Journal of the Korean Nuclear Society
Volume 27, Number 4, August 1995

《Technical Report》

Review of Emergency Procedures for CANDU Reactors

S.R. Kim, J.S. Kwon, J.H. Cho, S.H. Park, and S.K. Nam
Korea Atomic Energy Research Institute
(Received March 15, 1995)

캔두형 원자력 발전소 비상절차서 검토

김성래 · 권종수 · 조주현 · 박성훈 · 남상구
한국원자력연구소
(1995. 3. 15 접수)

Abstract

The generation, verification and validation of Emergency Procedures for Nuclear Power Plant is a difficult and complex process. Atomic Energy Control Board(AECB) requires that emergency procedure and plan be produced before obtaining the Operating License, that is, detailed plans and procedures to handle emergency situations for both on-site actions and off-site actions be developed. In this report, Emergency Operating Procedures Standard for Canadian Nuclear Utilities whic h makes reference to U. S. practices and the current direction of emergency procedures for CANDU reactors are reviewed and compared based on scope(events covered), methodology (event-oriented or symptom-oriented or hybrid) and format(method of presentation) preponderantly, and an attempt is made to integrate these procedures and as a result, the recommended strategy for Wolsong units 2, 3, & 4 is presented as event-specific procedures, generic procedures(when event is not diagnosed) and whose format is combination of logic diagram and text.

요 약

원자력 발전소의 비상운전절차서는 작성단계부터 난점이 많이 있고, 작성된 절차서를 확인 및 검증하는 데에도 많은 어려움이 따른다. 캐나다의 원자력 규제기관인 AECB에서도 원자력발전소의 운전 허가를 받는 데 있어 발전소 비상운전 절차서를 하나의 요구조건으로 삼고 있는데, 그 요구조건은 발전소 내외의 비상상황에 대처하기 위한 상세한 계획 및 절차를 개발하는 것이다. 본 보고서에서는 미국의 원자력 발전소 비상운전 계획을 참고하고 있는 캐나다 원자력발전소용 비상운전절차 표준지침서를 검토하고, 캐나다 비상운전 절차서 들의 현재 경향을 알아보았으며, 캔두형 발전소들의 비상운전 절차를 사고의 범위(개별적인 사고의 종류 지정), 사고진단 방법(사건 대응적, 징후 대응적, 또는 이 두 가지 방법의 혼합형), 절차서 형식 등을 중점으로 비교 검토하고, 각 절차서의 내용을 포괄적으로 종합하여 현재 건설중인 월성 원자력 발전소 2, 3, 4호기용 비상운전절차서의 기본방향을 징후대응적절차서(사고진단이 안될 경우 사용)와 논리도표와 문장이 혼합된 형식의 사건파악적절차서로 이루어진 비상운전절차서로 제시하였다.

1. Introduction

The development of Emergency Procedures(EPs) is a pre-requisite to obtaining an Operating License from Atomic Energy Control Board (AECB) in Canada [1]. In the early 1980s most utilities in the world concluded that "event specific" procedures had pitfalls associated with correctly/incorrectly recognizing the event and also with the assumptions made about how the plant would respond to that event. To address these and related concerns, "generic" Emergency Operating Procedure(EOP) was developed. Until recently, the EPs in nuclear power plants has been mainly event-oriented.

Following the accident at Three Mile Island, many utilities and regulatory agencies emphasized the importance of "SYMPTOMS RESPONSE" and, in addition, acknowledged the shortcomings of explicitly reflecting conservative safety analyses assumptions in developing EPs. In various ways, utilities identified how a Main Control Room Operator(CRO) should measure and decide whether the response of specific functions was acceptable or not. In all cases, the application of symptoms response required defining the specific functions to be assessed, the relevant parameters to be measured and the satisfactory specific responses. When an unsatisfactory response was found, a recovery procedure was needed. The recovery procedures are basically of two types, an event-based or a symptom-based. They are briefly described below.

Event-Based Procedures

Event-based procedures specify operator actions for a specific event. Each event-based procedure is written for a particular failure within the event class (typically the worst case). Use of event-based procedures requires numerous procedures to cover each specific type of event. Prior diagnosis of event by the operator is necessary in order to select the correct procedure.

Symptoms-Based Procedures

Symptoms-based procedures specify operator actions based on the plant's physical condition only, regardless of the specific type of accident. The plant's physical condition is determined by considering the values and trends of a few key parameters (symptoms). Operator actions are related to quantitative values of these parameters. The aim is to control the system as necessary so that the symptoms indicate that critical safety functions are being met or being improved. A single, plant-specific, symptoms-based procedures would be capable of all plant abnormal events, including multiple failures.

In 1987, the Canadian nuclear utilities, Ontraio Hydro, New Brunswick Power and Hydro Quebec, responded to an initiative of the AECB by producing the "Emergency Operating Procedure Standards for Canadian Utilities" [2]. This document reflects a joint effort of these three Canadian nuclear utilities to apply principles of Symptoms Response in developing and implementing any EOP Program. However, it should be recognized that the "Standards" have not been developed in accordance with and under the jurisdiction of the Canadian Standards Association.

The development of the EPs for Wolsong units of Korea Electrical Power Corporation(KEPCO), which are based on a Canadian Utilities practices, is required strongly. Because of the inherent characteristics of Wolsong units, it is natural to review CANDU practices and Canadian standards to develop the EPs for Wolsong units. In this report, Emergency Operating Procedures Standard for Canadian Nuclear Utilities which makes reference to U.S. practices and the current direction of emergency procedures for CANDU reactors are reviewed and compared based on scope(events covered), methodology(event-oriented or symptom-oriented or hybrid) and format(method of presentation) preponderantly, and comprehensive integration of these procedures is carried out.

2. Review of Emergency Programs for CANDU Utilities

The EPs of Point Lepreau, Pickering, Darlington and Wolsong Unit 1 were selected for a comparison. The comparison of types and terminologies of each plant EPs are shown in Table 2 and 3, respectively.

The technical basis for the EOP's at Point Lepreau is that control of a relatively few parameters("Critical Safety Parameters") will assure adequate fuel cooling and containment activity. By placing priority on control of certain parameters and by choosing parameters that the thermodynamic state of primary and secondary coolants, they parallel the "symptoms-oriented" approach. The EOPs at Point Lepreau [3], [7] are shown in Table 1.

The Point Lepreau EOPs are of two types [4]. One type deals with plant upsets where the nature of the cause of the upset is identified and an event specific EOP exists for that cause. The second type of EOP is complementary to the event specific EOP in that it is used for upset conditions where the Critical Safety Parameters(CSPs) are outside defined acceptable value or the CSPs are trending towards their

Table 1. Number of Events and Main Subsets in EPs

Point-Lepreau	Darlington	Pickering	Wolsong-1
8 events	13 events	12 events	12 events
· Dual Station Control Computer Failure · Loss of Feedwater · Loss of Instrument Air · Loss of Service Water · Loss of Class IV Electrical Power (Station Black-out) · Large LOCA · Small LOCA · Steam Generator Tube Failure	· Forced Shutdown · Steam Generator Pressure Decreasing · PHT Pressure Decreasing · Loss of PHT Inventory · Loss of PHT Inventory with Emergency Coolant Injection · Steam Generator Level Decreasing · Steam Generator Tube Failure · Channel Flow Reduction · Loss of Unit Class IV Power · Loss of Unit Instrument Air · Loss of Low Pressure Service Water Open System · Moderator System Failures · Failures While on Shutdown Cooling	· LOCA & ECC Operation · Feedwater Line Break · Main Steam Line Break · Loss of Class IV & Class III · Boiler Tube Rupture · Loss of Class IV · Loss of Class III · Loss of Instrument Air · Loss of Low Pressure & High Pressure Service Water · Dual Computer Stall · Moderator & Shield Cooling Failure · Loss of RCW	· Dual Control Computer Failure · Small LOCA · Large LOCA · Loss of Feedwater · Loss of Condensate Water · Loss of Electrical Power · Loss of Raw Service Water · Loss of RCW · Loss of Instrument Air · Moderator System Failures · Loss of Moderator Cover Gas · End-Shield Cooling System Failures

unacceptable or undesirable limits and the cause of the event is not recognized or the cause is recognized but no specific EOP exists.

Initially the EOPs were prepared in a format(IF···, DO TO···, ELSE···) but it soon became obvious that such a format was difficult to use and to comprehend. As a result, the present format of Logic Diagrams("Logigram"-Entry Conditions and Main Procedures) and Task Procedures(Tabs) was introduced. The logigram section represents the master logic for the EOPs, including required monitoring, instrumentation to be used, and a summary of corrective actions in priority. The Tabs provide the details of corrective actions and precisely specify which devices are to be operated or monitored. Each EOP contains the followings:

(a) ENTRY CONDITIONS-to confirm what event occurred
(b) MAIN PROCEDURES-to provide operator actions
(c) TABS-to provide detail operator actions

The Pickering Abnormal Incident Manuals(AIMs) have evolved over the last 15 years [5]. In the beginning, a large number of events (including e. g. loss of class I, II power) were addressed by the AIMs. But then it was decided to address only those events which potentially were a threat to fuel cooling and required operator actions at the beginning of optimal recovery. The events covered by AIMs are shown in Table 1.

Basically the type of AIM is an event specific, but in addition to the event based AIMs, there are two generic AIMs. One is a Power Reduction Action Guide, based on reactor trip/setback or stepback. This guide directs the operator to the event specific AIM. The other is a Critical Safety Parameters Monitoring and Restoration procedure. If the event cannot be cleary identified then this procedure instructs the operator to monitor and control certain key safety parameters to ensure fuel cooling, subcriticality, intact containment.

The Pickering AIMs consists of logic diagrams (Event Confirmations and Main Procedures with text format for option) and developed in a prose format (IF. OR. THEN.). The AIMs contain the following sections:

(a) OPERATING OBJECTIVES-to provide an overview of the procedure, at the beginning of the procedure
(b) EVENT CONFIRMATION-to confirm what event occurred
(c) OPERATOR ACTIONS+COMMENTS-in a prose form

The Darlington NGS A Operator Response Guidelines(ORGs) were developed based on Darlington Probabilistic Safety Evaluation (DPSE) to provide operations with a comprehensive and realistic information base for the preparation of abnormal incident, operating, and commissioning procedures, and for the training of operating personnel in handling accident situations [6]. The selection of events was performed based on thorough review of potential initiating events those which could lead to event sequences in which fuel failures occur and grouping of thes-

Table 2. EPs Types

Point-Lepreau	Darlington	Pickering	Wolsong-1
Event Specific + Generic Procedure	Hybrid : Event Specific & Symptom Oriented	Event Specific	Event Specific

e events together according to effect on the Diagnostic Parameters. The ORGs from re-grouping events is shown in Table 1.

The Darlington NGS A ORGs are in the form of a hybrid : symptoms-oriented, event-specific. This approach attempts to impose the rigor and discipline of the purely symptom based procedures on the familiar and direct event-based procedures. Symptom-oriented, event-specific procedures specify operator actions based on a symptom parameter hierarchy, which will be the same for all events, but a separate Guideline is written for each class of initiating events.

Each ORG contains the following:

(a) OBJECTIVES-to provide an overview of the procedure, at the beginning of the procedure.
(b) DIAGNOSIS-to allow for confirmation of diagnosis.
(c) OPERATOR ACTIONS-in flow chart form

The Wolsong Unit 1 Emergency Operating Procedures(EOPs) were prepared by Korea Electric Power Corporation based on Operational Documents (OPDOCs). The OPDOCs provide a detailed analysis of the operating considerations for severe problems of the safety related process systems. The systems for which detailed OPDOCs were produced are:

1. General Strategy
2. Feedwater Train
3. Electrical Power
4. Service Water System
5. Instrument Air System
6. Leakages from the Primary Heat Transport System(PHTS)
7. Emergency Core Cooling Operation
8. Moderator and End-Shield Cooling System
9. Control Computer

These documents reviewed potential system impairments, ensured adequacy of the alarms and identified corrective operator actions, and the events selected to be contained in EOPs are shown in Table 1.

The Wolsong Unit 1 EOPs were prepared based OPDOCs and are of event-oriented procedures type. IAEA SORT recommended to supplement Wolsong 1 EOPs with the proportion of EOP with a symptom-oriented procedure. The contents of each EOP are following:

- EVENT DIAGNOSIS-to confirm what event has occurred using a flow chart
- APPENDIX-contains following sections

1. Introduction - brief description of the event
2. Cause of Event
3. Decision of Event

Table 3. EPs Terminologies

Point-Lepreau	Darlington	Pickering	Wolsong-1
· APOP : Abnormal Plant Operating Procedure	· ORG : Operator Response Guideline	· AIM : Abnormal Incident Manual	· OPDOCs : Operational Documents
· EOP : Emergency Operating Procedure	· EOP : Emergency Operating Procedures		· EOP : Emergency Operating Procedures

4. Alarms and Indications
5. Actions-contains following sections in text form and each section consists of Basic Actions and Detail Actions
   5.1 Plant Automatic Response
   5.2 Operator Actions
   5.3 Long-Term Actions

3. Review of Emergency Operating Procedures Standards for Canadian Utilities

The Standards is a complex document which not only prescribes rules but also attempts to teach some of the physics fundamentals of CANDU type reactors [2]. The Standards have adopted a policy of specifying and measuring the sufficiency of any plant configuration via a limited set of Critical Safety Parameters(CSPs), reflecting Symptoms Response in its more general application. The Standards explicitly require that both "generic" and "specific" procedures to written recognizing different levels of sufficiency. The words NORMAL, ABNORMAL, UNDESIRABLE, UNACCEPTABLE-are used in the Standards to describe a degradation of plant sufficiency.

The EOP Standards require the application of a "Response Strategy to Upsets" (Figure 1) based on symptom-oriented operator response. To achieve this effectively, it requires recognition of the event and relevant CSP monitoring. The Response Strategy to Upsets must also include CSP monitoring beyond those parameters related to a specific event.

The Standards require the application of a strict management structure to life-cycle of EOPs-Production process is controlled by three elements or stages called

GENERATION,
VERIFICATION, and
VALIDATION
−in a more general engineering application these are
CONSTRUCTION,
INSPECTION,
ACCEPTANCE.

The intention is to impose a thorough quality control system on EOP production and its use. There are additional elements dealing with training of operating staff, implementation and updating. The Standards requires that EOPs to direct the operating staff to address threat to and deterioration of safety barriers-using specific procedures as well as generic proc edures.

Plant operating regions are a classification of plant operation by the status of a set of CSPs. Four plant operating regions have been defined: Normal, Abnormal, Upset and Emergency.

The CSPs in CANDU plants are representative of the adequacy of fuel cooling, and the integrity of the heat transport system and containment. These CSPs are monitored by users to determine the type of actions required to keep the plant in a safe state. As CSP values degrade and move towards the bottom

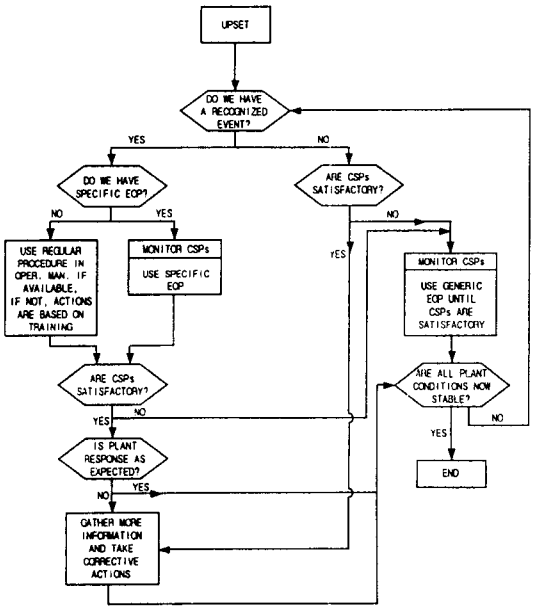

Fig. 1. Response Strategy to Plant Upsets [2]

part of the triangle in Figure 2, they become less acceptable in terms of the threat presented to safety barriers, and as a result the need for operators to take corrective actions become more imperative. These plant operating regions are described, including typical events and operating for each region.

The following statements further characterize plant states, typical events and operating practice for each plant operating region that is shown in Figure 2.

Normal

- Involves pre-planned operation activities under various plant states:

Reactor shutdown, cold, depressurized
Reactor at zero power hot, critical, power 〈 2%
Power = 60%(grid synchronization, poison-prevent state)
Power 〉 60%
Pre-planned shutdowns and startups
Testing
Maintenance

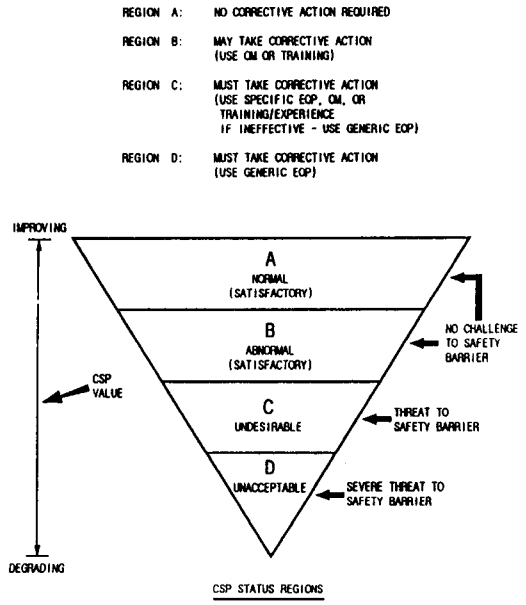

Fig. 2. CSP Status Regions [2]

Commissioning

- Procedures normally found in Operating Manuals (OMs)

Abnormal

- Involves pre-planned operation activities, under various plant states as in normal operation, plus:
- Unplanned operation activities in response to equipment malfunctions which cause CSPs to drift to Abnormal region. Generally, these activities consists of:

  Enabling alternative/standby equipment within a system.

  Restoration of failed equipment.
- CSPs have minor deviations near the end of acceptable ranges, but remain satisfactory, and imply no threat to safety barriers.
- Plant states remain stable and under operational control.
- Operators run the plant by executing actions replying on training and/or written procedures.
- Procedures normally found in OMs.

Upset

- Plant states change as a result of an unplanned but postulated events such as:

  Total or partial failure of a single process, special safety or a safety support system(e.g., air, water, electrical).
- No cross-link failures between two or more support systems.
- CSPs values becomes undesirable, constituting a threat to one or more of the following:

  Integrity of fuel sheaths

  Integrity of PHTS

  Integrity of Containment
- Operators would normally abandon execution of normal/abnormal operating procedures in favour of a specific EOP.

Emergency

- Plant states change as a result of an unplanned

and perhaps unpostulated events such as:
Total or partial failure of one or more process, special safety or a safety support systems including failures resulting from cross-links between two or more of these systems.
- CSPs values becomes unacceptable, implying a severe threat to safety barriers.
- Execution of an events-based EOPs is not effective to restore the plant to the Normal or Abnormal regions due to failure of more than one system.
- Operators are uncertain as to actual plant state.
- Operators would normally be required to abandon execution of event-based EOPs or any other procedure and address heat sink degradation by:
Execution of the generic EOP.
Actions to restore heat sink + subcooling margin.

CANDU design identifies EOP entry conditions by monitoring the CSPs [2]. The CANDU approach of monitoring CSPs and identifying appropriate operator action is developed on the basis of symptom-based operator response. The operator verifies diagnosis events by detailed development of CSPs associated with each event is guided by EOP entry condition. After identifying status of CSPs, the operator establishes corrective actions to achieve operational goal by virtue of operator response strategy to upsets.

4. Recommendation for Development of Wolsong 2, 3 & 4 Emergency Procedures

In an attempt to establish a standard EPs for the Wolsong utilities the CANDU EP practices and the Canadian standard for EPs are reviewed. However, it can be complex and difficult for an operator to fulfil the recovery action necessary to recover from the upset plant. When the abnormal conditions cannot be clearly diagnosed, when the plant or operator response to any diagnosed abnormal condition proves inadequate, or when the plant response or corrective actions cannot, or have not, been predicted, the event specific EPs may be inadequate. For appropriate responses to the plant abnormal conditions the developments of more specific and detailed event-based EPs are required. Under these circumstances, if the critical safety parameters are trending in an unsafe manner, the symptom-oriented EPs should be used. Both event-specific and symptom-oriented EPs are advisable for the Wolsong units. The pros and cons of each types of EPs are shown on the Table 4.

EPs should direct the operating staff to address threats to and deterioration of the safety barriers. The main safety barriers are:

(1) the fuel sheath
(2) the heat transport envelope, and
(3) the containment.

Actions to restore the integrity of the heat transport envelope and containment should also be addressed, where appropriate. As a minimum, the CSPs should include:

- PHT Pressure
- PHT Volume
- PHT Temperature
- Reactor Power
- Steam Generator Pressure
- Steam Generator Level
- Feedwater/Service Water Activity
- Containment Building Activity
- Containment Building Pressure

Wolsong Units 2, 3 & 4 are under construction and the second unit is to start its commercial operation in 1997. The emergency procedures for Wolsong Units 2, 3 & 4 consist basically of the procedures for handling the anticipated abnormal events. Scope of these procedures are discussed below:

A. OPDOCs

The scope of this procedure is similar to that of Wolsong Unit 1. The preparation of these documents thus will assist the control room design process in that

i) a systematic review of the significant failure modes of the safety related systems is performed and
ii) it is ensured that the design provides appropriate

Table 4. The Advantages and Disadvantages of Each Type

Type	Advantages	Disadvantages
Event-Based	· simple to use · familiar to operators · provide more detailed and rapid recovery actions · realistic in approach	· subdivision of event class lead to more detailed procedures · requires diagnosis prior to operator action · difficult to deal with multiple events · no guidance for unknown event
Symptoms-Based	· remedial actions independent of cause · allows single procedure to deal with all events · can handle with multiple failures	· if the event can be diagnosed, single procedure appears to be difficult to use · requires major change in training and operating philosophy · requires accident to have progressed far enough for unit trip; can lead to greater consequences
Symptoms-Oriented, Event-Specific	· if diagnosis is possible, numerous branchings of single symptoms-based procedure are eliminated handle minor misdiagnosis uniform hierarchy of symptoms leads to plant stabilization prior to diagnosis of event · detailed recovery actions · allow for variety of entry conditions · deal with concurrent failures · provides some guidance for unknown events	· includes extra steps not needed if event follows expected sequence · requires operator to diagnose the type of event (but not specific event)

alarms and indications in the main control room or the secondary control area.

B. Abnormal Operating Manuals(AOMs)

The following events are considered for Wolsong 2. 3 & 4:

Loss of Class IV Electrical Power
Small LOCA/PHTS Leakages
LOCA + ECC Operation
Shield Cooling System Failures
Moderator System Failure
Loss of Feedwater

Steam Generator Tube Ruptures
Main Steam Line Break
Loss of Class IV and Class III Electrical Power
Dual Control Computer Failure
Loss of Steam Generator Feedwater
Loss of Service Water
Loss of Instrument Air
Symptom-Oriented procedure

5. Conclusions

The following hierarchy is recommended for the Wolsong 2, 3 & 4 EOPs. The scope of the recommended hierarchy is based on the scope of AOM and the urgency of the event.

Symptom-Oriented Procedure
LOCA + ECC Operation
Small LOCA/PHTS Leakages
Loss of Steam Generator Feedwater
Main Steam Line Break
Loss of Class IV and Class III Electrical Power
Steam Generator Tube Ruptures
Loss of Instrument Air
Loss of Service Water
Dual Control Computer Stall
Loss of Class IV Electrical Power
Moderator System Failure/End Shield Cooling Failure

The AOMs can be presented in four sections, entry conditions, operating objectives, main procedures and technical basis documents. A list of entry conditions is recommended to give the operator of confirmation of appropriateness of his selection of procedure for the given emergency conditions. The AOMs can be easily recognized to the operator "Where he is", "Where he has come from" and "Where he may be going" via a logic diagram format. The logic diagrams shall contain governing conditions and operator actions. The purpose of the AOM concentrates on stabilizing the plant from the viewpoint of fuel cooling, heat sink and containment. Therefore, the contents of logic diagrams should be written in short and concise form to give appropriate and clear directions to the operator and to enhance comprehensive understanding under emergency conditions. The logic diagrams shall be presented on the left side of each page in order of importance with vertical direction following plant response. On the right side of each page, comments will be described to give the operator the further information about indicators to be monitored and equipments to be operated. At the beginning of each logic diagram, the operating objectives are recommended to be provided in brief and concise sentences to describe what is to be accomplished in the procedure. Each AOM should be complemented by a technical basis document, identifying the response of all relevant and major CSPs, explaining the strategies and tactics adopted, rationale for each operator actions and

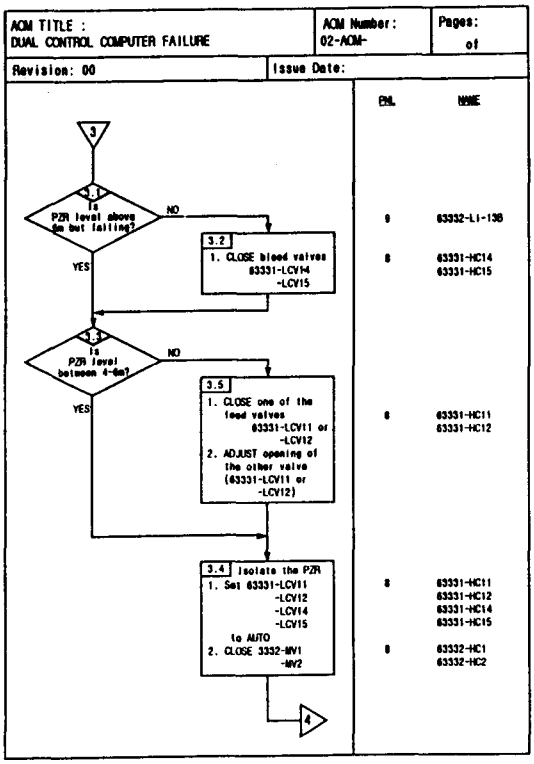

Fig. 3. Proposed Logic Diagram Format

identifying the specific limits of the AOM. The proposed logic diagram format is shown on Figure 3.

References

1. M. Joyce, "The Licensing Process for Nuclear Power Reactors," AECB-1139, Atomic Energy Control Board, Ottawa, Canada (1979)
2. The Joint Utility Task Group of Ontario Hydro, Hydro Quebec and NB Power, "Emergency Operating Procedures Standards for Canadian Nuclear Utilities," (1987)
3. R. Colqhoun, "The Emergency Operating Procedures at Point Lepreau," unpublished paper (1989)
4. R. Colquhoun Associates, A.R. Johnson, J.F. McCallum and D.F. Weeks, "Emergency Operating Procedures Based on Thermodynamics State," CNS 8th Annual Conference (1987)
5. Fax Communication with R. Jaitly of AECL on "Pickering AIMs"
6. C.W. Gordon, "Darlington NGS A Operator Response Guidelines Overview," Darlington NGS A Operator Response Guidelines (1985)
7. A. R. Johnson, B. Patterson and W. Pilkington, "Man-Machine Interface Improvements for Emergency Operating Procedures at Point Lepreau," Presented at IAEA Specialists Meeting in Schliersee. W. Germany (1988)