Safety Reports Series

No. 48

# Development and Review of Plant Specific Emergency Operating Procedures

IAEA
International Atomic Energy Agency

# IAEA SAFETY RELATED PUBLICATIONS

## IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (i.e. all these areas of safety). The publication categories in the series are **Safety Fundamentals, Safety Requirements** and **Safety Guides**.

Safety standards are coded according to their coverage: nuclear safety (NS), radiation safety (RS), transport safety (TS), waste safety (WS) and general safety (GS).

Information on the IAEA's safety standards programme is available at the IAEA Internet site

http://www-ns.iaea.org/standards/

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at P.O. Box 100, A-1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by e-mail to Official.Mail@iaea.org.

## OTHER SAFETY RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued in other publications series, in particular the **Safety Reports Series**. Safety Reports provide practical examples and detailed methods that can be used in support of the safety standards. Other IAEA series of safety related publications are the **Provision for the Application of Safety Standards Series**, the **Radiological Assessment Reports Series** and the International Nuclear Safety Group's **INSAG Series**. The IAEA also issues reports on radiological accidents and other special publications.

Safety related publications are also issued in the **Technical Reports Series**, the **IAEA-TECDOC Series**, the **Training Course Series** and the **IAEA Services Series**, and as **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. Security related publications are issued in the **IAEA Nuclear Security Series**.

# DEVELOPMENT AND REVIEW OF PLANT SPECIFIC EMERGENCY OPERATING PROCEDURES

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BANGLADESH
BELARUS
BELGIUM
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MOROCCO
MYANMAR
NAMIBIA
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
PAKISTAN
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA AND MONTENEGRO
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

SAFETY REPORTS SERIES No. 48

# DEVELOPMENT AND REVIEW OF PLANT SPECIFIC EMERGENCY OPERATING PROCEDURES

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2006

# COPYRIGHT NOTICE



Sales and Promotion Unit, Publishing Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna
Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
http://www.iaea.org/books



Printed by the IAEA in Austria
February 2006
STI/PUB/1226

**IAEA Library Cataloguing in Publication Data**

Development and review of plant specific emergency operating procedures. — Vienna : International Atomic Energy Agency, 2006.
p. ; 24 cm. — (Safety reports series, ISSN 1020–6450 ; no. 48)
STI/PUB/1226
ISBN 92–0–103705-8
Includes bibliographical references.

1. Nuclear power plants — Accidents. 2. Nuclear power plants — Safety measures. 3. Emergency management. I. International Atomic Energy Agency. II. Series.

IAEAL 06-00425

# FOREWORD

Emergency operating procedures (EOPs) are essential for maintaining fundamental safety functions and preventing core damage during design basis accidents and beyond design basis accidents in a nuclear power plant. Many plants are presently in the process of improving their EOPs. The level of implementation of such updates varies from plant to plant, from the preparatory phase up to fully implemented and validated sets of procedures. Therefore, drawing on international experience will be helpful in the development and implementation of EOPs in individual plants as well as for the independent review of EOPs.

The topic of EOPs has been addressed in a number of IAEA safety publications, including the revised IAEA Safety Standards Series, in particular safety requirements on the operation of nuclear power plants, operational limits and conditions, and operating procedures. These publications can be partially used as a basis for the development and review of EOPs. However, it was felt that a manual that would comprehensively cover all aspects of the implementation and review of EOP development programmes, that would rely on state of the art experience and that would be applicable to various reactor technologies, was needed. This need was further justified because several Member States were organizing IAEA missions and workshops to discuss and review the completeness and quality of their EOPs. The proposal to develop a corresponding reference publication was also supported at several IAEA workshops organized on this topic.

This publication discusses the elements and key steps that must be included in any programme for the development and implementation of plant specific EOPs. Its objective is to provide guidance and serve as a reference for teams of experts in charge of developing or reviewing EOPs at specific plants. The IAEA officer responsible for this publication was J. Mišák of the Division of Nuclear Installation Safety.

## *EDITORIAL NOTE*

*Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.*

*The use 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 names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.*

# CONTENTS

# 1. INTRODUCTION

## 1.1. BACKGROUND

One of the basic safety principles for nuclear power plants, as stated in Ref. [1], is that "Emergency operating procedures are established, documented and approved to provide a basis for suitable operator response to abnormal events". According to the same publication, emergency operating procedures[1] (EOPs) are an important component of the defence in depth concept for nuclear power plant operation. Consequently, EOPs can be viewed as an additional line of defence, after plant design, in preventing core damage as a result of unplanned transients.

Emergency operating procedures are also addressed in the IAEA Safety Standards Series. Paragraph 5.11 of Ref. [2] states inter alia that:

> "Operating procedures shall be developed which apply comprehensively for normal, abnormal and emergency conditions…The guidance provided in the procedures shall be clear, concise, and as far as possible verified and validated…Strict adherence to written operating procedures shall be an essential element of safety policy at the plant".

Paragraph 5.12 states that

> "Either event based or symptom based procedures shall be developed for abnormal conditions and design basis accidents. Emergency operating procedures or guidance for managing severe accidents (beyond the design basis) shall be developed".[2]

More specific information can be found in Ref. [3].
Paragraph 4.39 of Ref. [4] states that:

---

[1] Emergency operating procedures: plant specific procedures containing instructions for operating staff to implement preventive measures for managing accidents. Emergency operating procedures typically contain all preventive measures for both design basis accidents and beyond design basis accidents up to the point of core damage.

[2] Symptom based procedure/guideline: a procedure or guideline containing actions which are taken depending on the values of directly measurable plant parameters. A symptom is a measurable plant parameter that is available to the operator in the control room.

"For [nuclear power plants] …arrangements shall be made for mitigatory action by the operator to prevent an escalation of the threat, to return the facility to a safe and stable state, to reduce the potential for releases of radioactive material or exposures and to mitigate the consequences of any actual releases or exposures. These arrangements shall take into account the following aspects of the response to mitigate the consequences of a nuclear or radiological emergency: the operational actions necessary; the operational information needs; the workload and conditions of the operational staff (such as in the control room); the responder actions necessary in the facility; the conditions in the facility in which responder actions are necessary; and the response of the personnel, instrumentation and systems of the facility under emergency conditions. Arrangements shall include emergency operating procedures and guidance for the operator on mitigatory action for severe conditions, for the full range of postulated emergencies, including accidents beyond the design basis."

Emergency operating procedures have been discussed in a number of IAEA publications. In 1985, the IAEA issued IAEA-TECDOC-341[3], which provided guidance, based on the experience available at that time, on the scope, technical basis, organization and format of such procedures. More recently, in December 1998, the IAEA published IAEA-TECDOC-1058 [5], which was directed at nuclear power plant managers and covered good practices in the development and use of all kinds of nuclear power plant procedures. IAEA-TECDOC-1058 also partially dealt with some of the characteristics of EOPs. The role of EOPs in the framework of broader accident management programmes[4] (AMPs), that are designed to manage nuclear power plant accidents beyond the design basis, was described in Technical Reports Series No. 368 [6], published in 1994, and in its follow-up [7].

In the past, certain Member States invited IAEA missions to review the completeness and quality of EOPs. Several workshops were also organized on the subject of developing EOPs. In particular, participants of the IAEA Regional Workshop on Development and Validation of EOPs, held in Brno, Czech Republic, from 3 to 7 April 2000, recommended that a technical

[3] Developments in the Preparation of Operating Procedures for Emergency Conditions of NPPs, IAEA-TECDOC-341, IAEA, Vienna (1985) (out of print).

[4] An AMP comprises plans and actions undertaken to ensure that the plant and its personnel with responsibilities for accident management are adequately prepared to take effective on-site actions to prevent or mitigate the consequences of an accident.

document be prepared that would be devoted to the development, validation[5] and implementation of EOPs. It was further requested that this document provide guidance for both the developers and the reviewers of EOPs.

The IAEA Operational Safety Review Team (OSART) guidelines[6] provide some guidance on the review of EOPs. However, because the scope of an OSART review is very broad, dealing with all aspects of nuclear power plant construction and operation, these guidelines provide only very general guidance for EOPs.

## 1.2. OBJECTIVE AND SCOPE

As mentioned previously, several earlier IAEA nuclear safety publications have partially discussed EOPs and can be used as a basis for reviewing EOPs. However the present publication, which relies on state of the art experience, is intended to comprehensively discuss all aspects of the development, implementation and review of plant specific EOPs for all reactor technologies. Included in the discussion are the limitations and expectations inherent in the review process and the importance of the advance preparatory work. This publication is intended to serve as a reference for IAEA teams of experts in charge of the development or review of EOPs, or for plant managers and operational staff at specific nuclear power plants.

Consistent with the above objectives, this publication reviews all the elements, and especially the practical aspects, that must be considered in any plant specific EOP development programme. This publication is based on best international practices in the field of emergency operation, as well as on specific lessons from various programmes that have been successfully completed at nuclear power plants around the world. This publication reflects a variety of possible approaches, and the material presented therefore provides

---

[5] Validation: the process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation is broader in scope, and may involve a greater element of judgement than verification. EOP validation: the objective of EOP validation is to determine if control room operators can manage emergency conditions in the plant using the EOPs. This can be done by evaluating the EOPs with regard to the validation principles of usability and operational correctness. The usability is the provision of sufficient information understandable to the operator and operational correctness is the EOPs, compatibility with the plant response, plant hardware and the shift manpower.

[6] OSART Guidelines, 1994 Edition, IAEA-TECDOC-744, IAEA, Vienna (1994) (out of print).

general guidance. Flexibility concerning the proposed details will be necessary in order to reflect and adapt the programme to the specific context, background, conditions and constraints that prevail for any particular EOP development project.

Several 'standard' or 'reference' systems for EOPs have been developed by various groups of nuclear power plants, utilities and reactor designers around the world. This publication establishes that these are not 'portable' as such to all nuclear power plants. The type of reactor technology, the operational culture and staff organizations of the plant are examples of major elements that need to be considered when choosing among these systems.

There are two categories of review:

(1) Those that focus on assessing the status of an ongoing programme and provide recommendations for improvement or completion;
(2) Those that focus on providing a review — technical and administrative — of the final plant specific EOPs and possibly provide recommendations for improvements.

The present publication can also be used by a nuclear regulatory body as a basis for developing specific criteria for review/approval of a set of EOPs. However, it should not be seen as a prescriptive guide for developing or reviewing EOPs for a nuclear power plant.

## 1.3. STRUCTURE

Section 2 introduces the terminology of EOPs and explains the basic concepts and specific meanings as they are used throughout this publication. The details of the steps (tasks) necessary to develop or upgrade EOPs and those that are required for successful implementation of EOPs at an individual plant are discussed in Section 3. Section 4 provides general guidance for the review of EOPs. It addresses the formal steps in organizing a review and provides general guidance for important review areas. A reference checklist, which contains a set of questions to be considered by reviewers, is given in Appendix I. An outline of representative EOP reference systems is provided in Appendix II, describing six different systems for various reactor designs.

# 2. BASIC CONCEPTS OF EOPS

The word 'emergency' is used in many different contexts and different areas of human activity. In Ref. [4] emergency is defined in part as "A non-routine situation or event that necessitates prompt action primarily to mitigate a hazard or adverse consequences for human health and safety, quality of life, property or the environment". In IAEA safety assessment publications the following terms have been established for identification of different operational states and accident conditions of a nuclear power plant: normal operation, anticipated operational occurrences (AOOs) (abnormal operation), design basis accidents (DBAs), beyond design basis accidents (BDBAs) and severe accidents.

The development of terminology in the area of operational support introduced the terms emergency operation, EOP, emergency plan and severe accident guideline (SAG).[7] These terms are generally applied in a context that is worth some discussion. For example, even though a fire at a nuclear power plant would trigger the execution of an emergency plan with intervention of the fire brigade, as long as there are no serious consequences to the plant's operational status the event would not be considered to be an emergency operation and generally would not be covered by the EOPs. However, were the fire to impact plant operation or affect the operability of standby emergency equipment it would then be considered to be an emergency operation and appropriate emergency operating procedures would be needed to cope with the situation. Furthermore, it must be recognized that any conditions that would warrant the use of EOPs would be classified as an emergency (Ref. [4], para. 4.19) and would trigger a predetermined emergency response at the site. This may in turn place additional responsibilities on the control room staff.

To establish a common understanding of the terminology associated with the development and use of EOPs, a clarification of the basic concepts is provided in the following sections. A specific and detailed definition of EOPs will be presented, consistent with international practice and with their common usage in the nuclear industry.

---

[7] Severe accident guidelines: a set of guidelines containing instructions for actions in the framework of severe accident management. Severe accident management: the goals of severe accident management are: (a) to terminate core damage once it has started; (b) to maintain the capability of the containment as long as is possible; (c) to minimize on-site and off-site releases and (d) to return the plant to a controlled safe state.

This section also contains a discussion of issues related to the use of EOPs from the perspective of nuclear power plant staff (mainly operators). These human related issues play a major role and need to be clarified and resolved very early in the development project because they impact the reliability of operators and consequently the effectiveness of the EOPs. The coverage of plant operational modes by the EOP package is another general topic that will be briefly discussed in this section.

## 2.1. PLANT OPERATIONAL STATES AND PROCEDURAL GUIDANCE

### 2.1.1. Abnormal operation

Normal operation is defined as plant operation within specified operational limits and conditions. Examples include starting up and shutting down the plant, normal power operation, shutdown, maintenance, testing and refuelling.

Abnormal operation or AOO is an off-normal operational state which, because of appropriate design provisions, would most likely not cause any significant damage to items important to safety nor lead to accident conditions. In abnormal operation the plant is in a situation that represents a potential threat to the integrity of the reactor core but which can be handled by the normal control systems if there are no additional failures. Examples of abnormal operation events include loss of normal electrical power and faults such as a turbine trip, malfunction of individual components of a normally running plant, failure to function of individual items of control equipment, and loss of power to the main coolant pump (MCP). In some of the above events the reactor is tripped in order to quickly re-establish the equilibrium heat production/heat removal and to support the normal control systems in achieving a safe state. Normally, in simple cases of abnormal operating conditions (malfunctions), the operators will not need much guidance or support. Generally, they should implement an appropriate alarm response procedure, if available. Otherwise they have to use their own knowledge of the plant and its systems and identify/correct the malfunction using the skills they have gained through their regular training. For the control room operators malfunctions typically require a short term response, even if further repairs or fixes from field operators are needed. It is important that even such minor events are subsequently analysed with a conservative and questioning attitude.

There are more serious abnormal operating conditions when the operators face a malfunction or fault in one of the normal core cooling systems

or in a support system. This would normally result in a more complex operating condition, since such events impact the operation of more than one system or component. However, in some cases the direct effects of the malfunction or fault can be compensated for by the normally operating plant systems without the need to trip the reactor and/or actuation of safety systems. The operating documents, available to the operators to support their actions in such an operating condition, are termed abnormal operating procedures (AOPs). At most plants the AOPs are entirely event based procedures. However, some plants have developed a consistent, integrated set of interdependent procedures to cover events of all levels of severity.

### 2.1.2. Accidents

In IAEA publications, e.g. in Ref. [8], accident conditions are defined as deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents, beyond design basis accidents and severe accidents. Examples of such deviations include loss of coolant accidents (LOCAs), complete loss of residual heat removal from the core, and anticipated transient without scram.

The scope of the EOPs is to provide the procedural guidance for operators to deal with accident conditions up to the point of core damage. Thus the EOPs generally provide actions for a wide spectrum of operating conditions, ranging from abnormal operation up to accidents far exceeding the design basis of the nuclear power plant.

It is important to recognize that the operators will have to deal with very unusual situations, use systems they are less familiar with, and possibly face unexpected plant behaviour they have not experienced. In these situations the operators need reliable procedural support to adequately respond to the complex and stressful situations and identify and take the appropriate actions.

It is also important to keep in mind that a given plant event often evolves over time and crosses the borders between the different categories of operating conditions and corresponding operating documents. A typical example would be an unexpected transient or malfunction that degrades and evolves into a more serious or challenging condition. This is why it is very important to give proper attention to the interface or transition between individual groups of procedures (AOPs, EOPs and SAGs) and to ensure a strict level of consistency. An example of such a strictly defined interface (transition between AOPs and EOPs) is the entry condition into EOPs, reactor trip or emergency core cooling system (ECCS) actuation.

### 2.1.3. Severe accidents

Severe accident conditions are defined as accident conditions involving significant core degradation. Severe accident conditions begin when significant fuel damage occurs or is anticipated. This corresponds to the significant loss of integrity of the first barriers against the release of fission products (the fuel matrix and the cladding).

From the perspective of EOPs another definition would be to say that severe accident conditions occur when the provisions and guidance of the EOPs are no longer effective in preventing core damage. This second definition is more practical as it relates to the transition between EOPs and SAGs.

Generally, the major differences between EOPs and SAGs are the objectives (priorities) and the level of procedural guidance. The EOPs concentrate on protecting core integrity (i.e. prevention of core damage). It is only after this fails and core damage occurs or is imminent that the SAGs focus on maintaining other barriers for public protection, typically the containment/confinement and to a certain extent the coolant system boundaries (i.e. mitigation of consequences). This shift in priorities is one of the reasons why the SAGs are not normally incorporated as part of the EOPs, but constitute a totally separate set of tools. It is important to ensure that the SAGs for a specific plant adequately complement the EOPs by looking at the scope of coverage of these two categories of documents. For each reactor type, a concerted effort should be made to identify the transition between the EOPs and SAGs and clearly determine the scope of the EOPs. Reference [7] discusses all the important issues related to the development of EOPs and SAGs and their incorporation into the overall accident management plan in a nuclear power plant.

The EOPs represent one particular set of procedures in the entire spectrum of plant operating procedures. An example of a typical hierarchy of plant procedures for various operating conditions is given in Fig. 1, taken from Ref. [5].

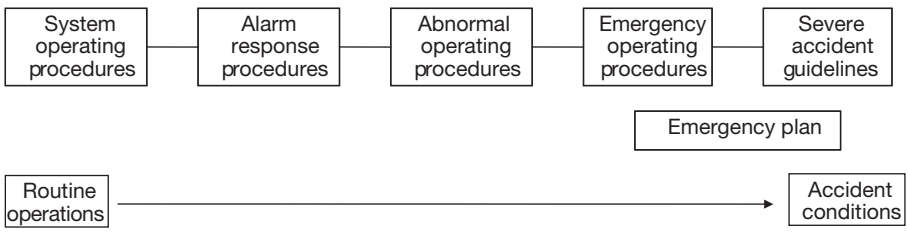



*FIG. 1. Hierarchy of plant procedures for various operating conditions.*

## 2.2. EOP TERMINOLOGY

The intention of the following discussion is to focus on some terms that are often subject to confusion:

(a) Scenario dependent/scenario independent approach;
(b) Event based procedures;[8]
(c) Symptom/state based procedures.

The objective is to establish a common understanding of these terms as they are used in the present publication while applying, as much as possible, the established terminology.

### 2.2.1. Scenario dependent/scenario independent approach

Scenario dependent procedure is a general term applicable to any event based (i.e. event specific) procedure. These procedures are developed and optimized to respond to a specific event or category of events, as would typically be the case for design basis accidents. It should be noted that the event specificity applies to individual procedures within the EOP package.

One of the primary characteristics of the scenario dependent procedures is that they are focused on minimizing the consequences to plant systems resulting from the specific event or accident, and they focus the operators' actions on the most effective means of minimizing the consequences of the event, restoring or isolating the affected systems and bringing the plant to a stable condition.

Scenario independent procedures do not handle any specific event or group of events. The need for such procedures follows from realistic anticipation of situations in which the operator is not able to identify the event or misdiagnoses the event (as occurred during the Three Mile Island (TMI) accident) and, consequently, a scenario dependent type of procedure is not suitable. While the objective of scenario dependent procedures is to provide the operator with instructions to recover from a certain event or accident, the primary objective of scenario independent procedures is to make sure that all the safety barriers remain intact. This objective is achieved by taking actions that ensure continuous monitoring/diagnosis of the status of all plant barriers

[8] Event based procedure: a procedure that contains actions which are appropriate only for a specific accident sequence (or set of sequences), which must be diagnosed before applying the procedure. An event based procedure may or may not be symptom based.

and providing for their protection/recovery independently of the development of the initial event. For this purpose the general concept of a set of safety functions has been applied, where any specific safety function is the representation of safety margins of the respective barrier.

The general method for developing these scenario independent procedures includes:

(a) Identification of the different barriers against radioactive releases (RRs), for PWRs typically the fuel cladding, the reactor vessel and primary coolant system boundaries and the containment/confinement);
(b) Identification of the possible challenges to each of these barriers;
(c) Definition of a set of plant specific safety functions that are representative of the status/safety margins of each of the barriers;
(d) Development of a tool — flow diagram, procedure, electronic system — to continuously monitor the status and challenges to each of the safety functions;
(e) Preparation of scenario independent procedures providing strategies for restoring any safety function if challenged.

### 2.2.2. Event based procedures

Historically, the first sets of emergency procedures used at nuclear power plants before TMI consisted entirely of event based procedures. This means that all the procedures in the package were scenario dependent. Behind any set of event based procedures is a triple initial assumption that:

(a) The event that occurs is one among a well defined set of anticipated events (usually limited to the list of DBAs for that plant);
(b) The operator recognizes (identifies) which particular event is actually going on;
(c) The event will evolve in a certain predetermined way and follow a well known and well defined sequence (typically obtained from a thermal-hydraulic analysis of that presupposed event).

The advantage of this approach is that the procedures are highly efficient for an initiating event included in the selected set of events and the linear (sequential) structure corresponding to the usual way of thinking. Typically, these event based procedures are descriptive and instruct the operator to proceed in a single series of steps without providing any contingencies to deal with additional dependent or independent failures. One of the characteristics of these event based procedures is that they focus the operator's attention on

those specific parameters and controls associated with the particular event being corrected or mitigated and they generally do not direct the operator to assess overall plant status by reviewing various plant parameters beyond those associated with the particular event. A diagnosis is made only at the beginning of the accident in order to select the most appropriate procedure.

### 2.2.3. Symptom/state based procedures

Procedures which use plant symptoms/states for the operator to diagnose the actual status of the plant are termed symptom/state based procedures. The concepts of symptoms/states have been introduced in order to respond to the need for reliable and continuous plant diagnosis. The operators in the control room monitor the evolution of the accident by means of the major plant symptoms/states:

(a) Symptoms are defined as one or more measurable plant parameters that are available to the operator in the control room;
(b) States are defined as sets of measurable plant parameters that are available to the operator in the control room.

In modern EOP packages the following implicit assumptions are applied in order to better reflect actual events:

(a) The event that occurs is not necessarily one from a limited predefined list, and in particular can be a combination of accidents (the scope of coverage of the EOP guidance should be documented);
(b) The event evolves in a way that might be very different from what an event analysis would predict, either because of other event(s) or equipment failures occurring later in the accident history, or because of operator errors;
(c) The EOPs should be the tool for the operator to diagnose and recognize the possibly very complex event by providing directly measurable diagnosis criteria that are checked on a continuous or repetitive basis (at a certain minimum frequency).

The advantage of these EOP packages is continuous or repetitive diagnosis, which helps to correct any initial misdiagnosis and to ensure that the operators respond to changing plant conditions that could be more threatening to the core integrity than the initial event. Experience indicates that events can also evolve differently than predicted by pure analysis because they can evolve into a combination of events and operator errors over time.

Symptom/state based EOP packages generally contain both scenario independent and scenario dependent procedures. However some consist almost entirely of scenario independent procedures. The operators are guided through an assessment of the overall status of the plant by focusing on a predetermined set of safety functions. Based on the status or state of those safety functions they are directed to use specific procedures within the EOP package to restore a safety function if it is degraded, or to correct or mitigate the event or events. The aspects governing the split between the scenario dependent and scenario independent part of the procedures in the EOP package are discussed in more detail in Section 3. Table 1 shows the current implementation status of EOPs in IAEA Member States.

## 2.3. HUMAN ASPECTS OF EOP DEVELOPMENT AND IMPLEMENTATION

### 2.3.1. Format of EOPs

The procedural guidance to the operators also involves deciding on the format of the new EOPs. The format has been shown to affect the reliability of the control room team in upset situations. This has been the subject of many studies in the past. Different EOP formats are commonly used in the world: one column (mostly used for abnormal procedures), two column (flow chart, etc.), and the selection between them should be based on factors like:

(a) Quality of the support documents (colours, diagrams, use of various ergonomic concepts, etc.);
(b) Cultural influences on the operator;
(c) Format of the other operating documents, etc.

Examples of various EOP formats are provided in Refs [9, 10].

In order to ensure consistency between all the procedures within the full set of EOPs it is recommended that a writer's guide be prepared to more fully describe the format and content of the procedures, transitions between the procedures and the exit from the EOPs. The writer's guide, along with a user's guide, should be developed prior to preparing the set of EOPs. These two documents will describe the scope of the EOPs and establish the overall guidelines for the preparation and maintenance of the EOPs.

### 2.3.2. Operator versus safety system logic

Nuclear power plants are provided with a series of automatic systems, in particular in the field of reactor protection and other safety systems. Many of these systems were designed to mitigate design basis events and may not be optimized for lesser events. Therefore, it may be necessary to override or modify the automatic safety functions as part of the EOPs. If it does become necessary to override or modify safety functions as part of the EOP actions the following administrative rules are recommended:

(1) The operator should be prevented from overriding any automatic protection during normal operation;
(2) In order to allow control of the safety systems by the operator the automatic logic should be provided with a hardware override capability, available in the control room;
(3) In order to prevent undesired or abusive use of these override features they should be locked during normal operation, with the key in a remote location (still in the control room, however) and unlocked only on explicit EOP instructions;
(4) An additional administrative control should be placed on the key, such as restricting access to the key to the unit or shift supervisor, or requiring that the unit or shift supervisor specifically authorize overriding of any automatic protection provided this will not be counterproductive (i.e. it should not be time consuming);
(5) Any intervention in the automatic logic by the operators during the accident situation is permitted only as a result of EOP instructions, which have been appropriately justified during the development, verification and validation of the EOPs. [9]

[9] Verification: the process of determining whether the quality or performance of a product or service is as stated, as intended or as required. Verification is closely related to quality assurance and quality control. It is the evaluation performed to confirm the correctness of a written procedure or guideline to ensure that technical and human factor concerns have been properly incorporated. EOP verification: The objective of EOP verification is to determine that consistency has been maintained between the EOPs and the EOP source documents. Consistency is determined by verification principles of written correctness and technical accuracy. Written correctness ensures that information is incorporated as specified by administrative guidance. Technical accuracy ensures proper incorporation of generic and plant specific technical information.

TABLE 1. EXAMPLES OF STRUCTURES FOR OPERATING PROCEDURES IN IAEA MEMBER STATES

| IAEA | | | Practice | | | | | |
|---|---|---|---|---|---|---|---|---|
| Plant status | Strategy | Procedures | According to Ref. [6] | USA | France | Germany | Rest of Europe and South Africa | WWERs [a] |
| Normal | Prevent unsafe condition | Written and authorized instructions | Normal Event based | Normal Event based | Normal Event based | Normal Event based | Normal Event based | Normal Event based |
| Anticipated operational occurrences | Verify normal control system functions to limit transients | Incident system instructions | Abnormal Event based | Abnormal Event based | Abnormal Event based + state based or generalized state approach | Abnormal Event based | Abnormal Event based or symptom based | Abnormal Event based or symptom based |
| DBAs (safety functions challenged) | Verify functions of engineered safety features | EOPs aimed at going to cold shutdown | EOPs Symptom based | EOPs Symptom based | EOPs State based or generalized state approach | EOPs Symptom based | EOPs Symptom based | EOPs[b] Symptom based |
| BDBAs (design basis barriers challenged) Prevention of degraded core conditions | Restore critical safety functions (CSFs) | Function restoration | AMP/ EOPs Symptom based | EOPs Symptom based | EOPs State based or generalized state approach | EOPs Symptom based | EOPs Symptom based | EOPs Symptom based |

TABLE 1. EXAMPLES OF STRUCTURES FOR OPERATING PROCEDURES IN IAEA MEMBER STATES (cont.)

| IAEA | | | | Practice | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Plant status | | Strategy | Procedures | According to Ref. [6] | USA | France | Germany | Rest of Europe and South Africa | WWERs [a] |
| Severe accidents (reactor core degraded) | Mitigation of degraded core conditions | Mitigate consequences of degraded core | Mitigation actions | AMP/ SAGs Symptom based | SAMG Symptom based | GIAG Symptom system based | | AMG Symptom based | SAMG[c] Symptom based SAM[d] |

[a] Some symptom based EOP programmes are still ongoing.
[b] Loviisa has an ongoing programme to develop state based EOPs.
[c] Some SAMG development programmes in Central Europe.
[d] Implemented SAMs in the Loviisa nuclear power plant.

### 2.3.3. Level of computerization

There are three possible options regarding the computerization of EOP usage in the control room:

(1) Full paper EOPs, no computerization;
(2) Stand-alone computerized EOPs;
(3) On-line computerized EOPs.

The paper version is the easiest to develop and requires the least investment. The EOPs then fully rely on the operator properly reading and understanding the procedures and the plant information displayed in the control room during actual use of the EOPs. The common consensus is that modern full paper EOPs provide for adequate support and computerization is not necessary to improve safety.

A stand-alone computerized version does not bring much advantage compared to the paper version. The operator is still in charge of reading and understanding the EOPs on the computer and of collecting the necessary plant information. Such EOPs can possibly improve navigation within the package, e.g. support the transitions from one part of the package to another. For instance going to another procedure could be done through a hypertext link. In the same way, some transitions that violate the rules of EOP usage could be made impossible. Most important, calling the continuous diagnostic page could be faster and some additional help could be provided in monitoring the execution of continuous steps (steps/actions that have to be performed as soon as specific conditions are satisfied). Altogether, the advantages are considered limited and trained operators should perform similarly with the paper version.

The next level is on-line computerized EOPs. This level is achieved by coupling the computerized EOPs and the plant process computer. This level of computerization can markedly affect the use of the EOPs. The integration of the EOPs and the plant computer can be more or less advanced.

The on-line computerized EOPs represent progress compared to the two other versions, mainly in that they greatly facilitate the handling of the continuous steps and continuous diagnostic, and contribute to decreasing operator errors or delays which are the major constraints of writing/using time independent EOPs. Reminders can be built into the system that appear whenever a condition of continuous automatic action appears, as well as for conditions of continuous diagnostic. From a safety perspective, the EOP screen can include a continuous display of each safety function status and thus alleviate the burden on the control room staff.

However, in deciding on the extent of computerization of the EOPs, care should be taken to properly reflect the control room organization and decision making and the degree of computerization already used in the control room. Computerization of the EOPs can also affect team organization in the control room.

Considerations of computerization of the EOPs should also take into account that a full paper set of EOPs must be available as a backup in case of unavailability of the computer system in the control room or if access to the control room, the emergency control room or the safety panels is denied. The existence of several versions of EOPs also creates additional requirements for the training of operators.

### 2.3.4. Role and attitudes of the control room staff

Paragraph 4.7 of Ref. [4] states inter alia:

> "For [nuclear power plants] … the transition from normal to emergency operations shall be clearly defined and shall be effectively made without jeopardizing safety. The responsibilities of everyone who would be on the site in an emergency shall be designated as part of the transition. It shall be ensured that the transition to the emergency response and the performance of initial response actions do not impair the ability of the operational staff (such as the control room staff) to follow the procedures needed for safe operations and for taking mitigatory actions."

To ensure the reliability of the control room staff it is recommended that clearly defined roles and responsibilities be assigned to all members of the team in charge of controlling or mitigating the accident situation. The early assignment of roles and responsibilities is a prerequisite to starting the development of EOPs, primarily in cases where the procedures used by different members of the team are different or when additional members are added to the control room team to aid in performing the EOPs. This must be done recognizing that, at the time the EOPs are used, an emergency will have been declared which may trigger a redefinition of roles and responsibilities (under the emergency organization) and may assign additional tasks to the control room staff. Thus the additional workload, new responsibilities, revised organizational structure and added stress during an emergency situation should be taken into consideration.

Embarking on a new EOP development project, therefore, may require redefinition of roles, addition of control room crew members (e.g. a safety engineer if there was none before) and clear identification of the interfaces with other nuclear power plant support entities, e.g. a technical support centre

(TSC). All of these items should be distinctly specified in the user's guide. The early involvement of safety authorities in the discussion may be useful.

Another relevant aspect is the attitude of the control room crew towards the new procedures, specifically in cases in which they apply a different philosophy from the original one. It is important that the operators have confidence in the procedures and consider them primarily as their support. Experience indicates that the acceptance of new EOPs is generally more natural and obvious for newer, less experienced operators who are being trained for the first time on these documents, than for experienced operators who are very familiar with the philosophy of the previous EOP package. Acceptance of new procedures is also greater if the change has been initiated or promoted by the operators themselves. It should be noted that the confidence of the control room personnel is highly dependent on the quality of the background documentation (analyses), training (theoretical and practical) and mainly on the drills on plant simulators which are conducted under conditions that realistically simulate those during an emergency.[10]

There are several ways of promoting the acceptance of new EOPs. One of the best is having the operators be actively involved in the development of the procedures. There are several benefits attached to this approach. In addition to the improved attitudes, the operators gain better knowledge, expertise and understanding of the EOPs and their backgrounds than they would ever gain through formal training programmes.

## 2.4. EOP COVERAGE OF PLANT MODES[11]

EOP packages generally do not cover operational modes other than normal power operation. However, it is also necessary to provide EOP guidance for other operational modes, including unit startup and shutdown, and during various shutdown and outage conditions. It has been demonstrated by several shutdown and low power probabilistic safety analysis (PSA) studies that the contribution to overall risk of these plant operational modes is

[10] Simulator: a computer based assembly of software and hardware which is capable of presenting the physical behaviour of the whole nuclear power plant or part of it during various operational states and malfunctions. Simulators are typically equipped with an advanced user interface (graphic or hardware interface) suitable for interactive operation and particularly suitable for training purposes.

[11] Plant modes: operating conditions as defined in the technical specifications of the plant such as normal power operation, hot shutdown, cold shutdown, cold shutdown with the primary system open and refuelling.

comparable to the risks associated with normal power operation. Therefore, development of specific shutdown EOPs is the next logical step in the evolution of EOPs.

Shutdown operations present several unique features that require special attention:

(a) Abnormal operation (incidents) detection is more difficult due to the inhibition of most of the automatic protection signals and the high number of alarms normally activated in a shutdown mode;
(b) The risk of incidents is increased due to human error during maintenance and periodic tests performed during shutdown;
(c) The unavailability of systems due to maintenance must be taken into account;
(d) The set of available instrumentation can be limited;
(e) Shutdown modes are unusual for operators, thus increasing the chance for human error;
(f) Some specific initiators have to be considered (e.g. loss of residual heat removal);
(g) Manual actions can be required within a short period of time due to lack of automatic protection signals (out of plant design).

Even if the time of operation in shutdown condition is limited as compared with power operation, the unavailability of many important systems and/or protections represents a challenge for safety. Improvement of mitigation for accidents occurring during shutdown conditions is an important contribution to the reduction of core melt probability.

# 3. DEVELOPMENT OF PLANT SPECIFIC EOPS

## 3.1. STRATEGIC ASPECTS

This section sets forth an EOP development plan that should be fulfilled before the start of the actual writing of any guidelines or plant specific procedures. It also contains a discussion of the role of the regulatory body and the required supporting role of the utility. The following sections provide guidance on how to produce a consistent package of technically correct plant specific EOPs.

### 3.1.1. Basic EOP principles

Strategic decisions on the principles to be applied in the EOP development/upgrade programme involve the items listed below. The basis for these decisions has been discussed in Section 2. The recommended state of the art approach is as follows:

(a) EOPs should be symptom based or state based;
(b) EOPs should be consistent with the design basis of the plant. EOPs may impact the final safety analysis report (FSAR), limits and conditions/ technical specifications and other safety documents, since the scope of EOPs extends from expected plant transients to BDBAs;
(c) EOPs should cope with all possible accident situations and provide guidance for a wide variety of equipment failures and operator errors.

Examples of other decisions to be made in the development of EOPs include the following:

(1) The role of EOPs within the plant procedure set, including procedures for abnormal operation;
(2) Initial plant conditions (power mode, shutdown modes, etc.) and the final state (e.g. safe conditions at the exit of the EOPs);
(3) Approach to possible plant hardware modifications that could be identified during the development/implementation of new procedures (enhancement of instrumentation and control (I&C), modifications of control systems, qualification of certain equipment, etc.);
(4) Shift organization (role and responsibility of each operator and how they work together);
(5) EOP organization (only one EOP for the supervisor or one EOP for each operator);
(6) EOP ergonomics (EOP format, EOP support, etc.);
(7) Organizational responsibilities after declaration of an emergency;
(8) Control room workload after declaration of an emergency;
(9) Instrument response under accident conditions;
(10) Hazardous conditions within the plant that may be present during application of the EOP.

Documentation of these decisions is recommended for inclusion in the EOP's technical basis documents. This will also satisfy quality assurance (QA) and facilitate future reviews.

### 3.1.2. General approach to EOP development

There are two possible approaches to apply in the development of a set of plant specific EOPs, evolutionary and reference/generic. The evolutionary approach consists of developing a new and original set of EOPs. Implementation of this approach would start by reviewing state of the art international practices and standards. This will necessitate development and documentation of every element of the EOP package on a plant specific basis. Application of this approach at the nuclear power plant level would be a demanding undertaking requiring considerable development efforts and analytical support.

The reference/generic approach makes use of existing EOP packages. This approach will require fewer 'first-of-a-kind' studies. This approach is easier when a reference/generic system exists for a similar reactor technology. In general, this approach is the most time efficient and economical.

The reference/generic EOP development method includes development of the following plant specific components of the EOP package (based on a reference package):

(a) Defined symptom/state based entry conditions;
(b) Plant stabilization following reactor trip;
(c) Initial diagnosis;
(d) Event or state based recovery procedures;
(e) Integrated event based or state based continuous diagnosis;
(f) Monitoring and recovery of safety functions;
(g) Contingency procedures to re-establish vital systems and recovery systems;
(h) Instrument response under accident conditions;
(i) Hazardous conditions within the plant present, under which on-site emergency workers may be required to take response actions associated with the application of the EOPs.

Appendix II presents a description of various reference EOP packages.

### 3.1.3. Scope of the EOP

One of the first tasks is to define the scope of the new EOPs. This encompasses two related decisions: should the EOPs only apply to power operation or to both power operation and shutdown conditions, and what should the relationship of the EOP to AOPs and to SAGs be. Once these

decisions are made the outcome will be a documented basis for the scope of coverage.

Depending on the previous decisions, the set of EOPs should cover the following:

(a) Postulated DBAs;
(b) Abnormal situations with the potential of leading to accidents;
(c) Some BDBAs (combination of accidents, time evolving accidents, operator errors, etc.);
(d) Situations that cannot be clearly diagnosed;
(e) Challenges to a safety function ensuring overall safety of the plant, etc.;
(f) Multiple simultaneous failures;
(g) Continuous diagnosis;
(h) Shutdown accidents (if not already covered by DBAs).

The EOP project might then include separate, but interfacing procedure sets covering all plant initial modes and having clear interfaces with AOPs and SAGs. Different sources of information can be used for definition and justification of the scope of the EOP. Examples of sources typically available at each nuclear power plant are:

(1) FSARs and other sources of analyses representing the sound engineering approach, based on the understanding of plant behaviour in accident conditions, that provide the minimum scope of EOP coverage.
(2) Regulatory body requirements: In defining the scope of the EOPs the safety authorities may also be a source of input since they may elect to impose specific scenarios.
(3) Operating experience: This source results from a thorough review of the operational feedback from experience collected by the nuclear industry worldwide and application of engineering judgement. All pertinent events should be evaluated in the definition of the scope of EOPs. Examples include:
    — High frequency of incidents due to maintenance errors during power/shutdown operation;
    — Major accidents, not limited to the specific reactor type (e.g. post-Chernobyl boron dilution concerns for PWRs);
    — Feedback from the Mihama event (which led to improvements in the management of small primary to secondary leaks);
    — Lessons learned from the Rovno steam generator (SG) collector accident (an optimized procedure was needed to cover this BDBA).

(4) PSA: Probabilistic techniques can be applied in the determination of the EOP's scope. Although deciding on the EOP's scope, as previously described, is better than limiting the guidance to just DBAs it is still deterministic in nature and remains too arbitrary. A method of avoiding this is the application of probabilistic techniques. In general, when the decision on the scope of EOPs is made (based on plant specific probabilistic reasoning), it should be made on the cut-off probability for events to be covered only in the scenario independent part of the EOP package. Typically, the acceptable cut-off frequency is $10^{-6}$–$10^{-8}$ per reactor-year. The final choice of the cut-off probability should be made in agreement with the regulatory body.

### 3.1.4. Role of the regulatory body

The position and role of the regulatory body in the EOP development and implementation project should be clarified as early as possible. Normally its function is to ensure that the EOPs provide the plant operators with reasonable, prudent and effective guidance. In performing this mission it will probably review various aspects of the EOP's development and implementation. These reviews might include the EOP's technical bases document, verification, validation and training programmes. The regulatory body will in many cases need to provide approval of the new EOPs before they are put into service. It is reasonable to create an atmosphere of mutual co-operation (consensus on the requirements and specific features of the EOPs) and understanding between the utility and the regulatory body, thus reducing the probability of disruptions later on.

In the case of sophisticated EOP concepts it may be necessary for the plant/utility to provide the regulatory body's experts with theoretical training to enhance technical discussions. This is especially important if an EOP reference system is being applied and the nuclear power plant is not able to present all the details of the development of the reference EOP package.

Some of the topics that should be discussed with the regulatory body are:

(a) Basic principles to be applied in EOP development: Strategic decisions on the basic principles of the yet to be developed EOPs may include aspects that will be of interest to the regulatory body. For instance, these strategic decisions may interfere with existing documents and/or regulatory policies.
(b) Scope to be covered: In general, when the decision on the scope of EOPs is taken (based on plant specific probabilistic arguments) the discussion may concentrate on the cut-off probability of scenarios that will be

covered in the scenario independent part of the EOP package. As stated previously, the acceptable cut-off probability is $10^{-6}$–$10^{-8}$ per reactor-year, but it should be established in agreement with the regulatory body.

(c) Assignment of priority to operator actions versus safety systems logic circuits: This major issue has a direct impact on the philosophy of the EOPs and may be limiting when applying a specific EOP reference system. It may be necessary to discuss the priority issue with safety authorities and possibly revise the legal administrative requirements.

(d) Licensing: Licensing requirements vary between countries. For example, one country's regulatory body might require approval at each step of the process while another country's regulatory body only requires consensus on the basic principles.

### 3.1.5. Role of the utility

A nuclear power plant embarking on an EOP project will need significant utility support during all phases of the EOP's development and implementation. The utility's support role is crucial because an EOP project is labour intensive, requires specialists and financial support and lasts for a number of years. Management should be fully committed to and supportive of EOP development and implementation because of the increase in operational safety that can be realized.

Once it has been implemented the nuclear power plant should be able to handle the responsibility of updating the EOPs with all plant specific changes, as well as continually retraining the operators on their use. A cost effective way to ensure that EOPs stay current with the industry is to support the formation of, and/or a continuing attendance of, an 'EOP working group'. These EOP working groups are normally formed on the basis of similar reactor types.

## 3.2. EOP PROJECT ARRANGEMENTS

### 3.2.1. Team organization

Development of EOPs requires knowledge and abilities in several disciplines. Since EOPs are critical to plant safety and must be very accurate it is recommended that an experienced, multi-discipline team be formed at the outset of the EOP development project.

It is important to stress that the development of EOPs should not be a part time job. Additionally, it is important that the staff selected to develop the EOPs should be experienced and respected in their fields. The following

disciplines should be involved in the EOP development from the very beginning of the project:

(a) Procedure writers;
(b) Operations experts;
(c) Analysts;
(d) Classroom and simulator training experts.

The number of members from each discipline will be determined by the scope of the project and the chosen development method. Procedure writers with operating experience can be very beneficial to the project.

As the project progresses there will be times when special expertise (systems engineering experts, etc.) is necessary. Additionally, the project resources required typically increase during the verification and validation processes. Management oversight, QA and quality control will be needed throughout the project.

Development of EOPs using the reference approach requires personnel with a high level of knowledge of the plant for which the EOPs are being developed, as well as of the reference plant design and reference strategies. For example, it is recommended that the development teams consist of personnel who already possess this knowledge and maintain this full time team throughout the project. Just providing an initial training programme for the procedure writers usually cannot adequately convey this knowledge.

### 3.2.2. Development method

As previously discussed, development of EOPs using the reference approach requires some team personnel to possess a high level of knowledge of the plant for which the EOPs are being developed, as well as other team personnel to have a sufficient level of knowledge of the reference plant's design and its reference strategies. The work is typically done in two stages:

(1) Exchange of knowledge between the two groups. Sharing of expertise from both plants is critical so that the entire team understands the differences between the two reactor technologies, as well as the bases of the reference methodology and the strategy of individual procedures.
(2) Development of plant specific strategies that are based on strategies in the generic reference system guidelines.

In almost all nuclear power plants there is a series of old event based procedures that respond to a wide range of events. Since the effort associated

with the development of a full symptom/state based EOP package is very significant a possible approach is to divide the work into two successive phases:

(i) The first phase would be dedicated to the development of new scenario independent procedures related to the specific safety functions. These new procedures will supplement the existing event based EOPs. This phase should come first since the implementation of these scenario independent procedures will significantly improve the safety of the plant by decreasing the core damage frequency, which would be shown by a Level 1 PSA.
(ii) The second phase would consist of developing new and/or upgrading existing event based procedures to be compatible with the chosen EOP methodology.

An example of such a specific situation is a major nuclear power plant reconstruction and safety upgrade programme where many hardware modifications have to be developed and implemented over a long period of time. The first step then would be to develop and implement the new scenario independent procedures, as discussed above. After completion and licensing of the safety upgrade programme the development of a full set of new procedures or upgrade of the original event based procedures can be started.

## 3.3. SUPPORTING ANALYSES

Analysis is crucial to the EOP development project because computer simulation is the only way of knowing how the plant will respond to the recovery strategies. Accordingly, at the very beginning of the EOP development project, there is a tendency to expect that a large number of analyses (several hundred scenarios) will have to be performed. Experience from several reference methodology EOP development projects shows that only a minimum scope of analysis is required to start work on the EOPs. These analyses, of course, are additional to what is already available in the FSAR and other available analytical documents for the nuclear power plant. Later in the project a larger number of additional analyses may be needed to support the development of individual strategies and to better document the EOPs. These analyses, however, can be carried out in parallel with EOP development.

The duties of the personnel who will be performing the analytical work also deserve attention. It is recommended that the EOP analyses be defined and interpreted by operations experts who know the details of the EOP strategies and that the analytical experts provide them with support, not the

contrary. EOP development is an undertaking that is primarily operationally oriented and requires a broad understanding of the entire plant response. Operationally oriented aspects, such as general trends of plant parameters, available symptoms, states, timing of actions, play a role in strategy development as well as verification of some safety criteria.

The following is a list of typical analytical support tasks:

(a) Identification of the applicability of the reference/generic method: This task is necessary to identify what complementary support analyses will be required for the specific plant. Several methods are available for assessing the existing support analyses of the reference plant. FSAR analysis may be used as the basis for assessing EOPs developed by the reference/generic method. Additional realistic best estimate analysis will be necessary and there are several methods available for determining this analysis. Reference vendors are a good source of information and experience on this topic. Additionally, the US Department of Energy's International Nuclear Safety Programme has developed a generic method for this determination. These additional analyses should include conclusions supporting the timing and effectiveness of the EOP strategies.

(b) Identification of the scope of the EOP: When identifying the scope of coverage of the EOPs, a good knowledge of the thermalhydraulics of the plant is necessary to identify the possible challenging accidents. This knowledge is usually available in the plant FSAR or any equivalent safety document containing all the safety analyses that have been done for the licensing of the plant. FSAR analyses generally cover the DBAs and, because they are typically conservative, operator actions are usually not considered. The deterministic knowledge can be complemented by a probabilistic analysis in support of the definition of EOP coverage, but this might not be strictly required if a reference methodology is used.

(c) Identification of plant vulnerabilities and specifics of plant behaviour to include instrument response under accident conditions and hazardous conditions within the plant. The FSAR analyses can also be applied for this purpose. In addition, numerous analytical results are published in various technical documents, development projects, research projects, etc. For some purposes, analyses for plants of similar design can be applied, but their applicability must be evaluated. The content and the assumptions of the analyses have to be reviewed very carefully. Whenever possible (since EOPs are intended to respond to real accidents), any additional thermohydraulic analyses in support of EOPs should preferably be done using a realistic (best estimate) method.

(d) Development and validation of strategies: Determining or justifying the strategies selected for individual EOPs, or sometimes selecting the strategy among different possibilities, might involve a number of best estimate analyses. It must also be understood that many accidents will not require any analysis because the recovery strategy is obvious. Analyses must be considered as only one of the different means that are available to support the definition of a recovery strategy. Engineering judgement, industry experience and practice, and references to existing analyses from similar plants are other elements that can be used to justify a given recovery strategy.

In summary, the need for computer analyses and systems analyses can be expected in the following areas:

(1) Analyses or calculations related to equipment and system capacities and limits;
(2) Specific values to be used for some of the safety functions;
(3) Specific values to be used for EOP set points and criteria;
(4) Time dependent parameters to be used in the EOPs;
(5) Specific plant data in the area of vessel resistance to pressurized thermal shock (PTS) (e.g. to specify the acceptable vessel cooldown rate);
(6) Specific plant data in the area of natural circulation operation (for evaluation of the heat sink capability);
(7) Specific plant data in the area of subcriticality margins;
(8) Analyses to define the required support systems and restoration strategies;
(9) Analyses to support priorities when multiple strategies or techniques are available;
(10) Equipment and instrumentation qualification and uncertainties.

## 3.4. EOP DEVELOPMENT

### 3.4.1. Structure of the EOP package and general strategies

The previous phases have resulted in the definition of the overall scope of the EOP and the event coverage of that scope. This has been distributed between the scenario dependent and scenario independent set of EOPs. The next step is to further distribute the scope within each of these categories into more specific individual procedures. The most important item at this level is to ensure that all the pieces of the overall scope are properly covered.

Optimal recovery from the event is provided by the set of procedures written for the diagnosed events. After definition of the scope it is necessary to establish the major operator actions (recovery strategy) to be implemented in response to any of these events. At this stage it is important to note that since these procedures are to be symptom or state based there is no need to develop a procedure for each scenario. This would actually be impossible considering the very high number of different combinations of credible equipment failures and/or human actions/failures. Moreover, the diagnosis of the proper procedure would become very difficult if there were a large number of procedures. Each procedure should therefore cover a number of variants or similar events of the same category. It is of prime importance to maintain the most straight and direct guidance and stay within one procedure to respond to the most risk-significant scenario (i.e. the most probable or the one with the worst consequences) within the family of sequences covered by that procedure. Since each procedure typically covers many different scenarios (size breaks, combination of equipment availability/failures, etc.) it will be necessary to include many contingencies, continuous diagnostics, changes of operational sequence and systems alternatives in the procedure.

A detailed structure of procedures will be established by grouping them into logical and technically consistent entities (series of major actions) from the standpoint of plant operation. This will dictate the number of recovery procedures and their individual scope of coverage. Great care should be given to defining the links between the individual procedures.

To ensure that exhaustive checking of the safety functions is addressed, all the safety functions and the possible challenges to them have to be identified and verified. This means that it is necessary to establish a complete, documented and explicit list of the safety functions that are applicable to the plant as well as the list of all possible challenges to any of these functions. The specific safety functions are the functions applied in the design intended to eventually protect the public by protecting the integrity of the successive barriers. Minimum barriers to be considered are:

(a) Fuel cladding;
(b) The physical boundaries of the reactor coolant system (RCS);
(c) The physical boundaries of the containment/confinement.

For example, typical safety functions that are representative of the status of the barriers and can be applied in safety function restoration guidelines (FRGs) for PWR technology are:

(1) Reactor core subcriticality (typically protects integrity of the fuel structure itself);
(2) Reactor core cooling (typically protects integrity of the fuel cladding or structure);
(3) Heat sink and any other function that protects the integrity of the RCS;
(4) Integrity of the RCS boundary;
(5) RCS inventory;
(6) Integrity of the containment structure;

Safety function restoration strategies (i.e. major operator actions) to cope with any one of these challenges need to be determined. The strategies depend upon both the severity of the challenge and the possible available measures for restoration of the specific safety function(s) in danger. Usually it makes sense to develop one strategy to respond to one challenge of a safety function. But since the safety functions are not independent from a thermal-hydraulic point of view, the effect on the other functions of restoring one particular function should be taken into account. The effect can be positive or negative and therefore the right balance has to be found and the priorities defined.

Extreme recovery measures will usually be implemented only with increasing severity of the challenge. For example, if a safety function restoration measure could result in severe damage to important plant equipment (e.g. a primary coolant pump, a secondary system, etc.) this measure will only be taken when all other possible restoration measures have been tried and have failed. The actions that must be taken are strictly a matter of priority. The optimal recovery procedures would normally be written in such a way as to protect the integrity of plant systems and equipment. However, since plant systems and equipment have a lower priority than the reactor core and preventing the release of radioactivity they will be sacrificed before the latter are allowed to occur.

During the development of individual recovery strategies the information support from the designer/vendor of the plant may be very useful. Some strategies may require using plant systems (safety systems as well as normal operating systems) in a way that is not addressed in the normally provided designer/vendor documentation. This designer/vendor documentation usually contains most of the information available to the EOP development team. Moreover, the reactor system parameters may approach their limiting values (defined under limits and conditions in their technical specifications), or even exceed them, and challenge margins that are often not known. These are typical areas needing additional analysis. However, in some cases such analyses may only be available to the designer/vendor of the nuclear power plant. The designer/vendor may also have data from real operational events

from different nuclear power plants whose systems were operated outside the design basis (without cooling water, etc.). Examples of typical EOP related information that could be available to the designer/vendor are the PTS characteristics of the reactor pressure vessel, behaviour of the MCP seals under loss of cooling conditions, thermal shock aspects of filling the dried out SGs, and susceptibility to failure of different pumps operated without supporting systems in out of design conditions (e.g. MCP operation in a PWR without seal injection and cooling or under two phase flow conditions).

The result of this stage is a definitive structure of the plant specific EOPs. For each of them the operating modes covered are identified, the entry conditions and the objectives of the recovery strategies defined, the major operator actions and the local (field) actions determined and the links with the other procedures in the package established.

It must be demonstrated that these arrangements were developed taking into account the operational information needs; the workload after declaration of an emergency and conditions of the operational staff (such as in the control room); the responder actions necessary in the facility; the conditions in the facility in which responder actions are necessary; and the response of the personnel, instrumentation and systems of the facility under emergency conditions (Ref. [4], para. 4.39). It must also be demonstrated that any local (field) actions needed to implement a recovery strategy can be safely carried out by the staff under anticipated emergency conditions (Ref. [4], paras 4.61–4.62).

At this point it is recommended that the status of the work be presented to the regulatory body in a completely documented report, listing all plant specific basic/generic principles and also listing all accidents to be covered. An explicit agreement with the regulatory body on this document is highly advisable before continuing with the next step of the work.

### 3.4.2. Development of individual procedures

For this particular task, reference will be made to Ref. [3]. It provides a list of those constraints that are to be applied in the development of any operating procedure, including EOPs. To facilitate both the development (writing) of the EOP procedures and the approval by the regulatory body (if applicable) all these items should be built into the plant specific EOP writer's guide. Figure 2 provides a flow diagram of the activities to be performed.

Consistency in how the information is written (wording) and structured throughout the package of procedures is a unique characteristic of EOPs. During the accident, depending on the scenario, the evolution in time of the accident and the plant and operator responses, there may be transitions

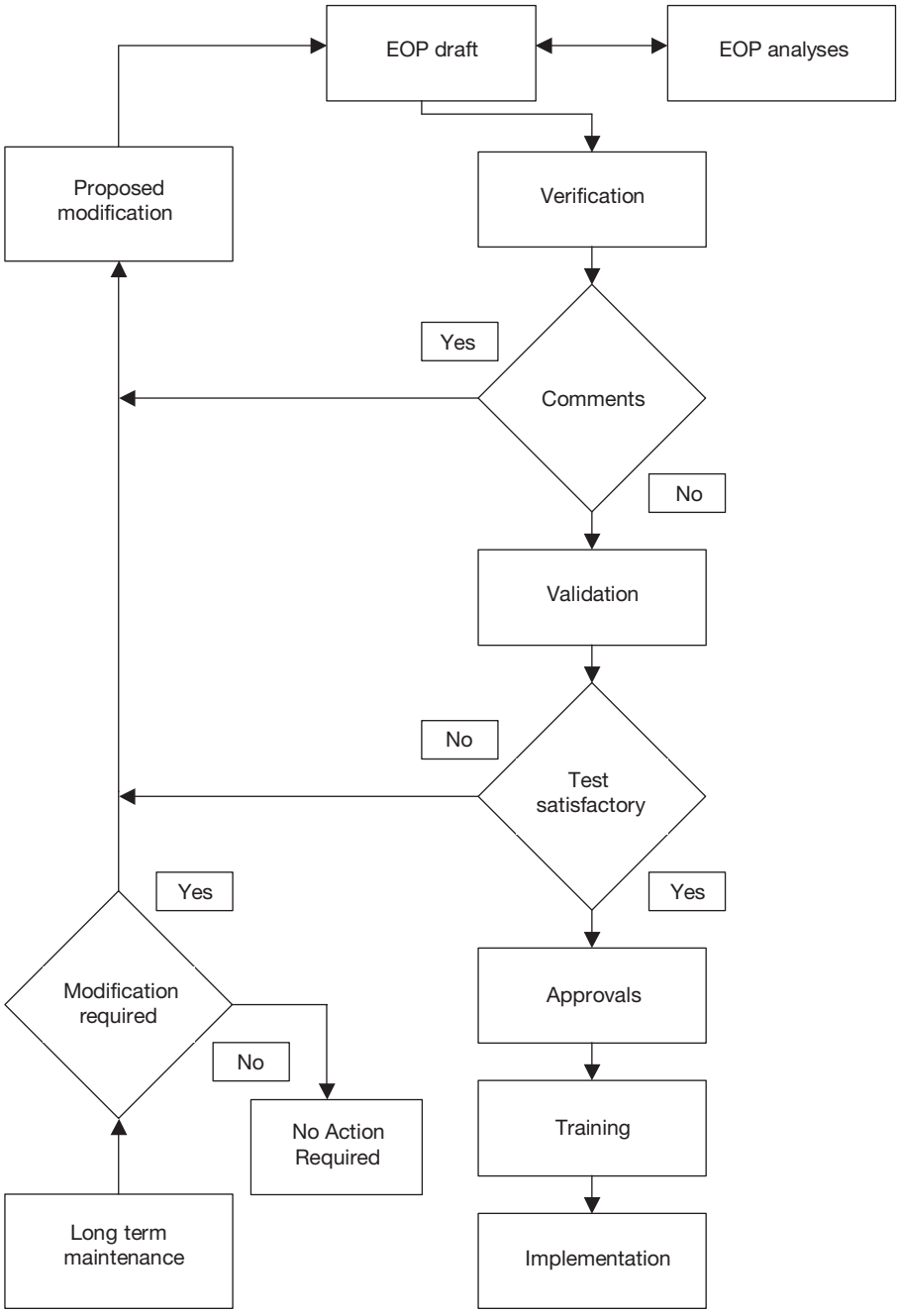



*FIG. 2. EOP development and maintenance flow chart.*

between unpredictable locations within the EOP package. From this viewpoint the EOPs constitute a set of interrelated procedures that cannot be considered to be independent of each other, like all of the plant procedure systems. It is necessary to maintain consistency among the individual EOP procedures, as well as with other ancillary procedures, with the objective that the whole package constitutes a single coherent operating guidance document interfacing with the procedures from abnormal operation to SAGs.

Therefore, when writing specific operator instructions at a certain place in a procedure, the writer should make sure that they are correctly written to reflect all the possible transitions the operator might have made before getting there and all the transitions which might have to be made afterwards. In other words, the wording and the structure used for certain instructions at one place in the EOPs might have an impact on the way instructions must be written and structured at other places in the package. This is why it is necessary to review the consistency of the entire EOP package. It may also make sense to run partial consistency reviews earlier in the project for smaller subsets of procedures. The consistency review should involve all the participants in the EOP development project, as well as any independent reviewer(s) who are technically capable and have adequate practical expertise in EOP development.

Other procedures or actions that will also be followed by the control room staff must be accounted for (such as determining if conditions warrant a change in emergency classification) in order to demonstrate that the control room staff will be able to effectively carry out all their assigned responsibilities during an emergency.

Verification of the consistency of procedures can be greatly facilitated by the use of dedicated procedure development tools specifically developed for EOP writing. These software tools have hardwired standard format structures defined in the user's guide and are equipped with a connection to the support databases (with action verbs, set points, component identifications, standard steps and sequences, etc.). The use of these databases is crucial for maintaining consistency. For example, the set points database allows the use of set point identifications during the writing of the EOP and the exact values of set points are the referenced database items. This ensures that the set point values can be easily modified simultaneously in many different locations throughout the EOP package.

## 3.5. EOP VERIFICATION

In the planning stages of EOP development one of the guidelines that should be written is the plant specific verification guideline. In combination with the plant validation process, verification ensures that the EOPs are written correctly, are technically accurate, usable under accident conditions, and are operationally correct. In this model verification is the checking of written correctness and technical accuracy. The following does not attempt to be a complete guide for verification but covers the highlights of a verification programme and gives numerous examples of items covered within this programme.

The verification process supports comparison of the EOPs with all of the documents used as sources in EOP development. These would include the plant specific writer's guide, the reference/generic set of EOPs, plant difference documents, plant technical specifications, FSAR, event based procedures used in writing EOPs, etc. Additionally, the verification guide will provide for preparation of the verification, assessment, resolution of problems and documentation of the verification process:

(a) Preparation for verification includes identification of the information needs, guidance on how to apply the evaluation criteria, identification of personnel to perform the task, and scheduling of the assessment. As verification must be done prior to validation, preparation should be done in a manner that minimizes the impact on validation. To this end, the assessment of the concepts with regard to written correctness and technical accuracy may be done separately.
(b) The assessment phase, as mentioned earlier, may have two parts, with written correctness and technical accuracy being checked separately. This is justified since these two parts can require diverse expertise. This phase identifies any discrepancies between the identified source documents and the EOPs.
(c) The resolution phase resolves any discrepancies between the EOP source documents and the EOPs. It should be noted that this does not necessarily mean that every discrepancy will result in a change to the EOPs. For example, changes in the order of the actions included in the EOPs might be acceptable, based on the control room design, if those changes did not impact the successful performance of the EOPs.
(d) Documentation provides a record of the progress in the EOP verification programme. This is important for future checking and possibly in terms of regulatory submittals. The documentation has to include the details of all the steps in the verification process.

As stated earlier, verification means checking of the written correctness and the technical accuracy of the EOP. Each concept is discussed briefly below.

Written correctness means that the EOPs are consistent with the plant specific writer's guide. Legibility, formatting, the presentation of the information, and procedure referencing and branching are part of the checks for written correctness:

(a) The legibility check is merely to ensure that the EOPs can be read. Potential problems include the faulty positioning of pages during copying and blurred text.

(b) Format inconsistency can present problems to the operator in terms of being able to find the information necessary to perform the EOP. The question answered by a check of format consistency is: "does the EOP have the organization required by the plant specific writer's guide?" This includes title, entry condition, operator actions, etc., presented in a consistent manner throughout the set of EOPs.

(c) Identification of information is another comparison made against the writer's guide. The questions answered are whether the EOP's purpose is clear, complete, approved, and in effect. Additionally, for example, it might include whether the procedure title is descriptive of the procedure's purpose, the title is on the cover page/first page, the procedure contains the correct number, revision number, number of pages and whether all of the pages are in the correct order.

(d) The presentation of information is also checked in this part of verification. This check determines if the instruction steps, notes and warnings are clearly and consistently presented, understandable, and distinguished from each other. This answers whether the steps and sequences are numbered correctly, operator optional sequencing is identified, steps correspond to one specific objective, sentences are short and simple, actions are specifically stated, and the logic is correct. Additional checks are made to determine whether notes and warnings are properly placed and contain no actions, that numerical values are properly written, set points are designated, and the necessary charts and graphs are included.

(e) Procedure referencing and branching determines whether transitions within the EOPs are consistent and compatible with rules of referencing and branching. Referencing can be defined as the use of supplemental information contained elsewhere in the procedure that is in use. Branching, meanwhile, implies that the operator leaves the procedure in use and implements actions contained there. The check of referencing and branching prevents transitions to inappropriate instructions, ensures that the transitions are appropriate, ensures that these transitions are

minimized and that in making a transition the operator does not bypass important information.

Technical accuracy means that the EOPs are consistent with the EOP source documents. These include all of the reference documents used to develop the EOPs. Examples are the EOP technical bases document, FSAR, limits and conditions, event based procedures, etc. The verification of technical accuracy requires that evaluation criteria be developed. These criteria should encompass entry conditions/symptoms/states, sequences/steps/notes/warnings, quantitative information and hardware:

(a) Entry conditions or symptoms/states should be checked to ensure that they are correct and not excessive;
(b) Sequences/steps/warnings and notes should be supported by source documents and differences between reference documents and EOPs should be explained;
(c) Quantitative information should be checked to ensure that specified values are correct and plant specific, that tolerance bands are included and computed accurately, and that this information is adequate for the operator;
(d) Plant hardware information is checked to ensure that the instrumentation exists at the plant, that the delineations are the same as those the operator will read and that the instrument is available during accident conditions.

Additionally, technical accuracy should check that strategies are unchanged as plant specific adaptations are incorporated. This check includes systems, instruments, limits, controls, indications, etc. Licensing commitments should be addressed and differences between licensing commitments and EOPs should be documented.

## 3.6. EOP VALIDATION

The objective of validation is to ensure that operators can manage emergency conditions using the EOPs. There are four recognized methods of EOP validation:

(a) The simulator method is a validation method by which control room operators perform control functions on simulator equipment according to a scenario and for an observer/reviewer.

(b) The walk-through method is a validation method by which control room operators follow a step-by-step enactment of their actions according to a scenario and for an observer/reviewer.
(c) According to the table top validation method by which personnel explain and/or discuss procedure action steps in response to a scenario and for an observer/reviewer.
(d) The reference method is a validation method by which similar plants use the data developed in a common EOP validation programme.

The validation method that will provide the most meaningful and thorough scrutiny for the EOP set is the simulator method. Consequently, this section will concentrate on it. However, the walk-through, table top or reference methods will have to be used when there is no simulator or if the simulator modelling is incapable of producing a situation that a specific procedure addresses. These alternate validation methods must also be performed when actions occur outside the control room. Modelling limitations of the full scope simulator that could typically be experienced in a complex thermalhydraulic accident with severely inadequate core cooling conditions (core uncovered, superheated steam, etc.) can be overcome by employing an engineering simulator in the validation exercise. The EOP developers could then validate the accidents that are not covered by the simulator models on an engineering simulator. In all cases the validation should be carried out under conditions that, to the greatest extent possible, simulate conditions during an emergency and include workload and instrument response.

Correct application of EOP validation will ensure that the EOPs are usable and correct. Usability encompasses two concepts, level of detail and ease of understanding. The level of detail must be sufficient but not excessive. There should be a balance between providing all possible information and the minimum information needed. The plant specific writer's guide should address the desired level of detail. During validation, the user and observer judge whether the level of detail is sufficient. Typical questions that are asked include:

(1) Was there sufficient information to perform each step or to adequately make the required decisions?
(2) Did the operator use the labelling, abbreviations, symbols and location information provided?
(3) Did the operator use the title and numbering to find referenced or branch information?

Ease of understanding reveals whether or not the material in the EOP is presented properly and whether the operator can understand the information under emergency conditions. Readable print, standard terminology, usable format and proper emphasis are evaluated to ensure ease of understanding. Typical questions that are asked include:

(i) Are the EOPs easy to read?
(ii) Are the values accurate and correct?
(iii) Are the notes and warnings recognized and understood?
(iv) Did the operators follow referencing and branching correctly?
(v) Did the operators comply with the EOPs?
(vi) Could the operators find the appropriate steps?
(vii) Did the operators return to the procedure exit point without omitting steps?
(viii) Did the operators enter the branch procedure at the right point?
(ix) Did the operator exit the procedure at the correct branch?

The next validation principle is that of correctness. This principle encompasses two concepts, plant compatibility and operator compatibility. In general, this is a test of whether the EOPs are compatible with plant responses, systems/instrumentation, shift manpower, control room information and existing EOPs.

The test of plant compatibility ensures that the operator is able to complete the required action with the hardware and systems that are in place. This includes ensuring that any action to be taken within the plant by shift personnel can be done so safely under anticipated emergency conditions (e.g. wearing protective equipment in hostile conditions). This may require that some plant systems or areas be modified (e.g. by adding shielding). If the plant does not respond as intended the operator loses confidence in the procedure. This concept evaluates the following:

— Can the actions be performed in sequence?
— Are there alternate success paths not found in the procedure?
— Does the plant's instrumentation provide the operator with the required information?
— Are the listed symptoms/states adequate to select the required procedure?
— Do the entry conditions correspond to the plant symptoms/states seen by the operator?
— Does the operator need information or equipment not provided or designated by the procedure?

— Do the technical bases agree with the plant's response?
— Are instrument readings (local and remote) and tolerances consistent with the EOP?
— Are the EOPs (books/flow charts) compatible with the work situation?

Lastly, the validation process is used to ensure that the EOPs are operator compatible. This tests whether shift manpower is adequate to comply with the actions specified within the EOPs and whether policies for operator duties and responsibilities conflict with actions specified in the EOPs. This evaluation also looks at whether time critical actions can be performed with the current shift and in the allotted time. It also tests whether actions assigned to specific shift personnel are coordinated by the procedure and whether the operating crews can follow the sequence of actions.

The preceding part of this section discussed the principles of validation. The rest provides suggestions and examples of how some utilities have applied these principles. It is recognized that the details of some of these examples repeat some of the previous part of this section but they have been included to ensure clarity of application.

When preparing for validation, a validation team which includes experienced personnel in various fields of expertise must be assembled. A team may be composed of plant operators, plant EOP writers, simulator instructors knowledgeable of EOP methodology, simulator model experts knowledgeable of EOP methodology, a human factors expert and an analysis expert. Note that the operators should not be involved in any activities that would affect their performance and consequently the validation exercises.

When developing validation scenarios the goal is to exercise as many procedures and transitions as possible. It is not expected that they will cover every conceivable scenario. Some aspects are presented in the following list, which should be considered when defining the scenarios and preparing for the testing:

(a) Logical sequencing of validation scenarios into days.
(b) Determination of the initial state, initiating event and any additional failures.
(c) Clear determination of the purpose of the scenario.
(d) Procedures and transitions expected to be used.
(e) Expected end state for stopping the simulation.
(f) Definition of the acceptance criteria, including criteria for the operator's task sharing, communication, decision making and ergonomics of the EOP layout.

(g) Operator training: for the validation test, normally only basic training, mainly on the rules of EOP usage, should be provided to the control room crew, the reason being that an operator knowledgeable in EOPs could inadvertently correct procedural mistakes through his knowledge and the mistake could be omitted by the observers.
(h) Review of scenarios with the simulator experts and instructors.
(i) Training of trainers: simulator instructors must be very knowledgeable of all aspects of: (1) the EOPs (as suggested earlier, they should have been involved in the EOP programme since the early stages of EOP development); (2) other actions to be carried out following the declaration of an emergency by the operating staff; (3) response of instruments under accident conditions; and (4) conditions within the plant (e.g conditions hazardous to the staff) during an emergency.
(j) Preparation of all the logistics (simulator room, debriefing room, blank forms to be used, sufficient number of copies of the EOPs, etc.).

Upon completion of each validation scenario some standard questions should be asked of the operators, as well as questions that each evaluator should answer.

Questions for the operators include the following:

(1) Was it difficult to identify the proper procedure?
(2) Did the procedure contain steps that were difficult to understand?
(3) Were there any problems in sequencing through the various actions?
(4) Was it difficult to decide on the proper branches in the block diagram?
(5) Was there any need for support in the orientation (route) through the procedure?
(6) Did the procedure contain unnecessary information?
(7) Were there any differences in the vocabulary used by the procedure compared to the ones generally used in the nuclear power plant?
(8) Were any charts and diagrams difficult to understand?
(9) Is any instrumentation/equipment considered in the EOP that does not exist in the nuclear power plant?
(10) Were there any differences between the accuracy of instrumentation readings in the control room compared with the requirements in the procedure?
(11) Can any parameter values in the procedures not be determined by the existing instrumentation?
(12) Does the procedure contain unclear or false instructions?
(13) Is there a need to include additional information in the procedures?
(14) Did you have any difficulties in reading and using the instructions?

(15) Did you feel comfortable during the handling of the emergency?
(16) Do you feel that the plant was always under control?

Questions to be included for the evaluators are the following:

(i) Were there situations when the entry conditions into the procedure were not recognized?
(ii) Did a crew fail to enter the proper procedure after diagnosing the entry conditions?
(iii) Were there any procedure step omissions?
(iv) Were there any mistakes in sequencing through the steps?
(v) Were there any erroneous operator actions?
(vi) Did the operators have any problems making decisions?
(vii) Did the operators have any problems understanding the instructions?
(viii) Did the operators have any problems following the routes in the block diagrams?
(ix) Did the operators have any problems reading or manipulating the EOPs?
(x) Were there any steps in the procedure that the operators could not execute?
(xi) Did the operators require more detailed instructions during the scenario?
(xii) Were there any discrepancies between instructions in different procedures?
(xiii) Was any instrumentation or equipment considered in the EOP that does not exist in the nuclear power plant?
(xiv) Could any parameter values in the procedures not be determined by the existing instrumentation?
(xv) Did the execution of any instruction require the use of special equipment whose location is not shown or is not known to the operators?
(xvi) Did the scenario lead to a situation in which the operator was unable to stabilize the parameters?

The validation programme must be well documented to assist in the review of the programme and provide reference when modifications to the procedures occur. Some examples of topics to be considered in the validation report are:

(a) A description of the objectives of the validation programme;
(b) A description of each phase of the validation programme;
(c) A description of the criteria used in the validation programme;
(d) Definition of test scenarios;
(e) A description and justification of results;

(f) General recommendations (assessment of the compatibility of the EOP with the plant design and its responses, proposals and justifications of any operator intervention with the protection system logic and signals, etc.);
(g) A complete set of discrepancy sheets with each sheet addressing the following:
   — Identification of procedure and step,
   — Identification of discrepancy type (according to the criteria),
   — Determination of whether a change to the EOP is required,
   — Resolution, i.e. proposed change of wording, change of transition, change of set point, etc.

## 3.7. EOP DOCUMENTATION

The documentation that supplements the plant specific EOPs and provides justification for the EOP development programme can be divided into two groups, the technical documents and the administrative documents. The list that follows is not exhaustive. There is no fixed requirement as to what type of documents should be available. It is up to the nuclear power plant to decide which specific documents will be added for the review, for licensing or QA purposes or any other reasons. Some of the documents logically follow the structure of the EOP reference system and its methodology if such has been used as a basis for the programme.

### 3.7.1. Technical documents

Items (a), (b) and (c) below are recommended as the minimum technical documentation supporting the EOP's development, verification, and validation:

(a) The EOPs:

These are a self-sufficient full set of documents providing the instructions which have to be available in the control room. They can be either computerized or in paper form. The EOPs shall contain all the information necessary for the operator to do his job. Not only do they need to contain the instructions themselves, but also all the diagnostic tools, the monitoring tools as well as the administrative and technical notes and/or warnings. The information can be in different formats: text, charts, flow diagrams, figures, tables of values, etc. A detailed list of possible elements contained in an EOP is provided in Ref. [3].

(b) The technical basis and background documents:

These documents provide a detailed explanation of the overall organization, purpose and structure of every procedure and its links with other procedures. They also provide details on each action, instruction and element of each procedure. The two basic purposes these documents serve are:

- The technical basis document provides the basis for each element of the EOP package. The availability of this information is mandatory when developing EOP training materials.
- The background documents track the history and reason of each element for every EOP procedure. During procedure revision these documents provide the required information to evaluate whether a particular element can be modified and, if so, how it should be modified.

During EOP development the proposed strategies and actions are checked through an analysis to optimize and validate the operating strategies before transcribing them into specific operator instructions. These analyses should also be included in the EOP background document, or at least referenced.
Different types of analyses are performed during the development of EOPs. Since these analyses mostly support and justify EOP strategies they should also be made available. Some of these analyses consist of the following:

- Specific EOP analysis reports (thermal-hydraulic, structural mechanics, experiment reports, etc.);
- Set points calculation report;
- Final EOP validation report;
- Description of generic principles used for the development of the EOPs. Also, during the documentation and implementation phase additional representative analyses may be incorporated to augment staff and operator training. These best estimate analyses include operator actions, as they are required in the EOPs.

(c) Additional reference documents.

Other documents that are used or generated during the development of the EOPs may include:

— The safety analysis report;
— Limits and conditions/technical specifications;
— Detailed system descriptions;
— Operating procedures;
— Equipment specifications and operating manuals;
— Sensitivity studies on various approaches;
— Review of applicability (and its limits) of the reference system to the plant, if used.

(d) Other general documents that are relevant to EOP development and implementation may include:

— Literature (scientific articles, technical reports, conference proceedings, etc.);
— Official guideline documents (IAEA guides, World Association of Nuclear Operators (WANO) reports, Institute of Nuclear Power Operations (INPO) reports, etc.);
— Legislative documents (regulatory requirements, legal provisions, etc.).

### 3.7.2. Administrative documents

Items (a), (b) and (e) below are recommended as the minimum administrative documentation supporting the EOP development project:

(a) Plant specific EOP writer's guide: Before starting to write the EOPs themselves a set of rules has to be established in order to ensure consistency from procedure to procedure and within the individual procedures themselves. Such rules are necessary because the procedures are a structured document which contains looping of steps, procedural transitions, conditional requirements, etc.
Consistency between the intentions of the procedure writers and the understanding of the procedure users is ensured by clearly defining all potentially ambiguous structures and through the adoption of a limited mandatory vocabulary (action verbs). Consistency significantly reduces the probability of operator misunderstandings/errors.
Following are some examples of rules that should be defined in a writer's guide. Most of these rules, as discussed earlier, can be built into dedicated software tools:

— Defining the procedure format as a whole;
— Defining a limited set of action verbs that will be used consistently throughout the procedures;
— Formatting of condition statements;
— Structuring of steps;
— Transfer between columns in a two column format;
— Looping;
— Rules for links within and between procedures;
— Creation of links to reference documents and set points database;
— Use of graphic symbols, tools, tables and diagrams;
— Indication of strategies;
— Indication of communication points for team coordination;
— Definitions of principal terms and abbreviations used in EOPs.

The writer's guide should define the general philosophy regarding how much detail should be provided in the procedures. In general, whatever is obvious should not be expounded upon in the procedures (for instance the location of the reactor trip control). Conversely, items that are not normally operated or are being used for out of the ordinary actions should be detailed in the procedure. For example, sufficient detail should be provided in the procedure for a seldom used valve so that no time is lost while an operator refers to a plant drawing or a system description for information. Operator guidance is not only required in the control room EOPs but also for local actions by the field operators.
The writer's guide must be consistent with the user's guide. The writer's guide can also define the QA process to be followed for the development and validation of the EOPs.

(b) Plant specific EOP user's guide: Similarly to the writer's guide that determines the rules to be followed while writing EOPs, the user's guide establishes the rules to be followed while using them. This guide complements the writer's guide and provides rules on how to use the procedures that were written according to the writer's guide. Because the user's guide is written mainly for the operators it also defines rules on how to use the EOP package as a whole.
Following are some examples of rules that should be defined in the user's guide:

- Entry conditions;
- Distribution of roles between control room personnel;
- Communication protocol in the control room;
- Priority rules for transitions between and within the scenario dependent and scenario independent parts of the EOP package;

- Progression rule through the procedures;
- Evaluation of CSF status trees/safety function status (when necessary for priority management).

(c) Plant specific EOP verification guide and EOP verification report: This guide establishes the verification criteria, documentation of findings, resolution of findings, etc.
(d) Plant specific EOP validation guide and final EOP validation report: This guide establishes all the administrative rules for validation.
(e) Licensing requirements: The regulatory body may require the utility to demonstrate compliance with a number of administrative and/or technical rules. If so, compliance with these rules will have to be documented.
(f) QA requirements: Since the development of EOPs is safety related, this has to be done in compliance with international QA standards. However, this does not necessarily mean that a specific QA programme has to be defined for the project. Reference can be made to an existing utility and/or a supplier's overall QA programmes.

## 3.8. TRAINING

Operator training is provided in two phases, initial training and continuing training. The training is provided at three levels:

(1) Rule based training;
(2) Skill based training;
(3) Knowledge based training.

These have been elaborated in Ref. [11].

### 3.8.1. Initial training

Initial training consists of classroom training and simulator training. During the initial EOP classroom training the operator receives an explanation of the EOP's philosophy, usage, bases and specific EOPs. This training is reinforced during simulator sessions in which the EOPs are practised and the crews are debriefed.

When the initial training programme for a new set of EOPs is being prepared it is important that preparation of the material begins prior to completion of the EOP validation. Otherwise, EOP implementation will be

stalled while the training programme is being developed. It is not recommended that operators be allowed to self-study the EOPs and the background documents because there is so much information that without prior knowledge of this material they will not be able to properly sort through and digest the salient information. The training material should include, as previously mentioned, guidance on EOP philosophy, usage, bases and on all procedures contained in the EOP set. Simulator training sessions should also have prepared simulator exercise guidance. Additionally, it is important that operators are aware of and trained in fundamental physical concepts and are able to apply this knowledge to the EOPs.

Note that involvement of operators and other operating personnel in the development of the EOPs in the framework of reviews, EOP verification, etc., provides valuable initial training as well as feedback to the development team.

### 3.8.2. Continuing training

Continuing training also contains some classroom elements but is typically mostly simulator based. In the simulator the operator should be exposed to all procedures in the EOP set approximately every two years. Emphasis should be placed on exercising procedures dealing with the most probable and complex accident. In the case of PWRs this might be an SG tube rupture. The SG tube rupture recovery procedure might be practised up to three times more often than less probable procedures.

Continuous simulator training obviously keeps the operators at a higher level of proficiency in the use of EOPs but an added benefit that will be realized is operator feedback on the EOPs. This feedback can have many forms but some of the more common ones are suggestions on improving EOP ergonomics and improvement in EOP strategies. Incorporation of relevant operator feedback is important since these improvements assure the operators that the EOPs are 'their procedures'.

During continuing training the classroom EOP training revolves around industry EOP experience, EOP related systems training and technical bases lessons. During continuing simulator training the crews will typically spend 50–75% of their time practising a portion of the EOP set.

As a part of the long term procedure maintenance programme and as a result of plant equipment changes, the operator will be trained on those changes affecting the EOPs. This training can be either classroom based or simulator based, depending on the scope of the change.

## 3.9. IMPLEMENTATION AND LONG TERM MAINTENANCE PROGRAMME

EOPs should never be considered complete. Improvements will be necessary throughout their lifetimes. An EOP maintenance programme, which is a good practice and should be implemented by each nuclear power plant for its own set of EOPs, provides a systematic way of maintaining the EOPs so that they are always as current, efficient and effective as possible. This programme collects feedback from simulator training, internal operational experience, plant design modifications, additional thermalhydraulic analysis, results from PSA studies, and regulatory requirements. Additionally, feedback may be obtained from other plants through review of generic operating experience and through owner's groups.

Changes to EOPs should be decided upon very carefully. It often happens that for one particular scenario an easy change in the text of the procedure would make the step sequence more efficient and the response more straightforward. However, many different scenarios can lead an operator to perform the same set of actions. Therefore, it is highly recommended that a consistency review or revalidation be performed before important changes are made to the EOPs.

## 3.10. REGULATORY BODY APPROVAL OF EOPs

Approval of EOPs by the nuclear power plant management is normally attained through the nuclear power plant's administratively controlled procedure approval process.

The role of the regulatory body in the review and approval (if required) of EOPs was discussed in Section 3.1.5. However, it should be repeated that early involvement and open discussions with the regulatory body from the beginning of the project will smooth the progress of the entire licensing process.

Regulatory body approval is typically a sequential activity:

(a) Submission of documentation to the regulatory body;
(b) Formal presentations concerning the submitted documents (method, procedures, supporting documentation, etc.);
(c) On the spot discussions;
(d) Receipt of a series of written questions and comments;
(e) Documented response to the authority.

This sequence of steps may be repeated more than once.

Another critical item that will greatly influence the licensing process is the quality of the documentation that is provided by the nuclear power plant to the regulatory body at each step of the development programme. Past EOP development programmes demonstrate that the time taken to document every aspect of the EOP project (EOP development, verification, validation) is never wasted. In fact, it has been shown to save time in the long run. This is why it is vitally important to obtain, before the start of the development programme, a clear list of regulatory body requirements for the final product.

# 4. REVIEW OF EOPs

This section provides guidance for an independent review of the development and implementation programme for one particular plant, including a partial review of the technical correctness of the EOPs. This section also describes activities that should be carried out during the review so that both the review team and the plant being reviewed will understand the objectives of the review and the review process itself.

The review can be scheduled either during the development or the implementation process of the EOP programme. The aim may be the review of an existing set of EOPs to identify deficiencies and issue recommendations for a successful completion of the programme, or for providing recommendations for the improvement of the EOPs. Although the guidance is written primarily for external review, many elements can also be used for internal review in the framework of a self-assessment process.

## 4.1. OBJECTIVES OF THE REVIEW

The typical duration of an external review is one week. During this period of time it is impossible to review all aspects of the EOP development programme and/or all documentation in detail. Therefore, the review should be focused on specific areas of the EOP programme. For example, the review may be oriented towards either administrative or technical aspects of the programme. While the administrative review will be mainly focused on a review of the development/implementation process and the QA and methodology used, the technical review will concentrate more on the

correctness and accuracy of the procedures themselves, including human factor considerations.

Review objectives generally involve verification of the adequacy of the entire EOP development and implementation programme and an in-depth review of one or more particular topics of the development and implementation programme. Topics for an in-depth review may be chosen from Sections 2 and 3 above or may be tailored to optimally respond to specific needs of the host organization.

## 4.2. REFERENCE DOCUMENTS FOR THE REVIEW

The review team needs to have appropriate documentation available prior to and during the review. It is also helpful if the host organization prepares presentations at the beginning of the review. Presentations should contain important information from the EOP's development and implementation process and thus render the team's familiarization process more effective.

Owing to the comprehensiveness of specific technical information such as respective FSAR chapters, EOP background documents, supporting thermal-hydraulic analysis, etc., it may be necessary to study some documentation in advance. The content and scope of such information, which will be made available to the review team, needs to be agreed upon beforehand and should reflect the intended scope of the review.

The typical list of documents for any particular plant includes the following:

(a) EOPs;
(b) EOP technical basis documents;
(c) Administrative documents related to EOP development;
(d) Relevant FSAR chapters, or any other relevant documents in which design basis can be found;
(e) Supporting thermalhydraulic analysis;
(f) Limits and conditions/technical specifications;
(g) Normal operating procedures;
(h) Alarm response procedures;
(i) Abnormal operating procedures;
(j) SAGs;
(k) Relevant QA manuals;
(l) Training programme and other training materials.

Some plants use a reference approach for the development of plant specific EOPs. If this is the case the documentation describing the reference approach and justifying deviations from that approach in detail should be presented to the team.

## 4.3. QUALIFICATIONS AND COMPOSITION OF THE REVIEW TEAM

Review of the EOP programme requires a team of competent experts to deal with different technical areas. The effectiveness of the review will be highly dependent on the quality and adequacy of the reviewers' profile. Because of the small number of experts on the review team it is recommended that all of them have adequate background in modern EOP philosophy in addition to their own specialization. The concepts of modern EOP packages are quite complex and the review process should not allow improvisation on the spot. The experts' qualifications in terms of their practical and technical expertise can be described as follows:

(a) Relevant plant design and technology;
(b) Plant specific operation, operations support;
(c) Process engineering and plant automation;
(d) Thermalhydraulic and accident sequence analysis;
(e) A general safety background capability to review the consistency of the approach used for EOP development with the overall plant safety approach;
(f) Specific EOP design, development and implementation;
(g) Human factor analysis;
(h) Training;
(i) Licensing.

The team should consist of a minimum of three experts (one IAEA staff member and two senior external consultants). Experts from the host country are not included on the team. This approach is consistent with similar IAEA activities such as OSART missions. Involvement of a writer of EOPs for a similar plant design would be of great benefit and would facilitate the transfer of information in both directions.

## 4.4. REVIEW PROGRAMME

A comprehensive programme should be developed for the review. This programme will determine the scope of the review and will be the key document for conducting the review. The programme should also be sent to the nuclear power plant well in advance in order to allow timely preparation of the review. The programme will be the basis for the definition of the preparatory work to be done by the plant, such as the preparation of presentations and documents which the plant should provide.

A review programme should address at least the following items:

(a) Objective of the review;
(b) List of areas to be reviewed (scope of the review) and estimated time for implementation;
(c) Composition and qualification of the review team;
(d) Evaluation criteria;
(e) Documentation of the review process.

The programme should also include the minimum requirements for the plant to conduct the review in specific areas, such as relevant plant personnel, facilities, administrative support, etc.

## 4.5. GUIDANCE FOR THE REVIEW OF SPECIFIC AREAS

### 4.5.1. Strategic aspects of the EOP

The aim of a review of strategic aspects of an EOP is to check if all basic/generic principles discussed in Section 3.1 were dealt with during the preparation phase, as is necessary for the project to be optimally managed and clearly defined for the chosen approach (reference methodology or stand-alone approach):

(a) Definition of the scope (initial conditions and events to be covered and interfaces with other procedures);
(b) Decision and justification of the type of EOPs and approach used for development;
(c) Priorities between automatic and manual operator actions in accident conditions;
(d) Organization in the control room under normal operation, abnormal operation and accident conditions;

(e) Allocation of authority and responsibilities in the nuclear power plant's overall accident response organization;
(f) Requirements and role of the safety authorities in the development of the EOPs;
(g) Role of the utility.

### 4.5.2. Project arrangements

The aim here is to review whether the general arrangements of the project have been adequately planned and prepared. The review focuses on aspects discussed in Section 3.2:

(a) Composition and size of the development team;
(b) Qualification and experience of the team members;
(c) Involvement of operators;
(d) Early involvement of simulator and training experts;
(e) Organization of EOP development work, information flow and allocation of responsibilities between the team members;
(f) Scheduling of the project and allocation of human resources.

### 4.5.3. Supporting analyses

The aim here is to review the scope and adequacy of supporting analyses that were used throughout the development of EOPs. Areas requiring analytical support are specified in Section 3.3. The review should focus on the scope of the analyses, whether they provide sufficient information on the plant's response to various accident conditions and a qualitative assessment of all recovery strategies used in EOPs. Careful evaluation should be made of the applicability of computer codes used for the analyses.

The review of relevant factors influencing the process and the scope of coverage are of particular concern, e.g. initial plant operating modes, operator actions, other factors known to challenge human performance and scenarios that have been adopted to justify the scope of EOPs.

Because of differences in their importance the analyses chosen for detailed review should be selected using the same criteria as those recommended in Section 4.5.4 for prioritization of procedures.

Examples of categories of analysis for detailed review are:

(a) Specific thermalhydraulic analyses from different sources, including those with the analytical background from the FSAR and PSAs, that were used for development of the EOP strategies;

(b) Probabilistic analysis in support of the determination of the scope of the EOP;
(c) Analysis related to equipment and system vulnerabilities, capabilities and set points;
(d) Analysis of specific parameter values for specific safety functions;
(e) Analysis in support of strategies applied in the EOPs;
(f) Specific data related to reactor vessel resistance to PTS.

### 4.5.4. EOP development

This phase involves a general review of the EOP package as a whole and an in-depth review of a representative sampling of procedures covering the following types: diagnosis procedure, scenario dependent procedure and scenario independent procedure. For a discussion of the relevant issues, see Section 3.4. Due to its limited scope the review should focus on the most important procedures.

The proposed criteria that can be used to prioritize the procedures in terms of importance are:

(a) Is the procedure addressing a severe safety issue/challenge (examples: diagnostic procedure, inadequate core cooling, total blackout, total loss of heat sink, PTS, SG tube rupture (SGTR), etc.)?
(b) Is the procedure responding to a higher probability event (examples: simple reactor trip, spurious ECCS actuation, SGTR, etc.)?
(c) Does the procedure require much operator involvement, with unusual actions (examples: SGTR, plant cooldown and depressurization with a small LOCA, etc.)?

Those procedures for which all answers are no can be screened out of the review. However, these criteria will generally screen out only a limited number of procedures. If the remaining list of procedures is still beyond the capability of the review team during the available period, then an additional criterion is to look at similar procedures. It often happens that procedures or their selected parts are similar in their writing and content (sequences of identical steps) or strategy. An example is the back end of procedures dealing with plant cooldown and depressurization. For these, the review may look at one representative procedure or part of one to have a complete view.

The review focuses on the following aspects:

(1) Review of the EOP's scope:
   — Accident sequences considered: consistency with the FSAR, with the plant specific PSA, with the regulatory body requirements, with the plant specific and international experience feedback;
   — Initial operating modes taken into account;
   — Conditions covered by the EOP package and the interface with other plant procedures (AOPs and SAGs);
   — Compliance with the present plant system status;
   — Strategy concerning planned modifications of EOPs.

(2) Review of the technical justification of the procedure or a set of procedures: For each of the reviewed procedures the following aspects should be addressed in detail:
   — Consistency with the basic/generic principles;
   — How the administrative reference documents have been used;
   — Consistency with the EOP writer's guide;
   — Consistency between the reviewed procedures;
   — Correctness and technical effectiveness of the strategies;
   — Technical basis and justification of the strategies.

(3) Review of the human factor related aspects of the entire EOP package or individual procedures. The review team should review the following:
   — EOP location and identification: The EOPs should be placed within easy access of the operators in both the main and emergency control rooms and should be clearly distinguishable from other operating procedures;
   — EOP format: The EOP format should be easy to use and the review team should also check whether an agreed format for statements used in procedures is consistently maintained throughout the EOP;
   — EOP support: The supporting documentation (drawings, charts, flow diagrams, etc.) should be available in locations where the EOPs are used and the ergonomics of the supporting documentation, instrumentation and displays needed for entry information, etc. (colour coding, quality and completeness of information) should be adequate;
   — Team organization aspects.

(4) In case of computerized procedures additional human related aspects should be reviewed:
   — Operator acceptance;
   — Team organization aspects;
   — Ergonomics of the computerized EOPs;
   — Ergonomics of the human–machine interface;
   — Rules for leaving the computerized EOPs following computer unavailability;

— Completeness of the paper backup set of EOPs;
— Ergonomics of the paper backup set of EOPs.

### 4.5.5. Verification

The overall process of EOP verification and its documentation should be reviewed. The review should focus on the adequacy of the verification guide and its implementation. The verification report should be reviewed. The subject of verification is addressed in Section 3.5.

### 4.5.6. Validation

The overall process of EOP validation and its documentation should be reviewed according to the recommendations in Section 3.6. The review should focus on whether the validation guide has been properly developed and applied. A detailed validation review should be carried out for a representative sample of procedures based on the validation report. It is convenient to select those procedures which have been reviewed in-depth as described in Section 4.5.4.

At least the following information, both human and technically related, should be addressed:

(a) Composition of the validation team;
(b) Timing of the simulations (were they real time?);
(c) Interaction between operators and the evaluation team;
(d) Consideration of inputs from other groups of the emergency organization in the validation session (e.g. radiological group, TSC);
(e) Type of simulation tools used;
(f) Physical models applied;
(g) Definition of the initial conditions and sequences;
(h) Technical justification of the selected set of sequences;
(i) Workload: Were all the tasks to be carried out during an emergency (e.g. classification) considered?

Additionally, the implementation of the changes identified during the verification should be checked in the final version of the EOPs.

### 4.5.7. EOP documentation

The review should concentrate on whether the development process (see Fig. 2) is adequately documented and whether the documents supporting the

EOP project have been created, used and appropriately referenced. If necessary, some of these documents may be reviewed in detail with respect to the recommendations in Section 3.7. The documents to be reviewed are:

(a) Technical reference documents that were used or produced during the development process, such as:
   — Existing analysis, technical specifications, system descriptions, operating procedures, equipment specifications, instrumentation and equipment qualification reports, etc.;
   — Background documents developed during the EOP development process, justifications for application of the reference development method, relevant supporting studies, specific thermalhydraulic calculations, verification of EOP strategies and validation reports, training materials, etc.
(b) Administrative documents such as:
   — EOP writer's guide;
   — EOP user's guide;
   — EOP verification guide and report;
   — EOP validation guide and report;
   — EOP training programme guide;
   — Report documenting compliance with the licensing requirements;
   — The QA programme, established for writing, implementation and maintenance of the EOP.

### 4.5.8. Training

A prerequisite to formal implementation and use of the EOPs is that operators must be sufficiently trained in the application of the EOPs.

At least the following areas should be covered by the review:

(a) Documentation of the training programme: Review of its correctness and the fulfilment of the training plan that should have been developed during EOP development.
(b) Instructor training: The prerequisite to efficient EOP training is the involvement of the instructors in the entire process early enough in the project. The objective of this review is therefore to evaluate the correctness of the overall training programme on EOPs covering the instructors as well as the operators, and to provide recommendations for improvement.
(c) Operator training: Type and extent of theoretical lessons received, practical lessons (simulator, control room, plant), exams etc.

(d) Operator retraining: Frequency and contents (ability to retrain all the EOPs, taking into account the operating feedback, significance of the procedures and the modifications included from the last revision), means (full scope simulator, engineering simulator, etc.) and evaluation tests.
(e) Training material: Training documents, video and computer training techniques.
(f) Proper assignment of priorities in the training.

The priorities of the training programme can be set according to the screening criteria described in Section 4.5.4.

The review of these areas requires analysis of the documentation developed specifically for the EOP's training programme. In addition, it is also suggested that different personnel involved in the training process be interviewed. The following may be taken into account:

(1) An interview with instructors should include topics like what has been their involvement in the EOP's development process, when they were involved, what difficulties they have to face with the operators regarding the acceptance of the new set of EOPs;
(2) An interview with operators should include topics like what has been their involvement in the EOP's development process, what were and what are their concerns about the newly developed EOPs, what is their opinion of the training and retraining received.

Attendance of simulator exercises is recommended to observe how the control room crew follows the EOPs during a specific accident scenario. This provides the team with additional important information, for example on the use of the EOPs under simulated accident conditions.

For the first revision of the set of EOPs it is recommended that an analysis of the experience feedback of all the initial training sessions be performed and the conclusion of this analysis be provided to the trainers and operators.

### 4.5.9. Implementation and long term maintenance programme

Because the process of EOP development is quite long it is possible that some assumptions taken in the development with regard to the plant status were not correct due to, for example, new or delayed hardware modifications or temporary unavailability of equipment addressed by the EOPs.

It is therefore necessary to review whether the plant has established a process for maintaining consistency of EOPs with the actual plant status. It is

also recommended that the consistency of the EOPs with the real plant status be verified to some degree. Guidelines dealing with this should be in line with the QA system at the nuclear power plant.

Examples of modifications related to the EOP's implementation include:

(a) In the control room: Specific displays defined for continuous monitoring, installation of new/improved instrumentation, using labels in the control room to identify the qualified instrumentation which can be used during an accident;
(b) In the operating documentation: Effect of the interface with normal and AOPs, required modification of the alarm sheets that address orientation into an EOP, addressing specific requirements in limits and conditions/ technical specifications to ensure required instrumentation availability;
(c) In other plant documents: The emergency plan and the procedures for the groups in emergency response as the TSC and/or the radiological group;
(d) In the plant systems: Modifications to allow timely operation of equipment used in the strategies (e.g. exchange of locally operated valves for control room operated valves).

The review team should compile a list of all these modifications in order to verify their correct implementation. It is recommended that the review team directly verify the adequacy of the modifications and the physical implementation of the EOPs by consulting the documents and visiting the control room or other locations in the plant.

For a multi-unit plant, EOPs may be developed in parallel. Differences between the units should be addressed and the review team should verify how these differences have been considered in the development.

The long term maintenance process for the set of EOPs should be prepared in parallel with the development of the procedures. Guidelines dealing with this aspect should be in line with the QA system at the nuclear power plant. The reviewers will have to evaluate this process developed by the plant to guarantee that the impact of any significant modification is correctly addressed in the EOPs and training documents.

The review should concentrate mainly on how the process of modification control, which has been established in the nuclear power plant, provides for proper maintenance of EOPs. Possible sources of modifications to EOPs include:

(1) Modifications of the plant design: equipment, systems, instrumentation, etc.;
(2) Recalculation of the thermalhydraulic analyses;

(3) Internal and external feedback on operational experience;
(4) Feedback on experience from training sessions;
(5) Changes to the reference EOP if a reference approach has been used;

## 4.6. REVIEW REPORT

During the course of the review each team member writes technical notes describing the situation in each of the review areas. These notes contain experts' observations, including any recommendations and suggestions. Good practices or good performances are reflected as well. Technical notes form the basis for a draft review report. The draft report is completed by the end of the review and presented to the host organization.

After completion of the review the team leader prepares the final review report based on the draft report. This is an official IAEA record which summarizes the team's main observations and conclusions including all recommendation and suggestions. Before the text is finalized the utility is given the opportunity to comment. This report is submitted through official channels to the Member State which hosted the mission. The IAEA restricts initial distribution to itself, members of the review team, the nuclear power plant, the utility and the national regulatory body. The report is derestricted after a specified period of time unless the Member State wishes otherwise.

## 4.7. REFERENCE CHECKLIST FOR THE REVIEW

Appendix I contains a list of typical questions to be used as a 'reference checklist' for the review. It is obvious that for most of the questions a yes or no answer is not sufficient to document the quality of the work and of the EOPs. EOP experts reviewing the work and the package will have to document the answer to these questions and also justify the relative value of each of them. Also, the review will result in a report which includes justified recommendations that preferably should be prioritized.

## Appendix I

## REFERENCE CHECKLIST

### I.1. TASK 1: PREPARATION FOR DEVELOPMENT OF EOPS[12]

1.1. Were the basic/generic EOP principles clearly established?
1.2. Were the interfaces with other plant procedures clearly defined?
1.3. Was the priority operator versus plant protection system logic clearly defined and accepted at appropriate levels?
1.4. Were the requirements related to the scope of the EOP clearly defined?
1.5. Were the regulatory body requirements identified and evaluated?
1.6. Was the development team made up of experts with appropriate backgrounds?
1.7. Was the operating personnel including the operators involved and how (in the writing, as reviewers, etc.)?
1.8. Was the training personnel involved early enough in the development process and how?
1.9. Were the organizational aspects of the EOPs clearly defined (role of control room staff and support teams, authorities and responsibilities after declaration of an emergency)?
1.10. If a reference methodology is used is there an adequate transfer of technology (know-how), i.e. not limited to the access to the reference documents?
1.11. If a reference methodology is used has the overall applicability of the method (to the particular plant) been evaluated and documented?
1.12. Was a QA programme for EOP development, implementation and maintenance developed and applied throughout the project?
1.13. Were all the tasks to be carried out during an emergency (e.g. classification) considered?

### I.2. TASK 2: SUPPORTING ANALYSES[13]

2.1. Did the analyses use a dedicated methodology developed for the purpose of the EOP's development?
2.2. Are the supporting analyses properly defined and technically correct?

---

[12] See Sections 4.5.1 and 4.5.2.
[13] See Section 4.5.3.

2.3. Is the approach to modelling and computer codes/models used for analyses up to date?
2.4. Were the scenarios for analyses defined by operations oriented personnel (see Section 3.3)?
2.5. Was there any independent assessment of the analysis results?
2.6. Were the conditions in the facility in which responder actions are necessary and the response of the personnel, instrumentation and systems of the facility under emergency conditions considered?

## I.3. TASK 3: EOP DEVELOPMENT[14]

**Scope of the EOP and general features of the EOP package:**

3.1. Do the procedures comply with system descriptions and operator actions specified in the safety analysis report?
3.2. Are the initial plant conditions covered by the procedures clearly defined and documented?
3.3. Are the transitions between AOPs, EOPs and SAGs clearly defined and consistent?
3.4. Is the final plant status (i.e. EOP exit conditions) clearly defined and documented?
3.5. Is the overall structure defined and justified?
3.6. Is the list of specific safety functions defined and justified?
3.7. Are all the possible challenges to these safety functions identified, classified and justified?
3.8. Is the list of procedures defined and justified?
3.9. Is there a proper verification of automatic actions?
3.10. Do the procedures contain an initial diagnostic section allowing discrimination between the events?
3.11. Are there continuous diagnostics which will allow the operator to recognize errors, combinations of accidents or time evolving accidents?
3.12. Are there explicit rules for transitions between procedures?

### I.3.1. Completeness and technical justification of individual procedures

3.13. Are the entry conditions, objectives and major actions justified and documented for every procedure?

[14] See Section 4.5.4.

3.14. Have all strategies been technically justified and documented for every procedure?
3.15. Does each procedure have sufficient background documentation to allow for operator training?
3.16. Is every action in each procedure properly documented for traceability (knowledge retention)?
3.17. Were the recommendations of Ref. [3] followed and implemented as appropriate for each procedure?
3.18. Were all procedures subject to independent review?
3.19. Were the consistency aspects addressed in Section 3.4.2 taken into account?

### I.3.2. Human factor aspects of EOPs

3.20. Does the format of the EOPs take into account human factor aspects according to current knowledge?
3.21. Is the supporting information to the operators provided in a user friendly way?

## I.4. TASK 4: VERIFICATION AND VALIDATION[15]

4.1. Was the verification programme properly defined and documented?
4.2. Was the validation programme properly defined and documented?
4.3. Was the validation team composed of experts with sufficient background and adequate knowledge?
4.4. Were the human factor aspects properly addressed?
4.5. Was the set of validation sequences representative of the EOP package as a whole?
4.6. Were the tools used as support (simulator, codes, etc.) adequate for their purpose (e.g. did they realistically represent the conditions under which the EOPs would be used)?
4.7. Were the operator shifts used for validation uninvolved in the development of the EOPs?
4.8. Were the operator shifts properly trained before the validation exercise (rules of usage only)?
4.9. Was a validation report issued?
4.10. Were the discrepancies properly documented?

[15] See Sections 4.5.5, 4.5.6.

4.11. Were the discrepancies properly resolved (complete documentation and justification of the resolution)?
4.12. Was the revised package revalidated? If not, is it adequately justified?

## I.5. TASK 5: EOP DOCUMENTATION[16]

5.1. Is the plant specific administrative documentation recommended in Section 3.7.2 available and has it been properly used in the development of EOPs?
5.2. Were the technical reference documents recommended in Section 3.7.1 developed and used in the EOP development?

## I.6. TASK 6: TRAINING[17]

6.1. Were the instructors involved in the EOP development process?
6.2. Did instructors complete their own training on the new set of EOPs?
6.3. Was a plant specific initial training programme for the operators developed?
6.4. Was the content of this programme adequate?
6.5. Does the training support documentation cover all aspects relevant to use of the EOPs (relevant phenomenology theory, safety concepts, etc.)?
6.6. Is there a programme to monitor/evaluate/improve the effectiveness of the training?
6.7. Is there a systematic process to collect, process and evaluate the feedback from training sessions?
6.8. Were the examination questions elaborated by technically competent experts in the field of EOPs?
6.9. Is an adequate retraining programme in place?
6.10. Is documentation of priorities in procedures available for training?
6.11. Is a sufficient part of the training dedicated to the most important procedures?
6.12. Are the operators and instructors properly trained on plant modifications?

[16] See Section 4.5.7.
[17] See Section 4.5.8.

## I.7. TASK 7: IMPLEMENTATION AND LONG TERM MAINTENANCE PROGRAMME[18]

7.1. Is there a systematic process to evaluate the effect of any plant design change on the EOPs?
7.2. Does the modification control in the plant include EOP maintenance?
7.3. Are the changes made to the EOPs properly documented (i.e. traceable)?
7.4. Is the feedback from the operator training programme (simulator and theoretical) effectively used in the EOP maintenance programme?

[18] See Section 4.5.9.

## Appendix II

## EOP REFERENCE SYSTEMS

Examples of the Westinghouse Owners Group (WOG), Electricité de France (EdF), General Electric Owners Group (GEOG), Combustion Engineering Owners Group (CEOG), CANDU and Siemens reference systems are briefly characterized below in terms of the general discussions presented in Sections 2 and 3.

### II.1. EOPS BASED ON THE WOG REFERENCE SYSTEM

Although some differences in procedure and format exist between different plants, emergency response guidelines (ERGs) are generally written in a dual column format. The left column lists operator instructions (actions) and the right column defines actions to be taken if the expected result or response detailed in the left column is not obtained (RNO — response not obtained).

The key elements of the EOP packages are:

(a) Immediate actions and diagnostics procedures;
(b) Event related symptom based optimal recovery guidelines (ORGs);
(c) CSF restoration guidelines (scenario independent);
(d) CSF status trees.

The key elements are discussed briefly below.

#### II.1.1. Immediate actions and diagnostic procedure

ERGs may not be entered into and used until a manual or automatic reactor trip or safety injection has been initiated, or conditions exist that should have resulted in either actuation. Regardless of the trip-initiating event, the first ERG entered is the 'reactor trip or safety injection' (E-0) procedure. This procedure serves four basic functions:

(1) It checks whether the minimum support conditions assumed for the EOPs are present;
(2) It determines if the event falls into the accident or incident category;
(3) It verifies proper automatic response and alignment of systems;

(4) It directs diagnosis of event symptoms and guides operating staff to an ORG.

Once the E-0 procedure is entered it is not exited until there is a direct transition to an ORG or an FRG as identified by the symptoms being monitored in E-0 or as being directed by the CSF status trees, respectively.

### II.1.2. Event related symptom based ORGs

Instructions for diagnosis and recovery from a broad spectrum of predefined event sequences, which are determined to be the significant risk contributors, are contained in the ORGs. These guidelines provide predefined symptom based event related recovery strategies. The guidelines are organized into four basic categories and are consistent with the four categories of non-accident and accident event sequences:

Category 0 — non-accident: This category includes the entry point to the ERGs and includes guidance for non-accident event sequences, including loss of all AC power and natural circulation cooldown.

Category 1 — loss of reactor coolant: This category addresses symptoms associated with the loss of reactor coolant and includes guidance for cooldown and depressurization following a loss of reactor coolant, reduction and termination of safety injection and switchover to long term recirculation.

Category 2 — loss of secondary coolant: This category addresses symptoms associated with the loss of secondary coolant, including loss of secondary coolant from multiple SGs. This procedure set includes guidance for isolation of faulted SGs.

Category 3 — SG tube rupture: This category addresses symptoms associated with SGTRs, including tube ruptures in multiple SGs and tube ruptures in combination with loss of reactor or secondary coolant.

Plant recovery will be directed by guidance provided in an ORG unless plant conditions dictate transition to the FRGs.

### II.1.3. CSF restoration guidelines

The concept of CSF restoration is based on the premise that radiation release to the environment is minimized if barriers to radiation release are protected. The CSF restoration guidelines are aimed at protection of these barriers between radioactivity contained in the fuel and the public and can be grouped into three major classes:

(1) Protection of the fuel matrix and fuel cladding;
(2) Protection of the RCS pressure boundary;
(3) Maintenance of containment/confinement integrity.

Because this set of procedures is entered only if a CSF is challenged, it is obvious that the recovery strategy in the optimal recovery procedure has failed. Restoration of the CSF becomes the highest priority and overrules all current activities. The challenge to the barrier is directly attributable to the challenge of the respective CSF. The basic strategy of the function restoration part of the EOPs is to maintain acceptable functioning of as many safety functions as possible, in order of their priority.

The CSFs applied in the WOG reference system, in order of priority, are:

(1) Subcriticality (protects the integrity of the fuel structure itself);
(2) Core cooling (protects the integrity of the fuel cladding or structure);
(3) Heat sink (protects the integrity of the RCS);
(4) Integrity (protects the integrity of the RPV);
(5) Containment (protects the integrity of containment/confinement);
(6) Inventory (indirectly protects the integrity of the RCS).

Corresponding to these six safety functions are six groups of CSF restoration guidelines, each containing several procedures with restoration strategies determined by the severity of the challenge.

### II.1.4. CSF status trees

The CSF status trees (flow diagrams) are basic tools used for directing the operating crew between the ORGs and the FRGs, and thus switch between scenario dependent and scenario independent activities. Monitoring of the status tree starts early in the accident and is done continuously by an assigned member of the control room crew (e.g. safety engineer). Continuous monitoring provides an event independent diagnosis of the safety status of the plant barriers, independent of the activities performed according to the event related procedures in effect. Based on the severity of the challenge to a specific safety function the operators are directed into a respective restoration guideline. After restoration of the safety function, the operator proceeds according to the ORG that was in effect before the transition or in accordance with a lower priority level FRG, depending on plant conditions existing at the time.

## II.2. EOPs BASED ON AN EDF REFERENCE SYSTEM

### II.2.1. Present status

At present, two EOP reference systems are implemented in French plants (34 units with three loops and 24 units with four loops):

(1) The 'generalized state approach' set of EOPs ('approche par état' in French), which is implemented on all four loop units (including a fully computerized version for the N4 plants, the most recent 4 loop units) and on some three loop units.
(2) The 'symptom/state based' set of EOPs ('événementiel' in French) which is still implemented on most of the three loop units. By 2005, all three loop units are expected to adopt the set of 'generalized state approach' EOPs.

### II.2.2. Scenario dependent/scenario independent approach

The 'generalized state approach' set of EOPs is a full set of scenario independent EOPs.

The 'symptom/state based' set of EOPs includes two subsets of procedures:

(1) A subset of scenario dependent procedures designed to provide optimal guidance for these scenarios;
(2) A subset of scenario independent procedures allowing control of the safety functions under all conditions, including multi-failure situations.

### II.2.3. Safety functions and states

The three fundamental safety functions (safety objectives) are to control the reactivity, to ensure the heat removal and the confinement of radioactivity. This is achieved by controlling the following state functions (also called safety functions in the present publication):

— Subcriticality;
— RCS pressure and temperature;
— RCS inventory;
— SG inventory;
— SG integrity;
— Containment/confinement integrity.

By using a well defined set of reliable plant parameters available in the control room, the 'state' of the plant can be evaluated at any time based on the status of each state function. According to this evaluated 'state' the safety functions are then prioritized and the associated operating strategies defined (taking into account the available systems needed for adequate operation).

The main parameters used for 'state' diagnosis include the RPV water level, the subcooling margin, the core outlet temperature, the SG water level, the SG activity, the containment/confinement pressure, and the containment/confinement dose rate.

For the 'generalized state approach' diagnosis is directly implemented in the EOPs used by the operators, as the operating strategies are designed according to the status and priority of the safety functions at any time. Full redundancy is built in through independent monitoring by the safety engineer who has a separate procedure.

For the 'symptom/state based' set of EOPs, diagnosis is included in the EOP package by a separate procedure for the safety engineer who monitors the status of the safety functions and asks the supervisor for complementary actions as defined in this procedure.

### II.2.4. Scope

Both EdF reference sets of EOPs cover incident procedures, DBA procedures and BDBA procedures which remain valid until fuel damage. Thereafter, the EOP set is no longer applicable and SAGs are to be entered. Transition criteria are clearly defined and concentrated in only one procedure executed by the safety engineer. On the other side of the spectrum of events, all incidents that may lead to an accident situation are included in the EOP set. Such typical examples are LOCA and SG tube ruptures without safety injection, spurious safety injection, electrical power losses and operation from a shut down panel. For BDBA, typical examples are total loss of essential water/component cooling, total loss of heat sink (SG feedwater), or total loss of electrical power (on-site/off-site).

### II.2.5. Plant modes

Both EdF reference sets of EOPs cover all plant modes from normal power operation down to hot and cold shutdown, cold shutdown with RCS open, and refuelling. The diagnosis procedure is valid for all shutdown plant modes where automatic protection signals no longer exist or are actuated with long delay.

### II.2.6. Structure

Both EdF reference sets of EOPs contain four essential groups:

(1) Diagnosis valid for all plant modes based on reliable plant information available in the control room;
(2) Optimal recovery of incident and accident situations up to core damage;
(3) Continuous safety function monitoring for recovery actions when the safety functions are challenged due to degradation of the situation, multi-failures and/or human errors;
(4) Local action sheets referenced in the set of procedures and to be implemented by field operators.

Both EdF reference sets of EOPs have four separate procedures: for the reactor operator, for the water and steam (turbine) operator, for the shift supervisor (containing a combination of reactor, water and steam operator procedures) and for the safety engineer. All procedures are in the colour flow chart format (paper based). The recent four loop N4 plants have fully computerized procedures (with computerized operating actions actuated from the operator video display units) as well as a complete backup paper based set of procedures for operating from the auxiliary panel if the computer system fails.

The 'symptom/state based' EOP package is structured as follows:

(a) One initial diagnosis procedure without safety injection actuation and another one with safety injection actuation. These procedures are implemented by the supervisor and by the operators.
(b) A set of symptom based procedures for recovery actions dealing with incidents (I procedures), DBAs (A procedures) and BDBAs (H procedures). These are scenario dependent procedures and implemented by the supervisor and the operators.
(c) One state based procedure for ultimate recovery actions when I, A and H procedures have become ineffective (U procedure). This is diagnosed and initiated by the safety engineer through his continuous safety function monitoring and constitutes the ultimate non-optimized recovery actions before potentially going to SAGs. This procedure is scenario independent and implemented by the supervisor and the operators.
(d) One state based continuous safety function monitoring procedure for continuous diagnosis and complementary actions when I, A, H procedures are in force and the residual heat removal system is not connected, and another one when the residual heat removal system is

connected. Both procedures are scenario independent and implemented by the safety engineer.

(e) One state based continuous safety function monitoring procedure for continuous diagnosis and complementary actions when the U procedure is in force. This procedure is scenario independent and implemented by the safety engineer.

The 'generalized state approach' set of EOPs is an important extension of the above mentioned state based procedures and is designed on the following principles:

(1) The set of EOPs is scenario independent: diagnosis and operation are not related to specific events but to the state of the plant.
(2) A limited number of representative states can be used to define the diagnosis, the EOPs, the safety priorities and the operating strategies.
(3) Each EOP has a limited number of operating strategies organized in sequences. Each sequence contains operating actions, important system surveillance, support system surveillance and a continuous diagnosis (loop structured).
(4) The continuous diagnosis at the end of each operating sequence induces the operator either to restart at the beginning of the sequence or change to another operating sequence or to another EOP.
(5) The systematic surveillance detects the loss of different support functions (electrical sources, air, cooling water sources). A separate action sheet is then used to guide the operator.
(6) The systematic surveillance detects the loss of systems which are required for implementing the operating strategy. An alternate system is then proposed to the operator (substitution).
(7) Concurrent with the use of team EOPs, a continuous state monitoring procedure is used by the safety engineer, providing the major safety actions with an additional degree of redundancy. This procedure provides a direct link with the states and actions to be taken independently of the operational logic diagram used by the control room operators.

The 'generalized state approach' EOP package is structured as follows:

(i) One initial diagnosis procedure when the residual heat removal system is not connected and another when the residual heat removal system is connected. This is implemented by the supervisor and the operators.
(ii) A limited set of state based procedures for recovery actions with graded response from no state functions challenged to several state functions

challenged, valid for all plant modes. This set is implemented by the supervisor and the operators. For example, the reactor operator has four procedures for non-shutdown plant modes, two procedures for shutdown modes with RCS closed, and one procedure for shutdown mode with RCS open.

(iii) Two continuous state monitoring procedures providing an additional degree of redundancy on the major safety actions (one for RCS closed and one for RCS open). These procedures are implemented by the safety engineer.

(iv) A set of action sheets for loss of support functions and restoration, valid for all plant modes.

(v) The impact of fire on operations is built into the EOPs through separate fire action sheets.

## II.3. EOPs BASED ON THE GEOG REFERENCE SYSTEM

GEOG methodology, approach and format have significant differences from those of PWR designs. The flow chart format employs symbols to replace much of the text and is organized such that all the parameters in a given flow chart are managed concurrently. Additionally, the flow charts themselves are managed concurrently. This arrangement is used for two reasons: (1) action taken to manage any parameter that affects the management of the others and, (2) prioritization cannot be predefined for one parameter over another without diagnosing the event and being reasonably confident of the event's outcome.

Therefore the EOPs are designed to be functional within the allotted space available in the plant control room and to accommodate these two factors while clearly indicating the concurrent nature of the parameter subsections. While they share the symptom based philosophy of the PWR EOPs, their approach is significantly different.

### II.3.1. Entry and exit

Each EOP flow chart is entered whenever any of its prescribed entry conditions occurs, irrespective of whether that procedure has already been entered or is presently being executed. An EOP flow chart is exited when either an exit condition specified in the procedure is satisfied or it is determined that an emergency no longer exists. After a procedure has been entered, subsequent clearing of all entry conditions for that procedure is not, by itself, a conclusive indication that an emergency no longer exists. If an EOP has already been entered and a new entry condition is reached, that procedure

will be re-entered and all steps addressed again from the beginning of the procedure.

### II.3.2. Procedure hierarchy

Exercise of EOP flow charts takes precedence over guidance provided in any other procedure that may be in the process of being carried out when an EOP entry condition occurs. Thus procedures that may be performed concurrently with an EOP must not subvert the EOP strategy or otherwise render equipment inoperable which might be required to complete EOP actions.

### II.3.3. Level of detail

GEOG EOP flow charts are designed to contain sufficient top level guidance as needed to implement the strategy that achieves the EOP objectives. Any guidance beyond this level may be a distraction to the user and impede the achievement of procedure objectives in rapidly progressing transients and is therefore not included in the flow chart procedures. However, this supporting information is available to the operator in basis documents located in the control room. Additionally, a great effort is made to replace text with quickly and easily recognized icons.

The amount of training on EOP bases that will be afforded to the user is a factor in determining the level of detail required in an EOP. The more training that can be provided, the more information can be relegated to memory, leaving less procedural information. Other factors that were considered are the complexity of the strategies, the command and management structure invoked in the control room, the prevalence of instrumentation and controls to manage parameters specified in the EOP, and the number and experience of operators available on-shift to carry out EOP actions.

### II.3.4. EOP organization

GEOG EOPs are organized into four flow charts (primary procedures) supported by six contingency procedures. The four primary EOP flow charts are:

(1) RPV control EOP;
(2) Primary containment (PC) control EOP;
(3) Secondary containment (SC) control EOP;
(4) RR control EOP.

The RPV control EOP is designed to maintain adequate core cooling, shutdown of the reactor, and decrease RPV temperature to 'cold shutdown' conditions. Entry into this procedure is required at an RPV water level below (low level scram set point), RPV pressure above (high pressure scram set point), drywell pressure above (high pressure scram set point), and SCRAM condition and reactor power above a certain value (average power range monitor downscale trip) or reactor power cannot be determined.

The PC control EOP is designed to provide a barrier to the uncontrolled release of fission products, contain and condense steam discharged through the safety relief valves and primary cooling system breaks, shield personnel from radiation emitted by the reactor, and provide a protected environment for key equipment important to safety. Entry into this procedure is required at a suppression pool temperature above the limiting condition for operation (LCO), a drywell temperature above LCO, a containment temperature above LCO, a drywell pressure above the high pressure scram set point, a suppression pool water level above maximum level LCO, a suppression pool water level below minimum level LCO, and an SC hydrogen concentration above the alarm set point.

The SC control EOP is designed to maintain SC integrity, limit radioactivity release to and from the SC, and protect equipment in the SC. Entry into this procedure is required at an SC pressure at or above atmospheric pressure, an area temperature above the maximum normal operating temperature, a cooler differential temperature above the maximum normal for operation, an exhaust fan radiation level above the maximum normal for operation, an area radiation level above the maximum normal for operation, a floor drain sump water level above the maximum normal for operation, and an area water level above the maximum normal for operation.

The RR control EOP is designed to establish a basis for isolating systems and controlling RPV pressure to minimize the off-site release of radioactivity and provide the interface/transition between the site emergency plan and the symptomatic control of RPV, PC and SC parameters. Entry into this procedure is required at radiation release levels requiring declaration of an alert.

If parameters cannot be stabilized using the four primary EOPs the operator will be directed to transition to one of the following contingency procedures, employing more severe mitigation strategies:

(a) The alternate level control contingency procedure contains more detailed instructions on the use of injection systems.
(b) The emergency RPV depressurization contingency procedure contains additional guidance on establishing or maintaining adequate core cooling, terminating or minimizing discharge from a primary system break,

minimizing RR from the RPV, reducing the energy contained in the RPV before conditions are reached at which the pressure suppression system is ineffective, and maximizing injection flow into the RPV.

(c) The steam cooling contingency procedure provides guidance on the optimization of heat transfer to the remaining RPV coolant inventory.

(d) The RPV flooding contingency procedure provides guidance to ensure adequate core cooling by a combination of submergence and steam cooling.

(e) The level/power control contingency procedure provides guidance to ensure that the reactor will remain shut down under all conditions.

(f) The SC flooding contingency procedure provides guidance on the restoration of adequate core cooling through core submergence.

## II.4. EOPS BASED ON THE CEOG REFERENCE SYSTEM

The CEOG EOP methodology, approach and format are very similar to WOG ERGs, with minor differences in terminology and structure. The elements of the EOP structure remain the same. Although some differences in the procedural format exist between different plants, emergency procedure guidelines (EPGs) are generally written in a dual column format. One column lists operator instructions and the opposite column defines contingency actions.

The key elements of the EPG package are:

(a) Standard post-trip actions and diagnostics procedures;

(b) Event related ymptom based ORGs (scenario dependent);

(c) Functional recovery guidelines (scenario independent);

(d) Safety function status check.

A brief discussion of each element is presented in the following sections.

### II.4.1. Standard post-trip actions and diagnostics procedure

The standard post-trip actions procedure serves as the stepping stone into the Combustion Engineering EPG structure. EPGs may not be entered and used for guidance until a manual or automatic reactor trip has been initiated or conditions exist that should have resulted in an automatic reactor trip. Regardless of the reactor trip initiating event, the standard post-trip actions procedure will be the first EPG utilized. Entry and utilization of another EPG of any type may not take place until completion of the post-trip actions. The standard post-trip actions procedure serves three basic functions, as follows:

(1) All relevant safety functions are checked against acceptance criteria to show the operator the entire status of plant safety;
(2) The check of safety functions provides the operator with objective decision making criteria as to whether action is required in the short term to restore plant safety;
(3) The status check distinguishes between an uncomplicated reactor trip (e.g. one caused by technician error) and more complex events.

The immediate actions to verify the safety function criteria are in a specific order of completion that prioritizes the safety functions as standardized by the CEOG guidelines.

After completion of the standard post-trip actions, diagnostic aids will be consulted to assist in quickly identifying the optimal procedural guidance. If all safety function criteria are satisfied the operator will be directed to a recovery procedure for an uncomplicated reactor trip recovery. If one or more of the safety function criteria are not satisfied by means of the diagnostic guidance, the operator will be directed to an optimal recovery procedure or the functional recovery procedure.

### II.4.2. Event related symptom based ORGS

ORGs are used to treat specific symptom sets that are identifiable or can be diagnosed following a reactor trip. As indicated earlier, the standard post-trip actions are performed before an ORG is implemented. The emphasis in the ORGs is on treatment of a set of symptoms according to an optimal strategy, as contrasted to treatment of a specific event. One of the first recovery actions will be to assess the safety functions against specific acceptance criteria using an ORG specific safety function status check. This serves a dual purpose. First, it is a check to verify that all safety functions are being satisfied. Second, it provides a means of verifying that the initial diagnosis was correct. If the guideline in use is adequately treating the symptoms the treatment is continued. If the treatment is inadequate, either because new symptoms appear that are not covered in the guideline or because the observed symptoms are not properly responding, each ORG has a step that requires the operators to exit the ORG and to implement an FRG. The checking process using the safety function status check continues as long as the guideline is in use. This is the way the EPG system manages multiple, significant failures or misdiagnosed symptom sets. Combustion Engineering ORGs that reflect specific symptom based event sets are as follows:

(a) Reactor trip;
(b) Loss of coolant accident (LOCA);
(c) Steam generator tube rupture (SGTR);
(d) Excess steam demand event (ESDE);
(e) Loss of all feedwater (LOAF);
(f) Loss of forced circulation (LOFC);
(g) Loss of off-site power (LOOP);
(h) Station blackout (SB).

### II.4.3. Functional recovery guidelines

Combustion Engineering defines a safety function as a condition or action that prevents core damage or minimizes radiation release to the public. These safety functions are involved with maintaining the integrity of barriers between the fuel and the public and can be grouped into three major classes, anti-core melt safety functions, containment integrity safety functions, and vital auxiliary safety functions. The functional recovery guidelines are aimed at establishing and maintaining these safety functions in order to protect the public. Because this set of procedures is entered only if a safety function is challenged it is obvious that the recovery strategy in the ORG failed or a specific event diagnosis was not possible. Restoration of the safety functions is the highest priority and overrides all other activities. The challenge to a barrier is directly attributable to the challenge to the respective safety function. The strategy of the FRGs is to maintain as many safety functions as possible in an acceptable condition. Challenged safety functions are restored according to priority.

The prioritized safety functions in the Combustion Engineering reference system are:

(a) Reactivity control (protects integrity of the fuel structure itself);
(b) Maintenance of vital auxiliaries (AC and DC power) (supports all safety functions);
(c) RCS inventory control (supports heat removal);
(d) Core heat removal (protects the integrity of the fuel cladding and structure);
(e) RCS heat removal (protects the integrity of the RCS);
(f) Integrity of the coolant boundaries (protects the integrity of the RPV);
(g) Containment integrity (protects the integrity of confinement);
(h) RCS coolant inventory (indirectly protects the integrity of the RCS).

Corresponding to these eight safety functions are eight groups of safety function recovery guidelines, each containing several restoration strategies

(success paths) to provide guidance in re-establishing safety functions, depending on the severity of the challenge.

### II.4.4. Safety function status checks

Safety function status checks are basic tools used for directing the operating crew between the ORGs and the function recovery guidelines and between scenario dependent and scenario independent activities. Each ORG has its own safety function status check that must be used whenever an ORG is in use. This is accomplished by comparing control board indications to safety function acceptance criteria tailored for each class of event. Monitoring of the safety functions is started early in the accident and is done continuously by a dedicated member of the control room crew (e.g. safety engineer). Continuous monitoring provides a diagnosis of the safety status of the plant barriers, independent of the activities performed according to the event related procedures in effect. Based on the severity of the challenge to a specific safety function the operators are directed into a recovery guideline. After restoration of the safety function, and assuming a success path has been satisfied for all safety functions, the operator proceeds according to guidance provided under the functional recovery guidelines' long term actions.

## II.5. CANDU (PHWR) GENTILLY-2 OPERATING RESPONSE STRATEGY TO ABNORMAL EVENTS

This general approach is based on implementation of the following safety functions;

(a) Shutdown of the reactor;
(b) Containment of radioactive substances if released to the reactor building;
(c) Maintenance and restoration of appropriate heat sink, if required;
(d) Monitoring and control of parameters that guarantee the integrity of safety barriers that have not sustained damage.

The improvement of scenario dependent EOP diagnosis allowed discrimination in favour of the most important parameters, which must be monitored continuously. As a result, monitoring procedures have been implemented. Four sets of parameters are defined in these procedures:

(1) Critical safety parameters (CSPs);
(2) Main safety parameters (MSPs);

(3) Other specific EOP diagnosis parameters;
(4) Main turbine parameters (MTPs).

The CSPs are a small set of parameters whose status, over a determined limit, indicates a threat to or a deterioration in the integrity of the safety barriers. For all CSPs, a restoration guide has been prepared aiming at the re-establishment of the parameters within acceptable limits or the mitigation of the consequences.

The CSPs are:

(i) Reactor power;
(ii) The subcooling margin at the four inlet headers;
(iii) Pressure in the reactor building;
(iv) Activity at the outlet of the reactor building;
(v) Activity in the SGs;
(vi) Activity in the service water.

The MSPs are a larger set of parameters and they give, if maintained within determined limits, a sure indication that the reactor power is under control, that the fuel is adequately cooled and that the radioactivity is properly contained. All the CSPs are included in the MSPs. Monitoring of MSPs aims to confirm the response of the plant and helps to anticipate deterioration of the general plan conditions. Some parameters other than CSPs and MSPs, which are key elements in the diagnosis of scenario dependent EOPs, must also be monitored continuously. The monitoring of this third category of parameters helps to re-actualize the diagnosis during the use of a scenario dependent EOP.

The MTPs are a small set of parameters and they give, if kept within predetermined limits, a sure indication that the turbine integrity is not threatened while unloading or decelerating.

Several computer display bar charts are specially dedicated to rapidly monitor those very important parameters (CSPs, MSPs, MTPs and other parameters of scenario dependent EOP diagnosis).

This global approach aims at facing any abnormal situation. This approach consists of nine major stages:

(1) Recognition of an abnormal situation (automatic power reduction or an identified event requiring an immediate power reduction greater than 10% of full power);
(2) Verification of the efficiency and of the completion of the actions of automated systems actuated (special and support safety systems);

(3) Actions in the main control room (MCR) prior to evacuation and actions in the secondary control area if the MCR becomes inoperative and/or uninhabitable;
(4) Verification and completion of the actions of emergency core cooling, if automatically actuated;
(5) Continuous monitoring of CSPs, MSPs, MTPs and other parameters of scenario dependent EOP diagnosis;
(6) Restoration of the subcooling margin, if required;
(7) Diagnosis;
(8) Application of scenario dependent procedures:
— Common mode event EOP,
— EOP,
— Alarm sheet procedure,
— Abnormal operating manual procedure,
— Abnormal general operating procedure;
(9) Criteria to reset a shut down system after a trip and increase power.

The operating response strategy to an abnormal event is presented in Fig. 3. Verification of the efficiency and of the completion of the actions of the automated systems actuated rely upon documented good practices and a set of scenario independent EOPs and EOP handouts.

## II.6. CONCEPT OF OPERATING PROCEDURES IN GERMAN NUCLEAR POWER PLANTS

### II.6.1. General description

The design criteria for KWU plants specify that no manual intervention by the plant staff be necessary for at least 30 minutes following an initiating event leading to an internal accident and 10 hours following an external impact. During this time the plant is automatically controlled by the reactor protection system and other automatic protection measures. Internal accidents are accidents originating within the plant. External impacts are earthquakes, pressure waves caused by explosions and aircraft crashing into a nuclear power plant installation.

The CSFs are permanently monitored using, on the one hand, specified individual parameters such as pressure, temperature and liquid level and on the other hand using the PRISCA® process information system that displays all CSFs graphically on monitors. The process information system also displays

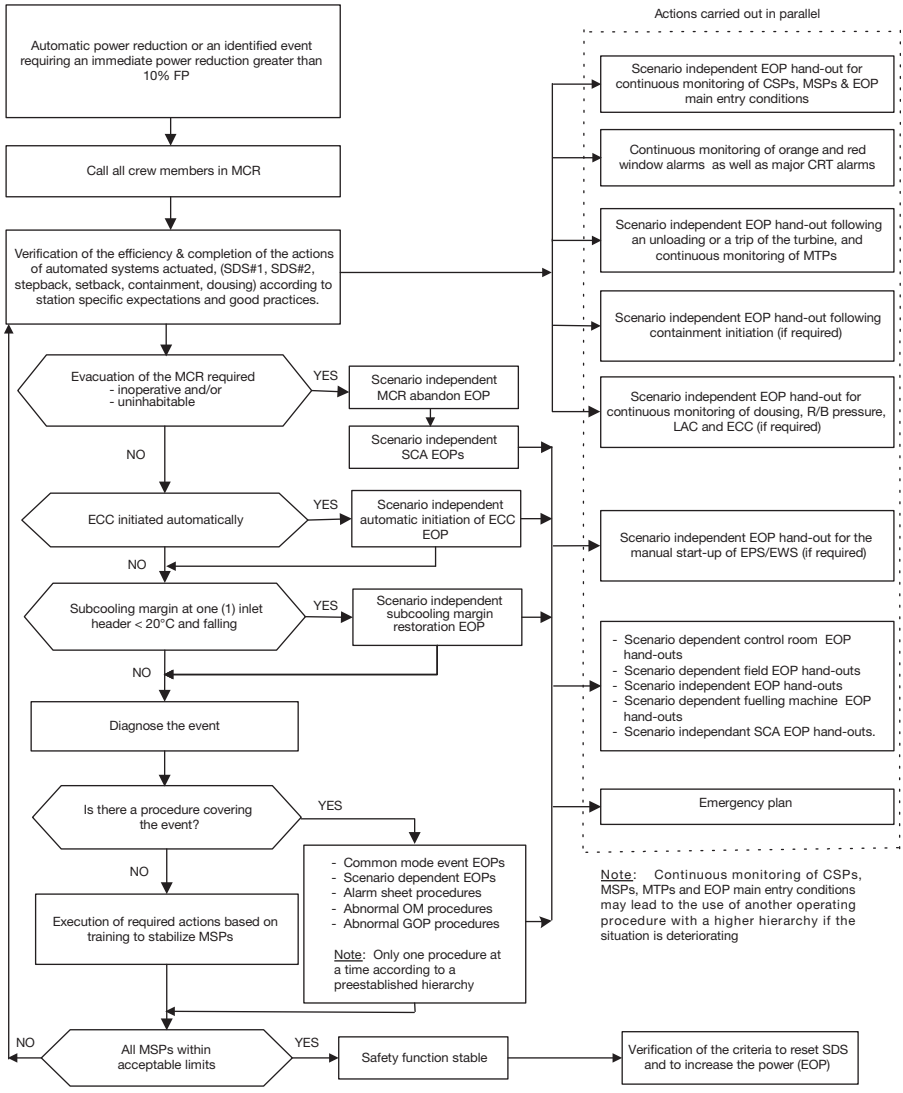



*FIG. 3. Operating response strategy to an abnormal event at the Gentilly-2 nuclear power plant.*

a diagnostic logic tree with the help of which the operator can, in the majority of cases, identify the accident initiating event. After a positive identification, the appropriate event oriented procedure is selected and carried out. In this case, event oriented procedures are preferable as they constitute an optimized, simulator verified procedure which brings the plant to a safe shutdown

condition with the least thermal and mechanical stresses to the plant components. While the event oriented procedure is carried out, the CSFs are, at all times, monitored in parallel.

Should the event oriented procedure not be successful, i.e. should, due to additional failures, erroneous diagnosis, human errors or any other reason, a CSF be challenged, the event oriented procedure will be abandoned and the control room staff will concentrate on monitoring the CSF. Uniquely defined CSF criteria alert staff to a CSF being challenged and preparatory measures (e.g. starting a pump) are taken. Another more severe criterion is used to determine a violation of a CSF and the appropriate measures to restore the CSF are then taken. These different criteria, which constitute a certain graduation, take into account the finite time required by the staff between recognizing the situation, preparing the necessary measures and carrying them out.

The CSF approach and event oriented accident management approach are not mutually exclusive. They are two complementary methods for dealing with an accident. The fulfilment of CSFs guarantees the safety of the reactor at any stage of an accident, regardless of the ability to identify the initiating event or despite the occurrence of multiple failures. The event oriented procedures, on the other hand, help in the case of positive identification of the initiating event to transfer the plant into a safe condition in such a way as to minimize thermal and mechanical stresses.

### II.6.2. Modular structure of EOPs

The modular structure of event oriented procedures and symptom oriented procedures has been developed to satisfy the requirement for increased clarity and manageability. Through this form of structuring, it is ensured that every user (shift supervisor, control room operator, on-site technicians, etc.) will receive the information necessary to carry out their respective tasks.

The central feature of modular accident handling, which is applicable to both event and symptom oriented procedures, is a flow diagram that shows in graphic form the sequence and overall strategy of the manual measures. This flow diagram is primarily designed for use by those personnel who will initiate the procedures, or those who will oversee the operation, i.e. the shift supervisor. He will transfer the plant into a safe condition with the aid of instruction elements and logical decision elements containing parameter values and criteria.

The detailed instructions for the control room operator are given in a separate section. The link between the manual measures given in the flow

diagram and the more detailed instructions needed by the control room operator to carry out a specific procedure is clarified through the use of special graphic elements.

If the same manual measures appear more than once in any particular flow diagram it is unnecessary to repeat the corresponding detailed instructions. Hence, another advantage of the modular structure is that the overall number of pages in the manual is significantly reduced, thus increasing its manageability.

An event oriented accident procedure, which is entered after identifying the initiating event, consists principally of:

(a) A flow diagram of event identification;
(b) A flow diagram of anticipated events followed by automatic measures;
(c) A flow diagram of manual measures;
(d) A detailed set of instructions for each of the automatic and manual measures referred to in the flow diagrams.

A symptom oriented accident procedure is entered independently of the initiating event or of the course the accident that has taken place to reach its current state. Therefore the description of the automatic measures is not included. The symptom oriented procedures are initiated after predefined criteria, which are based on a safety function being challenged, have been fulfilled. The procedures are carried out with the help of:

(1) A flow diagram of manual measures;
(2) A detailed set of instructions for each of the manual measures referred to in the flow diagrams.

# REFERENCES


[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1, INSAG Series No. 12, IAEA, Vienna (1999).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Operation, IAEA Safety Standards Series No. NS-R-2, IAEA, Vienna (2000).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000).

[4] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANISATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE CO-ORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Good Practices with Respect to the Development and Use of Nuclear Power Plant Procedures, IAEA-TECDOC-1058, IAEA, Vienna (1998).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Management Programmes in Nuclear Power Plants: A Guidebook, Technical Reports Series No. 368, IAEA, Vienna (1994).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Implementation of Accident Management Programmes in Nuclear Power Plants, Safety Reports Series No. 32, IAEA, Vienna (2004).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[9] OLIVIER, E., HAURE, J.M., "French emergency operating procedures for PWR 900MW and suggestions for their development on VVER plants", Safety and Reliability Systems of PWRs and BWRs (Proc. Int. Symp. Brno, 1995), Czech Nuclear Forum & Energovyzkum, Brno (1995).

[10] SAVOLAINEN, S., et al., "Development of the French emergency operating procedures for Loviisa power plant", Nuclear Power Plant Safety (Proc. 3rd Finnish–French Colloquium Lappeenranta, Finland, 2000).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of Simulation Techniques for Accident Management Training in Nuclear Power Plants, IAEA-TECDOC-1352, IAEA, Vienna (2003).

# GLOSSARY

**abnormal operation.** See anticipated operational occurrence.

**accident.** Any unintended event, including operating errors, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.

**accident conditions.** Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents. Examples of such deviations include a major fuel failure or a loss of coolant accident (LOCA).

**accident management.** The taking of a set of actions during the evolution of a beyond design basis accident: (a) to prevent the escalation of the event into a severe accident; (b) to mitigate the consequences of a severe accident; (c) to achieve a long term safe stable state.

**anticipated operational occurrence.** An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety nor lead to accident conditions. Examples of anticipated operational occurrences are loss of normal electrical power and faults such as a turbine trip, malfunction of individual items of a normally running plant, failure to function of individual items of control equipment, loss of power to the MCP. Some States and organizations use the term abnormal operation (for contrast with normal operation) for this concept.

**beyond design basis accident.** Accident conditions more severe than a design basis accident.

**design basis.** The range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems. Used as a noun, with the definition above. Also often used as an adjective, applied to specific categories of conditions or events to mean 'included in the design basis' as, for example, in design basis accident, design basis external events, design basis earthquake, etc.

**design basis accident.** Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

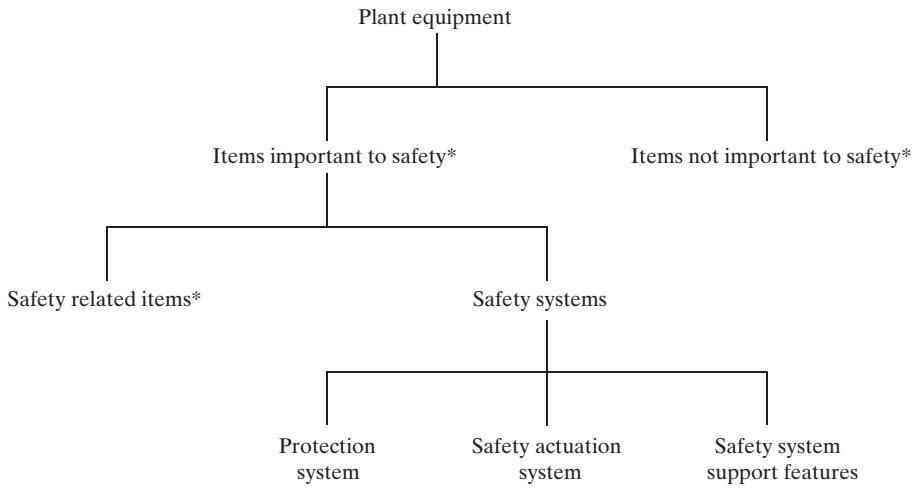
**initiating event.** An identified event that leads to anticipated operational occurrences or accident conditions and challenges safety functions.

**normal operation.** Operation within specified operational limits and conditions. For a nuclear power plant, this includes startup, power operation, shutting down, shutdown, maintenance, testing and refuelling.

**operational limits and conditions.** A set of rules setting forth parameter limits, the functional capability and the performance levels of equipment and personnel approved by the safety authorities for safe operation of an authorized facility.

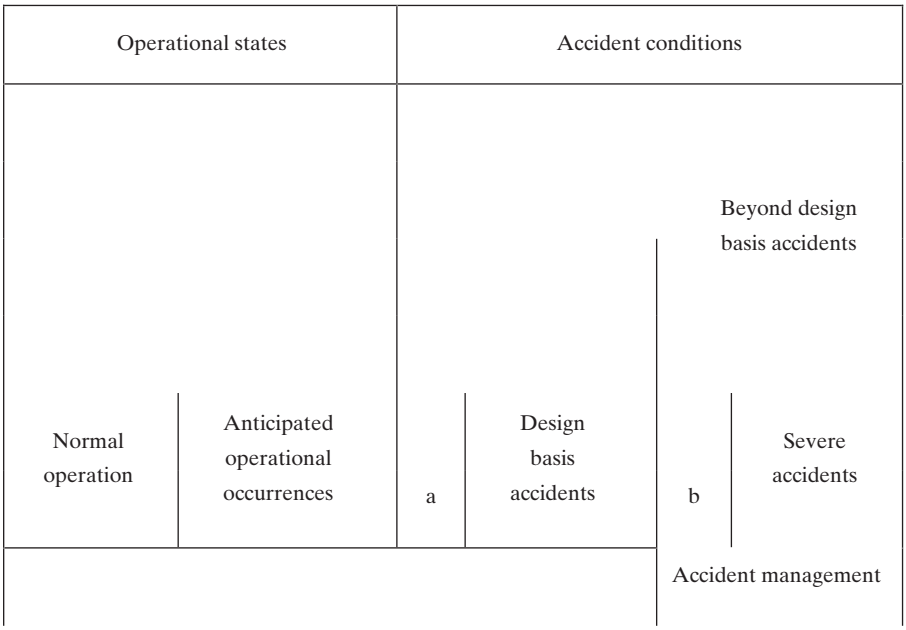
**operational states.** States defined under normal operation and anticipated operational occurrences. Some States and organizations use the term operating conditions (for contrast with accident conditions) for this concept.

**plant equipment.**




* In this context, an 'item' is a structure, system or component.

**plant states.**




[a] Accident conditions which are not explicitly considered design basis accidents but are encompassed by them.

[b] Beyond design basis accidents without significant core degradation.

**postulated initiating event.** An event identified during design as capable of leading to anticipated operational occurrences or accident conditions. The primary causes of postulated initiating events may be credible equipment failures and operator errors (both within and external to the facility), human induced or natural events.

**severe accident.** Accident conditions more severe than a design basis accident and involving significant core degradation.

**safety function.** A specific purpose that must be accomplished for safety.

**scenario.** A postulated or assumed set of conditions and/or events. Most commonly used in analysis or assessment to represent possible future conditions and/or events to be modelled, such as possible accidents at a nuclear facility, or the possible future evolution of a repository and its surroundings. A scenario may represent the conditions at a single point in time or a single event, or a time history of conditions and/or events.

## CONTRIBUTORS TO DRAFTING AND REVIEW

| | |
|---|---|
| Aleza, S. | Consejo de Seguridad Nuclear, Spain |
| Bansal, P.R. | Narora Atomic Power Station, India |
| Bath, N. | Bundesamt für Strahlenschutz, Germany |
| Boulay, D. | Gentilly nuclear power plant, Canada |
| Cappon, H.A. | Framatome ANP, France |
| Chen, Z. | Jiangsu Nuclear Power Corporation, China |
| Duchac, A. | Data Systems & Solutions, Czech Republic |
| Fagula, L. | Bohunice nuclear power plant, Slovakia |
| Fil, N.S. | EDO Gidropress, Russian Federation |
| Grudev, P. | INRNE, Bulgarian Academy of Sciences, Bulgaria |
| Gul, S. | Institute for Nuclear Power, Pakistan |
| Lhoest, V. | Westinghouse Energy Systems Europe, Belgium |
| Martin, T. | World Association of Nuclear Operators |
| Mišák, J. | International Atomic Energy Agency |
| Moffitt, R.L. | Pacific Northwest National Laboratory, United States of America |
| Schwarz, W. | Neckar nuclear power plant, Germany |
| Sherfey, L.L. | Pacific Northwest National Laboratory, United States of America |
| Spalj, S. | University of Zagreb, Croatia |
| Staneva, T.I. | Kozloduy nuclear power plant, Bulgaria |

| | |
|---|---|
| Vayssier, G.L.C.M. | Nuclear Safety Consultancy, Netherlands |
| Zold, T. | Mochovce nuclear power plant, Slovakia |

**Consultants Meetings**

Vienna, Austria: 23–27 April 2001, 12–16 August 2002

**Technical Committee Meeting**

Vienna, Austria: 27–31 May 2002

**Emergency operating procedures (EOPs) are essential for maintaining fundamental safety functions and preventing core damage during design basis accidents and beyond design basis accidents in a nuclear power plant. Many plants are presently in the process of improving their EOPs. The level of implementation of such updates varies from plant to plant, from the preparatory phase up to fully implemented and validated sets of procedures. This manual comprehensively covers all aspects of the implementation and review of EOP development programmes, relying on state of the art experience. It discusses the elements and key steps that must be included in any programme for the development and implementation of plant specific emergency operating procedures.**

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 92–0–103705–8
ISSN 1020–6450