IAEA SPECIALIST MEETING ON SYSTEMS AND METHODS
FOR AIDING NUCLEAR POWER PLANT OPERATORS DURING
NORMAL AND ABNORMAL CONDITIONS
- BALATONALIGA, HUNGARY, 1983 OCTOBER 4-6

CANDU ALARM SEQUENCE ANALYSIS FOLLOWING ABNORMAL CONDITIONS

by

P. GUMLEY, P.S. NARAYANAN AND J. SMITH

ATOMIC ENERGY OF CANADA LIMITED

IAEA SPECIALIST MEETING ON SYSTEMS AND METHODS
FOR AIDING NUCLEAR POWER PLANT OPERATORS DURING
NORMAL AND ABNORMAL CONDITIONS
- BALATONALIGA, HUNGARY, 1983 OCTOBER 4-6

CANDU ALARM SEQUENCE ANALYSIS FOLLOWING ABNORMAL INCIDENTS

ABSTRACT

In setting the requirements for the capability of the safety and safety support systems, analysis of reactor plant transients following abnormal incidents has traditionally used worst case conditions and assumptions. The transient information from these analyses is so constrained that it would be of little value to the operator in developing meaningful abnormal operating procedures.

An analysis program was started in 1975 with the specific goal of predicting plant failure modes as close to reality as possible. Serious process failures covering major plant processes were subjected to detailed fault tree analyses.

The event sequences from these studies have been used to define specific operator actions required in handling accident situations. These sequences have been a major input into the station Abnormal Operating Manuals and Operator License Certification.

This paper reviews some typical event sequences and the expected response of the station alarms and indications.

The system of station alarms is comprehensive and alarm priority selection has been incorporated in the alarm system design. Some of those priority indications (window alarms) are used as a basis for developing diagnostic procedures.

Details of the alarm and indication analyses are presented in developing operator cues from the event sequences. The analyzed sequences are scrutenized for commonness of alarms and confirmatory checks are proposed to enable an accurate diagnosis of the initiating process failure and resultant plant conditions.

The paper concludes with a brief description of how the information contained in event sequences could be developed into event sequence alarm diagrams in a form suitable for the future anomaly identification and operator support system being developed at AECL.

1. INTRODUCTION

1.1 Reactor Licensing in Canada

Reactor licensing practice traditionally uses 'worst case' type of analyses. The conservative choice of plant conditions, trip parameters and setpoints, heat transfer parameters, etc. usually taken for these analyses gives a plant response which is untypical and likely far more severe than would actually be experienced.

These constraints applied to licensing analyses can distort our understanding of the more probable event sequences. Realistic event sequences are required to review the expected safety role of the operator following process failures.

These sequences are developed in a safety review using Fault Tree and Event Sequence (FTES) analyses. An outline framework of such a safety review was first proposed in 1975 January. This review has developed into an analysis package for each reactor plant based on 15 separate studies, and now forms part of the licensing submissions for reactors licensed in Canada.

Essential operator actions are defined in these FTES reviews and form the basis of station operating procedures for accident management.

1.2 The FTES Analysis Program

The FTES review of a reactor design determines the most probable failure frequency for a number of process failures and the subsequent sequence of events. The main elements of this review were presented at an IAEA Conference in Stockholm in 1980 (Reference 1). This review complements the existing licensing analyses 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 endpoints from which an evaluation of actual risk can be made.

The FTES analysis program is a 'whole plant' review. Considerable supporting analyses are required to predict the failing sequences and the corresponding plant systems interactions. The failure studies which form the FTES review package are listed in Table 1. There are presently 15 studies undertaken.

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 cause failures or other credible failure combinations.

(b) A performance analysis of the plant systems (process and safety) during and immediately following the period of the process failure.

TABLE 1

SELECTED 'PROCESS FAILURES' FOR ANALYSIS IN THE SAFETY REVIEW

	PROCESS FAILURE
1)	Failure of station electrical power supplies
2)	Service water system failures
3)	Instrument air system failures
4)	Moderator and shield cooling system failures
5)	Dual computer failures
6)	Loss of steam generator as heat sink
7)	Reactor building flooding
8)	Turbine and service building flooding
9)	Operation after earthquake
10)	Inadvertent addition of positive reactivity
11)	Large loss-of-coolant accident and emergency core cooling operation
12)	Small loss-of-coolant accident and emergency core cooling operation
13)	Shutdown cooling system operation
14)	Use of moderator as an emergency heat sink
15)	Containment operation

(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.

Because the sequences are best estimates, these studies are particularly valuable in defining the alarms and indications and the role of the operator expected for each failure sequence. It would be wrong to give the impression that all failure modes and combinations are identified for each reactor plant. Times to failure of supporting equipment and the effectiveness of the operator in live accident management give rise to many variations of the predicted sequences. However, the distinguishing features and required operator actions for these sequence variations will likely remain unchanged.

Designing for independence between safety and process systems and identifying where this independence may be affected by the process failure, or its postulated effects, gives considerable assurance that the operator can effectively manage the accident conditions.

This assurance however is affected by the operator's ability to diagnose the failure conditions from the alarms and indications available and his knowledge of the essential operations required to stablize the plant. Hence, a review in detail of the alarms and indications which occur for the more probable event sequences of the FTES review (alarm diagnostic analysis), is undertaken specifically to assist in accident diagnosis.

The alarm diagnostic analysis is directed at:

(1) Diagnosis - enabling the operator to accurately diagnose a severe problem from the available alarms and indications in the main control room and thus to take appropriate action to alleviate or correct the problem.

(2) Prevention - encouraging a prevention rather than cure outlook, i.e. responding to alarms when problems may be severe but are still at a relatively early stage and thus preventing escalation into a major accident scenario.

This paper illustrates the application of these techniques by worked examples and outlines the present status of the work. The application of the results of these studies to future automatic diagnostic routines is discussed.

2. PROCESS FAILURES AND THE DEVELOPMENT OF CREDIBLE EVENT SEQUENCES

2.1 Study Assumptions

One of the major difficulties in preparing Abnormal Incidents Manuals to assist the operator in his accident management, is predicting the failures and other possible equipment failure combinations that the operator may experience. For these reasons, giving an estimate of the process failure

frequency is an essential part of the review and PRA methods are used extensively to assess possible system failure combinations.

It is assumed for these studies that:

(1) The station is operating normally and the reactor is at full power prior to the process failure. In general, full power operation sets the design requirements for reactor shutdown and decay heat removal.

(2) The initial operating conditions are within the accepted normal operating bands. Accidents from non-standard operating conditions are assumed to be of lower frequency, and with special procedures in place to cater to accidents while in this non-standard mode of operation.

(3) Operator actions in event sequences following the process failure are assigned a probability. A failure to take corrective action is assigned a probability dependant on the elapsed time from the process failure and the clarity of information presented. The design of the CANDU system and the automatic systems provided do not require fast operator actions. No corrective operator action is assumed to have a probability of one early in the transient, although the affects of early corrective action are also evaluated.

(4) The effects of process system actions responding automatically to the process failure is included in the development of the expected event sequences.

(5) Special safety system action unavailability is 10^{-3}. (This is a Canadian licensing requirement and determines the safety system equipment redundancy and test frequency.)

(6) The event sequences are terminated when either stable plant conditions have been achieved or the event sequence frequency reaches 10^{-7} events per year or less.

These study assumptions form the framework for developing credible event sequences within which the operator is expected to base his accident management for CANDU systems.

2.2 Development of Event Sequenes

A detailed description of the event sequences developed in the FTES review is not possible here. However, a typical event sequence taken from the review is described as an example. This example illustrates the analysis steps which subsequently identify the key requirements placed on the operator.

The example selected is a total loss of service water supplies and the systems primarily affected are the heat transport system; the moderator and shield cooling system; the feedwater system and the instrument air system.

A brief description of some of the essential features of a CANDU 600 MW(e) station is necessary here to understand the consequences of a severe water loss.

A flowsheet of the heat transport system is shown in Figure 1. The primary circuit has two heavy water loops interconnected by a pressurizer and a heavy water feed system during normal operation. In the event of a large LOCA, a rapid depressurization occurs and the two heat transport loops are isolated automatically. Emergency core cooling primarily directed to the broken loop also acts as a makeup source of light water to the intact loop if required.

A heavy water moderator system, independent of the heat transport system is another feature of the CANDU design. Under some abnormal operating conditions the moderator system can provide decay heat removal capability.

Essential cooling of the calandria and end shields during normal operation is provided by a separate light water system which is itself service water cooled.

Two interdependant service water systems are usually provided; a raw cooling water system and a recirculating cooling water system. In this simplified example only one combined system is assessed since failure of either system will result in a loss of essential station cooling supplies. The event sequence from this review is shown in simplified form in Figure 2.

The likely causes of service water supply interruptions are:

(1) pumphouse intake system failures,
(2) piping failures, and
(3) filter and screen blockages.

The frequency of a total loss of service water with electrical power available is typically of the order of 1.2×10^{-1} events per year. Some of these failures may prove to be recoverable within a period of a few minutes (i.e. filter blockages). However, it is assumed that the service water remains unavailable for an extended period ranging from minutes to many hours and no credit is taken for a restoration of service water supplies.

Both raw and recirculating service water systems are connected to many users in the plant so the effects are far-reaching and many alarm will appear. The operator will receive different window alarms depending on which service water system has failed. A set of alarms which is common to both failures is overheating of the moderator (Note: The moderator and heat transport systems are separate systems in the CANDU plant.) Here the operator must act to prevent boiling of the moderator and a consequential release of tritium into containment. There is no dirct reactor trip provided on loss of service water. However, an automatic reactor power setback and/or reactor trip occurs on high moderator temperature which the operator should confirm. Failure to shut down the reactor by these actions results in a reactor shutdown by any one of the two shutdown systems provided on a high building pressure signal as the boiling moderator is discharged through bursting discs into containment.

The next concern for the operator following service water failures is to ensure the integrity of the heat transport system. Heat transport pump

bearing cooling is lost and bearing damage could occur resulting in an indeterminate loss-of-coolant accident (LOCA) unless bearing cooling is restored or the heat transport pumps tripped within one hour. Although thermosyphoning has been shown to be adequate for reactor decay heat removal, a pumped mode of cooling is preferred particularly during the heat transport cooldown period. During this cooldown period, the heat transport system pressure could fall giving rise to spurious emergency core cooling initiation signals and isolating the pressurizer automatically. This may have the adverse effect of isolating heat transport water in the pressurizer from the circulating volume. The operator is therefore expected to ensure that the pressurizer remains connected to the heat transport system with the heaters maintaining heat transport pressure.

The steam generators are the only heat sink following a service water loss. The maintenance of feedwater supplies to the steam generators is a major requirement. The main feedwater pumps require service water and would trip automatically in approximately ten minutes unless backup cooling was provided. This time span is considered insufficient to manually restore backup cooling when these supplies are also required for a cooldown of the heat transport system. Automatically initiated backup cooling to the main feedwater pumps together with an automatically initiated auxiliary steam generator feedwater pump is therefore provided. Should both of these systems fail, the operator is able to depressurize the steam generators to bring in an alternate low pressure water supply from the containment dousing system holding tank under gravity feed.

The instrument air system is another major plant system affected by service water failure. Instrument air is the motive power for many remotely operated control valves. In particular, the main feedwater regulating valves fail closed on loss of instrument air.

On loss of compressor cooling, following a service water system failure, the compressors would trip within five minutes. Again, this time span is not considered adequate to allow for manual intervention by the operator. An automatically initiated backup cooling water supply to the instrument air compressors has therefore been provided. In addition, local air tanks have been provided for certain essential users to maintain valve operability during the crucial plant stabilization period, should the backup supplies provided also fail.

Loss of cooling to the shield cooling system will cause the shield water to boil without operator intervention. The end shields will eventually boil dry and cause distortion and an overstressing of the heat transport system pressure tubes. It is calculated that at least 60 minutes are available to the operator to initiate a cooldown and prevent such damage.

In Figure 2, the process failure frequency for a service water interruption is taken as 0.12 events perr year. This high failure frequency has had a considerable impact in determining the degree to which automatic systems are provided to deal with the consequential effects on plant equipment. Each one of the event paths can lead to undesirable consequences of not maintaining an adequate heat sink. In general, the automatic systems are required to cover the immediate post-accident period (within minutes). It is during this time that the operator will be under the greatest stress in deciding the nature and extent

of the plant failure. Although fast operator response is not excluded in the modelling, it is not credited in a probabilistic sense in this time frame.

2.3 Accident Management of a Service Water Failure

The specific operator actions required following service water failures are summarized as follows:

(1) Initiate controlled cooldown of the heat transport system at maximum rate using the steam generators as the heat sink.

(2) Keep the heat transport pumps running as long as possible (i.e. alternate operation of one pump per loop).

When the bearing temperatures prevent further pump operation, the pumps should be shut down either manually or automatically. The cooldown rate should be reset either to the minimum or medium rate on the steam generator pressure control program.

(3) Ensure backup cooling to the main feedwater pumps and the instrument air compressors is provided.

(4) Ensure the pressurizer remains connected to the heat transport system with the heaters maintaining heat transport pressure.

(5) Monitor deuterium concentration in the moderator cover gas and purge when necessary to prevent deuterium deflagration.

(6) Prevent injection of hot heavy water to the heat transport pump glands.

(7) Trip the main moderator pump motors to reduce pump heat input and start the pony motors to ensure moderator circulation continues.

Unavailability estimates for backup equipment and for the operator failing to take corrective actions are included in Figure 2. The frequency of the event sequence endpoint (loss of reactor heat sink following service water failures) is approximately 10^{-7} events per year. The figure illustrates also the balance that has been achieved between reliance on the operator and automatically initiated backup equipment.

Specific operator actions for other process system failures have been developed in a similar manner in the FTES review and supporting analyses, and form a major input to the acident management schemes detailed in the plant abnormal incidence manuals.

3. ALARMS AND INDICATIONS

3.1 CANDU Alarm Systems

A very comprehensive alarm system is provided in the control rooms of CANDU stations. The station is computer controlled in normal operation and all of the major processes have deviation alarm indications in the control room.

Trending and system status can also be called up on the cathode ray tube (CRT) displays by the operator and a printout of all alarms and their sequence is provided.

In addition to this alarm system carried out by the computers, an array of window alarms is provided on the reactor panels in the control room and signal major system upset conditions. These indications are independent of computer control. There are typically about ten window messages available on most panels and these are triplicated on the safety panels. A typical panel arrangement is shown in Figure 3. A more detailed review of the annunciation and display systems is given in a companion paper to this presentation (Reference 2).

In any major accident, these window messages are considered to be the primary alarms for the operator. There would likely be a large array of alarms and indications from the computer controlled information system for a major process failure, such as service water. These indications are used for confirmatory checks by the operator and for giving detailed information of the plant status in CANDU stations.

3.2 Alarm Diagnostic Analysis

An alarm diagnostic analysis, based on the conclusions of the FTES review, is undertaken for the major process failures. This analysis identifies the significant alarms and indication and the corresponding window messages are used in developing an accident diagnosis evaluation.

Eight analyses have been produced which analyze in detail the alarms and indications which occur when severe problems arise in the following systems:

(1) feedwater train system,
(2) electrical power distribution system
(3) service water system,
(4) instrument air system,
(5) heat transport system - small leakages,
(6) heat transport system - large loss-of-coolant accident,
(7) moderator and shield cooling systems, and
(8) dual computer plant and reactor control system.

Details of the alarms and indication for each of these studies have been prepared and grouping of the window alarms illuminated have been identified following the process system failures. An example of the window alarms illuminated for a failure of the recirculating service water system is shown in Figure 4. Here six window alarms can be expected to be illumunated. The most significant window message for this postulated initiating event is window 8 on panel 14, "Recirculated Service Water Temperature High - Pressure Low". It is a composite alarm window responding to abnormal temperature and/or pressure conditions in the recirculating service water system.

A loss of raw service water would be identified by a similar number of window alarms with some alarms being common. However, in this postulated initiating event, the most significant window messages are windows 6 and 8 on

panel 14 annunciating abnormal conditions in both the raw and the dependant recirculating service water systems.

A similar window alarm analysis has been completed for other postulated initiating events and these are summarized in Table 2, together with a brief description of the corrective operator actions required.

The commonality of alarms for the different failures can readily be appreciated and the significant differences which permit the operator to identify specific failures are indicated.

This is particularly important for those failure events which give rise to many alarms and indications where the significance of each alarm is easily lost. As an example, a total loss of normal electrical power will give rise to 37 window alarms of which there are only three significant alarms giving clear indication of the process failure.

The alarm system analysis described is readily amenable to some form of data processing to produce an operator interactive diagnostic capability on a small desk top computer located in or near to the main control room.

4. FUTURE DEVELOPMENTS

The analysis of the alarms and indication from window messages alone is somewhat restrictive but does provide a firm starting point for diagnosis of actual initiating events, especially when many alarms windows are illuminated. These same events will also tend to overload the alarms and indications presented as CRT displays. In this respect identifying the most significant window messages is an important contribution in assisting the operator in his accident management.

This simplified approach, however, does not consider the sequencing of the window messages or other alarm indication. A significant refinement is considered possible in the diagnosing of initiating events if the information contained in the event sequences of an FTES review is developed into corresponding alarm sequence information. Furthermore, quantifying the time delays within these alarm sequences will in many cases determine the severity of the initiating event.

The development of a software package, incorporating alarm sequences, into a comprehensive abnormal event diagnostic tool for the operator is discussed in the companion paper (Reference 2).

5. CONCLUSIONS

The FTES review program undertaken as part of CANDU licensing and the subsequent 'severe problem' alarm analysis has been a major step in the management of abnormal events. The key elements of this program are summarized in Figure 5. A particularly important result from this program has been the appreciation of potential failure modes which require a fast operator response (within minutes of the initiating event). The FTES program, based on a probability assessment, provides a rational basis for determining potential

TABLE 2

SUMMARY OF POSTULATED INITIATING EVENTS AND CORRECTIVE ACTIONS

POSTULATED INITIATING EVENTS	CORRECTIVE OPERATOR ACTIONS
Loss of recirculating service water: Loss of raw service water:	Cooldown using steam generator pressure control. Long term use of steam generators as a heat sink.
Loss of feedwater to all steam generators:	Off-normal initiation of shutdown cooling system with heat transport pumps operating.
Large loss-of-coolant accident: Small external leakages:	Emergency core cooling - automatic or manual. Use of shutdown cooling in the intact loop.
Loss of feedwater to one steam generator: Total loss of Class IV power: Loss of end shield inventory: End shield loss of cooling or circulation: Dual computer failure: Loss of instrument air: Loss of moderator inventory: Loss of moderator circulation: Loss of moderator cooling:	Normal cooldown using steam generator pressure control and normal use of shutdown cooling.
Total loss of grid supply and on-site standby generation.	Rapid cooldown of heat transport system by opening main steam safety valves. Dousing water injected into steam generators.

Window Alarms from Figure 3 ▷ A

accident sequences. These sequences have been used to evaluate the role of the operator and the extent to which automatic systems are provided to deal with the accident consequences. In a number of cases, system changes were made where particularly severe abnormal operating conditions, giving rise to a high risk of fission product release, were identified. The selection of the optimum solution where potential plant changes were involved usually required some degree of iteration with the resulting event sequences.

6. REFERENCES

(1) IAEA-CN-39/7, "Use of Fault Tree/Event Sequence Analysis in a Safety Review of CANDU Plants", P. Gumley, IAEA Conference, Stockholm, 1980 October.

(2) "Abnormal Event Operator Aids in CANDU Nuclear Power Stations", Dr. J. Pauksens and M.A. Sillamaa, IAEA Specialists Meeting, Balatonaliga, Hungary, 1983 October.

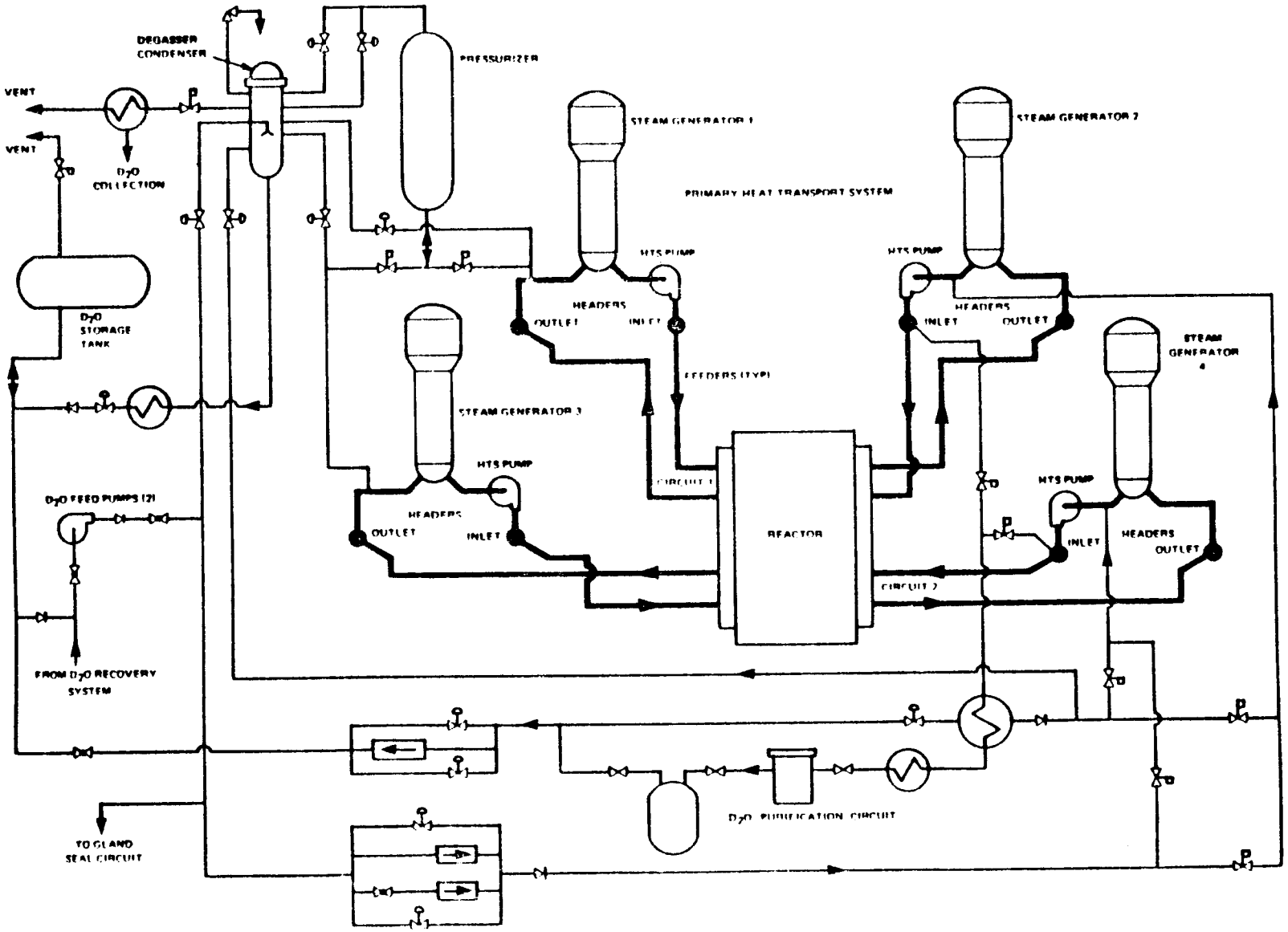

FIGURE 1 HEAT TRANSPORT SYSTEM FLOWSHEET

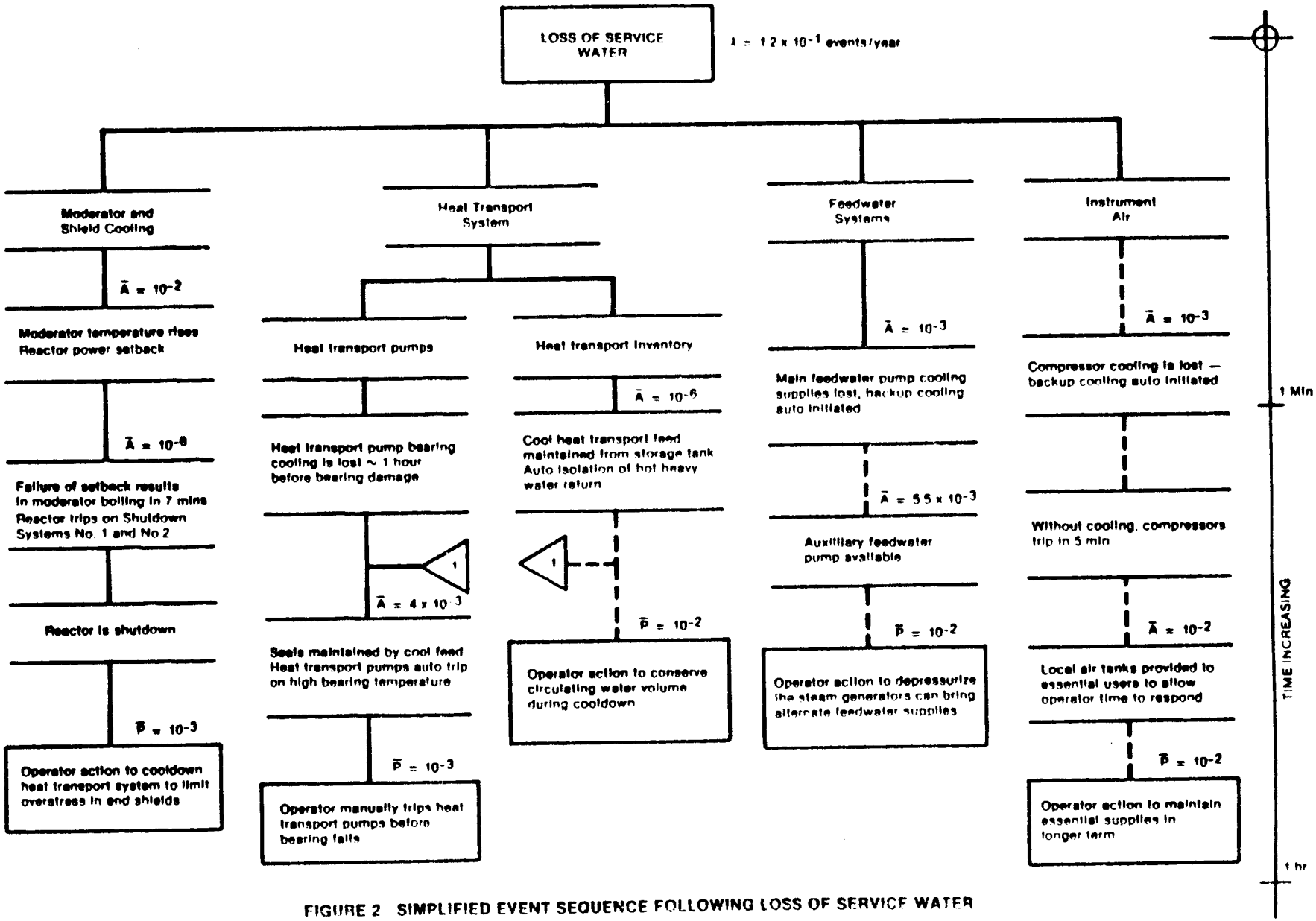

FIGURE 2 SIMPLIFIED EVENT SEQUENCE FOLLOWING LOSS OF SERVICE WATER

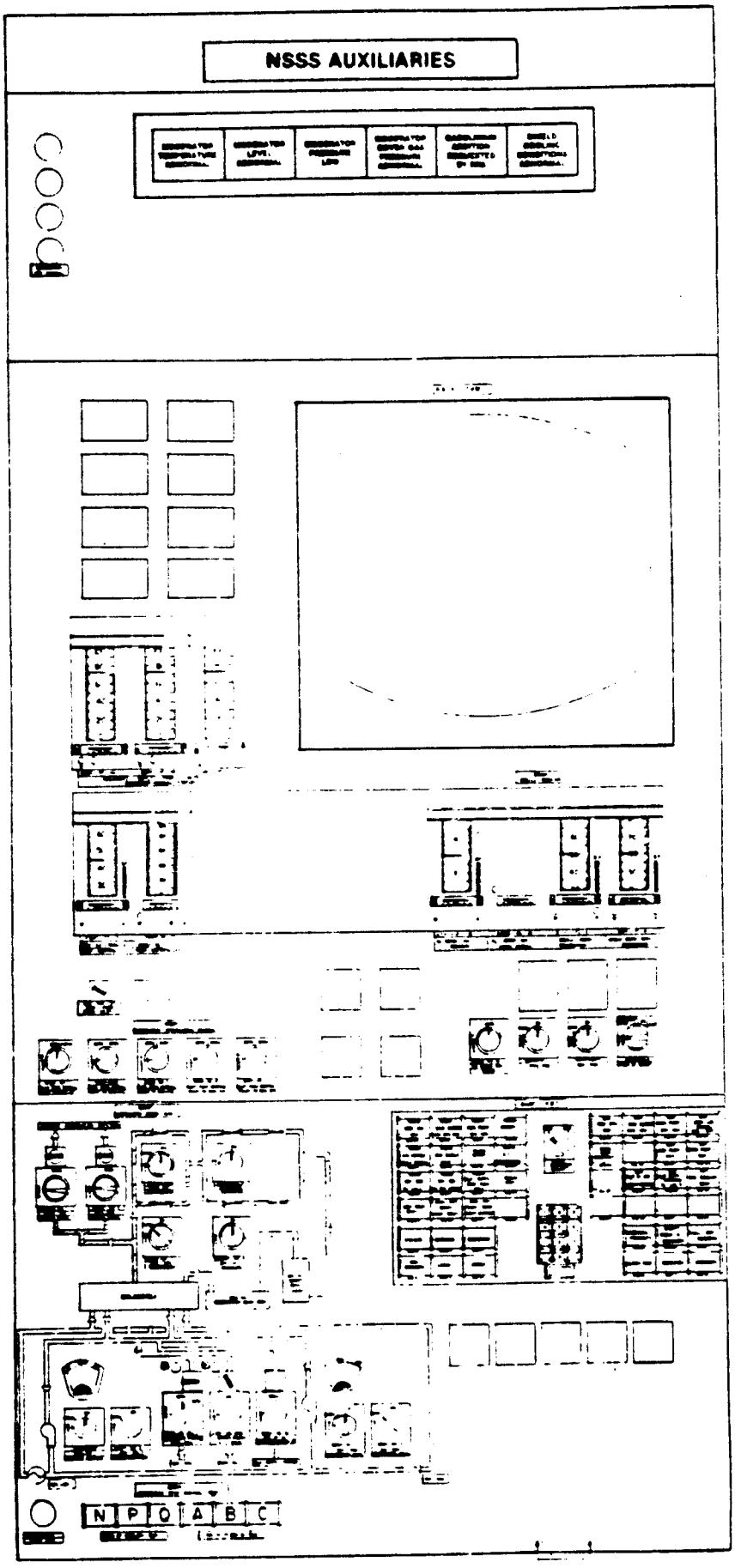

FIGURE 3 TYPICAL CONTROL ROOM PANEL — CANDU 600 MW REACTOR

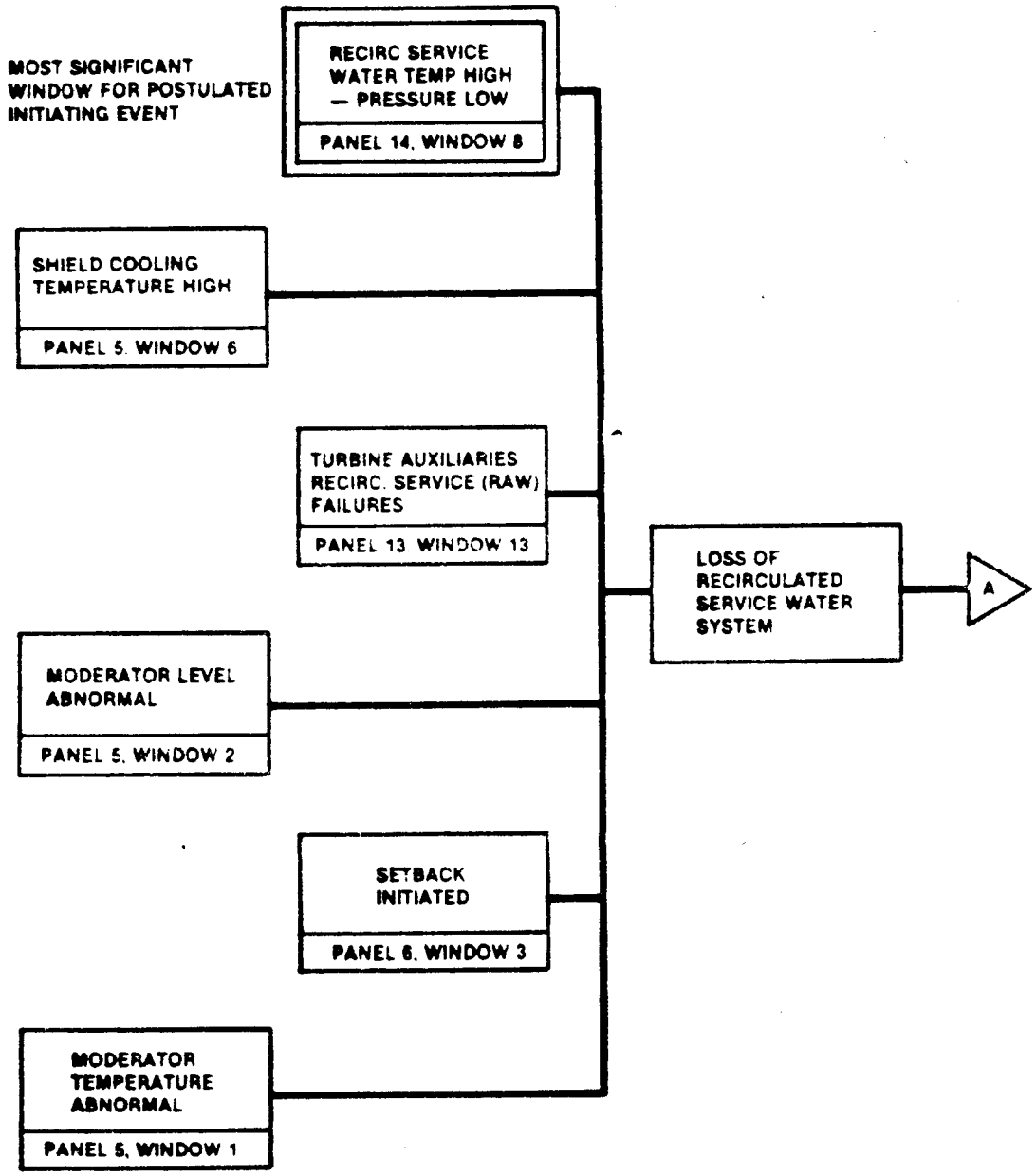

FIGURE 4 WINDOW ALARMS FOLLOWING LOSS OF RECIRCULATING SERVICE WATER SYSTEM

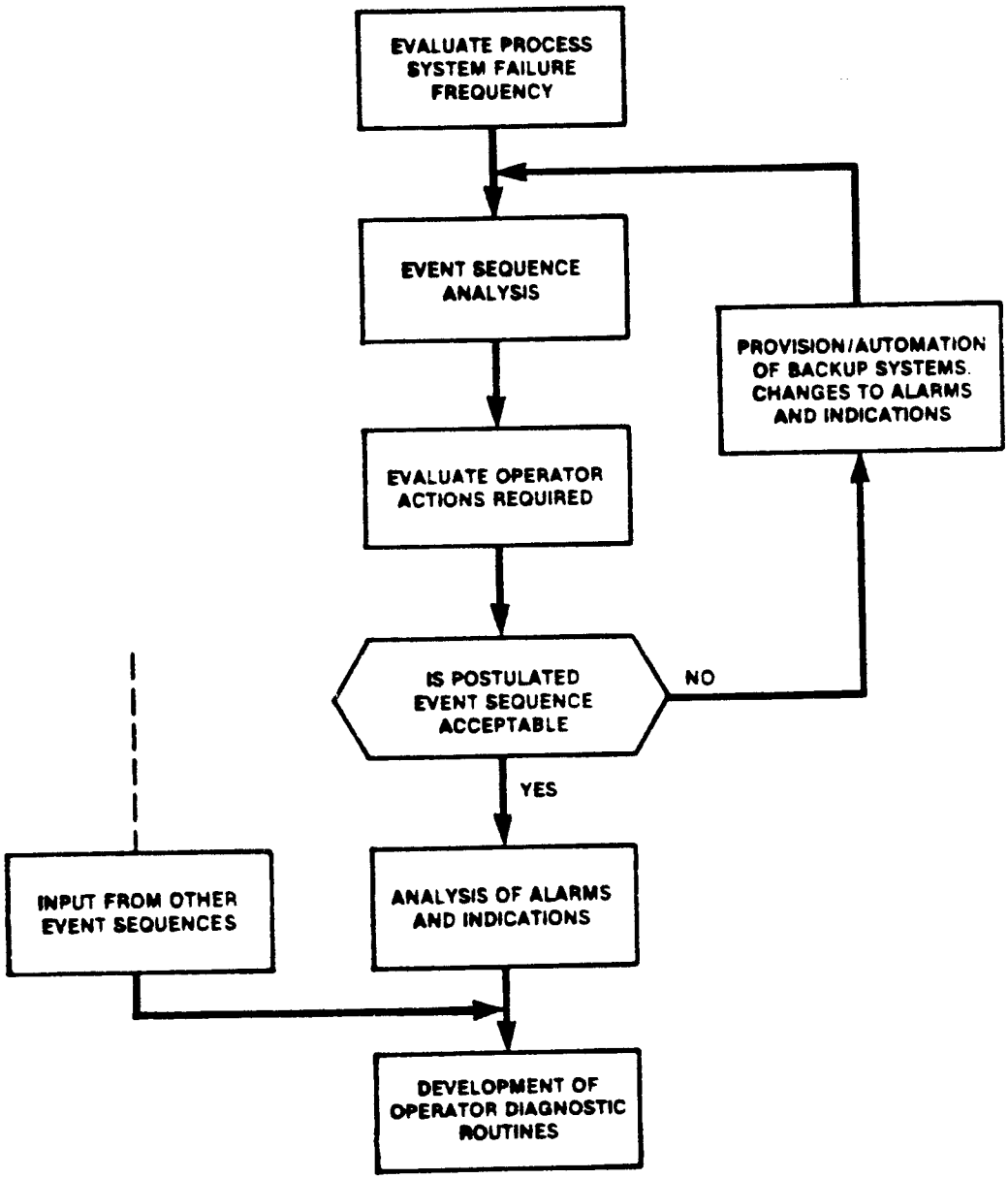

FIGURE 5 ELEMENTS OF A FAULT TREE/EVENT SEQUENCE AND ALARM ANALYSIS PROGRAM