IAEA-TECDOC-341

DEVELOPMENTS IN THE PREPARATION OF OPERATING PROCEDURES FOR EMERGENCY CONDITIONS OF NUCLEAR POWER PLANTS

A TECHNICAL DOCUMENT ISSUED BY THE
INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1985

DEVELOPMENTS IN THE PREPARATION OF OPERATING PROCEDURES
FOR EMERGENCY CONDITIONS OF NUCLEAR POWER PLANTS
IAEA, VIENNA, 1985
IAEA-TECDOC-341

Printed by the IAEA in Austria
June 1985

PLEASE BE AWARE THAT
ALL OF THE MISSING PAGES IN THIS DOCUMENT
WERE ORIGINALLY BLANK

The IAEA does not maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 80.00 in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

FOREWORD

In recent years, increasing attention has been paid to managing the safety of nuclear power plants. One of the areas on which development focused was operator response to abnormal occurrences and emergency situations (see example 1). In particular, this includes provision of additional diagnostic aids, development of comprehensive operating procedures and training of operators in their specific response to a wide range of emergency conditions. Although more work has to be done in this field, sufficient progress has been made to encourage the IAEA to open further discussion on this topic with a view to disseminating the available information to those working with these problems (see example 2).

Accordingly, the IAEA convened a group of experts to prepare a discussion document "Developments in the Preparation of Operating Procedures for Emergency Conditions for Nuclear Power Plants" which was subsequently reviewed by a Technical Committee. The present document, therefore, represents a review of the developments in some Member States. It is intended primarily to draw attention to these developments and to stimulate further international discussion on these problems (see example 3).

The IAEA wishes to express its appreciation for the efforts of the Working Groups and Technical Committee and would welcome comments from interested parties.

EDITORIAL NOTE

In preparing this material for the press, staff of the International Atomic Energy Agency have mounted and paginated the original manuscripts and given some attention to presentation.

The views expressed do not necessarily reflect those of the governments of the Member States or organizations under whose auspices the manuscripts were produced.

The use in this book of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of specific companies or of their products or brand names does not imply any endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

In recent years a substantial effort has been devoted by the nuclear community to extend Emergency Operating Procedures (EOPs) to cover all conceivable events and to develop procedure formats that transmit the essential guidance to operators in an optimum way.

The general practice adopted in the nuclear industry has been to provide operating procedures for postulated events that are analysed and discussed in the safety report. Such procedures are mainly limited to single initiating events, their consequences and the action following the operation of safety systems designed to respond to those events. Experience at some operating plants has indicated a need for EOPs that include information on the actions required to maintain the plant in a safe state irrespective of the initiating event. Such EOPs should also assist operators if they are required to cope with very unusual events and to select the most appropriate action(s) for the establishment of safe conditions. In addition there is a need to consider the format of EOPs to assure their most efficient use from the standpoint of human engineering.

The information given in this report is based upon the most recent developments in formulating and applying EOPs. It should therefore provide guidance to those involved in preparing or reviewing EOPs on the scope, technical basis, organization and format of such procedures. It also outlines the actions required to validate the adequacy and applicability of these procedures so that the correct operator actions are achieved. Examples are given to illustrate the developments in some Member States.

2. DEVELOPMENT OBJECTIVES

In the design and operation of a nuclear power plant the main safety goal is to prevent significant radioactive release to the environment. For that reason it is necessary to protect the various barriers between radioactive products and environment and to assure functions important to safety such as shut-down and removal of residual heat.

For this purpose the plant is equipped with protection systems that monitor the plant status and automatically actuate appropriate safety systems if important plant parameters go beyond predetermined safety limits.

Whenever protection systems are actuated, plant operators continuously present in the control room, follow predefined procedures which are set out in documents designated as emergency operating procedures (EOPs). These procedures are used to:

- verify the automatic operation
- diagnose the situation by following a predefined logical process for selecting the appropriate operating procedure
- take action, as directed by this specific operating procedure in order to transfer the plant to a long-term safe status up to the point of possible expert intervention (see examples 1 and 2).

It is important that the procedures provide systematic and adequate guidance from the beginning of any event or transient. This allows operating personnel to initiate appropriate responses without having to spend time diagnosing the event itself and without having to rely on memorized event responses when facing a complicated event. Good procedures should assist operating personnel in focusing priority attention on the most important information and developments; they must bring order out of the possible confusion caused by numerous simultaneous alarms and prevent misdirection of attention to matters and information of lesser importance.

In the past the general approach adopted in the nuclear industry has been to provide a set of EOPs covering the list of single initiating events taken into account in the design and analysed and discussed in the safety report. The diagnosis consisted of identifying at the beginning of the transient, which event in this list could explain the values reached by principal parameters measured on the plant. In "event-oriented approach", the corresponding "event-specific" EOP defined the sequence of actions required after this identified initiating event.

In recent years experience of plant operation and tests on simulators showed the need to take into account more realistic and/or complicated situations (from the view point of plant operators) corresponding to both different combinations of initial status of the plant, initiating events, and possible deviations in the response of plant operators, reactor and protection systems in accident situations from those theoretically predicted.

This extension of the scope of EOPs concerns not only "out of design" situations of very low probability but also more realistic situations enveloped by the set of design basis accidents.

The two main reasons for recent developments in EOP preparation are to provide this extension to cover a broader range of situations and to take into account error in diagnosis. Their main objective is improved diagnosis featuring:

(1) Redundancy

(2) Periodicity

(3) Comprehensiveness

(4) Applicability, by limiting the number of EOPs.

Objectives 1 and 2 need human redundancy in the operational organization; objectives 2, 3 and 4 cannot be reached by the event-oriented approach and need new approaches based on the idea that is generally not necessary to know the list and chronology of past events and actions that have determined an actual situation in order to define required actions in a new situation (see example 2).

Three similar approaches, symptom-, function- and state-oriented, have been developed by different countries. The differences between them is as follows:

- The symptom-oriented approach defines a direct relation between each symptom indicated by plant parameters and required actions to control these parameters. Different symptoms are considered independently;

- The function-oriented approach combines all parameters relating to the same safety function in order to decide required actions to control this function. Different functions are considered independently;

- The state-oriented approach combines all parameters of all functions of the plant in order to define the plant state and to decide required actions to transfer the plant to a safe condition.

Chapter 3 discusses the application of these different approaches in the preparation of EOPs.

Consistent with this development, the nuclear community has made a substantial effort in the following directions:

- Improved technical bases for EOPs by using more realistic and diversified post-accident physical states and transients analyses (see chapter 4).

- Improved possibility of following and continuously characterizing the physical state and evolution of the systems by appropriate instrumentation. (This effort, including development of additional instruments and their post-accident qualification is noted here but not developed in this report);

- Improved format and style of both EOPs and the control room aids for applying them (see chapter 5);

- Improved EOP-training of operators and related technical support (see chapter 6);

- Improved validation of EOPs and related technical supports (see chapter 7).

3. DIFFERENT APPROACHES

The emergency operating procedures can be based on four different approaches:

Event-oriented
Symptom-oriented
Function-oriented
State-oriented.

3.1 Definition of different approaches

Event-oriented

Event-oriented EOPs are developed on the basis that before or during the recovery process the operator will identify the specific event causing the transient or accident, or at least can assign it to a broader class of events. This will facilitate the optimum response to mitigate the consequences of the transient or accident, but it also implies an increase in the number of procedures to extend the scope of covered events.

Symptom-oriented

In this approach the entire safety of a nuclear power plant is assumed to be controlled by a certain number of safety-related plant parameters, which (as in medicine) can be called "symptoms". As long as all safety-related symptoms are within pre-determined safety limits, plant safety is maintained.

If any symptoms exceed safety limits, operators have to initiate actions in accordance with the appropriate symptom-oriented procedure in order to return to acceptable conditions. (As in medicine, the illness of a patient is diagnosed by symptoms, and measures are taken for recovery.)

Function-oriented

With function-oriented EOPs, assuring safety of a nuclear power plant is achieved by controlling a determined number of safety functions. When an incident occurs, these functions are to be controlled and if the safety systems designed to fulfill these functions do not work properly, operators must initiate contingency actions in order to take the failing systems out or bring redundant systems into operation.

Function-oriented EOPs provide operators with guidance on how to verify the adequacy of important safety functions and how to restore these functions if they are degraded.

State-oriented

In the state-oriented approach, the values of all parameters related to all safety functions are combined by logical equations that define periodically the state of the plant. For each possible state the actions to transfer the plant to a long-term safe condition are defined independently of the way this state was achieved. This has the advantage that the number of possible states, in the sense of required actions, is finite.

While event-oriented actions are based on the specific events causing the transient, the actions of symptom-, function- or state-oriented

procedures are derived from the behaviour of continuously observed safety-related plant parameters. The symptom-, function- or state-oriented procedures are very similar: they differ only on how to recognize deviations of the parameters from pre-determined safety values and on the level they are combined in accordance with the complexity of the different types of plants. For this purpose individual symptoms, safety-related functions or determined states have to be observed continuously both from the beginning of the event and also during recovery until a final long-term condition is achieved.

3.2 The different approaches in use

To obtain redundancy many utilities apply several approaches. Event-oriented procedures enable the writer to quote the most suitable actions for mitigating event consequences. However they require that the operators diagnose the specific event. State-, function- or symptom-oriented procedures on the other hand are written in a way that operators need not diagnose the event causing the emergency conditions. They cover a wide range of emergency conditions comprising events beyond the design basis of the plant, undiagnosed events, multiple failures and so on, all as far as they can be covered by the technical equipment available after an incident and during plant recovery (see example 3).

It is thus desirable to apply event-oriented procedures, quoting the optimal actions, in combination with symptom-, function- or state-oriented procedures for coping with undiagnosed or unanticipated events. However, if more than one procedure approach is applied, it then becomes necessary to solve the problem of possible contradictions between the different procedures.

In one Member State the control room operators apply event-oriented procedures while a shift technical advisor simultaneously monitors the overall safe status of the plant according to state-oriented procedures. In cases of deficiency in the event-oriented procedure, when certain state criteria are reached the shift technical advisor orders the operator to leave the event-oriented procedure and apply the state-oriented procedures.

In another country, while the main emphasis is on the optimal recovery paths of event-oriented procedures, additional symptom-oriented

procedures are being developed to monitor simultaneously the overall plant safety. In case of deviations from pre-determined limits, contingency actions are to be taken in order to return to permissible conditions.

3.3 Procedure entry

Independently of the approach used, the EOPs can be written as an integrated package which operating personnel will use after receiving any of a few pre-determined entry signals. The relation between entry signal and procedures must be clearly and uniquely defined. It is important that the relative priority of entry signals and procedures are clear in case more than one entry signal occurs simultaneously. In general, the occurrence of a reactor trip signal is considered very important. There may be other specific alarms and safety system actuation signals generated by the plant protection system that occur before or after a reactor trip signal. Operating personnel should be able to recognize and respond to the most important signals first. In recent years a variety of diagnostic aids have also been developed for use in control rooms. Entry signals used to initiate EOPs in various plant types are shown in example 4 of the annex.

When an abnormal condition occurs, the first tasks are to verify the proper response of certain plant systems and to take corrective action on possible malfunctions. These immediate actions, especially after a reactor trip, can be common for a variety of events. Thus, the procedure to be entered first should be written so that it is applicable without detailed knowledge of the initiating event. Event diagnosis or its classification within a broader class of events to the accuracy necessary for transient termination and long term recovery, is done only after the immediate response has been completed. Systematic guidance on event diagnosis or event classification has to be provided in the set of procedures.

When planning the immediate actions special attention has to be given to transients that may potentially cause further failures. Timely termination of such transients is ensured by organizing the procedures to help operating personnel identify such transients early on and to take appropriate action. In formulating EOPs consideration should also be given to the input and actions required of technical management personnel. An illustration of the involvement of the technical support group in an abnormal situation is given in example 5 of the annex.

3.4 Alternative approaches

An optimum recovery from abnormal conditions can in most cases be assured by providing a set of event-oriented procedures that are used as follow-ups to the first generally applicable procedure. Each of these procedures would apply to a situation where the initiating event belongs to a class of postulated failures and no important safety system is lost or reduced below the design basis. Procedures organized on this principle (event-oriented procedures) are shown in example 6 of the annex.

An alternative method of developing procedures would be to establish a set of procedures that are applicable for broader spectrum of events and that are meant primarily for transient termination. Such procedures may be supplemented with an additional set of procedures for long term recovery. This symptom-oriented approach is shown in example 7 of the annex.

Specific procedures should be established to assist operating personnel in the event of certain unique failures or failure combinations that are of general concern and that require procedures with a strictly limited scope. Examples of these are anticipated transients without scram (ATWS), total loss of AC power and failure combinations of relatively high probability that may result in loss of entire safety functions if not catered for properly. Such contingency procedures are entered as soon as the failure diagnosis is evident.

At all times, including recovery from abnormal conditions, operating personnel must ensure that critical safety functions of the plant are maintained or that appropriate action is taken in cases where any of these functions is threatened. Procedures for monitoring, maintaining and restoring critical safety functions must be established. Procedures related to critical safety functions should direct operating personnel to take appropriate action to protect or restore these functions without having to wait for diagnosis of the specific event. Such action need not be an optimum response but should protect or tend to restore critical safety functions until they are not threatened and until sufficient event diagnosis is complete so that optimum recovery for specific events can begin. It is for this reason that these procedures are often described as function-oriented, since they are intended to be applicable to a plant condition regardless of the event sequence that leads to that condition. One function-oriented approach to procedures is illustrated in example 8 of the annex.

The procedures related to safety functions may form a separate package that supplements the event-oriented procedures. In this case the monitoring of safety functions can be done by a person not directly involved in operation. Another possibility is to provide operating personnel with an integrated set of procedures covering both critical safety functions and event-oriented actions. Procedures should be organized so that if action is needed to restore a critical safety function the related procedure takes priority over all other procedures.

4. TECHNICAL BASES

Before the procedures can be written, it is necessary to identify all situations that must be catered for and to gather together for each one all basic information concerning the behaviour of the plant. On the basis of this information it should be possible to select the appropriate recovery method(s) and justify the choice for:

- Entry signal(s), such as alarms and actuation of certain protective systems that determine the need for implementing the EOP;

- The operational route to recovery (criteria, means and limits);

- Final plant conditions to be achieved.

As a first step in producing the basic technical information, a list of initiating events that can occur with a certain probability and lead to emergency conditions must be provided. (A list of the initiating events used as the basis of EOPs for one design of PWR is given in example 9 of the annex.) For each event a comprehensive analysis should be prepared to determine the plant behaviour and the anticipated response of safety systems. The results of these analyses should also provide information on the anticipated control room display that the operator would use in diagnosing the plant state. It should be noted that an initiating event can lead to more than one sequence of events and may require different recovery methods for different plant states. For example, the recovery method will be different after the total loss of cooling water when the plant is operating at full power from that when it is being refuelled with the vessel cover away.

In most cases a simple and qualitative analysis will permit the choice of the main recovery path for each initiating event. This should provide for the safest and most rapid recovery to the final safe plant condition. All systems and equipment required to be operable on this path have to be identified. The importance of each system and equipment is then considered to see what is the impact of its failure during the recovery process. The conclusion can be one of the following:

(1) A back-up system or equipment exists that can do the same job;
(2) Another recovery method has to be used; or
(3) The event will develop towards more severe conditions.

The alternatives 2 and 3 represent new operational paths that have to be explored in the same way as the main path. Thus for each initiating event, a number of operational paths leading either to recovery or to core damage and possible severe radiological consequences will be identified.

Some form of risk assessment may be necessary to show which recovery paths should be covered by the EOPs (i.e. to determine the scope of EOPs) and to demonstrate that the paths with unacceptable results are of extremely low probability.

After the different operational paths for an initiating event have been determined, an engineering assessment is performed to see if quantitative analyses are necessary to verify the applicability of the planned actions or to make a proper choice between alternative actions. While most of the operator actions are obvious and their consequences are readily understood, there may be operating conditions where a qualitative judgment is not sufficient. In these cases, it is necessary to provide some calculational results or simulations.

The conservative calculations called for in licensing may underestimate the capability of various systems to respond to initiating events and thus overlook some useful recovery methods. They may also cause poor perception of the accident time scale. For this reason, the calculations to support the development of operating procedures should preferably be done with realistic best-estimate models. These models must be improved each time that a real transient or accident has shown a deficiency. In such cases the calculations must be redone and, if necessary, the procedures and related technical documents revised.

In most of the cases it may be difficult to identify the ongoing event before safe action must be initiated, otherwise initial operator actions may not produce a satisfactory situation. For these situations it is necessary to define a set of safety functions that are not event-dependent but, if maintained, are sufficient to prevent core damage and radioactivity release to the environment. For each of these safety functions it is necessary to specify the main parameters that represent the status of the function and the limits beyond which it is guaranteed to perform a specific action to restore the safety function. A safety function must be sufficiently specific to permit unambiguous indication of its status and of the influence of the proposed restoration actions. On the other hand, a safety function must be general enough to have the minimum of connections with the other functions: one action performed to restore a function must have only small, if any, effect on other safety functions. Safety functions that have been suggested for LWRs are given in example 10 of the annex.

Related to each safety function the need for quantitative calculations has to be considered. These may be necessary to support the selection of limits used for status monitoring, or to indicate the capabilities and risks of the restoration actions.

All the basic information produced in developing emergency operating procedures must be recorded in a document (the technical basis document). This document will have three principal functions:

(1) A record of the choices and their justification. (It is important to establish the justification for the selected procedures in order to ensure that proposed future changes are fully considered and composed against the original choice);

(2) A basis for preparing training materials;

(3) A guide for procedure writers.

This document should also permit procedure writers readily to compare the recovery paths chosen in each procedure and consequently to unify them. In this way the number of EOPs can be reduced and the common actions in EOPs can be standardized where possible. The main and alternative recovery routes are preferably presented in the form of a logic diagram. This is illustrated in example 11 of the annex.

Modifications to a procedure should not be made without evaluating the need for and making corresponding improvements to the technical basis document.

5. PROCEDURE FORMATS

A variety of different procedure formats has been developed in Member States and there seems to be no single format that could be regarded as preferable for all types of plants. It is thought that a sufficient degree of clarity and usefulness to the operating personnel can be reached in several alternative ways. Among the possible formats are:

- Step list (see examples 12 to 13 of the annex)
- Flow chart (see example 14 of the annex)
- Block diagram (see example 15 of the annex), and
- Logic chart (see example 11 of the annex).

In most cases the emergency operations are not performed by only one operator but by a clearly defined operating team. Thus a decision has to be made if the entire team will use a common set of procedures, or if members of the team have their own specific procedures. In the case of common procedures it would be desirable to indicate the distribution of tasks between team members. The more widespread practice is to have common procedures but operator-specific procedures are also in use in some Member States. The choice preferred depends on the plant and control room layout, on the timing of required actions and on the distribution of tasks within the operating team. Example 16 illustrates the approach of one Member State in this area.

EOPs should be easily distinguished from other plant procedures. A consistent format should be used throughout, but if separate sets of procedures are written for separate operators, it may be practical to use more than one format. Each set should be consistent within itself, however. The procedure title should be short and descriptive so that operators will quickly know the abnormal condition to which it applies. The cover page should indicate the title, number, current revision and date, number of pages, approvals and any reference to the technical basis documents. Each page should identify the procedure, the page number, total number of pages and revision number. The end of the procedure should be indicated.

Explanatory information at the beginning should be avoided, except when a brief indication of scope or purpose is necessary. Explanatory information should also be avoided within the procedure. The procedures shall be limited to instructions that require the operator to carry out an action or verify plant state ("action/verification" steps) along with "warning/cautions" and only short supplementary "notes". The number of these "notes" should be kept at a minimum by appropriate training and by information given in the technical basis documents.

Long narrative paragraph style is not appropriate for procedures. The "action/verification" steps should be presented in a short, concise form in the imperative mode useful in stressful situations. One step shall either include one action only, or a group of actions that form an entity and can clearly be referred to with a common directive. Example 12 in the annex demonstrates how the "action/verification" steps can be put into a more concise format.

A standardized format should be developed for statements that are used throughout the procedures. Instructions should be made as simple as possible with consistent use of the logic words "if", "and", "or", "then", "not", "if not" and "when".

The "action/verification" steps may be presented in more than one level of detail (main steps and substeps). The main steps give directives in a general way to provide a fast comprehension of the purpose of the step. Related substeps provide more detailed guidance for performing the action mentioned in the main step. Main steps and substeps provide different levels of support as needed by operators during abnormal situations. Detailed information in substeps may be unnecessary in near-normal conditions but under stress it may improve operator performance. For easy reference and identification at least each main step should be suitably coded.

For each action given in the procedure, consideration should be given to the need for a contingency action to be taken in the event of a unsuccessful action. For example, what should be done if equipment does not respond as it should or if a parameter to be verified is not within expectations. Contingent steps should be presented in a format such that operating personnel will not have to look at them if the plant responds as expected. Thus they will not disturb smooth progress along the main recovery

path. In the case of abnormal response, contingencies will provide immediate guidance to operators. Example 13 of the annex illustrates a format that is applicable for presenting contingencies.

"Warnings/cautions" and "notes" should not include any actions. These should be presented in a format that clearly differs from the "action/ verification" steps. They should directly precede the action step for which they apply so that operators are made aware of them before taking the related action.

Words and definitions used in the procedures should be the same as those used by the operating personnel to facilitate prompt recognition and understanding during abnormal conditions. There should be consistency with their usage in training for abnormal conditions, control room labelling and other plant procedures.

In some cases it may be helpful to include spaces for operator checkoff of completed steps or for essential calculations. However, to the extent practicable, requirements to make calculations should be eliminated. Checkoff spaces should be used in a consistent manner to avoid confusion and calculations should be made simple and basic by showing the formula, including units and conversions.

Instrument values should be presented in the same units of measurement as displayed on the instrument and should be consistent with the accuracy that can be quickly determined by operators.

If the operator has to control or adjust certain parameters, it may be useful to indicate in the procedure which measurements and devices monitor the influence of the control actions. If there is a risk of erroneous or inaccurate indication, a "warning" should be provided. If the control of a safety parameter takes significant time (e.g. primary system cooldown to a certain temperature) this should be related to other steps in the recovery process.

Since abnormal conditions may require that relatively unfamiliar tasks be performed, consideration should be given to including information on the location of appropriate instruments and controls. This should not compromise training on the plant layout and this information should only be incorporated if it makes a significant contribution to operator action.

Printed and computer-driven operator aids can assist operating personnel in some situations. Such aids may be presented, for example, as decision trees, flow charts, tables and graphs. Information of this type should be presented so that it is readable and easily understood by operating personnel in the expected conditions of use. The aids should be consistent with the procedures (e.g. identical units of measurement and symbols) and should minimize the interruption to operators following the procedures. Disruption of smooth reading of action steps in the procedure may be reduced by placing aids, notes and other information on facing pages and fold-out sheets.

6. OPERATOR TRAINING FOR PROCEDURE APPLICATION

It is a fundamental requirement for nuclear power plants that a suitable standard of operator competence is achieved. Comprehensive training programmes must therefore be provided to ensure that all operators fully understand and are familiar with their operating procedures, especially for emergency conditions. To achieve this it is suggested that a technical information package drawn from the technical basis documents be prepared as a supplement to the emergency operating procedures, prior to their implementation, with the object of conveying the writer's intent to those applying the procedures. Such a technical package would serve as a training aid during classroom training of the operators and would minimize the need for explanatory notes in the actual procedures. In the following paragraphs proposals are made on the possible content of such an information package for operator training in the event-oriented operating procedures now widely used in most Member States.

A description of plant response to various types of initiating events should be given, using graphic examples incorporating the aids referred to in chapter 4. This description should be based on best-estimate calculations or on actual operating data. A few alternatives of each type of event would be helpful and should show how the plant is brought to a safe shutdown state by controlling the symptoms.

The basic recovery strategy for each type of event and its possible alternatives should be discussed. Results of calculations as well as limiting conditions and constraints involved in the alternative strategies must be given. The discussion could be supplemented with clarifying flow path diagrams.

The principles of assuring plant safety by maintaining a set of critical safety functions should be explained.

For procedure application, the logic and organization of the procedure package should be explained including the role of individual members of the operating team.

A description of individual procedures should contain a summary of recovery methods and a separate discussion of the purpose of each step. The conditions and requirements under which procedures can be modified including the required reference or possible changes to technical basis documents should be explained. It should be noted, however, that introducing new or changed procedures at operating plants can pose difficulties for the operators and care must be taken to ensure that the operators are fully trained in the new procedures before they are introduced. In addition, it is very important to maintain operating personnel confidence in the procedures. This means making sure that they understand the reasons for the changes and that the guidance given is consistent with current plant conditions and knowledge of plant behaviour.

Training manuals should be presented in a style that will meet the needs of the operating personnel and should avoid burdening them with unnecessary detailed technical justifications. The technical information shall be structured in a way that is suitable for information as well as for reference.

For optimized training in a power plant simulator a specially prepared simulator-teaching programme is necessary. Such a simulator-teaching programme should provide the instructor with all information important for simulator-education, for example:

- Programmed starting conditions;
- Short description of the approach of the simulator-training;
- Timetable of the simulator-training;
- Description of the differences between the plant and the simulator;
- Possible additional simulated failures;
- Information on particularly important points of the procedures that should be stressed during training;

- Indication, where applicable, of simulator characteristics that are insufficient for training purposes and that must be avoided in simulator training so that trainees will not be misled in their understanding of the real plant behaviour.

Although advantage can be taken from computerised simulators that incorporate full-scale control rooms in order to ensure that operating procedures are properly understood, care should be taken to avoid operators becoming too dependent on computer assistance. It is also necessary to train operators to develop and maintain their individual diagnostic capabilities. This enables them to recognize departures from normal operating conditions and the underlying causes for such departures.

Recent developments in symptom-, function-, and state-oriented procedures allow extensive coverage of all plant states. In the event of departures, they enable remedial actions to be proposed or taken to avoid any major core degradation. These procedures are used in conjunction with event-oriented procedures after an abnormal event has occurred: the event diagnosis is continuously checked against certain criteria and allows transfer to another procedure if the situation becomes untenable.

Already applied in some Member States, this approach will be introduced more widely in the year to come. The training of personnel to use emergency operating procedures may also be programmed such that event-oriented procedures are followed as a supporting aid. However, for such training, simulators which simulate nuclear power plants very closely are required to have the trainees react to critical parameters realistically and in real-time. One of the important training objectives is timely intervention. Such intervention would be based on symptom-, function-, or state-oriented procedures, and cut into on-going actions following event-oriented procedures, when the initial event diagnosis turns out to be wrong (see Annex, example 2). This underlines once more the importance of having highly qualified trainers who are thoroughly familiar with these procedures.

7. VALIDATION AND UPDATING

Once operating procedures are drafted, they should be subject to further review, and necessary revised with a view to better applicability or timely updating. The procedures must also be validated as adequate from the standpoint of technical accuracy, function and scope.

Technical validation has to prove that the guidance given in the procedures is correct and that it results in recovery as expected. The procedures should be technically sufficient for mitigating transients and accidents at the plant. They should also properly reflect the existing plant and control room design. Validation may also be based on operating experience if this is available. Other approaches include independent best-estimate calculations and validation tests using on simulators.

Functional validation has to demonstrate the compatibility of the procedures with the control room environment. For example, it must be certain that the assumed information on plant parameters is available in a useful form and that the proposed control functions are realistic (e.g. the response is neither too fast nor too slow, and that the frequency of control cycles does not pose limitations). Another point to check is that there are no time- or distance-related deficiencies that might impair the operator's ability to execute the procedures. All operator actions required by the procedures should also be within the capability of the minimum control room staff required to be available by the Technical Specifications. Decisions and actions that the procedures require from operators should be consistent with the training and experience of control room personnel. The clarity and unambiguity of the procedure format is also a subject of functional validation. It must be established that the desired responses are so clearly described that operating personnel are able to understand them promptly and to apply them correctly in stress situations. The basic methods of functional validation are control room walk-throughs and test runs on a simulator that sufficiently represents the plant in question.

Feedback from experienced operating personnel during training, control room walk-throughs and simulator training are beneficial in achieving good clarity of the procedures from the operators' perspective. Such discussions will also have a positive effect on their attitude and will improve their acceptance and confidence in the usefulness of the procedures.

Validation of scope can be done by assessing how the various recovery paths for each initiating event are represented in the procedures. Methods used in probabilistic risk assessment (PRA) of a nuclear power plant are helpful when considering completeness of the procedures. In addition, the scope can be examined by postulating multiple failures that go beyond the assumed initiating events, and assessing how the procedures would work in such more complicated cases.

Comparisons with analogous procedures used at similar nuclear plants can be beneficial in confirming the correctness of new procedures and may also reveal some omissions in them.

The procedures should be reviewed in accordance with modifications in plant systems, operational rules, safety requirements and shift crew formation.

The procedures should also be developed and updated to feed back the experience from their use in plant incidents and transients. Account should be taken of significant events on other plants, particularly those of the same type. The suitability of current procedures in coping with such events should be reviewed and updated where appropriate.

8. CONCLUSIONS

The foregoing developments in emergency operating procedures should enable operators to face any kind of event including even those resulting from situations beyond the design basis.

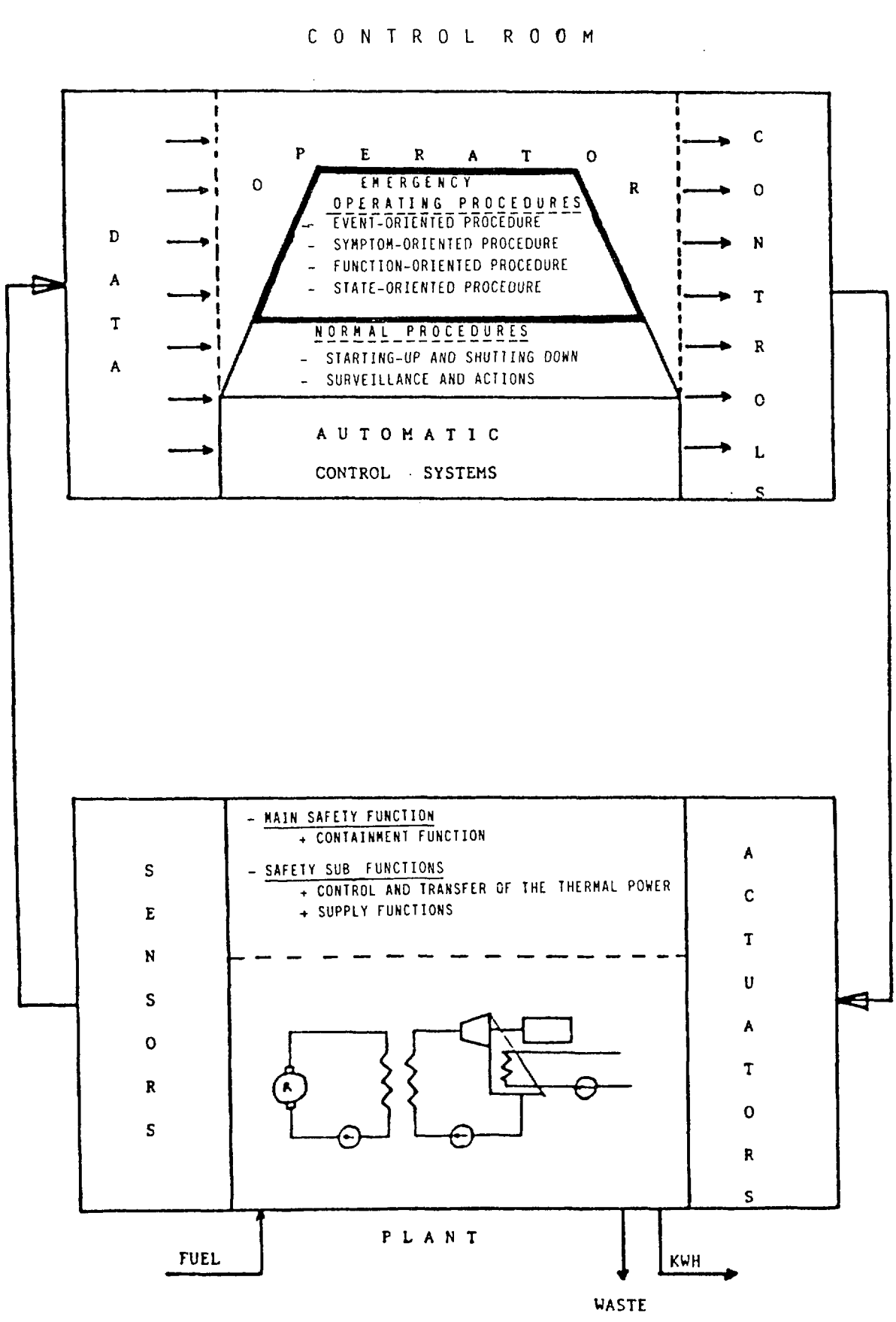
Symptom-, function-, or state-oriented procedures supplement the set of event-oriented procedures given to the operators at the very beginning of the operation of a nuclear power plant. Such moves will help bring operational safety levels of nuclear power plants closer to their optimum.

ANNEX

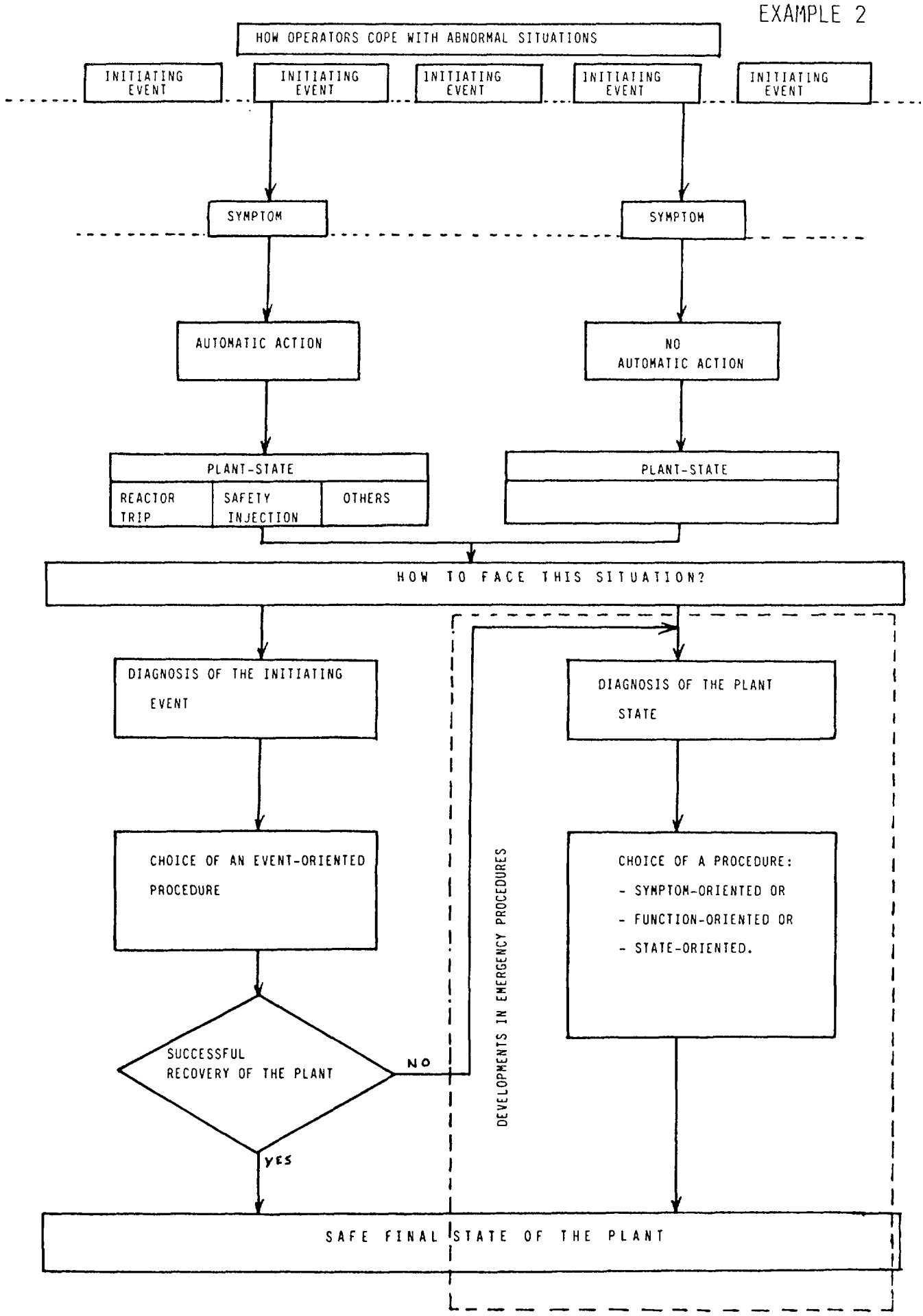
EXAMPLES ILLUSTRATING DEVELOPMENTS IN PREPARING EMERGENCY OPERATING PROCEDURES

PLANT OPERATING DIAGRAM

EXAMPLE 1



EXAMPLE 2


HOW OPERATORS COPE WITH ABNORMAL SITUATIONS
INITIATING EVENT
INITIATING EVENT
INITIATING EVENT
INITIATING EVENT
INITIATING EVENT
SYMPTOM
SYMPTOM
AUTOMATIC ACTION
NO AUTOMATIC ACTION
PLANT-STATE
REACTOR TRIP
SAFETY INJECTION
OTHERS
PLANT-STATE
HOW TO FACE THIS SITUATION?
DIAGNOSIS OF THE INITIATING EVENT
DIAGNOSIS OF THE PLANT STATE
CHOICE OF AN EVENT-ORIENTED PROCEDURE
CHOICE OF A PROCEDURE:
- SYMPTOM-ORIENTED OR
- FUNCTION-ORIENTED OR
- STATE-ORIENTED.
SUCCESSFUL RECOVERY OF THE PLANT
NO
YES
DEVELOPMENTS IN EMERGENCY PROCEDURES
SAFE FINAL STATE OF THE PLANT

ORGANIZATIONAL REQUIREMENTS FOR SUPPLEMENTING EVENT-ORIENTED EMERGENCY OPERATING PROCEDURES WITH A SET OF OPERATIONAL SAFETY-ORIENTED PROCEDURES

(symptom-oriented, function-oriented or state-oriented procedures)

In one possible approach for supplementing the set of event-oriented emergency operating procedures by a set of symptom-oriented or function-oriented or state-oriented emergency operating procedures, the objectives are to:

- define criteria that would enable the operator to diganose proper or improper execution of the safety functions;
- make an inventory of the plant resources for ensuring safety functions and to verify their availability at all times;
- assess the capability of the safety functions for maintaining the plant in a long-term safe state;
- propose compensating actions when a safety function is not available.

This type of approach requires a detailed knowledge of how the plant operates and how the operational safety is to be assured. A group of plant-operating experts with such a professional background, could easily conduct a study, which should only take into account the overall safety objectives and the plant as it is designed or built.

The resources required could be as follows:

- 6 to 8 experts
- 4 to 6 periodical meetings to discuss the objectives and write the safety procedures.

The conclusions of the work would be one or more safety-oriented procedures written with the aim of being useful to operators when coping with any kind of event including those beyond the design basis.

These procedures should be given to the operators in the control room as soon as possible. Nevertheless, these reflections could also reveal that further improvements affecting either the plant operating organization or the plant design could make the emergency operation easier.

If they are recommended by the expert group, an accurate assessment of the cost-benefit of such improvements should be carried out in order to enable operators to make decisions in the case of the particular nuclear power plant. This task goes outside of the terms of reference of the working group and should therefore be entrusted either to the designer (for significant technical improvements) or to the operating organization (for organization improvements).

ENTRY SIGNALS FOR INITIATING EOPs FOR LWRs

A. PWR

The initial diagnosis for one PWR type is done by hard wired electronic logics and the entry signal to procedures is given by a lighted signal lamp. The logic trees are cross-connected to permit only one signal lamp to be lighted at a time. The following signal lights, each indicating an entry to an event-specific procedure, are used:

1. Reactor coolant system leakages

   - Small primary leakage
   - Medium primary leakage
   - Large primary leakage
   - Stuck-open pressurizer safety or relief valves

2. Secondary line breaks

   A total of 20 entry signals will lead to 11 procedures depending on the leak location and possible additional sequence failures (e.g. leak in main steam line at steam generator 3 inside containment plus additional steam generator tube rupture).

3. Steam generator tube ruptures (SGTR)

   - SGTR without additional disturbances
   - SGTR and additional disturbances (e.g. loss of off-site electrical connections; spurious safety injection; loss of steam dump station)
   - SGTR during start-up or cool-down without initiation of automatic measures (4 entry signals due to 4 steam generators)

B. PWR

The main entry signal for another PWR type is the reactor trip and the same procedure is always used as the entry procedure. A side entry directly to the steam generator tube rupture procedure is made if high radiation is detected in a steam line before reactor trip. Also in this case the operator goes back to reactor trip procedures as soon as reactor trip occurs (if the trip does not occur automatically the operators actuate it from small power level after a controlled power runback).

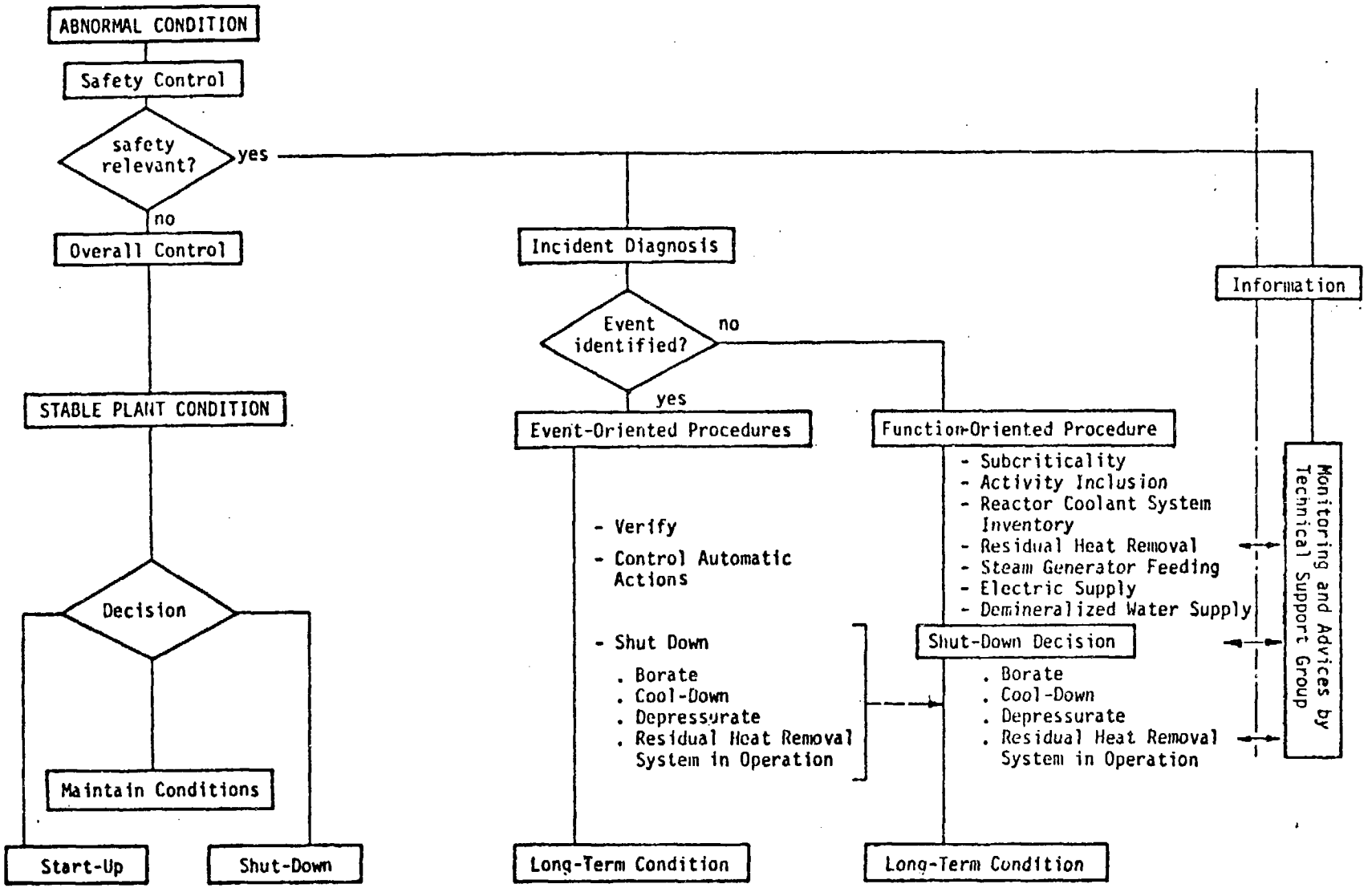
C. PWR

In a third PWR type, the events actuating the Safety Injection System have a common entry procedure. This procedure includes advice for event diagnosis and guides the operator to appropriate event -specific procedures for final recovery. The other events that do not actuate safety injection need to be diagnosed before a direct entry to the event-specific procedure can be made. The list of event-specific procedures is the same as the list of initiating events presented in example 9.

D. BWR

The plant protection signals in one BWR type are grouped in chains. Each chain includes the signals that are most probably received after a certain initiating event. If the plant protection system actuates some safety functions, a lamp indicates which chain has tripped and the operator engages the respective procedures. In many transients more than one chain may trip. In such cases the operator enters the procedure that appears first on the following list of chains:

- High-energy line break inside the containment;
- Steam-line break outside the containment;
- A leak outside the containment in rooms containing reactor auxiliary systems;
- Loss of feedwater;
- A leak outside the containment in rooms containing engineered safety systems;
- Reactor trip.



The involvement of the Control Room and the Technical Support Group in Abnormal Conditions

EVENT-ORIENTED PROCEDURES FOR ONE TYPE OF PWR

The following set of procedures aims at providing optimum recovery.

1. Reactor trip of safety injection (SI) - the common entry procedure:
2. Reactor trip recovery;
3. Natural circulation cooldown;
4. SI termination following spurious SI;
5. Loss of reactor coolant, supplemented with subprocedures for:
   - SI termination following loss of reactor coolant;
   - Post-LOCA (loss of coolant accident) cooldown and depressurization;
   - Transfer to cold leg circulation, following loss of reactor coolant;
   - Transfer of hot leg recirculation;
6. Loss of secondary coolant, supplemented with subprocedures for:
   - SI termination following loss of secondary coolant;
   - Transfer to cold leg recirculation following loss of secondary coolant;
7. Steam generator tube rupture (SGTR), supplemented with subprocedures for:
   - SI termination following SGTR;
   - Alternate SGTR Cooldown;
   - SGTR with secondary depressurization;
8. Anticipated transients without scram;
9. Loss of all AC power recovery without SI required;
10. Loss of all AC power recovery with SI required;
11. SGTR contingencies covering multiple tube ruptures in single steam generator (SG) and single tube ruptures in more than one SG.

SYMPTOM-ORIENTED PROCEDURES WRITTEN FOR ONE TYPE OF PWR

The following example of symptom-oriented procedures was written for one PWR type. The aim of this set is to provide timely termination of the initial transient.

- Immediate actions and vital system status verification after reactor trip (the main entry procedure);
- Treatment of lack of adequate subcooling margin;
- Treatment of lack of primary-to-secondary heat transfer in either steam generator;
- Treatment of too much primary-to-secondary heat transfer;
- Steam generator tube rupture.

After the plant has been stabilized using one or more of the above procedures (one at the time in the order given, as required by the indicated symptoms), long-term recovery is started using one of the alternative cooldown procedures. The procedures to be used is defined on the basis of the plant state after transient termination.

FUNCTION-ORIENTED PROCEDURES

There is one main safety function:

- Containment function (radioactive products confinement)

There are several safety subfunctions, for example:

- subcriticality
- primary pressure
- core cooling
- coolant inventory
- heat sink
- auxiliary functions as electrical supplies, cooling water, compressed air, (which are considered as necessary means for carrying out the main safety function).

One of the operators (or other persons not involved in actual plant operation) continously montiors the plant status using performance aids called critical safety function status trees. Only one status tree is used at a time. If the conclusion made on the basis of a tree is that the safety function is not under challenge, monitoring continues with the next tree. A new monitoring cycle is started immediately after all trees have been scanned. If some safety function is lost or threatened, the operator is guided to an applicable safety function restoration procedure. For each safety function there is more than one restoration procedure, depending on the type and severity of the possible challenge. When the operation is started on the basis of the selected restoration guideline, any other operations based on an event-specific recovery procedure are terminated (if any have been underway). After the safety function has been restored, a new diagnosis of the event is made and operation is continued with an event specific procedure. This procedure may or may not be the same as that used before going into the restoration proecedure.

EXAMPLES OF INITIATING EVENTS USED AS THE BASES OF EOPS FOR ONE DESIGN OF PWR

	IN DESIGN SITUATIONS
INCIDENTAL CONDITIONS	Loss of main off-site electrical connection; Loss of all off-site electrical connection; Loss of all off-site electrical connections and one diesel generator; Loss of all AC power; Loss of one DC power train (each safety-related train considered separately);
ACCIDENTAL CONDITIONS	Small break LOCA; Large break LOCA; Secondary line break outside the containment; Secondary line break inside the containment, resulting in primary system cooling; Secondary line break inside the containment, not resulting in primary system cooling; Steam generator tube rupture; Failed-open pressurizer relief or safety valve; LOCA when residual heat temoval system is in operation; Abnormal boron dilution;

	OUT OF DESIGN SITUATIONS
EMERGENCY CONDITIONS	Loss of compressed air system; Loss of all cooling water (ultimate heat sink); Loss of all water for steam generators. Loss of all electrical supply (offsite and diesel generator)

SAFETY FUNCTIONS SUGGESTED FOR NUCLEAR POWER PLANTS

MAIN SAFETY FUNCTION

- Containment function·

  - to confine radioactive products inside the barriers in order to prevent any significant release

SAFETY SUB FUNCTIONS

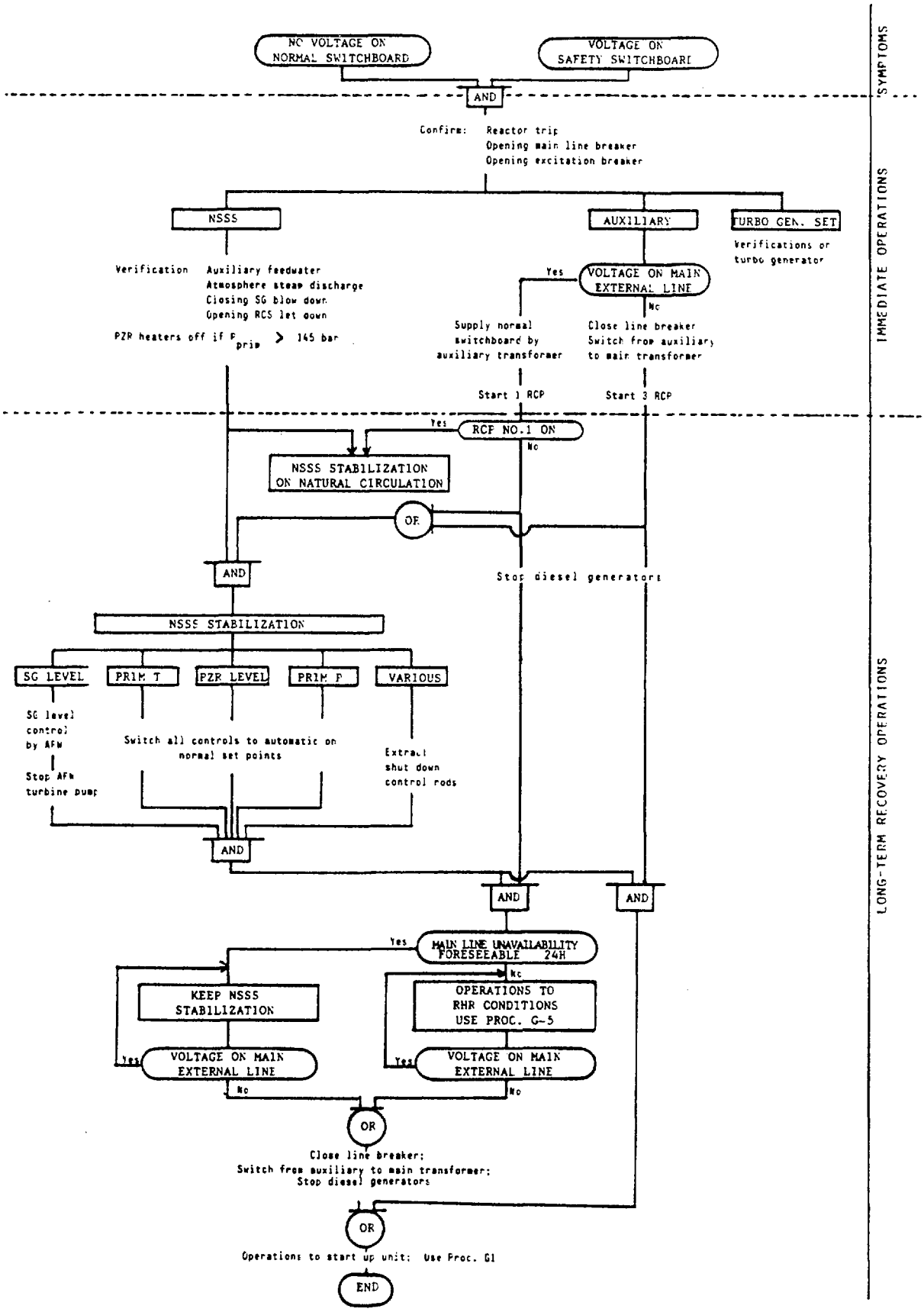
- Control and transfer of power from the core to the environment through the barriers

  - subcriticality
  - coolant inventory
  - primary pressure
  - heat sink

- Supply functions (sources)

  - off-site electrical supply
  - on-site electrical supply
  - cooling water from sea, river, cooling towers
  - compressed air

LOGIC DIAGRAM FOR RECOVERY ROUTES FOLLOWING LOSS OF MAIN POWER SUPPLY



HOW TO IMPROVE A STEP LIST FORMAT

A. Example of poor format

"25. IF all of the symptoms a through c are met and when the following d through g are exhibited:

d. Reactor coolant pressure is greater than 2000 psig and increasing AND

e. Pressurizer water level is greater than programmed no load water level AND

f. The reactor coolant indicated subcooling is greater than (insert plant-specific value which is the sum of the errors for the temperature measurement system used, and the pressure measurement system translated into temperature using the saturation table) AND

g. Auxiliary feedwater flow of at least (insert plant-specific value derived from method in Appredices B to E-0) gpm is injected into the steam generators OR indicated wide range water level in at least one steam generator is above the top of the steam generator U-tubes.

26. THEN

h. Reset safety injection and stop safety injection pumps not needed for normal charging and RCP seal injection flow."

The same information can be given in an improved format as follows:

B. Example of an improved format providing the same information

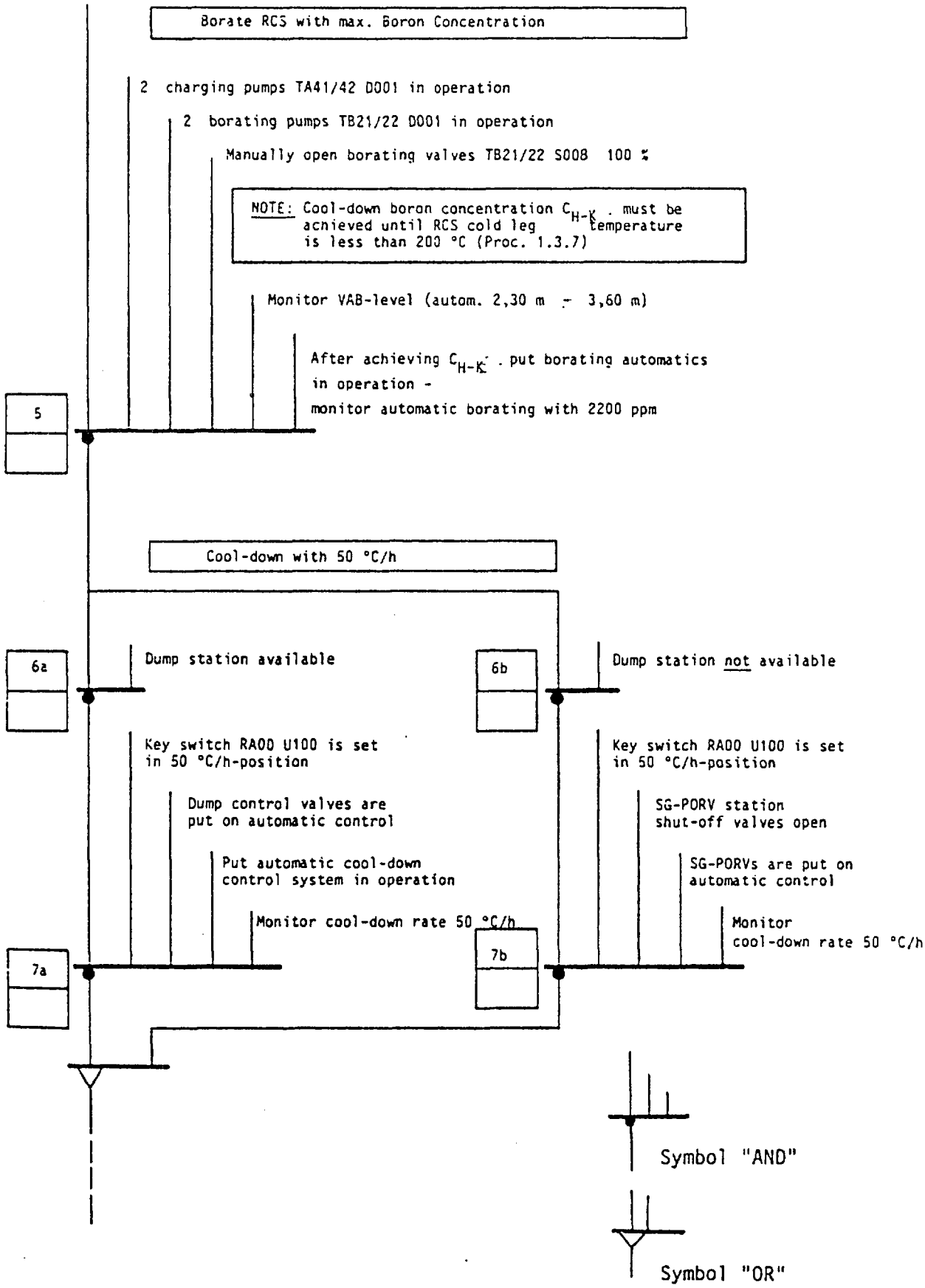
ACTION/EXPECTED RESPONSE	RESPONSE NOT OBTAINED
25. Check if SI can be terminated	25.
a. RCS pressure - GREATER THAN 2000 PSIG AND INCREASING	a. DO NOT TERMINATE SI. Go to step 27.
b. Pressurizing level - GREATER THAN (1) %	b. DO NOT TERMINATE SI. Go to step 27.
c. RCS subcooling - GREATER THAN (2) ^{o}F	c. DO NOT TERMINATE SI. Go to step 27.
d. Secondary heat sink: 1. Total AFW flow to non-faulted steam generators GREATER THAN (3) GPM OR 2. Wide range level in at least one non-faulted steam generator - greater than (4) %	d. IF neither condition is satisfied, THEN DO NOT TERMINATE SI. Go to step 27.
26. Terminate SI:	
a. Go to ES-0. 3, SI TERMINATION FOLLOWING SPURIOUS SI.	

Inclusion of contingency actions in step list format

If the plant responds as expected, the operator proceeds down the left hand column and does not look at the steps on the right. If the response in some steps on the left is not as expected, the operator takes the actions described in the corresponding step of the right hand column.

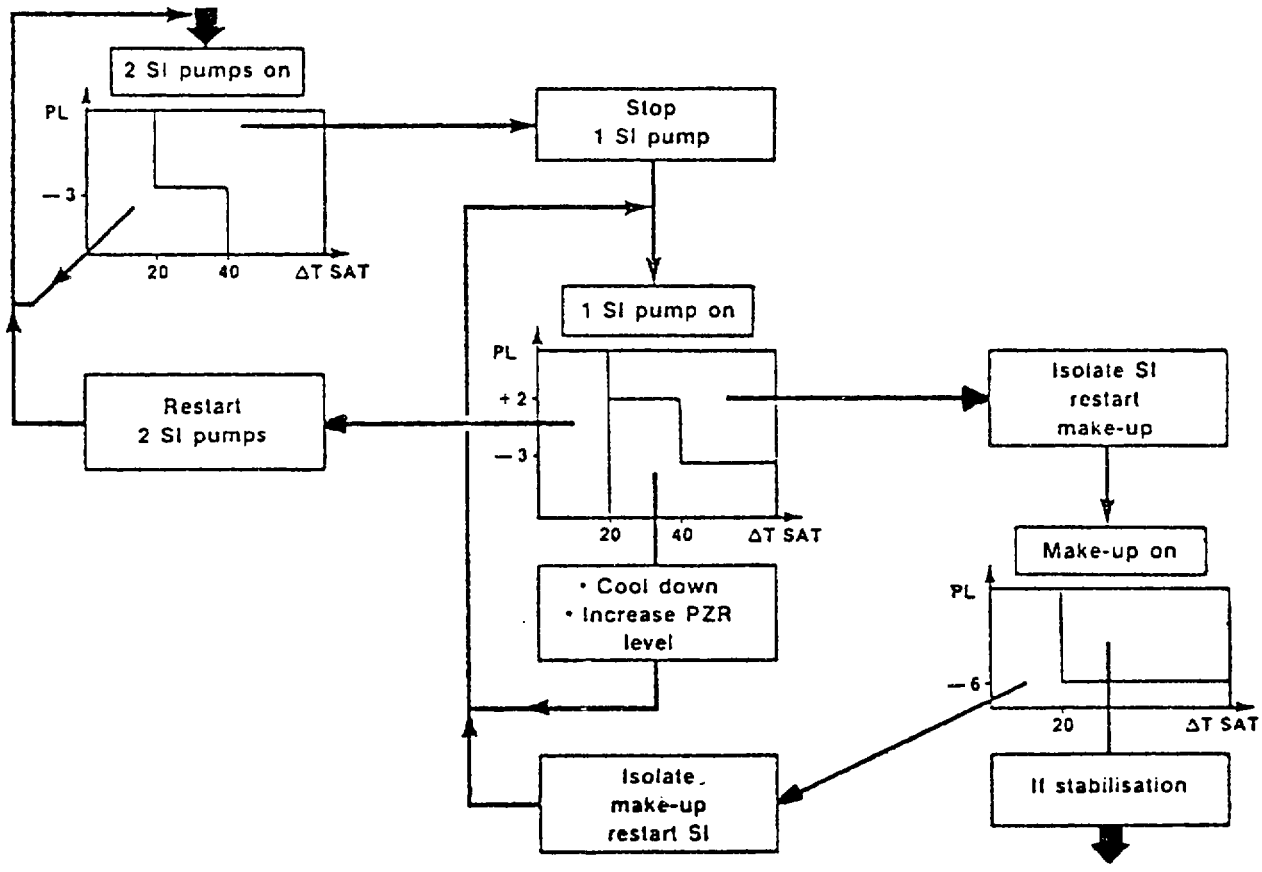
ACTIONS/VERIFICATIONS	CONTINGENCY ACTIONS
5.4 Check RPV water level: a. above 13 in	5.4 IF RPV water level cannot be maintained above 13 inches, THEN go to E-40, "Level Control".
5.5 Monitor containment parameters every 5 minutes a. Pool temp. 70-95°F b. Pool level 22-24 ft c. Drywell temp. 70-95°F d. Drywell press. 0.5 - 1.69 psig	5.5 IF any containment parameters gets outside its normal range, THEN follow E-20, "Containment Control."

Using flow charts for procedure formats



Examples of block diagrams for procedure formats

PWR

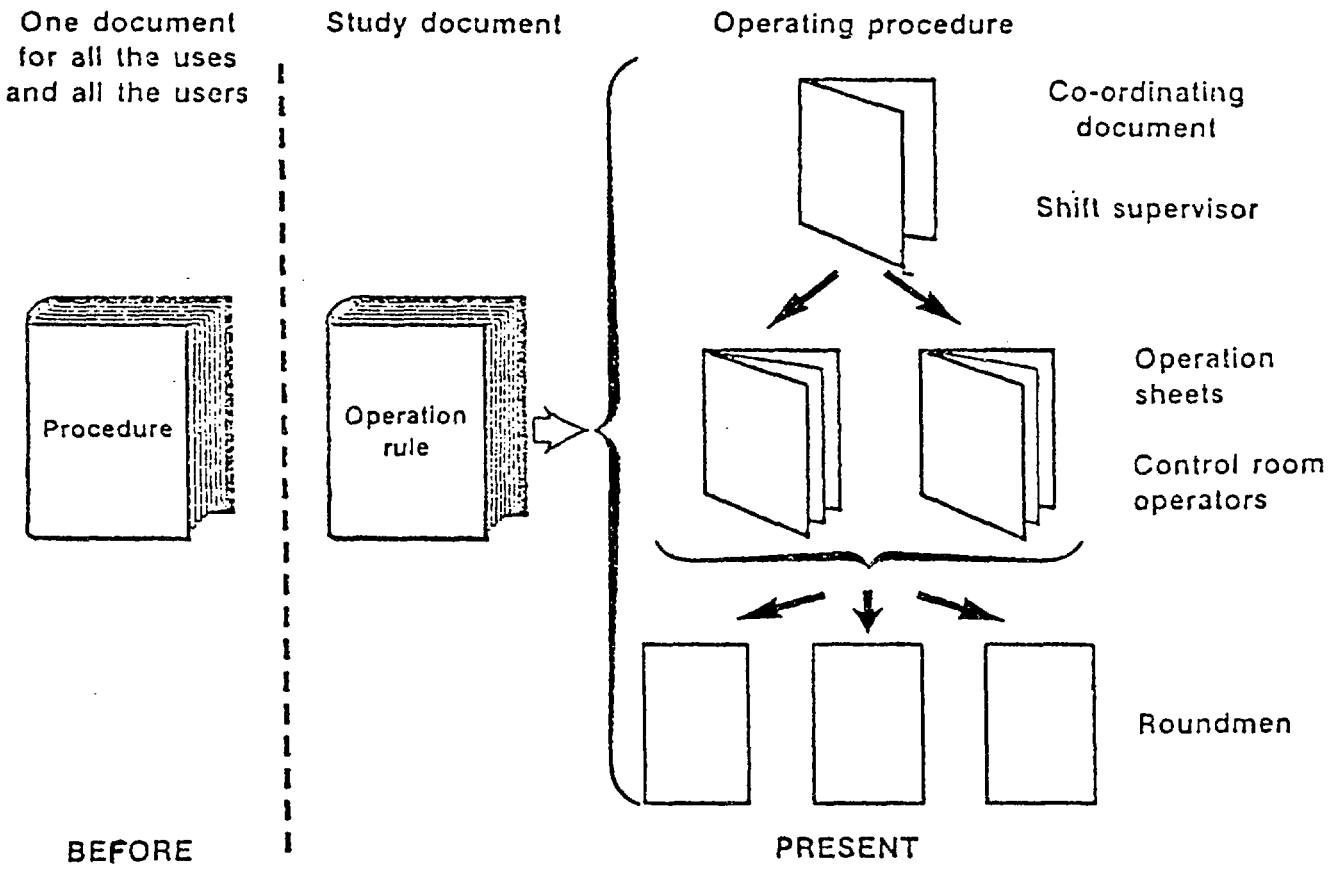


PL = Pressurizer level

SI = Safety injection

PZR = Pressurizer

The procedure elaboration used in one Member State



REFERENCES

The following documents provided by consultants and Technical Committee members were considered in the preparation of this document.

Provided by Technical Committee Members:

Butragueno, J.L.: Operating Procedures for Abnormal Conditions in the Spanish Nuclear Power Plants

Laaksonen, J.: Operating Procedures for Abnormal Conditions in Finnish Nuclear Power Plants

Marcille, R.: Improvement of Operating Procedures for Abnormal Conditions PWR Steam Supply Systems

Nadkarny, G.V.: Operating Procedures for Abnormal Conditions; A Brief Review on Present Practice in Indian Nuclear Power Stations

Ross, W.M.: Operating Procedures for Abnormal Conditions; Brief Review of the Position in United Kingdom

Other materials referred to:

Appell, B., Marcille, R. and Perrin, B.: Amelioration de la Conduite et de la Surveillance des Chaudiers PWR en Situation Post Accidentelle, IAEA-SM-265/45, Munich, 11-15 October 1982

Kelly, J.J. and Williams, D.H.: Abnormal Transient Operating Procedures for Nuclear Power Plants, paper presented to American Power Conference, Chicago, 27-29 April 1981

Summary of Westinghouse Owner's Group Emergency Response Guideline Program Private Communication 1982

Sureau, H. and Mesnage J.: Physical State Approach to PWR Emergency Operating Procedures: Recent Developments in France, ANS/ENS meeting in Karlsruhe, September 1984.

LIST OF PARTICIPANTS, CONSULTANTS AND CONTRIBUTORS

Consultants Meeting on Operating Procedures for Abnormal Conditions, October 1982

FINLAND	J. Laaksonen, Institute of Radiation Protection
FRANCE	R. Marcille, Electricité de France
GERMANY, FED. REP. of	H. Mayer, Rheinisch-Westfälische Elektrizitätswerke
UNITED STATES OF AMERICA	C.D. Wilkinson, Institute of Nuclear Power Operation

Technical Committee on Operating Procedures for Abnormal Conditions, 7-11 March 1983

BULGARIA	G. Stefanov, Nuclear Power Station Kozloduy
FINLAND	J. Laaksonen, Institute of Radiation Protection
FRANCE	R. Marcille, Electricité de France
GERMANY, FED. REP. of	H. Mayer, Rheinisch-Westfälische Elektrizitätswerke
INDIA	G.V. Nadkarny, Rajasthan Atomic Power Station
SPAIN	J.L. Butragueno, Consejo de Seguridad Nuclear
UNITED KINGDOM	S. Gronow*, HM Nuclear Installations Inspectorate
	W. Ross, HM Nuclear Installations Inspectorate
COMMISSION OF THE EUROPEAN COMMUNITIES	G. Mancini
IAEA	A.P. Vuorinen, Scientific Secretary

Consultants Meeting on Operating Procedures for Abnormal Conditions, 26-30 November 1984

FINLAND	A. Piirto, Teollisuuden Voima Osakeyhtio
FRANCE	H. Sureau, Electricité de France, SEPTEN
GERMANY, FED. REP. OF	H. Mayer, Rheinisch-Westfälische Elektrizitätswerke
JAPAN	A. Higashi, Japan Atomic Power Co. Ltd.
IAEA	P.A. Bliselius, Scientific Secretary
	B. Thomas

* Chairman