization(s). *In particular, neither the IAEA nor any other organization or body sponsoring this meeting can be held responsible for any material reproduced in this preprint.*

INTERNATIONAL ATOMIC ENERGY AGENCY

IAEA-SM-275/15

# PROBABILISTIC ASSESSMENT METHODS AS A TOOL FOR DEVELOPING NATIONS TO MAKE SAFETY DECISIONS

## ABSTRACT

This paper advocates the use of probabilistic safety assessment methods in making safety decisions. It discusses the question of adequate safety - what it means to a country buying a nuclear power plant, and how probablistic safety assessment studies of the reference plant can be used for ensuring this adequate safety.

It is proposed that adequate safety means ensuring that the plant would behave, in accident conditions, in a manner similar to the way it is expected to behave were it in the country of origin. For this one needs to know how the plant responds under somewhat altered conditions. These altered conditions can arise from such factors as varying reliability of electrical grids, different manufacturing technology, local systems design and operator capability.

In the design of nuclear power plants, the traditional approach to safety has led to the belief that availability and effectiveness of safety systems alone is all that is required to ensure plant safety. This belief, can result in design oversights leading to potential problems arising out of the power production systems and the service systems. Participation by the buying country in the design of such systems, and understanding the safety implications thereof, can be facilitated by probabilistic safety assessment methods. This philosophy is illustrated in this paper by examples.

## 1. INTRODUCTION

A country, purchasing a Nuclear Power Plant (NPP), usually desires a high degree of participation in all the facets involved i.e., siting, design, manufacture of components, construction, commissioning and operation. However, an additional concern on top of these desires is to ensure that the plant is adequately safe.

The latter concern would generally be satisfied if the NPP would in fact perform as adequately in the buyer's country as it would in the country of origin. The question is how the buying nation should effectively review the safety of the plants. Should the buying nations spend resources on nuclear island aspects, e.g., blowdown analysis, or is there a more effective approach. For a demonstration of adequate safety there is a need to know how the plant responds under the altered conditions of the buying nation, in comparison with the original conditions on which the reference design is based.

To ensure adequate safety, therefore, it is of importance for the buying country to recognize all the factors that influence in some way or the other, the response of the plant in accident situations in its actual 'environment' compared to the reference plant. Some of the more important factors that make a key difference are:

- Effect of a different local manufacturing source for the equipment.
- Different Balance of Plant (BOP) configurations.
- Involvement of different contracting parties in different areas of the plant, e.g., civil, nuclear island systems and balance of plant systems.
- Stability and reliability of the electrical grid.
- Different Quality Assurance Standards.
- Operator experience and capability.
- Different site conditions.

It is as important to know what to do with the recognized factors as it is to recognize them. It is proposed that the probabilistic safety assessment tools can be effectively used to assist the buying nations in making decisions in these areas.

## 2. PROBABILISTIC SAFETY ASSESSMENT STUDIES - A PERSPECTIVE

With the early beginnings in the aircraft industry, the concept of design on a probabilistic basis was notably used in Canada and the UK [1]. Following the U.S. Rasmussen study [2] and the post TMI experience, the most important fact that has crystallized out of the various probabilistic safety studies [3] is that the quantitative estimates of public risks are not nearly as important as the engineering and safety insights gained from the structured logic and the thought processes involved in arriving at the results. This requires the accident sequences to be based on realistic assumptions and conditions to be of real value. It is usual to design for a high degree of independence between the safety systems and the power production systems. As a consequence, probabilistic safety assessment studies have tended to concentrate on the nuclear island (NI) systems with the underlying presumption that if one takes care of the nuclear island systems, particularly the safety systems within the NI, everything else is automatically taken care of. Probabilistic safety assessments can, and should be extended to include assessments of all power production systems, including the BOP systems, in making safety decisions.

Power production systems are an important factor in good safety design of the plant and an appreciation of this can be obtained from studies of accident event sequences. This appreciation can form the basis for taking safety decisions to improve overall plant safety by changes to power production system design, as an alternative to changes to the safety systems used to mitigate the accident consequences. In many cases the production system design changes can also be shown to have a significant economic benefit in terms of improved station availability.

Included in the power production systems are the BOP Systems and the service systems (electrics, air and water) which can be a source of an accident in themselves or serve to introduce subtle cross-links between various nuclear island systems.

The team of engineers responsible for the design of the power production systems usually only address themselves to good sound design practice from an economic point of view with little or no regard for any adverse effects that the power production systems, particularly the service systems, may have in accident situations. These are the kinds of

systems that the buying country is most likely to get involved with. A high failure frequency of a service system can place a demanding role on the operator in his accident manangement particularly where many systems are simultaneously affected. The longer the period before post accident recovery, the lower the reliability of the service system. The shorter the period, the more critical is the role of the operator to maintain or bring on other systems to ensure adequate fuel cooling.

Each of the probabilistic safety assessment studies done for the CANDU design basically involves combinations of fault tree and event sequence analyses [4]. A fault tree analysis is conducted to derive the frequency of the initiating event or "serious failure" (serious process failure in CANDU terminology). An event sequence analysis then follows from the serious failure to evaluate the response of the affected plant systems including those that are required to satisfy the basic safety functions. The plant systems response analysis is satisfactorily terminated when either the stable plant conditions are achieved or when the event sequence frequency is sufficiently low.

Event sequence analyses help to assess resultant plant conditions and the expected role of the operator. The sequences are developed as a function of time and as such they help determine or confirm system automation requirements in the short term and the adequacy of the mitigating systems and operator actions in the medium and the long term after the accident.

To ensure safety, the essential role of the operator in mitigating accidents has to be detailed in the station abnormal incidence manuals and operating procedures.

Developing failure scenarios probabilistically gives an insight into potential system failure combinations to which the operator is required to respond. All accident sequences bounded by the initiating event failure frequency and the accident sequence cutoff frequency ($10^{-6} \sim 10^{-7}$) require operator intervention to ultimately stabilize the plant and maintain long term cooling of the reactor.

Operator actions in accident sequences can be classified into two distinct categories, restorative actions and mitigating actions. Restorative actions are almost always associated with the operators' ability to correct a power production system failure in its early stages. Power production systems are required during normal operation and

the operator can therefore be expected to know the operational status of such systems at all times and be thoroughly familiar with the system controls, alarms and indications. Alarms and indications from these systems will normally be acted upon immediately and every attempt can be expected to be made by the operator to maintain continued production. This preoccupation with attempting to restore or maintain a failing production system and the economic consequences usually associated with initiating safety systems are among the reasons for allowing sufficient time for the operator to respond to accident situations.

Where immediate safety system action is demanded, it is usual to automate its initiation. In CANDU 600 reactors it is the design intent to require no operator action for at least 15 minutes into any identified accident sequence.

The influence of restorative actions by the operator on his essential safety role in mitigating accident sequences is plant specific, to the extent that the design of the power production systems is plant specific. In addition, the design targets used in the reference plant design for safety system automation may not be acceptable to the buying nation on economic grounds and this will itself be a key factor in making safety decisions.

Probabilistic safety studies done for the reference plant, covering both the nuclear island and the BOP systems are usually available. It is these reference studies that can form the basis for a comparative assessment by the buying country.

## 3. COMPARATIVE PROBABILISTIC SAFETY ASSESSMENT STUDIES

It has been our experience with the CANDU 600 reactors currently in operation that small changes, to reflect local site differences, can have a significant effect on the safety of the whole plant.

The factors of local influence affect both the fault tree and event sequence aspects of a given probabilistic safety assessment study. Different failure frequency and unreliability estimates when inserted into event sequences to reflect altered conditions, may change the end results to the extent that certain sequences no longer reach the sequence cutoff frequency of $10^{-6}$ to $10^{-7}$ events per year. Judgements

based on how far a given sequence is from the established target (such as $10^{-7}$) may lead to safety decisions of providing an additional system or changing an operating policy and so on.

The cost of undertaking probabilistic safety assessment studies can be high. It is however not necessary for a buyer to repeat all the probabilistic safety assessment studies usually provided with the reference plant design. What is very important for the purchaser however is for him to understand the safety effects arising from the differences from this reference plant design.

The reference design studies can form the basis of 'comparative' probabilistic safety assessment studies where only the essential key safety issues that have changed due to local changes are highlighted for review by the buyer.

These 'comparative' probabilistic safety assessments have many distinct advantages for the buyer. Some of these advantages are as follows:

i) They provide a basis for determining the adequacy of local system design by giving system reliability/availability targets (based on the reference design).

ii) They provide a means of assessing the safety effects of plant changes.

iii) They can identify where changes are necessary to the safety role of the operator due to 'local' system design features and are a major input therefore to the stations Abnormal Incidents procedures.

iv) They are relatively inexpensive.

v) They provide a basis for making safety/economic decisions particularly where the reliability of a production system may be improved as an alternative to providing or upgrading a specialised safety system capability.

vi) They give an important insight into potential cross-linked or common cause failure modes that can affect the mitigation of the accident sequences.

vii) They can provide the basis for defining a "minimum equipment list" for continuing 'normal' operation of the plant. The unavailability of standby equipment even for power production purposes has a significant effect on initiating event failure frequencies and mitigation.

In any accident sequence, the unreliability associated with the operator is the most difficult and controversial parameter to evaluate in probabilistic analyses. Considerable progress has been made in recent years to identify and quantify probabilistically the different types of operator errors possible.

Although absolute assessment of operator unreliability is difficult, again comparative assessments of different operating environments and procedures can be made. Different operating procedures to the same initiating event can be brought about by optimizing the procedures alone to minimize the release consequences, or by system design changes, or a combination of both of these.

Differences in operating procedures and the handling of abnormal incidents can be expected to be influenced by such diverse environmental parameters as the nature of local site operating conditions and procedures and the hierarchy of station command. These factors can all have an influence on the decision and action times of the operator to abnormal incidents.

Accident sequences which show a high dependance on operator corrective actions to stablize the accident transient are singled out by this process. Typically a high dependance is taken to mean those sequences which are mitigated by operator corrective actions where a total operator unreliability of $10^{-4}$ or less is claimed. A re-examination of these accident sequences would involve a more detailed review and assessment of operator unreliability incorporating other relevant human factors analysis techniques.

Changes to support the failing production system may be all that is required in these instances to reduce the extent of operator dependance. Alternatively, automation of some of those necessary operator actions to bring in safety system action, which may result in economic penalties, may be the preferred solution. The example of the feedwater interruption scenarios given in Section 4 illustrates how

probabilistic safety assessment studies have been used in making these safety decisions involving the operators.

Probabilistic safety assessment studies have to reflect the 'as built' plant if they are to be used in defining such items as the safety role of the operator for use in the station Abnormal Incidents Manual. The reference plant probabilistic studies for CANDU were undertaken at a stage in the plant construction where all the design details of the process and safety systems were known, but at a stage when small plant changes could be made where such changes were found to be necessary.

With the reference plant information available, comparative probabilistic assessment studies can be used by a buying country to identify any safety concerns early in the construction schedule. This is particularly important for the power production systems where changes from the reference design are to be expected. Follow up studies at the detail design stages would then need only be of a confirmatory nature and the risk of major late plant changes arising from these studies would be kept to a minimum.

This process of comparison and the resultant safety decisions are illustrated in the following selected examples.

## 4. SELECTED EXAMPLES OF COMPARATIVE SAFETY ASSESSMENTS

Three selected examples, taken from probabilistic safety studies of the CANDU 600 design, are presented here to show how these studies have been used to make safety decisions. These are typical examples of the lessons/experiences of our work to date. In these examples, the lessons learned were incorporated in the final design. A fourth example is of an actual account of a feedwater failure on a CANDU 600 reactor at power. All of these examples explore safety system/power production system interactions and the safety role of the operator on a comparative assessment basis.

### Example #1

The first example is taken from a safety assessment of the consequences of a total feedwater interruption. The most frequent interruption can occur as a consequence of an extended loss of normal station AC power supplies and essential backup AC power supplies, or following a loss of

normal AC supplies during a period when the auxiliary feedwater pump is unavailable. The normal AC power is supplied to the station via both a unit service transformer from the main generator and via a system service transformer fed from grid supplies. In the event of a total loss of these supplies, essential AC supplies are restored via standby diesel generators within two minutes. Normal feedwater is supplied via three 50% feedwater pumps powered from the normal supplies. A single, auxiliary feedwater pump is provided to maintain feedwater supplies for decay heat removal in the event of normal AC power loss.

A loss of AC power and a failure to restore the backup essential AC supplies has an event frequency of $9.2 \times 10^{-5}$ events per year. An unavailability of the single auxiliary feed pump from other causes coupled with a loss of normal AC power would have similar plant consequences at a frequency of $6.3 \times 10^{-5}$ per year.

The available inventory in the steam generators is sufficient for 60 minutes of decay heat removal without a primary and secondary depressurization before a loss of heat sink develops. Under these circumstances, depressurization of the secondary side is essential to bring in a low pressure cooling spray onto the steam generator tubes to maintain the primary heat sink. This cooling spray is provided with its own power and water supplies independent from the normal process systems.

Studies have been undertaken to demonstrate that the resulting stresses on the tube and tube sheets from the spray effects would not cause a steam generator tube(s) failure, but considerable tube distortion can be expected, the extent of damage being dependant on the temperature difference between the SG tubes and cooling spray at the time the cooling spray is introduced. A failure to depressurize and introduce low pressure cooling supplies to the steam generators would eventually cause a loss of primary circuit inventory and overheating of the fuel and pressure tubes, resulting in possible pressure tube failures. The earlier the depressurization can be started the less severe the safety consequences. This places a heavy reliance on timely operator action and his ability to maintain a controlled cooldown.

The time at which the operator commences his controlled cooldown is critical. In both of these scenarios there is a high probability that normal AC power will be restored to the switchyard within 30 minutes. With sufficient cooling water

inventory within the steam generators to sustain a heat sink for 60 minutes without a cooldown of the primary circuit, there is a strong economic incentive to maintain the primary circuit conditions and concentrate on attempting to restore the normal feedwater supplies. Delaying the cooldown however increases the likelihood of steam generator tube damage should normal AC supplies not be restored in time. The simplified event sequence is shown in Figure 1. To remove the critical dependance on timely operator action, the CANDU reference plant design features an automatic depressurization of the steam generator secondary side initiated by low steam generator level which would meet all the independance requirements expected of a safety support system. However, this system also introduces other operational complications associated with its spurious initiation. Based on probability arguments alone, a more attractive solution would have been to reduce the failure frequency of the initiating event itself by changes to the feedwater system, a balance of plant process system.

The impact of a spurious auto-depressurization coupled with the potential dilemma of optimizing safety and economic considerations without an auto-depressurization feature, was considered by one of the utilities to be sufficient grounds to consider alternative ways of maintaining essential cooling.

The safety decision using probabilistic arguments was taken by this utility, to install a second auxiliary boiler feedpump, steam turbine driven, to maintain essential feedwater supplies. An unreliability target for this second auxiliary boiler feed pump is $1.5 \times 10^{-2}$ based on reasonable test intervals for this equipment. A comparative probabilistic assessment of these alternatives is summarized in Table 1.

TABLE 1

COMPARISON OF ALTERNATIVE MITIGATING ACTIONS
FOLLOWING A FEEDWATER INTERRUPTION
DUE TO A COMPLETE LOSS OF NORMAL
AND BACKUP AC POWER SUPPLIES

| Initiating Event or Mitigating Action | Initiating Event Frequency or Mitigating System Unavailability | | |
|---|---|---|---|
| | Sequence 1 | Sequence 2 | Sequence 3 |
| Loss of Normal AC power (Class IV) | 0.3/year | 0.3/year | 0.3/year |
| Unavailability of Backup AC power supplies (Class III) | $3.1 \times 10^{-4}$ | $3.1 \times 10^{-4}$ | $3.1 \times 10^{-4}$ |
| Auto-depressurization of steam generators | - | - | $1 \times 10^{-2}$ |
| Unavailability of second aux feedpump | - | $1.5 \times 10^{-2}$ | - |
| Operator depressurizes secondary side of SGs after 30 minutes | $1 \times 10^{-2}$ | $1 \times 10^{-2}$ | $1 \times 10^{-2}$ |
| No S.G. Heat Sink event frequency | $9.3 \times 10^{-7}$ | $1.4 \times 10^{-8}$ | $9.3 \times 10^{-9}$ |

Note: Low Frequency Event Sequence Cutoff = $10^{-7}$ events per year

Provision of this equipment removes any doubt by the operator in delaying a cooldown pending a restoration of normal AC power supplies . A 'no heat sink' scenario is reduced to a frequency less than 1 x $10^{-7}$ events per year by this change. However, the onus of establishing independence of the second auxiliary feedwater pump from all potential initiating events clearly rests with the owner and has to be demonstrated in the supporting assessments.

Example #2

The second example of how probabilistic studies have been used to make safety decisions is concerned with failures of the instrument air system.

Instrument air is traditionally accepted as a service system required for the normal operation of the station but not having any significant safety impact should a loss of instrument air supply occur. In the event of instrument air supply losses, the nuclear island system designers ensure that the essential control and safety functions are maintained by the use of instrument air system reservoirs and local equipment air receivers.

A typical instrument air supply system general arrangement for a CANDU 600 design is shown in Figures 2 and 3. The air supply system also provides general compressed air service supplies and mask (breathing) air. In normal operation two compressors are sufficient to meet the air supply demand. One compressor is in continuous operation in the 'ON' position, the second compressor is operating intermittantly in the 'auto' mode and the third is in a standby mode. The compressor operating modes are changed once a month to ensure that each compressor accumulates similar running hours and operating histories.

The three compressors supply a common header and four air reservoirs are provided on this header with three dedicated to the instrument air supplies. The reservoirs are sized to maintain compressed air supplies at a pressure in excess of 552 kPa(g) (80 psig) for at least five minutes in the event of a loss of compressors.

In addition to the air reservoirs at the compressor station, local tanks are provided on the instrument air system to maintain essential supplies.

These local tanks maintain supplies to such essential systems as:

i) The containment dousing system
ii) The emergency core cooling system
iii) The containment isolation system
iv) The second shutdown system
v) The feedwater system
vi) The PHT pressure relief system

In general, a loss of all instrument air supplies to local equipment results in a 'fail safe' condition where the essential safety function is maintained if required. There are important exceptions to this generalization, however, that merit closer examination of the system failure causes and consequences.

The probabilistic assessment of the instrument air supplies for a particular CANDU 600 reactor gave a predicted failure frequency of $7.1 \times 10^{-2}$ events per year for an instrument air supply loss to the reactor building. The importance of maintaining local support supplies at this failure frequency was quickly realized. For local tank supplies to be effective following an instrument air loss requires proper functioning upstream check valve or system isolation valves to close and prevent back leakage into the failed service supply pipework. Check valve unavailability on demand under normal (i.e. designed for) conditions can be expected to be $\sim 3 \times 10^{-3}$.

Debris was identified in the fault tree analysis of the system as the most likely common mode failure cause for the check valves to fail to close on instrument air supply losses. The air system design includes filters and drying equipment to maintain acceptable air quality control. This equipment together with the extensive cleaning of all pipework during system commissioning was considered adequate to ensure that the probability of debris in the air system pipework downstream of the filters during normal operation was less than $10^{-2}$, giving a frequency for a total loss of all air supplies of $8.5 \times 10^{-4}$ events per year.

Significant debris problems were however experienced during the commissiong of one plant and these were quickly associated with an unfortunate choice for process piping material (carbon steel) in the service and turbine buildings. The relevance of this choice of material was not readily forseen but did significantly affect the safety statement for the plant. Corrosion products could not easily be removed

from this pipework during systematic cleaning operations but could be shaken free as a result of the pipes being vibrated subsequently. Only after repeated cleaning and testing operations could the pipework achieve an acceptable standard of cleanliness while still leaving some doubts about future corrosion product buildup. With this doubt still existing a safety decision was taken to install local filters on the essential local tank supplies. The provision of local filters, while removing the concern of common cause check valve failures, did introduce the possiblity of system blockage at the filters from the same debris causes. This condition could, however, be readily monitored during normal operation and any economic consequences resulting from increased maintenance requirements were considered acceptable.

Example #3

A third example of how probabilistic analysis can be useful in making safety decisions is taken from a review of service water system failures and is interesting in that it shows the importance of maintaining close control of production system/safety system interface requirements particularly where different design teams have been used in the detailed design.

On salt water sites, it is standard design practice for process cooling to use recirculating service water systems. Recirculating service water (RCW) systems have the big advantage of maintaining controlled water quality throughout the plant. These systems, however, usually have limited water volumes and although supplied with a head tank, it is not uncommon to find that these systems can be quickly drained (within minutes) by comparatively small system leakages. In CANDU 600 reactors, the recirculated service water system is the main process cooling in the reactor and service buildings. This system is also used in a safety support role for the long term cooling of the emergency core cooling (ECC) system. An alternative pumped fresh water cooling supply is provided from a fresh water reservoir located on the site to supply the ECC heat exchanger on RCW cooling system loss.

On the loss of RCW cooling, this fresh water supply can be brought manually to the ECC heat exchanger, by a series of valving operations to maintain essential cooling. The general arrangement of these cooling supplies is shown in Figure 4.

A review of the operator actions required to initiate this alternate cooling supply revealed a critical dependance on the correct sequencing of these operator actions particularly during testing. An incorrect sequencing of the valving operations could result in the whole recirculated service water being drained within minutes to the fresh water reservoir resulting eventually in a complete loss of heat sink to the primary circuit.

A probabilistic analysis of the initiating events and the accident sequences showed this event to have an expected frequency of $10^{-1}$ events per year and would become, if uncorrected, the major contributor to the recirculated service water loss.

To ensure correct valving sequences a simple interlock arrangement was all that was required. This has been provided to prevent the simultaneous opening of the RCW supply to the ECC heat exchanger and the emergency water drain from the ECC heat exchanger to the fresh water reservoir. The frequency of RCW loss from this cause is reduced to an acceptable $1.5 \times 10^{-3}$ events per year.

These three examples have been chosen as representing the critical interdependances that can exist between safety systems and production systems in spite of the best of design intentions of making them independant. Probabilistic safety assessment studies made a significant contribution in both identifying and resolving the safety concerns before the station went critical. It would, however, be misleading to say that they would have only been 'discovered' by probabilistic assessments. Many design checks and reviews are also undertaken during the various construction phases of a CANDU NPP.

Interdependances usually occur at the design interfaces of production systems and safety systems where it is normal practice to subcontract the design of the nuclear island systems and the balance of plant systems to different consulting organizations in the construction of a power plant. The CANDU 600 reactors are no exception in this respect. Such an arrangement, however, can give rise to interdependances between production systems, safety systems, and the service systems unless special precautions and review procedures of the type described are undertaken in a methodical manner. Comparative probabilistic safety assessment studies to study plant differences from the reference design can be helpful and are usually all that is needed to make any necessary safety decisions.

Example #4

The last example is an actual account of a process system failure of a CANDU reactor. A detailed probabilistic safety assessment had not been undertaken as a part of the contractual requirements of that plant. It is very likely that a methodical probabilistic analysis of these failure modes would have shown the availability of certain equipment to be a prerequisite to safe system operation.

The failure that occurred was again a complete loss of feedwater supplies. A short description of the general arrangement of the feedwater pumps is required to understand the nature of the failure. The essential features of the design are shown in Figure 5. Three main feedwater pumps BFP 102 A, B and C and one auxiliary feedwater pump are provided. Each pump has a motorized discharge valve operable from the control room, a suction valve and a check valve with a counterweight arm to assist it in closing. All the pumps have a common discharge header in the feedwater train.

Prior to the incident, there had been a history of BFP suction filters plugging and the check valves sticking and having to be assisted in closing by banging on the counterweight arm. At the time of the accident. The main feedwater pump P102C was isolated for repair and the motorized discharge valve for P102B was not operable either manually or remotely.

High $\Delta p$ readings indicated that the BFP B suction filter was plugging and the BFP 102 B pump was stopped. Almost immediately BFP 102 A gave high flow, high current alarms with reverse rotation alarms being given on BFP 102 B indicating that the check valve to P102B had not closed. Within 30 seconds after the alarm for irrational flow pump P102A tripped on high flow and the auxiliary BFP started up but was again unable to deliver feedwater due to the reverse flow through pump P102B. This reverse flow could not be stopped remotely due to the unavailability of the discharge valve turning gear. To complicate matters further the high suction pressure developed at the pumps by the reverse flow through P102B caused a gasket to blow at the suction relief valve creating a hot water leak at the BFP station. Because of the leak, the operator was unable to immediately respond to close the suction valve to P102B locally.

It took another three hours before the operator was able to close the suction valves on BFP 102 A and BFP 102 B and

restore feedwater to the boilers via the auxiliary boiler feedwater pump.

The subsequent sequence of events is equally interesting. The falling boiler levels caused a reactor stepback on low boiler level and a turbine trip resulting in a partial loss of AC power supplies. These supplies were restored manually by the operator. In an attempt to maintain heat sinks, the operator increased the purification flow to the maximum possible to make use of the purification cooler for decay heat removal. The purification system is connected to the PHT system assymetrically and this caused an imbalance between the boiler water levels. Although cooldown was started by the operator, it was suspended in an attempt to conserve boiler water.

It was at this point, approximately one and a half hours from the feedwater loss that the operator attempted to introduce the shutdown cooling system without completing a prior cooldown of the PHT system (a permissible operation in emergency conditions). Water hammer effects were observed at the shutdown cooling heat exchangers on the service water side and movements of the service water pipework by up to 2-3 cms were noticed. Other balance of plant pipework was observed to move as much as 20 cms due to these effects. Cooling was maintained without invoking the safety system spray cooling on to the hot boiler tubes until the feedwater supplies were eventually restored.

Because of the abnormal way in which the feedwater train was being operated, the whole feedwater supply was dependant solely on the correct functioning of a single check valve which had already had a history of sticking open. It is interesting to note that this whole failure sequence could have been avoided had the turning gear of the discharge valve of BFP 102 C, the pump removed for service, been transferred to the operating boiler feedpump BFP 102 B at that time such that it could have been closed from the control room.

The operator actions during this incident clearly indicate the pressure the operator is under to minimize economic consequences. At all times during this sequence of events the operator could have initiated a boiler depressurization to permit low pressure spray cooling of the boiler tubes. It should be noted that auto-depressurization was not a feature of the station design in this instance.

## 5. CONCLUSIONS

Probabilistic safety assessment studies have been found to be an invaluable tool for making safety decisions for CANDU 600 reactors. These studies however have to reflect the detailed design of each station and have to be plant specific to be of value.

Since it is usually only the power production systems that change significantly from station to station for a reference design, the high cost of preparing these studies can be considerably reduced by undertaking comparative assessment studies only based on the comprehensive studies usually available for the reference plant.

Comparative probabilistic safety assessment studies undertaken can be used to establish design and performance targets, at the design stage, for those systems that differ from the reference plant design.

Similiar comparative probabilistic studies can be used at the design verification and licensing stages of the construction schedule. These studies may also be used to identify those site specific features that affect significantly the safety role of the operator and which are required to be included in the station Abnormal Incidents Manuals.

Comparative probabilistic safety assessment studies offer the potential for a greater return, in terms of real plant safety, than investing in other areas of safety assessments that have already been extensively investigated in the selling nation (such as blowdown analyses, etc).

## REFERENCES


[1] Cave, L., "Some Reflections on the Rasmussen Report and Its Implications for Reactor Design", Nuclear Engineering International, 19 223 (1974) 1012

[2] Reactor Safety Study, An Assessment of Accident Risks in the U.S. Commercial Nuclear Power Plants, Wash 1400 (Nureg 74/014), USNRC, Oct. 1975

[3] Levine, S., Stetson, F., "Applying the Lessons of PRA - An American Perspective", Nuclear Engineering International, 29 350 (1984) 38

[4] Gumley, P., "Use of Fault Tree/Event Sequence Analysis in a Safety Review of CANDU Plants", Current Nuclear Power Plant Safety Issues (Proc, IAEA Conf. Vienna 1981) Vol. II, IAEA-CN-39/7

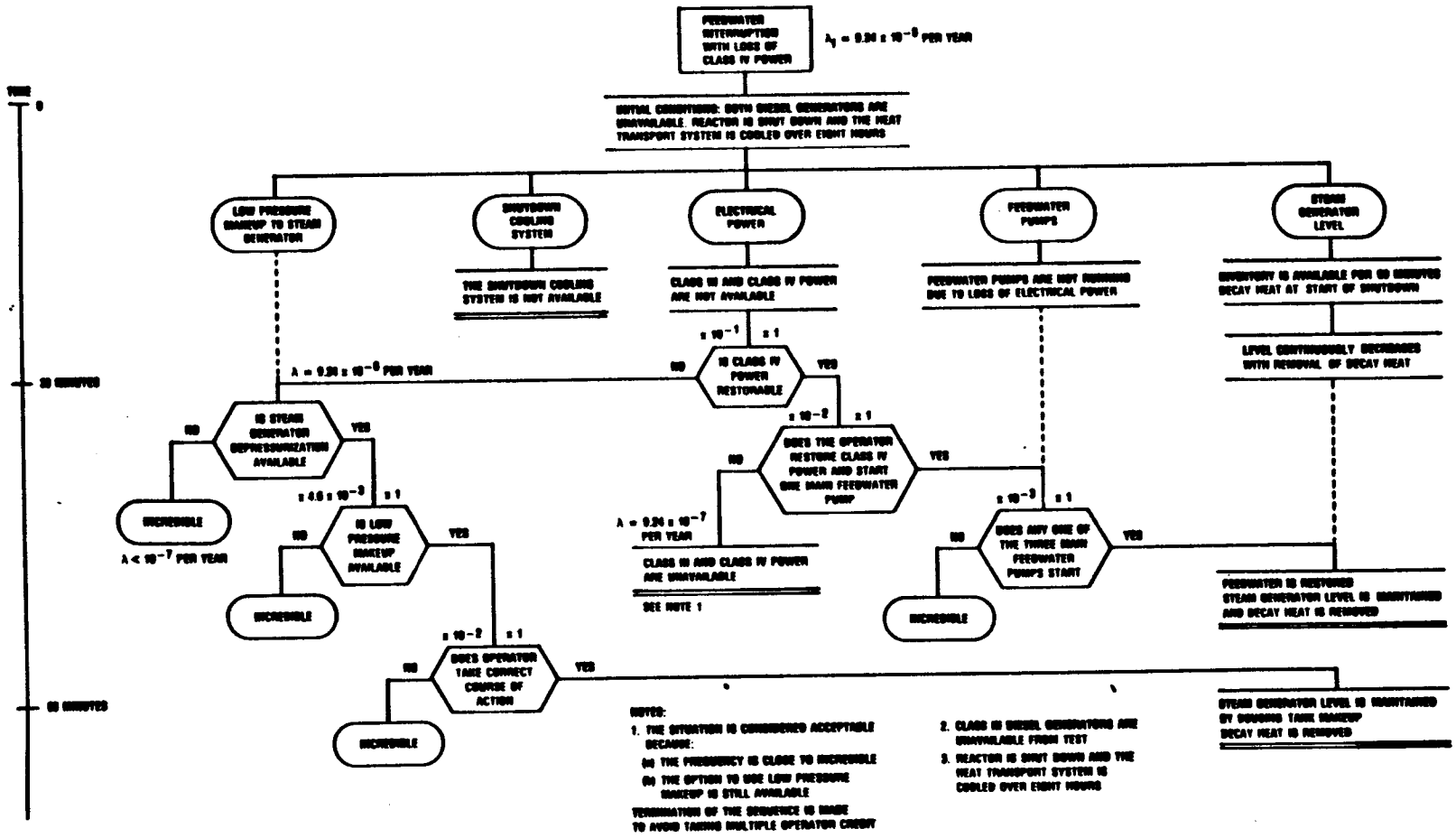



FIGURE 1 EVENT SEQUENCE DIAGRAM — STEAM GENERATOR FEEDWATER INTERRUPTION WITH LOSS OF CLASS IV POWER

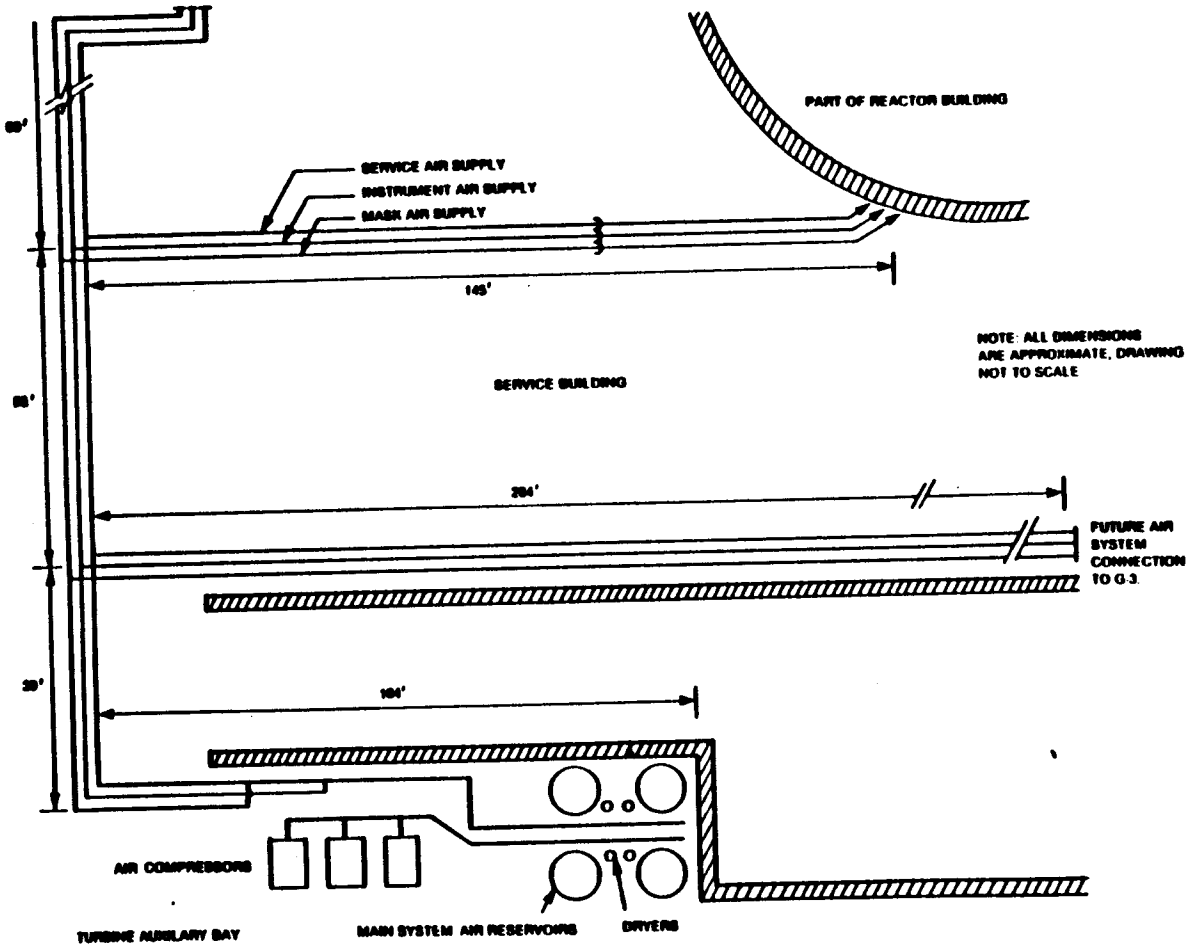



FIGURE 2 SERVICE AIR SYSTEM PIPEWORK ARRANGEMENT PLAN OF MAIN HEADER SUPPLIES

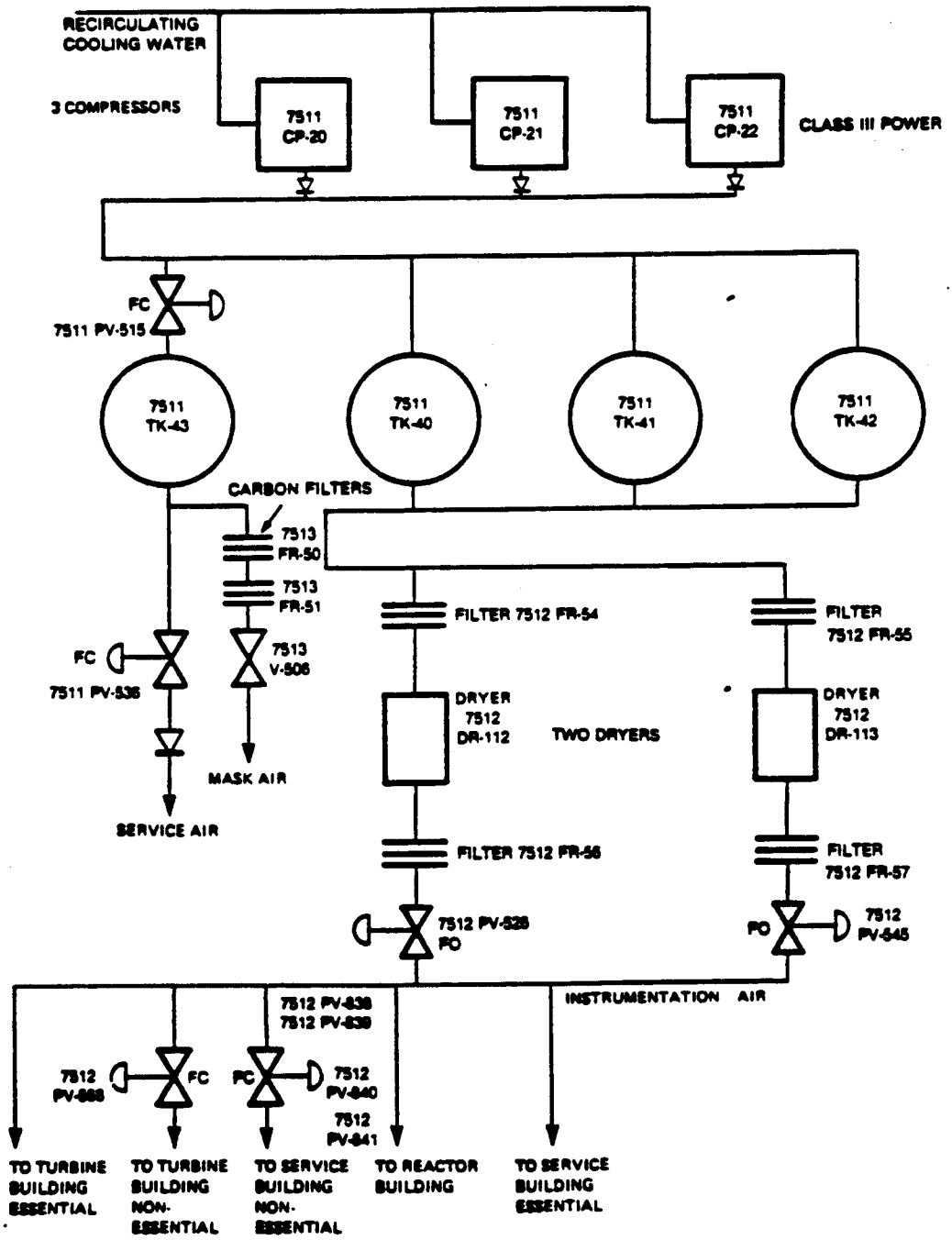



FIGURE 3 SIMPLIFIED COMPRESSED AIR SYSTEM FLOW DIAGRAM

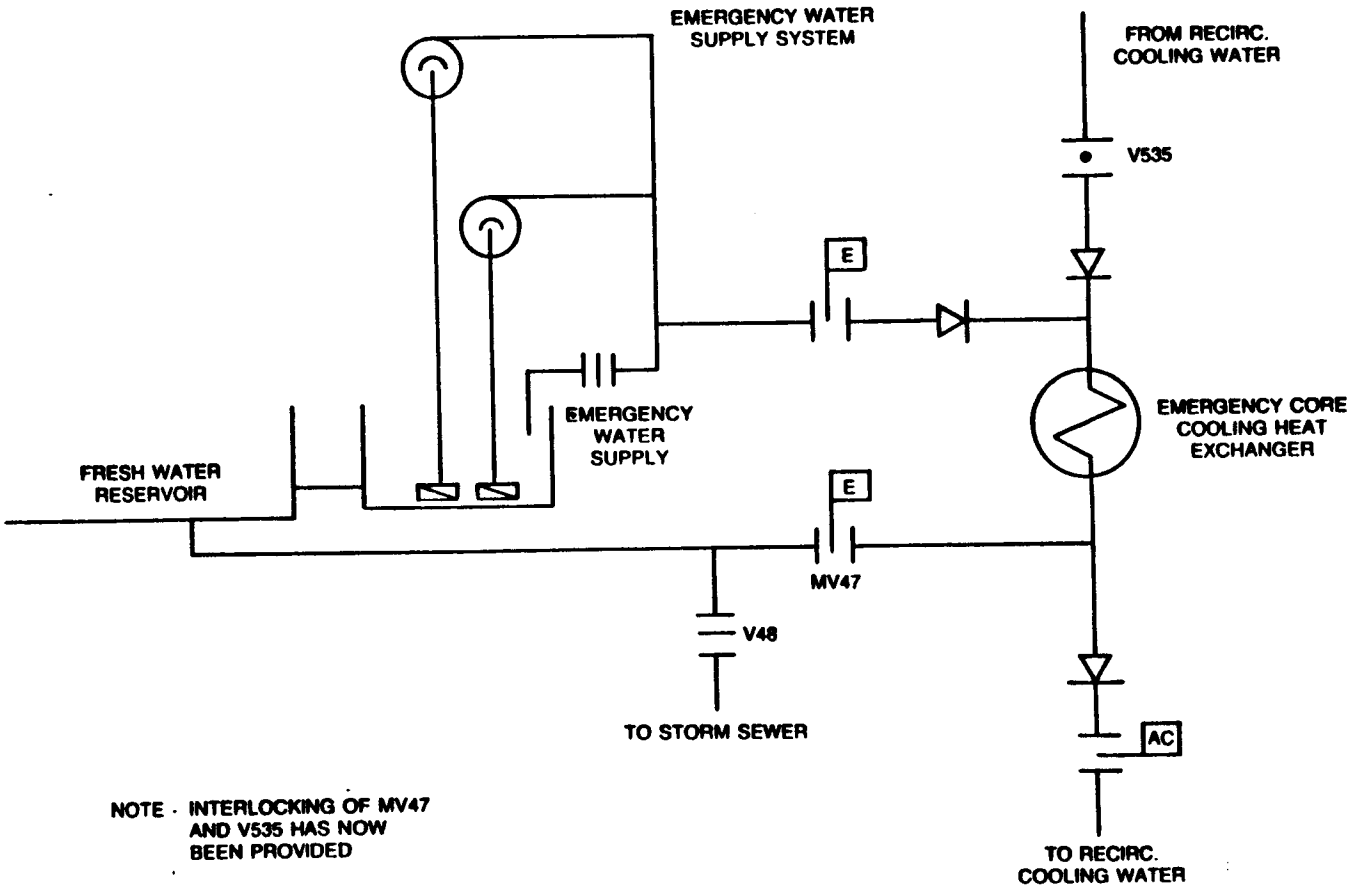



**FIGURE 4 GENERAL ARRANGEMENT OF ALTERNATIVE COOLING WATER SUPPLIES TO THE ECC HEAT EXCHANGER**

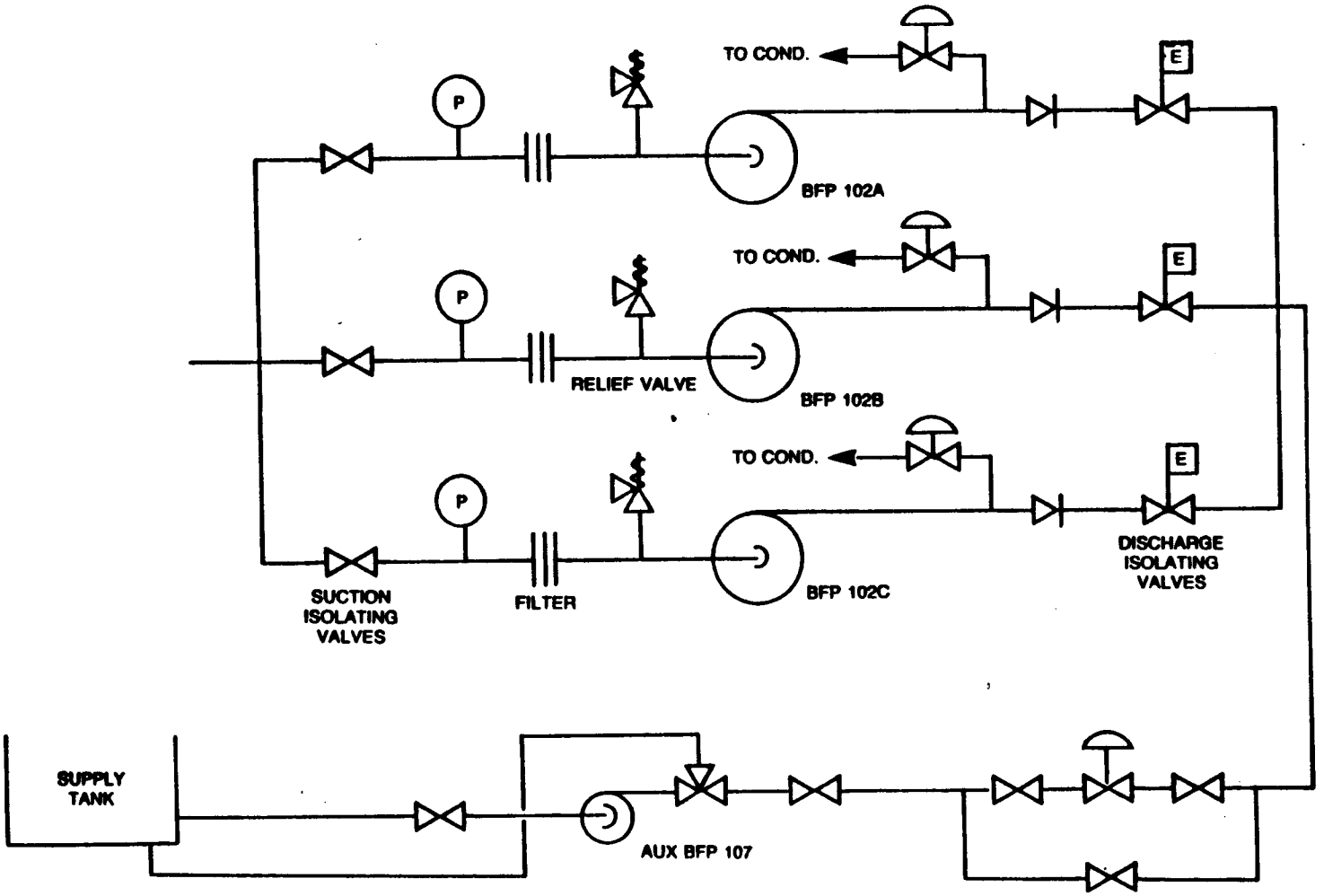



**FIGURE 5 GENERAL ARRANGEMENT OF BOILER FEEDWATER SUPPLIES**

*Proceedings of the American Power Conference*

# ENHANCEMENTS IN SAFETY RESULTING FROM PROBABILISTIC SAFETY ASSESSMENTS

DONALD F. RENNICK
Business Development Manager

and

VICTOR G. SNELL
Manager, Risk Assessment and Safety Design Branch

Atomic Energy of Canada Limited
CANDU Operations
Mississauga, Ontario, Canada

## A. INTRODUCTION and PURPOSE

This paper describes our perspective on the preparation and use of Probabilistic Safety Assessments (PSAs) in enhancing the safety and operability of the CANDU reactor system. We outline the history of their development and use, and describe our future plans based on experience so far. We also show how these studies parallel the Probabilistic Risk Assessment process used in the USA and elsewhere.

PSAs are a method of systematic review of the safety and operation of any complex process system or mechanism, for example: aircraft, production lines, petrochemical plants, nuclear reactors, and waste disposal facilities. The focus is on predicting the frequency of possible failures and analyzing the associated consequences so that reliability and safety can be achieved in a cost-effective manner.

Like any major project, nuclear reactors are designed in modules by teams of engineering staff, frequently supplied by different organizations. Design requirements usually specify the interfaces between systems and make implicit assumptions on the availability of support systems. Even if these were perfect, one could not determine, a priori, all the demands on the integrated plant in off-design conditions. The global picture is obtained only by a systematic review.

In section B, we give a summary of the long history of risk and safety analysis at Atomic Energy of Canada Limited (AECL). In section C, we describe our PSA analysis program, and the methods used. Section D summarizes the results of our studies. Section E discusses the shortcomings of the studies done to date, outlines improvements AECL has made for future work, describes the benefits of the AECL methods, and compares them with Probabilistic Risk Assessment methods used elsewhere.

## B. HISTORY OF RISK ANALYSIS AT AECL

AECL is the designer of the CANDU reactor, and pioneered reliability and risk assessments as an integral element of the CANDU design since its inception. Together with prudent operation, these have been major contributors to the consistently high performance records achieved by CANDU reactors. Typically, CANDUs occupy four or five of the top ten positions for capacity factor, for all reactors world-wide with electrical output greater than 500 MW(e).

In the early 1950s, the Canadian nuclear industry set design targets for safety such that the risk from nuclear generation accidents was to be less than 1/50 of the risk from accidents in comparable manufacturing or electrical generation industries. This was achieved by reducing the risk of a catastrophic failure to very low values. To prove these values were achievable, separate reliability targets were derived for the process systems which run the plant, and the safety systems which protect it. These targets had to be demonstrated by test during operation, and the two classes of systems had to be physically and functionally separate to reduce the chance of common failure modes. This approach has evolved (1) into the single/dual failure approach used today in the safety design and licensing of CANDU power reactors. The result is a two-level system of radiological public dose limits--a low dose for the failure of a single process system (the frequency must be shown to be less than one per three years) and a somewhat higher value for a "dual failure" consisting of the process failure plus the assumed unavailability of anyone of the safety systems designed to mitigate the consequences of that process system failure (overall frequency must be shown to be less than one per 3000 years). Thus, loosely speaking, the regulatory dose limits are frequency-based.

The demonstration that the design meets these dose/frequency targets is the analysis found in the Safety Report. The approach is evolutionary still: within the last four years, the Canadian regulatory, in consultation with the nuclear industry, has introduced a number of approaches which place even more emphasis on doses related to frequency of failure (1).

The dormant unavailability requirements for each of the special safety systems ($10^{-3}$ for shutdown, emergency core cooling, and containment) must, as noted above, be demonstrated during operation. If the system is normally dormant, the reliability must be shown by test. Fault trees for these mitigating systems provide the perfect vehicle for establishing the test interval. For active systems, such as process systems, the unsafe failure rate must likewise meet regulatory and economic targets. While this can be established from experience, to avoid expensive backfitting, fault trees are used to give some assurance that the reliability target is achievable in practice.

The single/dual failure approach did not explicitly treat support systems in a logical fashion. Thus in 1975 (2), AECL initiated, as a

6) Surveys are done for crosslinks between the initiating event and the mitigating systems.
7) Fault trees for the selected scenarios are merged and analyzed to determine the frequency of the scenario.
8) The final scenario frequency is judged against an acceptance criterion (see below). If the frequency or extent of core damage is unacceptable, then equipment or procedural changes are made.
9) Utility operations and engineering staff review all stages of the analysis and their comments are incorporated.
10) Designers and/or operations staff prepare normal and abnormal operating procedures, which incidentally are also valuable for operator training.

## FAULT TREES

Fault trees are used to model the failure logic of a system based on its components. This logic is described in AND or OR gates which are readily reducible to Boolean expressions.

The system failure of interest is defined as the "Top Event". The tree is then constructed using a top-down approach and the principle of "immediate cause": i.e. for any event in the tree, events leading directly to it from the next lower level must be those which are immediate, necessary and sufficient to cause the occurrence of that event. This process continues until it reaches the component level or a "basic event". (A basic event is one which may be known from previous analysis or does not warrant further development.)

The tree is then evaluated by formulating the Boolean expression and collecting it into a sum of products. Each product is a minimal cut set, i.e. a set of basic events which, if they occur simultaneously, are sufficient to guarantee the occurrence of the top event.

Quantitative evaluation is done by applying probabilistic equations to the minimal cut sets and substituting reliability data for the basic events into these equations. Failure frequencies are derived from auditable data bases or, for basic events, from previous reliability analyses of the same or identical systems.

The use of fault trees yields two important advantages over other methods used for nuclear plant failure assessments:

a) It ensures that possible common-cause events between initiating events and mitigating systems are accounted for in the analysis of the scenario.
b) It gives a more realistic and defensible estimate of the frequency of rare initiating events than trying to estimate them from statistically sparse historical data.

## EVENT SEQUENCES

We believe AECL is unique in its development of event sequences/event trees because a time line is added to show the scale of events. This enables the analyst to confirm that the mitigating equipment is available and capable in the time window and to calculate what its mission time must be. Because alarms and operator actions are shown explicitly, the human role can be included realistically.

## ACCEPTANCE CRITERION

Very rare events should not require design changes. Since the PSA is a design/operational tool, events with a frequency less than $10^{-7}$ events per year (once in ten million reactor-years) do not need further mitigation. This is in line with international practice. For values between $10^{-6}$ and $10^{-7}$, engineering judgement is used, depending on the situation and the possible severity of consequences.

## OPERATOR MODEL

The operator model used by AECL takes credit for operator action as a function of the stress of the situation, the time from the first clear indication of the initiating event, and the clarity (unambiguity) of alarms available to him/her. The actual numbers used are shown in Table III.

**TABLE III**
**OPERATOR INACTION PROBABILITIES**

| Time (Minutes) | Low Stress | High Stress |
|---|---|---|
| A. Unambiguous Signals To Operator | | |
| No Operator Action Within 15 Minutes | 1 | 1 |
| No Operator Action Within 30 Minutes | $10^{-2}$ | $10^{-1}$ |
| No Operator Action Within 1 hour | $10^{-3}$ | $10^{-2}$ |
| B. Confusing Signals To Operator | | |
| No Operator Action Within 15 Minutes | 1 | 1 |
| No Operator Action Within 30 Minutes | $10^{-1}$ | $10^{-1}$ |
| No Operator Action Within 1 hour | $10^{-2}$ | $10^{-2}$ |

This is an approach unique to AECL--by including operator actions in the event trees, and by retaining a time-line in them, the event trees are firmly tied to the actual phenomena of the incident, and hence operator response can be evaluated in the context of alarms shown, time-scale of required actions, etc.--all of which are also apparent from the tree (3). In practice,

### DESIGN ANALYSIS REQUESTS

In each of the studies, scenarios developed for which there was no operating experience or analytical prediction. To establish that the plant reached a stable state, specific analyses were requested from the safety analysis groups, using best-estimate assumptions to reflect real plant expected response.

This process was responsible for initiating a study of two-phase thermosyphoning of the heat transport system with reduced coolant inventory. It culminated in a program of analysis and supporting experiments which showed successful thermosyphoning down to inventories around 70%.

### IMPORTANCE OF BALANCE OF PLANT (BOP)

The overall plant availability is much better than one would find in an equivalent industrial situation. Indeed, the main contributors (about 80%) to plant unavailability are from BOP systems. This is not unexpected because a considerable amount of attention is traditionally paid to the design, operation, and maintenance of the nuclear island so its reliability is exceptionally good.

### INPUT TO ABNORMAL OPERATING PROCEDURES AND ACCIDENT DIAGNOSIS

A major benefit was the insight gained into the sequence of events which is most likely to occur after an accident or a process upset transient. In co-operation with utility operations staff, AECL prepared Operational Documents (OPDOCS) for all the support systems (air, water, power, etc.) to guide operations in the event of a failure. For instance, OPDOCS can indicate the most probable cause of a particular set of alarms.

In one case, the analysts discovered that an emergency support system would be completely disabled by an incorrect sequence of valve opening. This resulted in item 7 of Table V.

### MAINTENANCE PLANNING

The PSA studies have been used to establish procedures for maintenance outages. For example, during maintenance of the steam generators, the shutdown cooling (residual heat removal) system is the heat sink. This system relies on electrical power. It was determined from the electrical power supply fault trees that a major contributor to unavailability of electric power supply to the shutdown cooling system was the failure of the standby diesel generator(s) to start following a loss of offsite power. Thus the utility decided to run the diesel generators continuously while repairing the steam generators.

### REGULATORY USAGE

The SDMs were undertaken at AECL initiative with the primary aim of increasing production effectiveness and safety. However, they have proven so useful in their secondary purpose of making regulatory submissions that they have become de facto Licensing Support Documents. While there is still no formal acceptance criterion for them by the Canadian regulatory, it is doubtful that any reactor could be licensed in Canada without a probabilistic study of the generic design.

## E. DISCUSSION

### POTENTIAL SHORTCOMINGS OF SAFETY DESIGN MATRIX ANALYSIS VS. PSA METHODS NOW USED

Despite the success of the Safety Design Matrix (SDM) approach (2) in cheaply identifying the most frequent contributors to plant damage, from both an economic and a safety point of view, there were some aspects which the SDM approach either could not, or did not, address. These were (5,6):

1. The SDM's did not attempt to determine a summed risk for the plant. The initiating events for the dominant risk sequences are believed to have been comprehensively identified, but they were not systematically carried through to either PLANT STABLE or NO HEAT SINK for end-point frequencies below about $10^{-7}$ per year. This of course reflects the thrust of the studies, which was to identify and fix real problems. It can be argued that a full Probabilistic Risk Assessment gives poor value for money, because the extra effort spent on identifying and quantifying very low frequency events gives answers which are disbelieved by nuclear critics, mistrusted by decision makers and the regulatory, and not understood by the public. On the other hand, PRAs are the only way of objectively comparing various energy technologies, and, in the international market, of ensuring there are not gross differences from a risk point of view among various commercial reactor types (7). Thus a PRA should be done once, for each major reactor type. The generic report can then be evaluated for significant site specific influences.

   The SDM approach ensured all the large-consequence events fell below $10^{-6}$ per year, since if an event ended in "no heat sink" above that frequency, design changes were made. Most such events were in fact below $10^{-7}$ per year. This was possible on the CANDU without adding major systems because of the already existing dual redundant shutdown systems (which essentially eliminated the possibility of Anticipated Transients Without Scram--ATWS), and the ability of the moderator to act as an emergency heat sink for the core following a loss of coolant and loss of emergency core cooling. Since the initiating event classes were chosen fairly broadly (we were careful not to continue to subdivide

and also that there is no unneeded equipment. It is also used to determine realistic reliability targets for each major system, so designers know what they are aiming for. Typically it takes from a couple of person-months to a person-year of effort. Practically it fosters communication between designers and analysts at an early stage. The second stage is a more detailed study as the detailed design is completed, and the final stage reflects the as-built plant, and is suitable for writing abnormal operations manuals, and for submission to the regulatory. The typical effort is several person-years, depending on the size of the facility and the level of detail in the fault trees.

We have incorporated these refined methods in a prototype PSA for the planned Point Lepreau Unit 2 station. In a unique and iterative process, AECL has reached agreement in principle with the Canadian regulatory on the overall process and methodology.

## F. BENEFITS OF AECL's PSA METHODS

The main strengths of the SDM/PSA approach are that it is cheap, very effective at identifying plant weaknesses and in forcing real issues to be addressed, and can be used either as a screening model or as a basis for a regulatory submission.

Technically the operator model is simple enough to be applied by non-experts in human factors, yet stands up well in comparison with established models of human behaviour.

Retention of the time-scale in event sequences forces a realistic view of plant behaviour and interaction with the operator. For example, New Brunswick Electric Power Corporation (NBEPC), the owner of the CANDU-600 at Point Lepreau, used the SDMs to do a review of all operator actions from a utility perspective (9), including such factors as:

* how much action time does he/she realistically have?
* can he/she do the required actions in that time?
* does he/she have the necessary information in understandable form to make the correct decisions?

The SDM studies are further used in operations in developing advanced training manuals for licensed operators and shift supervisors, and in simulator training where possible.

The fault trees identify sensitive areas which led to a modification of operating practice: for example routine surveillance of expansion joints in large service water pipes was initiated at Point Lepreau when the SDMs showed the consequences of failure and contribution to system unavailability of such pipes.

Faults during operation at other than normal full power conditions (e.g during shutdown cooling) and partial failure modes (e.g. failure of one of the two electrical busses) are routinely examined, and ensure that the more likely accidents are catered for. An example of this was given in Section D, where maintenance procedures were revised to include continued diesel generator operation.

In short, both the SDMs and the improved PSA techniques provide a cost-effective understanding of a plant that can lead to real improvements in safety and economics.

## G. REFERENCES


1. Snell, V.G., "Probabilistic Safety Assessment Goals in Canada", Presented to the IAEA Technical Committee on Prospects for the Development of Probabilistic Safety Criteria, Vienna, January 1986. (Also Atomic Energy of Canada Limited Publication AECL-8761.)

2. Gumley, P., "Use of Fault Tree/Event Sequence Analysis in a Safety Review of CANDU Plants", International Atomic Energy Agency Publication IAEA-CN-39/7, Vienna 1981. (Also Atomic Energy of Canada Limited Publication AECL-7373.)

3. Gumley, P., Narayanan, P.S. and Smith, J.E., "CANDU Alarm Sequence Analysis Following Abnormal Conditions", International Atomic Energy Agency Specialist Meeting on Systems and Methods for Aiding Nuclear Power Plant Operators During Normal and Abnormal Conditions, Hungary, October 1983.

4. Swain, A.D. and Guttmann, H.E. "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", United States Nuclear Regulatory Commission Publication NUREG/CR-1278, August 1983.

5. Shapiro, H. and Smith, J.E., "Probabilistic Safety Assessments in Canada", presented to the 1986 Summer National Meeting of the American Institute of Chemical Engineers, Boston, August 1986.

6. Gumley, P., "Safety Design Matrices (SDMs) as Used in Canada for CANDU 600MW Licensing", International Atomic Energy Agency Workshop on Advances in Reliability Analysis and Probabilistic Safety Assessment, Budapest, Hungary, October 1985.

7. "Probabilistic Risk Assessment: An Emerging Aid for Nuclear Power Plant Safety Regulation", U.S. General Accounting Office, GAO/RCED-85-11, June 1985.

8. Schwartzblat, M., Arellano, J., Gumley, P. and Smith, J.E., "PSADAT: A Database System for Probabilistic Safety Assessment Studies and Its Intended Role in Future AECL Licensing Studies", ANS/ENS International Topical Meeting