



INTERNATIONAL ATOMIC ENERGY AGENCY

INTERNATIONAL CONFERENCE ON CURRENT NUCLEAR POWER PLANT SAFETY ISSUES

Stockholm, 20-24 October 1980

IAEA-CN-39/ 6

SAFETY ENGINEERING SERVICE CENTRE

SP 2 F4

2

USE OF FAULT TREE/EVENT SEQUENCE

IN A SAFETY REVIEW OF CANDU PLANTS

BY P. GUMLEY

ATOMIC ENERGY OF CANADA LIMITED

-ENGINEERING COMPANY

Circulate to

V. Smele

N. Spinks

J. D. Kovat

M. Gocera

for info / etc

BBP
11/3



October 1980

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.

USE OF FAULT TREE/EVENT SEQUENCE ANALYSES
IN A SAFETY REVIEW OF CANDU PLANTS

ABSTRACT

Safety reviews of CANDU nuclear power plants are carried out by the owner/designer for each plant. One of these reviews uses modified fault tree/event sequence analysis and is a methodical safety review of the whole plant. There are typically fifteen different studies conducted for this type of review. Most studies review the consequences of major plant function loss; others are included as building blocks in the construction of event sequences. The studies cover event sequence in detail, including potential common mode failures with other systems. Typical examples of process functions reviewed are : Service Water, Instrument Air and Feedwater Systems.

The objective is to determine the event frequency of a radioactivity release, if any, and thereby estimate risk.

Because of their nature, the most desirable time to perform these studies is when the detailed design of the plant is nearly complete, but still at a stage permitting design adjustments.

The studies are conducted as follows: The frequency of loss of a process function is established using fault tree analysis. This covers, for example, process equipment failure, operator error, control and instrumentation faults, and common mode failures. The plant conditions at the time of the process failure are also determined. Having established these parameters, event sequences are analysed.

The role of the operator is included in the studies by assigning probabilities for failure to take corrective action. This is dependent on the circumstances (speed of development of the event, and complexity of symptoms).

The development of the event sequence is determined by the design, the automatic systems, and operator action. For automatic systems over the short term, the study amounts to an assessment of their capability.

on operator
inaction ?
↓

1. INTRODUCTION

1.1 REACTOR LICENSING PRACTICE IN CANADA

All systems in a CANDU Nuclear Power Plant fall into one of two categories:

1) Process Systems. These are all the nuclear and conventional systems in the plant required for operation in any defined state expected during the life of the plant e.g. plant startup, normal power plant maneuvering, normal plant shutdown operation, and transient disturbances.

2) Special Safety Systems. These systems limit or mitigate the consequences of failures in process systems. These systems have no active function in the normal operation of the plant and are only called upon to function when the process systems have failed. The Special Safety Systems are designed to be independent of each other and independent of the process systems to minimise common mode failures.

Reactor Licensing practice in Canada defines radioactive dose limits for two categories of accidents. These accident categories are defined in Reference 1 (Reactor Licensing and Safety Requirements D.G. Hurst and F.C. Boyd) to be:

- a) Single Failures, where a normal reactor process system is assumed to fail completely.
- b) Dual Failures, where a process system is assumed to fail coincidentally with an impairment or non-function of one or other of the special safety systems.

The single "process failure" in this context can either be an operator error or an equipment failure i.e. the cause is irrelevant. Events which do not cause a power excursion or loss of heat removal capability are ignored as they do not contribute to risk.

This review complements existing licensing analysis in two ways:

- 1) It gives the operator the most likely event sequences on which to base his accident management, and
- 2) It determines the accident end points.

An outline framework of such a safety review was first proposed in January 1975. This review has developed into an analysis package for each reactor plant based on fifteen separate studies.

The failure studies, listed in TABLE 1, are selected for analysis where subsequent event sequences are unclear and where many potential common mode failure causes are known to exist.

In general, each study requires:

- a) Development of failure modes starting with some initiating events and leading up to the "process failure". These events take into account common mode failures or coincident effects on the plant.
- b) The performance analysis of the plant systems (process and safety) during, and immediately following the period of the process failure.
- c) An analysis of any common cause effects on other systems of the process failure itself.
- d) An analysis of the system behaviour and operator actions in the longer term.

For each process function loss, i.e. "the process failure", a failure frequency is established by fault tree analyses. In some instances this leads to a study of more than one event sequence for each process failure where resulting plant conditions differ.

In the construction of the event sequence, the adequacy of the design is established for each time interval, by ensuring that a heat sink is always available and that there is always an activity release barrier present. The relationship between licensing analyses and the FTES review is shown in Figure 1.A. and the typical activities of the FTES safety review are shown in Figure 1.B.

- iv) Process System Action. The effect of all process system action including the response of the reactor regulating system behaviour are included in the development of the expected event sequences.
- v) Special safety system unavailability is generally taken to be 10^{-3} . This is a Canadian licensing requirement and dictates the safety system equipment redundancy and its test frequency.
- vi) Event sequences are terminated when either stable plant conditions have been achieved or the event sequence frequency reaches 10^{-7} events/year or less.

Risk assessment for activity releases at a higher frequency than 10^{-7} events/year is based on an extrapolation/interpolation of the existing licensing single and dual failure limits.

The assumed cutoff frequency of 10^{-7} events/year is consistent with Canadian licensing criteria. It is a licensing requirement that the maximum frequency of all serious process failures should not exceed 1 per 3 years of reactor operation. In addition each special safety system has to meet an unavailability target of 10^{-3} . All dual failures have therefore a maximum allowable failure frequency of 1 per 3000 years of reactor operation or 3×10^{-4} events per year assuming safety system independence. On this basis all triple failures have a frequency of $3 \times 10^{-4} \times 10^{-3}$ or 3×10^{-7} events per year. For such failures, no further design provision is necessary and this is reflected in FTES safety review study limit of 10^{-7} .

A safety review, based on predicted failure frequencies, can only be as good as the failure rate data on which it is based. This is often cited as a major drawback to analyses based on probability. There is now however, a substantial failure rate data base available and a broad survey of equipment failure rates within the nuclear industry is reported in Reference 2. This data source was selected as the prime source for these studies. Additional field data for specialised items of equipment are incorporated where directly applicable.

4. APPLICATION OF THESE TECHNIQUES

A FTES safety review is being undertaken on a number of 'CANDU' nuclear power stations that are currently nearing completion. A simplified CANDU reactor flow diagram for the 'nuclear island' systems is shown in Figure 2 and nine of these studies of the FTES safety review are directly concerned with these systems.

This information is carried over to Figure 4 where fault tree logic is developed for two cases of feedwater interruption to the steam generators.

With power supplies available, a feedwater interruption from a loss of all feedwater pumps has a predicted frequency of 3.0×10^{-5} events/year, and a corresponding unavailability (a measure of the system down time from this cause) of 8.8×10^{-7} . With power supplies, a number of alternate means of removing heat from the reactor are available to the operator. The low failure frequency and redundancy of backup cooling gives this failure mode trivial consequences in a safety sense.

Most major process systems within a nuclear plant have redundancy in their design, and a high predicted failure frequency for the "process failure", i.e. loss of feedwater to the steam generators in this case, is usually indicative of an undesirable feature of the design beyond the design intent. In many instances simple logic changes or alarm indication is all that is needed to correct the design.

The high failure frequency of a total feedwater interruption, resulting from a loss of station power supplies, is more serious. It imposes higher demands on the operator and backup systems in the corresponding analysis of the event sequences. The failure frequencies and unavailabilities of the station power supplies shown in Figure 4 are developed in another FTES review and illustrates the interdependency between studies. In this instance backup power supplies are provided to maintain an adequate heat sink. Since it requires operator action to ready these systems they are included later in the event sequence analyses for this study.

Having defined the process failure, its failure frequency and associated plant conditions at the time of failure, event sequence diagrams are prepared. These diagrams are intended to follow the effect of the process failure on the behaviour of the whole plant. An approximate time axis is included in these diagrams. Three time periods are assessed in a review of the whole plant response. In the short term, seconds and minutes, the plant response is automatic and no credit is given to the operator to intervene and take control. Plant transient codes may be used to follow the effects of the more severe process failures in this time frame.

condensate supply interruption for reasons unrelated to station electrical supplies. The behaviour of affected systems over the short time interval up to 15 minutes is shown. Over this period, steam generator feedwater supplies become unavailable. The feedwater storage tanks are depleted as feedwater is demanded and the condensate return is lost.

The event sequence identifies an automatic power reduction, a turbine generator unloading and a trip of the main steam generator feed pumps. A loss of station power supplies and a failure of the auxiliary boiler feed pump to start are possible consequences which have to be developed further in these sequences.

In some instances, event sequences may not reach the cut off failure frequency of 10^{-7} events/year assumed for the studies. A system deficiency, or an over reliance on corrective operator action is usually indicated. In these cases, simplified event sequence diagrams, highlighting only the essential features of an event sequence, are prepared. These diagrams assist in decision on design changes, where a number of alternative solutions are possible. An example of a simplified event sequence is shown in Figure 7. Although the time axis is not included on this diagram, the time constraints have been allowed for in the failure probabilities used.

DISCUSSION AND CONCLUSIONS

The very real value of this type of study, is that it sets into perspective the relative contributions of plant systems and the operator to overall safety. Preliminary analyses could be used to establish target reliability figures for all plant systems at the design stage.

One of the more surprising findings of this whole plant review is the effect of using conventional equipment protection practise in the balance of plant systems, with little regard for overall station availability. The reliability of many of these systems has been dramatically improved by the removal of many local trips on equipment, particularly pumps. In some instances it is found that these local protection parameters are provided on equipment to support manufacturers guarantees and could be removed with no adverse effects.

Essential operator actions identified in these studies are incorporated in Operating Manuals covering the abnormal events.

TABLE II

OPERATOR FAILURE PROBABILITIES

CASE 1 - CLEAR UNAMBIGUOUS SIGNALS GIVEN TO OPERATOR	PROBABILITY	
	LOW STRESS	HIGH STRESS
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}
CASE 2 - CONFUSING SIGNALS TO OPERATOR		
No Operator Action For 15 Minutes	1	1
No Operator Action Within 30 Minutes	10^{-1}	10^{-1}
No Operator Action Within 1 hour	10^{-2}	10^{-2}

It is a design intent that the safety and safety related systems manage the immediate consequences of any process failure. No operator intervention is demanded for at least fifteen minutes. This design intent sets the requirements for the support systems and the degree of automation necessary to maintain adequate cooling.

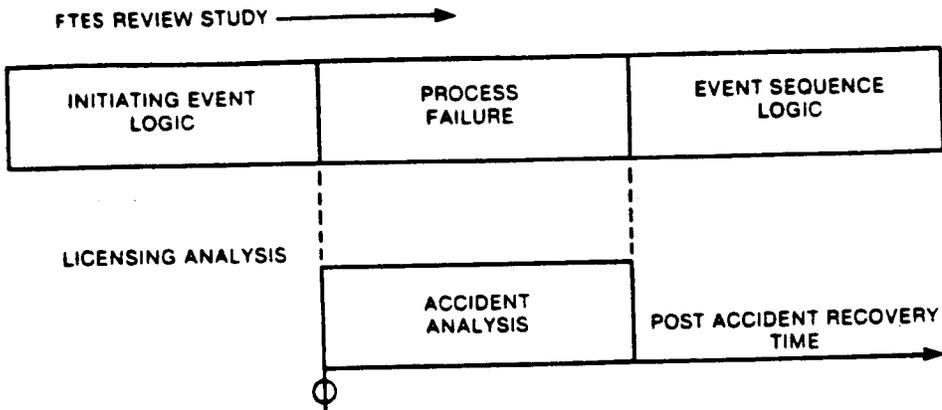


FIGURE 1A BLOCK DIAGRAM COMPARISON OF REVIEW STUDIES WITH LICENSING ANALYSIS

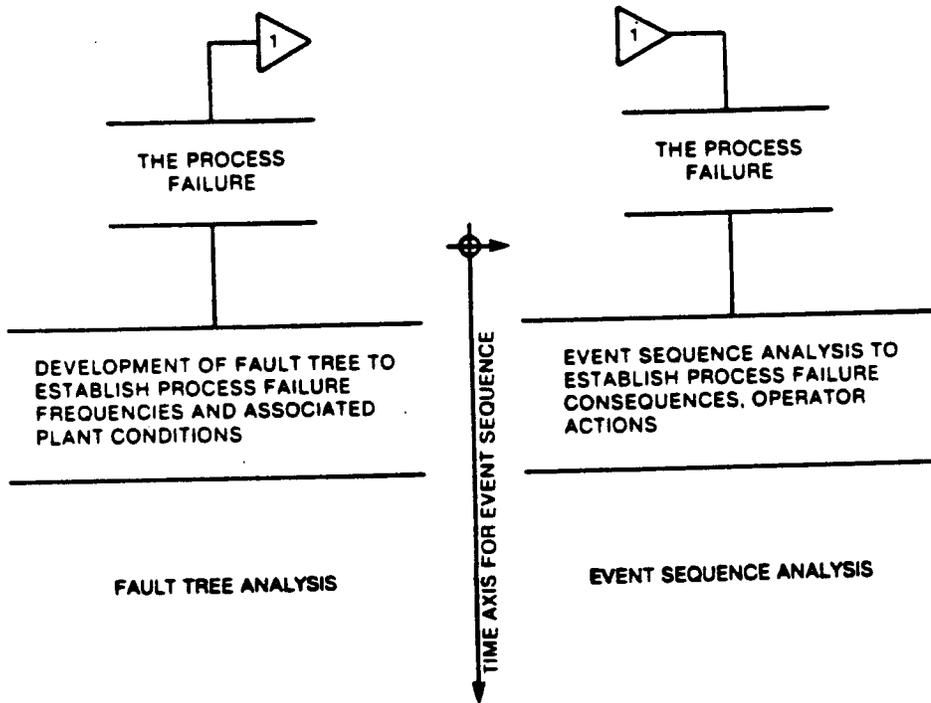


FIGURE 1B TYPICAL ACTIVITIES OF A SAFETY REVIEW STUDY

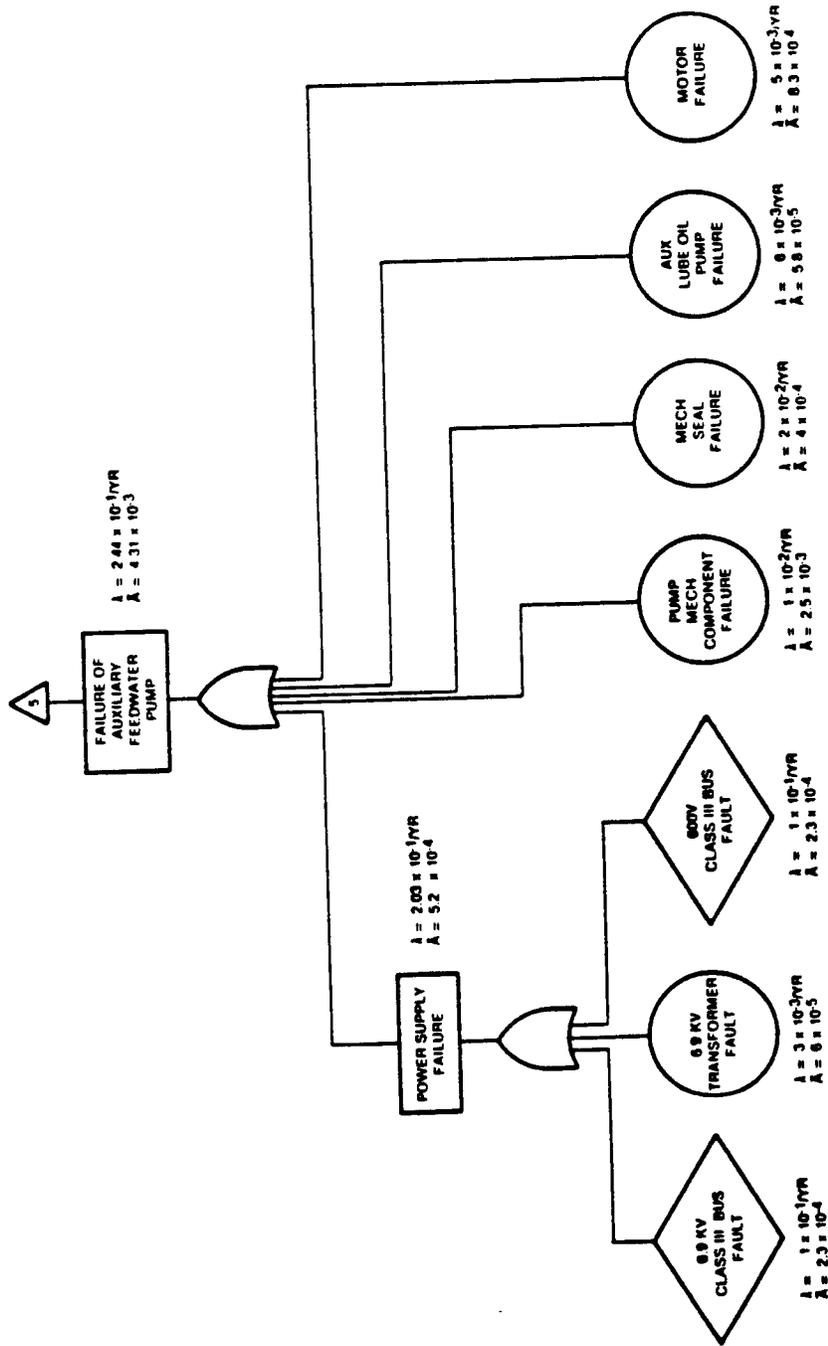


FIGURE 3 FAULT TREE LOGIC FOR FAILURE OF AUXILIARY FEEDWATER PUMP

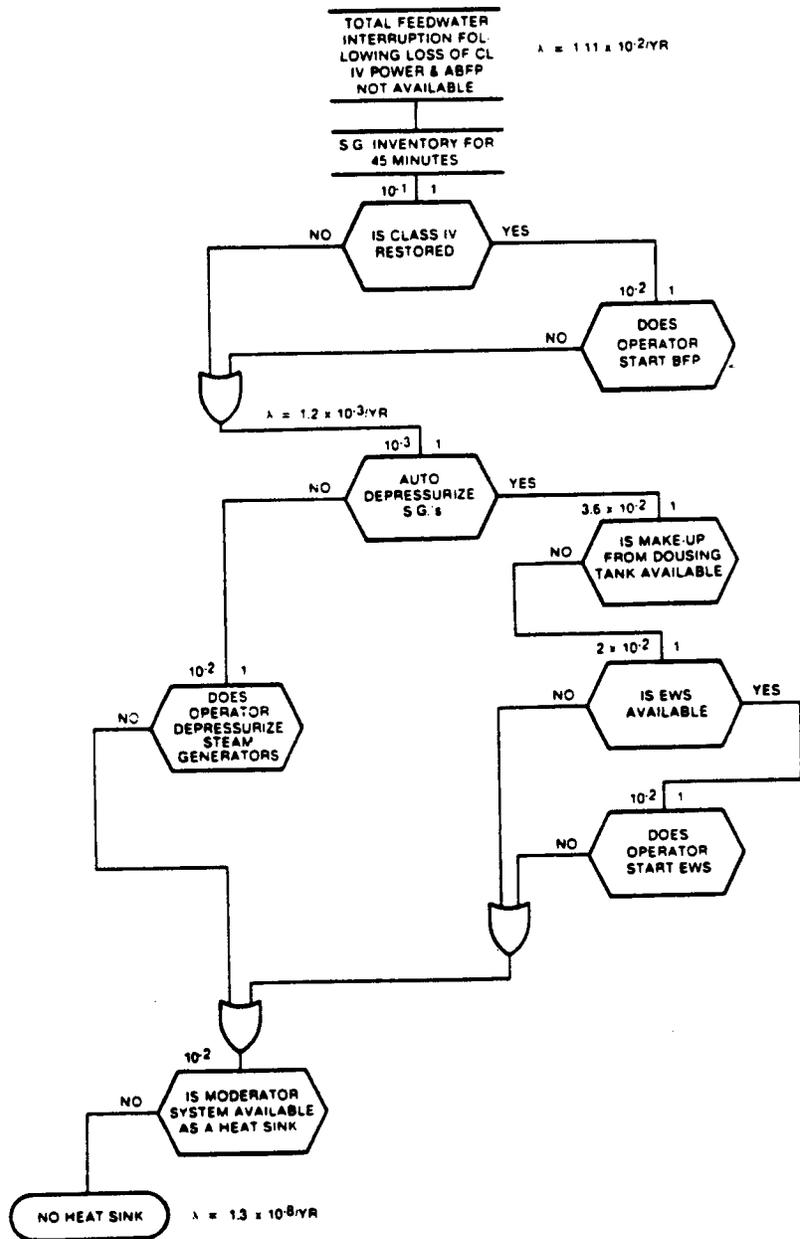


FIGURE 7 SIMPLIFIED EVENT SEQUENCE FOR DECISION MAKING