Safety Reports Series
No.32

Implementation of Accident Management Programmes in Nuclear Power Plants

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 standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides.**

Safety Fundamentals (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

www-ns.iaea.org/standards/

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA 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 series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related publications are the **Technical Reports Series,** the **Radiological Assessment Reports Series,** the **INSAG Series, the TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series,** the **IAEA Services Series** and the **Computer Manual Series**, and **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. The IAEA also issues reports on radiological accidents and other special publications.

IMPLEMENTATION OF ACCIDENT MANAGEMENT PROGRAMMES IN NUCLEAR POWER PLANTS

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
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
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".

Printed by the IAEA in Austria
March 2004
STI/PUB/1167

SAFETY REPORTS SERIES No. 32

IMPEMENTATION OF ACCIDENT MANAGEMENT PROGRAMMES IN NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2004

IAEA Library Cataloguing in Publication Data

Implementation of accident management programmes in nuclear power plants. — Vienna : International Atomic Energy Agency, 2004.
p. ; 24 cm. — (Safety reports series, ISSN 1020–6450 ; no. 32)
STI/PUB/1167
ISBN 92–0–113803–2
Includes bibliographical references.

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

IAEAL 04–00351

FOREWORD

Many Member States operating nuclear power plants (NPPs) are at present developing accident management programmes (AMPs) aimed at the prevention and mitigation of severe accidents. Such developments are in compliance with a revised set of IAEA Safety Standards, in particular with Safety Requirements on design, on operation, and on preparedness and response for a nuclear and radiological emergency. However, the level of implementation varies significantly between NPPs. The exchange of experience and best practices can contribute considerably to the quality and facilitate the implementation of AMPs at the plants.

Various IAEA activities assist States in the area of accident management. Several publications have been developed which provide guidance and support in the establishment of accident management at NPPs. Various technical meetings and workshops are also organized to provide a forum for presentations and discussions and to share experience in the development and implementation of AMPs at individual NPPs.

This report provides a description of the elements which should be addressed by the team responsible for preparation, development and implementation of a plant specific AMP at an NPP. The issues addressed include formation of the team, selection of accident management strategies, safety analyses required, evaluation of the performance of plant systems, development of accident management procedures and guidelines, staffing and qualification of accident management personnel, and training needs. The report is intended to facilitate the work to be done by NPP operators, utilities and their technical support organizations, but it can also be used for the preparation of relevant national regulatory requirements.

This Safety Report serves as a basis for other, more specific publications. It also provides the basis for the safety service on Review of Accident Management Programmes, which is offered to Member States to perform an objective assessment of the status of various phases of AMP implementation as compared with international experience and practices.

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

1.1. Background 1
1.2. Objective 2
1.3. Scope 4
1.4. Structure 4

2. BASIC FEATURES OF AMPs 6

2.1. Objectives and background of accident management 6
2.2. Preventive and mitigatory features of accident management . 7
2.3. Accident progression and degrees of severity 9
2.4. Assessment of vulnerabilities and capabilities 10
2.5. Accident management strategies 11
2.6. Information needs 12
2.7. Plant equipment performance and material support needs ... 14
2.8. Procedures and guidelines 16
2.9. Phases of the AMP 17

3. PREPARATION OF THE ACCIDENT MANAGEMENT PROGRAMME 18

3.1. Team formation 18
3.2. Familiarization 20
3.3. Selection and definition of an AMP 20
3.3.1. Procedures versus guidelines and degree of proceduralization 21
3.3.2. Symptom based procedures and guidelines 22
3.3.3. Coverage 22
3.3.4. Entry and exit bases and interfaces 23
3.4. Review of available safety analyses and specification of further information needs 23
3.4.1. General 23
3.4.2. Analyses needed for AMP development 24
3.4.3. Preliminary analysis for EOPs 25
3.4.4. Preliminary analysis for mitigatory severe accident management actions 26

3.5. Evaluation of the plant equipment and instrumentation performance 27

4. DEVELOPMENT OF AN AMP 29

4.1. Selection and development of severe accident management strategies 29
4.1.1. Selection of severe accident management strategies 29
4.1.2. Development of severe accident management strategies 32
4.2. Development of accident management procedures and guidelines 33
4.2.1. Development and writing 33
4.2.2. Preparation of background material and documentation 35
4.3. Supporting accident analysis for development of procedures and guidelines 36
4.3.1. Development analysis of EOPs 36
4.3.2. Analysis for the development of severe accident management guidelines 37
4.4. Determination of the needs for plant instrumentation, equipment and material, and necessary upgrades 38
4.5. Integration of procedures, guidelines and the plant's emergency arrangements 39
4.6. Verification and validation of procedures and guidelines 42
4.6.1. Verification 42
4.6.2. Validation 42
4.6.3. Supporting analysis 43
4.7. Specification of training needs 44
4.8. Review of the AMP 44
4.9. Involvement of the regulatory body 45

5. IMPLEMENTATION 45

5.1. Overview of the plant's emergency organization 45
5.1.1. General 45
5.1.2. On-site emergency organization 46
5.1.3. Organizational aspects of implementation 48
5.1.4. Involvement of the regulatory body 48
5.2. Training 48
5.2.1. General 48

5.2.2. Scope and means 49
5.2.3. Skills of staff members 49
5.3. Staffing and qualification 51
5.4. Revisions to the AMP 52

APPENDIX I: PLANT DAMAGE STATES 53

APPENDIX II: CANDIDATE HIGH LEVEL ACTIONS 57

APPENDIX III: COMPUTATIONAL AIDS 61

APPENDIX IV: TYPICAL PARAMETERS AND MECHANISMS USED FOR INITIATION OF PREVENTIVE AND MITIGATORY ACTIONS 64

APPENDIX V: PREVENTIVE ACCIDENT MANAGEMENT ACTIONS 67

APPENDIX VI: REVIEW OF AN AMP 75

APPENDIX VII: TRANSITION FROM THE EOP DOMAIN TO THE SEVERE ACCIDENT MANAGEMENT GUIDANCE DOMAIN 94

APPENDIX VIII: USE OF PSA IN SAMG DEVELOPMENT 97

REFERENCES 101

ANNEX I: SUMMARY OF INTERNATIONAL ACTIVITIES IN SEVERE ACCIDENT MANAGEMENT 103

ANNEX II: OVERVIEW OF THE SEVERE ACCIDENT MANAGEMENT GUIDANCE APPROACH AND IMPLEMENTATION IN SOME MEMBER STATES . . . 105

ANNEX III: TYPICAL TSC ORGANIZATION AT A BWR IN THE USA 115

DEFINITIONS 117

CONTRIBUTORS TO DRAFTING AND REVIEW 121

1. INTRODUCTION

1.1. BACKGROUND

According to the generally established defence in depth concept in nuclear safety [1, 2], consideration in plant operation is also given to highly improbable severe plant conditions that were not explicitly addressed in the original design of currently operating nuclear power plants (NPPs). Defence in depth is achieved primarily by means of four successive barriers which prevent the release of radioactive material (fuel matrix, cladding, primary coolant boundary and containment), and these barriers are primarily protected by three levels of design measures: prevention of abnormal operation and failures (level 1), control of abnormal operation and detection of failures (level 2) and control of accidents within the design basis (level 3). If these first three levels fail to ensure the structural integrity of the core, e.g. due to beyond the design basis multiple failures, or due to extremely unlikely initiating events, additional efforts are made at level 4 to further reduce the risks. The objective at the fourth level is to ensure that both the likelihood of an accident entailing significant core damage (severe accident) and the magnitude of radioactive releases following a severe accident are kept as low as reasonably achievable. Finally, level 5 includes off-site emergency response measures, with the objective of mitigating the radiological consequences of significant releases of radioactive material. The implementation of the emergency response is usually dependent upon the type and magnitude of the accident. Good co-ordination between the operator and the responding organizations is needed to ensure the appropriate response.

Accident management is one of the key components of effective defence in depth. In accordance with defence in depth, each design level should be protected individually, independently of other levels. This means, in particular, that accident management provisions should take place in any case, even if all provisions within the design basis are adequate.

This report focuses on the fourth level of defence in depth, including the transitions from the third level and into the fifth level. It describes good practices and developments in Member States and is intended as reference material for NPPs, as well as an information source for other organizations such as regulatory bodies. It is a follow-up to the IAEA report on Accident Management Programmes in Nuclear Power Plants, published in 1994 [3], and reflects the considerable progress made since that time.

An overview of earlier IAEA efforts in the area of accident management and an outline of work in this area by the Organisation for Economic

Co-operation and Development (OECD) and the European Commission (EC) is contained in Annex I.

Various aspects of the prevention and mitigation of severe accidents have been partially reflected in 'traditional' documents used for the operation of NPPs such as safety analysis reports, probabilistic safety analysis (PSA) studies (especially level 2 PSAs), emergency operating procedures (EOPs) and emergency plans. However, the importance of the issue requires the integration of all available relevant plant specific information into a comprehensive set of consistent documents, the accident management programme (AMP). The exchange of experience and best practices can considerably facilitate and contribute to the quality of such a document to be developed for individual plants.

1.2. OBJECTIVE

The objective of this report is to provide a description of the elements to be addressed by the team responsible for developing and implementing a plant specific AMP at an NPP. Although it is intended primarily for use by NPP operators, utilities and their technical support organizations, it can also facilitate preparation of the relevant national regulatory requirements.

Severe accidents are addressed in a revised set of standards in the IAEA Safety Standards Series, including the Safety Requirements publication on Safety of Nuclear Power Plants: Design [4], which supersedes the former Code on the Safety of Nuclear Power Plants: Design (Safety Series No. 50-C-D (Rev. 1), issued in 1988). In these requirements it is stated that:

> "Consideration shall be given to these severe accident sequences, using a combination of engineering judgment and probabilistic methods, to determine those sequences for which reasonably practicable preventive or mitigatory measures can be identified. Acceptable measures need not involve the application of conservative engineering practices used in setting and evaluating design basis accidents, but rather should be based upon realistic or best estimate assumptions, methods and analytical criteria. On the basis of operational experience, relevant safety analysis and results from safety research, design activities for addressing severe accidents shall take into account the following:
>
> (1) Important event sequences that may lead to severe accidents shall be identified using a combination of probabilistic methods, deterministic methods and sound engineering judgement.

(2) These event sequences shall then be reviewed against a set of criteria aimed at determining which severe accidents should be addressed in the design.
(3) Potential design or procedural changes that could either reduce the likelihood of these selected events, or mitigate their consequences, should these selected events occur, shall be evaluated, and shall be implemented if reasonably practicable.
(4) Consideration shall be given to the plant's full design capabilities, including the possible use of some systems (i.e. safety and non-safety systems) beyond their originally intended function and anticipated operating conditions, and the use of additional temporary systems to return the plant to a controlled state and/or to mitigate the consequences of a severe accident, provided that it can be shown that the systems are able to function in the environmental conditions to be expected.
(5) For multiunit plants, consideration shall be given to the use of available means and/or support from other units, provided that the safe operation of the other units is not compromised.
(6) Accident management procedures shall be established, taking into account representative and dominant severe accident scenarios."

With reference to the Safety Requirements [4], this Safety Report describes the AMP and elaborates on its preparation, development and implementation in any NPP. The report is based on developments that have been made in the accident management field worldwide.

The status of implementation of accident management varies widely throughout the world. The process is determined mostly by national regulatory requirements. The accident management approach chosen also depends to some extent on plant design. More experience is available with the implementation of preventive measures than with mitigatory actions, but in some countries NPPs have already implemented both. Upgraded preventive accident management in the form of modern, symptom based EOPs has either been implemented or is in preparation in most countries operating LWRs. Implementation of severe accident management guidelines (SAMGs) has also commenced in numerous countries. These efforts include control room (CR) reviews, upgrades of equipment and instrument displays, improvements to safety related equipment, and emergency plan enhancements. In some cases, the approach involves the development of generic guidelines by vendors, engineering consultants and owners groups, followed by adaptation of these guidelines by the individual plant to reflect its own specific design features. In other cases, AMPs are developed specifically for each plant. Although many features are common to the implementation of all AMPs, it is recognized that a variety of means may be used to achieve the same goals.

1.3. SCOPE

The relationship between different components of an AMP is illustrated in Fig. 1. Although many practical examples are taken from the applications for LWRs (PWR, BWR, WWER), the general guidance in this report can be used for any NPP.

This report focuses on SAMGs. Emergency operating procedures are addressed on a more limited scale, with emphasis on those parts that are relevant for the later transition to SAMGs.

Both internal and external events are covered. A specific class of events is violent actions by third parties. Where the physical consequences of such events are comparable to those from other origins, they are also covered in this report. Preventive measures and/or the restoration of systems to service are in that case mostly dependent on physical protection measures which are, however, beyond the scope of this report.

The report concentrates on full power operational states: low power and shutdown states are not discussed. It is also limited to conditions under which a certain amount of control over the main power plant functions still exists — no large scale disruption or destruction of the NPP is assumed.

The focus here is primarily on existing plants, i.e. plants which are either in operation or under construction. New plants, obviously, are not excluded from consideration; it is expected, however, that for new plants many severe accident prevention and mitigation features will have already been included in the design.

Accident analysis is typically also a significant component of the development of the AMP. The issue of accident analysis is covered by another IAEA publication [5] and is therefore only partially covered here.

1.4. STRUCTURE

This report consists of a main body, eight appendices and three annexes. The main body is subdivided into an introductory section and four additional sections. Section 2 covers the basic principles of the AMP, including the specification of its objectives, a short description of severe accident progression, possible accident management strategies, and characterization of plant equipment performance under severe accident conditions. The detailed actions and project steps of the proposed AMP are divided into three phases: preparation, development and implementation. Section 3 discusses the actions to be taken during the first phase, mainly related to preparation and programme definition. Section 4 describes the second phase, in which most of the work on the devel-

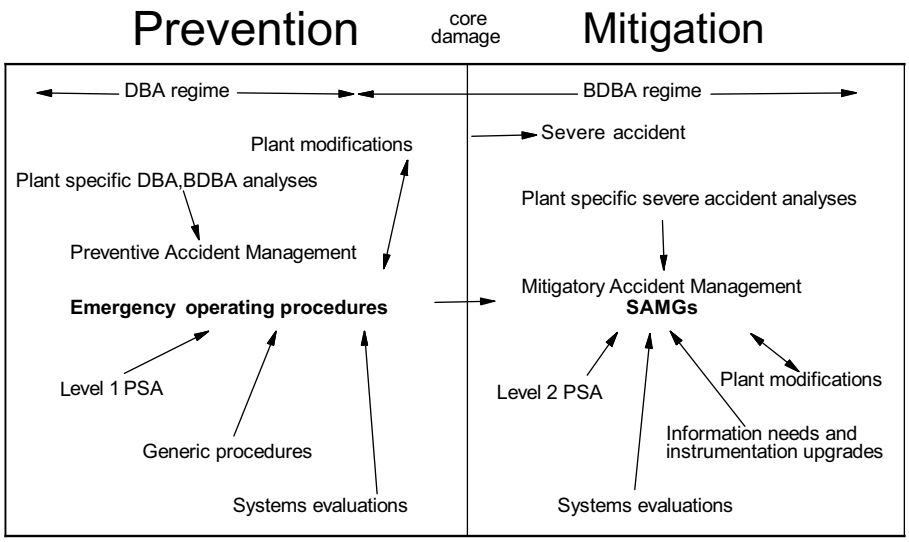

FIG. 1. Different components of an AMP[1] (DBA: design basis accident, BDBA: beyond design basis accident).

opment of the AMP has to be done. The work includes, for example, the detailed development of the procedures and guidelines, preparation of supporting analysis, and determination of equipment upgrades. Section 5 deals with phase 3, which outlines the actions to be taken for implementation of the AMP in the plant.

The appendices provide additional information, sometimes referring to programmes already in place. The annexes provide practical examples of how various components contributing to an AMP can be performed, including actual applications. Appendix I describes the plant damage states in more detail and presents examples of logic trees which enable the plant damage states to be determined. Appendix II is devoted to candidate high level actions (CHLAs), which are responses to the plant damage state in compliance with the accident management strategy adopted. Appendix III describes and gives examples of computational aids (CAs). Appendix IV presents typical parameters used for initiation and control of preventive and mitigatory actions. Appendix V is devoted to preventive accident management actions. Appendix VI gives an example of the methodology for a comprehensive review of an AMP. Appendix VII describes, for various

[1] A further subdivision could possibly be made between the DBA and BDBA area in the prevention regime. This subdivision is addressed in Section 2.8.

approaches, how the transition from the EOP domain to the severe accident management domain can be achieved. Appendix VIII gives an overview of the use of PSA in the development of SAMGs.

Annex I gives an overview of earlier IAEA actions in this field, as well as those of the OECD and the EC. Annex II gives a limited overview of severe accident management applications in various Member States. Annex III presents an example of the organization of a typical technical support centre (TSC) in an NPP in the USA.

2. BASIC FEATURES OF AMPs

2.1. OBJECTIVES AND BACKGROUND OF ACCIDENT MANAGEMENT

Depending on the level of defence in depth breached, the following are the four main objectives of accident management:

(1) Prevention of the accident from leading to core damage,
(2) Termination of core damage,
(3) Maintaining the integrity of the containment for as long as possible,
(4) Minimizing on-site and off-site releases and their adverse consequences.

The latter three items constitute the objectives of severe accident management. It should be noted that objectives (2)–(4) may not be achieved solely by plant personnel.

The first priority of nuclear safety is to prevent accidents in plants. However, it must be recognized that, although it is unlikely, those preventive actions may fail. Hence it is appropriate to give attention to measures to control the course of an accident in both the short and the long term, and to prevent or mitigate its consequences to the greatest extent possible.

It is important to develop plant specific EOPs and SAMGs to make best use of the systems available to halt the progression of an accident by protection of the primary system boundary, the containment, and any additional systems and structures that augment the functions of core cooling or containment of fission products (FPs), such as filters, sprays, water pools and auxiliary buildings. The purpose is to reduce the fuel temperature and maximize the length and complexity of the pathway by which FPs would escape to the environment.

In order to optimize the management of an accident, the operating staff should understand the mechanisms of reactor accidents and know how plant systems can be used to control a developing situation. This should include all plant systems, both dedicated safety systems and non-safety related systems. Use of these systems and their components under accident conditions should be anticipated, even outside their intended range of operation.

Although there are still questions which require further investigation, and the fact that uncertainty associated with current research results remains large, the understanding of severe accident phenomena has reached a level at which the development of accident management measures is appropriate. Further, these research results permit improvements in new plant designs which can increase the resistance of the plant to severe accidents, often at little cost. For a new plant design, for example, the geometry of the cavity beneath the reactor pressure vessel (RPV) can be configured at little, if any, additional cost so as to minimize expulsion of core debris to the containment atmosphere and to maximize the chances of quenching core debris. Plants belonging to previous generations could be modernized in the light of the wealth of information obtained from severe accident research.

The translation of insights from severe accident research into actual safety benefits for operating plants requires a process which includes the assessment of vulnerabilities under different plant conditions (from DBAs to severe accidents), the development of accident management strategies and the establishment of a systematic process to ensure that strategies exist to deal with all identified vulnerabilities, and implementation and validation of these strategies in the form of procedures and guidelines.

To achieve this, it is necessary that people who understand the implications (and uncertainties) of results of current severe accident research co-operate with the operators of plants. Operating organization staff, supported by such experts, eventually also involving the vendor, should develop the guidelines. Alternatively, a group of similar plants may set up a generic guideline, to be transformed into plant specific guidelines later.

2.2. PREVENTIVE AND MITIGATORY FEATURES OF ACCIDENT MANAGEMENT

Preventive accident management integrates actions and measures needed to prevent or delay severe damage to the reactor core. Mitigatory accident management refers to those actions or measures which become necessary if the preventive measures fail and severe core damage occurs or is likely to occur.

Mitigatory accident management (or severe accident management) therefore mitigates the consequences of a severe accident which involves significant core degradation.

Preventive accident management is usually covered by the plant's EOPs and used by the plant operations staff in the main CR during an event. Mitigatory accident management (or severe accident management) guidelines are primarily used by the on-site TSC or crisis centre in the form of guidelines or handbooks.

Whenever plant protection systems are actuated, operators follow predefined procedures which are set out in documents designated, for example, as EOPs. These are used to verify the automatic operation of safety systems, to diagnose the situation by following a predefined logical process for selecting the appropriate procedure, and to take actions as prescribed by this specific procedure. It is important that these procedures provide systematic and adequate guidance from the beginning of an event. This enables operators to initiate the appropriate response without having to rely on memorized responses when facing a complicated event. Effective procedures have to be designed to assist operators in focusing their attention on the most important information and developments. They must help prevent or overcome possible confusion caused by numerous simultaneous alarms and prevent misdirection of attention to less important matters.

In order to cover a broad range of accidents and to take into account errors in diagnosis or inadequacy of operator intervention, sufficiently general EOPs should be developed. Many Member States have done this. These procedures are based on the idea that it is not generally necessary to know the chronology of the past events and actions that have determined an actual situation in order to be able to take the required actions in a new situation. Such an approach needs to be based on a set of generic symptom (or function, or state) oriented procedures with only a few safety objectives to be fulfilled.

A procedure or guideline is symptom based if it contains actions to be taken that are based on the values of directly measurable plant parameters. In a symptom based procedure or guideline, the user (operator, TSC member, other person) is not required to know plant conditions which are not directly measurable in order to apply the procedure. For example, the following cannot be used as symptoms: loss of coolant accident (LOCA) break location and size, and location and degree of damage to the core. Procedures may also use a combination of such parameters, from which a degree of understanding of the plant's damage state is obtained, to decide on useful actions. Suitable symptoms include such parameters as core exit temperature, primary and secondary system pressures and containment hydrogen concentration.

If the restorative actions in the EOP domain fail to achieve the desired objectives, core damage is expected to occur. Priority now shifts to severe accident management. The basic aim here is to terminate the progress of core damage, to keep the containment intact as long as possible, and to minimize on-site and off-site releases. Halting the progress of core damage will also prevent failure of the RPV, which in itself is a major asset. To achieve these objectives, a limited set of guidelines, based on appropriate strategies, need to be available, as the situation can be very complex and not well suited for improvisation and ad hoc decision making. The set of guidelines may be limited, as it will need to satisfy only the basic safety objectives as defined under severe accident management. The situation may be characterized by multiple equipment failures and/or procedural errors, and loss of instrumentation due to harsh environmental conditions, which may have resulted in confusing signals to the operators. It is important that the operators, supported by the technical staff, assess the current situation and follow the appropriate guidance. Essential elements to be assessed are the status of FP boundaries, actual or imminent core damage, and challenges to RPV and containment integrity. If containment integrity cannot be maintained, substantial benefits can be gained by delaying its failure to minimize the consequences of the release. These benefits include the extension of time available to the operating staff to restore or replace failed safety systems.

The guidelines, which identify the most suitable actions to prevent or mitigate the release of FPs, normally take plant specific details into account. These vary quite widely between different types of reactor (e.g. the type of fuel, the type and pressure of the coolant, the size and strength of the containment) and also between different reactors of the same type.

2.3. ACCIDENT PROGRESSION AND DEGREES OF SEVERITY

In the case of an accident sequence with sustained loss of core cooling, the accident progression can involve two phases, with fundamental differences in the challenges to safety functions and the source term: the in-vessel phase and the ex-vessel phase. For both phases the phenomena involved need to be identified for the operator's specific reactor type. An example of the sequence of in-vessel phenomena for an LWR reactor type follows:

(a) Overheating of fuel and cladding;
(b) Onset of exothermic oxidation of the cladding, accompanied by production of hydrogen;
(c) Damage to and melting of the fuel cladding;

(d) Rapid increase in hydrogen production, with a possible challenge to containment integrity due to deflagration/detonation;
(e) Melting of the cladding, fuel and core materials and downward relocation of the corium;
(f) Interaction of the molten corium with the residual water in the RPV;
(g) Potential steam explosions caused by a molten corium–water reaction;
(h) Heating of the RPV by the molten corium.

At the last stage the possibility of RPV failure must be seriously considered. Cooling of the lower head of the RPV may be restored by flooding the core in-vessel or by using water to cool the lower head from the outside. If attempts to arrest the accident progression at this point are not successful, vessel melt-through will occur and the ex-vessel phase of the accident will commence. During this phase a variety of phenomena challenge the containment integrity. They include:

(1) Damage to the containment due to high pressure expulsion of the corium (direct containment heating (DCH)).
(2) Hydrogen combustion (deflagration/detonation), with hydrogen produced during the in-vessel phase and later during the ex-vessel phase by core–concrete interaction (which may also produce carbon monoxide, which is also combustible) or a molten corium–water reaction; apart from the threat of global combustion there is a danger of local deflagrations/detonations which can generate missiles that may challenge the containment integrity.
(3) Core–concrete interactions which directly jeopardize the integrity of the containment through foundation melt-through.
(4) Long term pressurization and/or temperature increase, ultimately leading to failure of the containment.
(5) Bypass of the containment, e.g. through a damaged steam generator (SG) due to tube creep rupture, or through some other pathway, e.g. an interfacing system LOCA.

2.4. ASSESSMENT OF VULNERABILITIES AND CAPABILITIES

A necessary step in accident management planning is to identify those vulnerabilities of the plant which are likely to cause challenges to the safety functions, and the mechanisms by which the barriers preventing the release of radioactive materials can be challenged.

Vulnerabilities should be assessed on the basis of an analysis of the plant's response to beyond design basis accidents. This should be done in a realistic manner using best estimate methods, taking note of the uncertainties associated with such methods. The assessment should also include all possible plant situations and modes of operation. This analysis should be supplemented by as many of the following inputs as are available:

(a) Probabilistic safety assessment,
(b) Research on severe accident phenomena,
(c) Study of operational experience and precursor events,
(d) Generic studies and analyses done for similar or reference plants,
(e) Review of existing procedures to assess their limitations,
(f) Evaluation of instrumentation behaviour and limitations for accident identification and control,
(g) Evaluation of operating organization capability in emergency situations,
(h) Plant specific operational experience,
(i) Generic operational experience (e.g. IAEA database).

Although plants are designed to withstand a specified number of incidents and accidents, their actual capability to cope with accidents is usually considerably greater. A plant may be able to cope with more serious accidents than those considered in its design basis. This is mainly due to the fact that only dedicated systems have been considered in the design basis and are therefore considered in the safety analysis. Use of other systems can greatly enhance the plant's capability, all the more so if systems are also allowed to operate outside their intended range of operation for a short or possibly a longer period of time (non-conventional use of systems). It is therefore useful to investigate all of a plant's capabilities to fulfil the safety functions, including hook-ups of non-dedicated systems and temporary connections (hoses, mobile equipment).

2.5. ACCIDENT MANAGEMENT STRATEGIES

On the basis of the vulnerability assessment and an understanding of accident behaviour, as well as of the plant's capabilities of coping with accidents, the next step is to develop accident management strategies. The objectives of the strategies are specified and related to the basic safety functions, e.g. to protect the core integrity by maintaining subcriticality and restoring core cooling, to protect the integrity of the reactor coolant system (RCS), to protect the

containment[2] integrity and to minimize radioactive releases if the containment fails or is bypassed. One of the first steps in developing strategies is the establishment of criteria which use identifiable physical states in the plant as either action levels or thresholds for the various steps of operator response. These steps are aimed at preventing or delaying each of the stages of progressing severity described in Section 2.3.

Failure of a strategy at one stage must leave options open for achieving the objectives at subsequent stages. It is important to systematically evaluate the strategies which can be adopted at each stage. Suitable strategies need to be workable under the physical plant conditions associated with the specific challenge to the safety function which the strategies are intended to restore. The impact of these strategies on different plant conditions during the subsequent phases of a severe accident has to be investigated. Both positive and negative consequences will be considered in this report in order to provide the basis for a decision as to which strategies constitute a proper response under a given plant damage condition. A detailed example of this is given in Ref. [6].

An overview of the strategies which can be applied to prevent RPV failure, containment failure and mitigation of FP release is given in Appendix VI, using a methodology of safety objective trees which contain safety functions, challenges and mechanisms. When implementing a strategy in a given plant condition, operators need to know:

— When to initiate a procedure for that strategy;
— That the procedure has been initiated;
— That the procedure is effective;
— If the procedure is ineffective, when to abandon it and what to do next.

2.6. INFORMATION NEEDS

Sufficient information from plant measurement systems must be available to NPP staff so that they can:

(a) Determine the status of plant safety functions during accidents, including severe accidents;

[2] It should be recalled that 'containment' has a wider definition here, as described in the Definitions.

(b) Identify trends in the progression of an accident to be able to develop timing projections;
(c) Select accident management strategies and assess their effectiveness.

The instruments and indicators that can relay information on the state of the plant and the level of severity of an accident, and which can be used to implement the preventive strategies, will cover:

(1) Neutron flux,
(2) Temperatures in the primary and secondary systems and containment,
(3) Coolant inventory in the primary and secondary systems and containment,
(4) Pressures in the primary and secondary systems and containment,
(5) Radiation in the primary and secondary systems and containment,
(6) Composition of the containment atmosphere (e.g. hydrogen concentration),
(7) A post-accident sampling system,
(8) Status of safety equipment,
(9) Other areas as needed for plant specific countermeasures.

The instrumentation listed above is typical of PWRs or WWERs; it varies slightly for BWRs. The instruments and indicators are assessed for their capability to function in certain anticipated accident environments and to cover those ranges of the parameters which are beyond normal operating ranges. Where information is not available through direct measurement it should be obtained from indirect sources or derived using CAs. An example of such an indirect measurement is the pressure of a connected residual heat removal (RHR) loop where the main RCS pressure is not available. The functioning of instruments during a station blackout should also be considered, as well as the potential for instrument destruction during a severe accident.

Taking into account the high demands that are likely to be placed on an operator during accidents, information on the plant's status should be presented in a convenient form, concentrating on a few critical parameters. It may be helpful to have the displays of instruments qualified to operate under accident conditions clearly identified on a separate panel to avoid confusion with instrumentation designed for 'normal' conditions, which may well have failed. It should, however, be recognized that qualification for operation under accident conditions usually does not extend to the severe accident environment. Ranges and qualification of relevant instrumentation may also be documented separately in tables which are easily accessible during accident conditions.

2.7. PLANT EQUIPMENT PERFORMANCE AND MATERIAL SUPPORT NEEDS

Strategies depend on the availability of safety systems as well as the availability of non-safety related systems to perform the required safety functions. Therefore, as part of the preparation for accident management, it is necessary to identify all plant systems that could possibly be used, perhaps in a non-conventional manner (i.e. outside their intended range of operation), to control an accident and mitigate its consequences. This should include the identification of backup systems which could be used to perform the same functions.

In an accident situation, consideration has to be given to obtaining additional equipment and materials from another part of the site or elsewhere. For example, it may be possible to use a non-standard water source to provide long term cooling to the reactor core, or special equipment may be needed to bring fire fighters close to the scene of a fire and to protect them from high radiation levels or contamination. The availability of such materials and equipment needs to be considered at the planning stage, as well as the means of transport needed in the event of a rapidly developing accident.

In order to implement a strategy for such cases, it may be desirable to consider the introduction of additional equipment. This may in some instances require a permanent modification to the plant.[3]

The likelihood of the CR becoming uninhabitable during a severe accident should be assessed to evaluate whether accident management strategies need to be implemented from an emergency control centre. Dedicated information and communications systems should also be required. For multiple unit sites, particular attention should be paid to the potential effect of positive and negative interactions with the unaffected units on the site.

The availability of advanced diagnostic aids, decision making aids (expert systems) and computational tools may permit improved strategies to be developed. Such CAs would also provide estimates of parameters which affect accident management decisions, such as RCS and containment leak rates, time remaining to key events (e.g. core uncovering, RPV failure, containment failure), and core and containment conditions. They should also provide a basis for assessing the effectiveness of strategies under consideration or in progress during an accident. The CAs might take the form of a series of nomographs, a set of formulas, a compilation of plant specific information, a handbook of severe

[3] Examples are filtered containment vents and catalytic hydrogen recombiners.

accident analyses, small computer programs, or even fast running severe accident analysis codes. These are described further in Section 4 and Appendix III. The success of the accident management strategy will depend on the ability of personnel at the plant to perform actions under potentially hazardous conditions. The anticipated hazardous conditions in which emergency workers may be required to perform accident management functions are required to be identified (see para. 4.61 of Ref. [7]). It is required to make arrangements for taking all practicable measures to provide protection for emergency workers for the range of anticipated hazardous conditions in which they may have to perform response functions (see para. 4.62 of Ref. [7]).

To determine whether or not equipment will perform as required to ensure a successful outcome of the strategy, the following steps should be performed:

(a) Identification of equipment that will be operating outside its design range and/or environmentally qualified limits,
(b) Determination of whether equipment will perform its function if operating outside its design range,
(c) Determination of whether the harsh environment which may result from a severe accident will prevent equipment from performing its intended function,
(d) Evaluation of the potential influence of failures in support systems,
(e) Determination of whether equipment failure would have adverse consequences,
(f) Identification of alternative equipment to implement strategies.

These actions will then provide information on:

(1) Equipment that will accomplish the proposed strategies;
(2) Requirements for alternative/additional equipment, if necessary;
(3) The potential negative impacts of strategy performance on equipment, such as limitations or restrictions that must be placed on equipment owing to its inability to perform its required function or its inability to operate under certain environmental conditions;
(4) The failure modes of the equipment.

During an accident, it may be appropriate for such deliberations to take place in the TSC or through some other type of organized technical support provided by experts in the various disciplines involved in accident management. Organizational matters are further discussed in Sections 4.5 and 5.1.2.

2.8. PROCEDURES AND GUIDELINES

This section presents approaches to developing procedures and guidelines to be implemented to prevent severe accidents and mitigate their consequences. Consideration should be given to the formulation of procedures that go beyond the plant's design basis. The purpose of such procedures is to guide the CR staff and other emergency response personnel in halting the progress of potential severe accidents and in mitigating their consequences, making maximum use of all existing plant equipment including equipment that is not part of the standard plant safety systems. These extended procedures may be called accident management procedures to distinguish them from EOPs that cover only the design basis.[4] In other cases these procedures form an integral part of the (symptom based) EOPs.[5] In addition, guidelines known as SAMGs for use by the TSC or equivalent support or crisis teams during severe accidents, should be considered. The SAMGs would address actions which may not be appropriate for accident management procedures because of potential negative effects, operational and phenomenological uncertainties, and the predominantly long term (late) nature of these actions.

A procedure comprises a step-by-step list of required actions and responses on the part of the procedure user, which must be followed word for word. These procedures must generally be followed in the specified order, and in accordance with other 'rules of usage' in which the procedure users (usually the reactor operators) are highly trained. A procedure is therefore a highly structured means of specifying a well defined series of actions to be taken and is based on the values of individual parameters or combinations of parameters (i.e. the symptoms).

A guideline is usually used to describe a less strict and prescriptive set of instructions — more correctly, guidance. As with a procedure, a guideline can be structured and consist of a sequence of steps and branch points.[6] Generally, a guideline differs from a procedure in the following ways:

(a) Verbatim compliance with a guideline is not normally required.

---

[4] For example, France uses I and A procedures inside the design basis and H procedures for conditions beyond the design basis (but not yet severe accidents). The term 'AMP' is not used in this context.

[5] For example, Westinghouse uses EOPs to cover conditions beyond the design basis.

[6] In some approaches, guidelines are much less structured and more closely resemble handbooks, in which alternative strategies are described (e.g. Sweden).

(b) The order of the actions specified in a guideline may be altered based on the judgement of the trained guideline user.
(c) The actions to be taken will depend upon evaluation of plant conditions by the user as specified in the guideline. These actions will include the available alternatives (based on plant equipment availability at the time), and will also include the option of not implementing a particular action. The decision will be based on the user's evaluation using the guidance contained in the guideline.

It is also important to keep the long term perspective in mind when developing and implementing an AMP. Otherwise, the short term measures and actions may cause unnecessary problems and irreparable obstacles for the long term handling of the plant.

Accident management measures in the short term may also have a long term impact on the conditions of the plant. It is important to distinguish between short term and long term accident management, where actions are taken a long time after the initiating event. Short term in this context means within a few hours to a few days and long term implies a timescale from about one week up to several years. An example of a short term action with a potential long term impact is the altering of the water chemistry in the containment after an RPV failure. Addition of chemicals may reduce the release of iodine, but corrosion may increase. Therefore a balance should be sought in the remedial actions adopted.

2.9. PHASES OF THE AMP

An AMP should ensure that in-depth knowledge of the expected plant behaviour and the capabilities of the plant personnel and equipment are combined in the identification and development of appropriate accident management strategies. These attributes are also required to ensure that these strategies will be implemented properly. Implementation of an AMP is separated into three logical stages:

— Phase 1: Planning and familiarization,
— Phase 2: Development and validation,
— Phase 3: Implementation and improvement.

The attributes form an iterative process by which an AMP can be developed during the above three stages and include the following:

Phase 1: Planning and familiarization

(a) Developing an understanding of the capabilities and vulnerabilities of the equipment and personnel of the NPP under possible accident conditions.

Phase 2: Development and validation

(a) Identifying and evaluating a set of accident management strategies to prevent core melting or mitigate the consequences of FP release for the identified plant vulnerabilities.
(b) Ensuring that engineered methods, personnel, procedures and guidelines are available at the appropriate levels for the implementation of strategies.
(c) Ensuring that adequate plant status information is available to allow selection of a strategy and assessment of the feasibility and effectiveness of possible strategies.
(d) Delineating the lines of decision making, responsibility and authority within the plant and emergency response teams of the corporate TSC for managing accidents.
(e) Ensuring that the performance of the AMP is validated using available and appropriate means.

Phase 3: Implementation and improvement

(a) Ensuring that adequate training is provided for all personnel involved in accident management and that it is a continuing process.
(b) Implementing a means to incorporate new information into the AMP.

The three phases are discussed in detail in Sections 3, 4 and 5.

3. PREPARATION OF THE ACCIDENT MANAGEMENT PROGRAMME

3.1. TEAM FORMATION

To ensure the success of the AMP development, it is crucial to assemble a team of a selected number of experts in various disciplines at the operating organization. This team will be the staff responsible for the development and implementation of the AMP. The project leader defines the responsibilities for

the work within the different phases of the project. The team should be able to call upon experts in other fields on an 'as-needed' basis. Several bases of knowledge will be needed for an effective project: phenomenological knowledge, plant knowledge and knowledge of human factors. Preparation of an AMP involving accidents with severe core degradation will require specialized expertise in various areas including:

— Process engineering and plant automation,
— Thermal-hydraulics,
— Chemistry,
— Health physics,
— Off-site consequences of a radioactive release and the actions to be taken by off-site officials to protect the public,
— Other areas such as fission product transport behaviour and metallurgy and material technology.

The core team should consist of staff familiar with the following disciplines:

— Operations, operations support, plant technical support;
— Systems engineering;
— DBA and BDBA analysis, severe accident analysis, PSA;
— Emergency planning (with knowledge of the plant specific emergency arrangements, off-site response and provisions off the site for assistance at the site by emergency services such as fire fighters or police);
— Project management (with knowledge of scheduling and integrated development of work);
— Security.

If a generic accident management approach which has been developed by an organization outside the operating organization is adopted, and the outside organization has not provided conversion instructions, the team should consist of representatives of both the operating organization and the developer of the initial approach. The involvement of engineering organizations providing regular support to the operating organization or plant is necessary in cases where the original generic design differs considerably from the design of the NPP in question (e.g. Western PWRs versus WWERs).

When setting up the core team, consideration should be given to the availability of plant personnel to support the development activities in addition to their normal roles. Early involvement of staff who will be concerned with control room or TSC operations, e.g. the accident assessment team (AAT), in development of EOP and severe accident management guidance is practical, because

it provides an invaluable training for future tasks and brings feedback in early stages of the project. There are advantages to holding regular meetings (working sessions) at the plant itself, especially in the later phase of the programme. If the operating organization decides to prepare and realize the AMP on its own, the principles of future co-operation with engineering support organizations providing scientific support should be clarified, and the development team could also include representatives from those organizations with allocated responsibilities.

3.2. FAMILIARIZATION

At the beginning of the project work it is necessary that all members of the core team familiarize themselves with the relevant background information, e.g.:

- Existing documents and results of research work related to the project objectives,
- Supporting accident analyses and PSA studies available and/or needed,
- Plant design and systems capabilities,
- Time and resources available for the project,
- Personnel that will be using the final document,
- Training that will be needed for end product use.

Methods for such familiarization are varied. An informal approach can work well, but for certain aspects a more formal (classroom training) approach is suggested to improve efficiency. An extensive information exchange meeting involving all core team members is recommended at the beginning of the project. Basic training covering phenomenological aspects of the accident management for team members with operational and system engineering background has to be considered. This training could also include basic information on the capabilities, limitations and uncertainties of the computational tools and methods used throughout the project in order not to overestimate the current knowledge or computational tools and to encourage engineering judgement.

If a generic AMP will be used as a basis, a comparison of the important design features of the actual plant needs to be prepared and the development team members require a good knowledge of the design specifics.

3.3. SELECTION AND DEFINITION OF AN AMP

At the project definition stage the operating organization takes a fundamental decision on its scope and links to other projects, NPP upgrade policy,

safety policy, existing or expected regulatory requirements, etc. The selection of requirements or attributes for the AMP ultimately defines the overall structure and content. This section reviews some of these key attributes and provides some examples based on actual programmes. If a 'generic' approach is adopted, some of these attributes will already be proposed in the generic programme. In this case this section can provide a form of 'checklist' when evaluating the applicability of different generic approaches.

At this stage, it is also important that a list of specific issues or plant features known to be of potential importance for future aspects of the project be assembled (for instance, particular system capabilities beyond the normal design conditions, special instrumentation aspects, the ability to flood or drain a normally dry cavity).

3.3.1. Procedures versus guidelines and degree of proceduralization

It is generally believed that a strict and detailed stepwise format is an appropriate form of presentation of EOPs. However, severe accident management guidance does not easily lend itself to proceduralization (although some approaches do this) because of:

— Difficulties in evaluating the plant specific status, equipment availability and the use of this information to develop a recovery strategy;
— Phenomenological uncertainties and the multitude of sequences of severe accidents.

These aspects have led most developers of severe accident management instructions to use a guideline approach.

Decisions regarding the degree of proceduralization of the SAMG and the degree of evaluation and judgment needed by the responsible NPP staff (usually TSC members) to use the guidelines should be made at early stages of the development project. In making these decisions, it should always be remembered that:

— There are a very large number of unique severe accident progressions to be managed and the guidelines should be capable of covering all relevant scenarios;
— In many cases there are also negative consequences associated with taking a certain action;
— A well trained and responsible staff (TSC or equivalent organized support) will be capable of making informed judgements, especially when equipped with well structured guidance.

If guidelines are to be developed from an existing generic approach, this step simply becomes one of reviewing the degree of detail and content of the generic guidelines to ensure applicability at the plant. This step, however, requires more effort if the generic guidelines are to be applied to an NPP of a comparable type but built by a different supplier.

The guidelines present a method for the systematic, logical evaluation of the possible strategies that might be used to respond to a given challenge. The guidelines will help the responsible staff (usually the TSC staff) to consider important aspects such as the possibility of implementing the strategy with the current plant configuration, the balance between the potential positive and negative impacts associated with implementing a strategy, determining whether the strategy was successfully implemented, and the long term concerns associated with the implementation of a strategy.

3.3.2. Symptom based procedures and guidelines

The symptom based approach is considered to be a good practice for both preventive procedures (EOPs) and mitigatory guidelines (SAMGs). The first step for the operating organization in developing the AMP could be to develop symptom based or state oriented EOPs.

In preventive accident management, in order to provide coverage of beyond design basis accidents (BDBAs) and unpredicted accident scenarios, EOPs need to be at least partly independent of the event. This involves the monitoring of plant 'critical safety functions' (CSFs) or 'plant states' which do not require that the event progression be diagnosed in order to decide on the necessary recovery actions.

3.3.3. Coverage

Preventive accident management should provide all the guidance necessary to implement actions to prevent or delay damage to the reactor core. Most approaches do not distinguish, within the preventive accident management package, between DBAs and BDBAs (the required actions, strategies and priorities remain the same up to core damage).

Mitigatory accident management must cover the full spectrum of potential events involving core damage, RPV failure, release of fission products to containment and containment challenge, and must also address issues not usually considered in analytical studies of plant safety, such as the use of recovered equipment and the interpretation of instrument readings during severe accidents.

3.3.4. Entry and exit bases and interfaces

Entry and exit conditions or symptoms for the different forms of guidance are to be defined.

The boundary between 'normal' and 'emergency' operation and the symptoms used to monitor it are to be defined as the entry condition for EOPs. Actuation of an automatic reactor trip or safeguards system actuation is often used, giving due attention to coverage of anticipated transients without scram (ATWS) as well. Exit from EOPs is allowed once the plant has achieved a stable and safe shutdown condition and core damage has been largely prevented.

If preventive accident management is unsuccessful, the transition to mitigatory severe accident management measures should be defined. Such transition is based on symptoms indicating the onset of core damage or the fact that core damage is imminent. This is done by recognizing certain plant parameters, e.g. the core exit temperature (some PWRs) or the failure to meet a minimum level in the RPV (some BWRs), or by recognizing a predefined degraded state following an analysis of a set of related parameters (for some other PWRs). The transition may be fixed and irreversible, i.e. the EOP domain is left. Alternatively, the EOP domain is not left and SAMGs are executed in parallel. In that case, consistency with the upcoming SAMG is checked and the EOP in process is left where a conflict would appear. Further details and examples of actual transition schemes for several types of PWR and BWR are presented in Appendix VII. Termination and exit from SAMGs are based on measurable data indicating that safe and stable conditions have been successfully achieved.

3.4. REVIEW OF AVAILABLE SAFETY ANALYSES AND SPECIFICATION OF FURTHER INFORMATION NEEDS

3.4.1. General

The supporting analysis requirements depend on the development approach that may vary for the development of preventive measures resulting in EOPs and the development of mitigatory measures resulting in SAMGs. Also, developing a new EOP and severe accident management guidance package from scratch is quite different from modifying an already existing one for a similar design.

Development of a completely new EOP and severe accident management guidance package from scratch is a lengthy and difficult undertaking and can

be a very demanding task on the operating organization level. The crucial task in the initial stage is reviewing and preparing background analyses and other information necessary to develop basic strategies and make fundamental decisions on project scope and timing.

The main objective of the initial review is to ensure that sufficient information is available allowing assessment of plant behaviour, finding of the basic vulnerabilities, assessment of the adequacy of information from plant measurement systems for determining the status of plant safety functions during accidents, identification of trends in the accident progression and development of projections of the timing of expected behaviour. These aspects are fundamental to develop basic accident management strategies and assess their effectiveness. Some of the analyses for those purposes need not be available from the very beginning and may be provided while developing individual procedures.

The review seeks to identify plant safety function challenges, to facilitate selection of the accident management strategies and monitor their effectiveness, either by measurements supplying the necessary information or by identification of the means of obtaining the information through precalculated curves or nomographs that relate variables to plant conditions or the addition of new measurements, preferably qualified for the process parameters and environmental conditions that may arise.

3.4.2. Analyses needed for AMP development

In this section an example is presented to identify supporting analysis requirements for a plant specific AMP development project which takes as basis a set of generic guidelines. For development from 'scratch' a more basic type of analysis may be needed, for which the development path described in Section 4.2 will give guidance.

With the approach of developing plant specific EOPs from the generic ones, it may not be necessary to perform thermal-hydraulic analysis of accident sequences for all recovery strategies. In many cases, the analysis performed to support the generic guideline development may be applicable, even though the plant design is different. Careful evaluation of such applicability is, of course, necessary. If the generic analysis is found to be not applicable, new analyses should be performed to meet the specific needs of the procedure (for example to develop new criteria to initiate a certain set of recovery actions). Often, changes to recovery strategies are found to be necessary due to system design differences (for example, reduced safety injection sequences for systems with different numbers of pumps and pump characteristics). Thus, in several cases,

thermal-hydraulic transient analyses will be needed. The nature of these analyses is further described in Section 3.4.3.

Severe accident management guidelines contain the guidance for implementing mitigatory accident management actions in the case of an event which involves core damage. There are some important differences with regard to EOPs at this point of the project. The focus of SAMGs is on protection and restoration of ultimate barriers to fission product release (i.e. containment or confinement, steam generator (SG) tubes, etc.) and not (as in the EOP case) on integrity of the fuel, which has already degraded when SAMGs are needed. Therefore, severe accident analyses are required that involve core melt, potential RPV failure and challenges to containment or confinement boundaries. The tools used to perform this type of analysis must be capable of modelling severe accident phenomena and are in general quite different from those used to perform analysis in support of EOPs. The nature of these analyses is further described in Section 3.4.4. Plant specific analysis requirements are discussed in the following sections in terms of three categories of analysis:

— Preliminary analysis (see Sections 3.4.3 and 3.4.4) needed for evaluating basic strategies of EOPs and SAMGs,
— Procedure and guideline development analysis (see Section 4.3) needed for confirmation of strategies and set point calculations,
— Verification and validation analysis for procedures and guidelines (see Section 4.6.3).

3.4.3. Preliminary analysis for EOPs

The preliminary analysis provides an understanding of the response of the plant to various types of accident. It is used as an input to the process of evaluating basic recovery strategies. Normally, such analysis will not model any operator actions. Since this type of analysis usually already exists, additional new analyses might not be needed. The existing analyses may come from various sources, including the safety analysis report, analyses performed in support of level 1 PSA, and operational experience feedback, focusing on severe accident precursors. It is important that all such analyses be assembled during the first phase of the project. The preliminary analyses, together with the generic guidelines themselves, represent the main inputs to the first phase of the project.

3.4.4. Preliminary analysis for mitigatory severe accident management actions

Preliminary analyses are informative in nature and provide an understanding of the response of the plant to various types of severe accident. In particular, the preliminary severe accident analyses are sufficiently detailed and plant specific to identify:

— The nature of the challenges to fission product boundaries from various severe accidents and the challenges that are most dominant,
— The timing of various potential challenges from the severe accident (in order to assess the priority of various recovery actions),
— The plant parameters which can be used to monitor the different challenges.

If a good plant specific level 2 PSA exists, it should normally contain adequate severe accident analysis to meet these needs. However, for those plants that do not have an adequate level 2 PSA it may be necessary to perform new preliminary severe accident analyses. The following analyses are considered basic for the approach:

— Definition of a spectrum of severe accident sequences which provides broad coverage of the potential severe accident classes which can occur. A plant specific level 1 PSA (available for most plants) is the best source of this information. A level 1 PSA for a plant of similar design may be helpful if a plant specific study is not available.
— A series of 'base case' severe accident analyses of the identified sequences, using a best estimate severe accident analysis tool, and an analysis of the cases over a sufficiently extended timeframe to identify all challenges to fission product boundaries and their associated timing.
— An extensive uncertainty evaluation (including a series of sensitivity calculations) aimed at investigating the importance of severe accident phenomena. Important phenomena would include:

  • hydrogen generation, distribution and combustion,
  • high pressure melt ejection and associated phenomena,
  • molten core debris dispersal,
  • in-vessel and ex-vessel steam explosions,
  • molten core concrete interaction,
  • containment/confinement overpressurization,
  • containment/confinement bypass (e.g. steam generator tube failure).

To identify dominant challenges to fission product boundaries, information on the likelihood of a given severe accident sequence is desirable. In the absence of a level 2 PSA, approximations may be possible using the results of level 1 PSA together with an evaluation of the results of the preliminary severe accident analyses. A further description of the use of PSA is given in Appendix VIII.

3.5. EVALUATION OF THE PLANT EQUIPMENT AND INSTRUMENTATION PERFORMANCE

The degree to which implementation of the AMP leads to requirements for plant modifications is normally considered at an early stage. An AMP can be implemented with the intention of making maximum use of existing plant capabilities, or it can be used to help in defining upgrades. The approach is identified at this stage and needs to account for the national requirements, where these exist. One example is given in the following, related to the use of essential instrumentation in AMPs. The two extreme possibilities are:

— Provision of new, dedicated and qualified instrumentation designed to survive the harsh severe accident environment;
— Use of existing instrumentation only, without modification.

In practice, a position in between the two extremes can be adopted, which recognizes the need for information concerning plant conditions without imposing an unbalanced resource burden on the plant owner. Such an approach will consist of evaluating survivability of the existing plant instrumentation in severe accident conditions, and developing a very limited list of recommended instrumentation upgrades to achieve the AMP's aims. Another aspect of this approach is to list all available means of measuring a given plant condition, in order of expected reliability, thereby giving the staff the best basis on which to make judgements if faced with conflicting information displays.

It is important that the essential instrumentation be capable of functioning in a station blackout at least as long as is required. The possibility of bringing portable generators to the site to recharge batteries could be considered as one way to extend their functioning.

Throughout the development of an AMP it is necessary to consider the reliability of instrumentation, as it may be exposed to unusual process and/or environmental conditions. A similar philosophy is normally adopted for the use or updates of equipment included in the AMP, especially in mitigating severe accidents. In either case, whether upgrades are expected or not, which equip-

ment is able to perform as required for the success of individual strategies needs to be determined. This evaluation includes:

— Identification of equipment that is expected to operate beyond its original design range and margins,
— Determination whether the severe accident environment may prevent equipment from performing its intended function and the failure modes of equipment,
— Identification of alternative equipment that can be used for the strategy selected.

In addition, information and measurement needs and information availability should be assessed, including the following five steps:

(1) Identification of information needs:

— To determine the status of the plant's safety functions,
— To identify challenges to safety functions,
— To identify the mechanisms causing the challenges,
— To initiate actions to prevent or mitigate challenges in accordance with the appropriate severe accident management guideline.

(2) Identification of the capability of existing instrumentation and measurements to supply needed information to:

— Determine design classification,
— Assess the measurement range of the available instruments,
— Determine the environmental qualification conditions.

(3) Determination of plant conditions (pressure, temperature, radiation level, humidity, hydrogen concentration) for relevant sequences and accident scenarios.

(4) Determination of adequacy of existing measurements for accident conditions identified in the previous step through comparison of:

— Range,
— Qualification conditions.

(5) Determination of means to meet information needs not provided for by existing instruments, owing to failure during severe accident conditions:

— Extending the range of instruments,
— Protecting instrumentation,
— Developing CAs to supply missing or supplementary information,
— Installing new instruments.

In accordance with Ref. [4], adequate consideration needs to be given to the availability and capability of various plant systems and provisions, in particular:

— Emergency core cooling,
— Heat transfer to ultimate heat sink,
— Containment integrity,
— Containment leaktightness,
— Containment penetrations,
— Containment isolation devices,
— Containment heat removal,
— Control of fission products, hydrogen and other substances released during the accident.

4. DEVELOPMENT OF AN AMP

4.1. SELECTION AND DEVELOPMENT OF SEVERE ACCIDENT MANAGEMENT STRATEGIES

4.1.1. Selection of severe accident management strategies

Severe accident management strategies are selected after a review of all severe accident insights relevant to a particular plant or group of plants. These insights are obtained from various sources, including the analyses described in Section 3:

(a) Severe accident research at a variety of institutes and laboratories;
(b) Potential accident management strategies from other sources, e.g. Ref. [8];
(c) Industry studies on severe accident management guidance, e.g. Ref. [6];
(d) The PSA or individual plant examination (IPE) of that plant or group of plants.

Based on this material, the different stages and processes of a severe accident are studied to determine whether they apply to the plant(s) being considered. A binning process may be followed, in which consequences of phenomena and countermeasures are considered. An example of such a binning process is given in Table I, based on material from the BWR Owners Group in the USA.

Once insights have been determined, a path can be set out to obtain suitable strategies with due consideration being given to the remaining uncertainties in severe accident insights. Such strategies are single actions or a series of actions to be initiated after a degraded condition has been

TABLE I. EXAMPLE OF THE DEVELOPMENT OF SEVERE ACCIDENT MANAGEMENT INSIGHTS FOR AN NPP

Steam explosion	In-vessel: will or will not fail containment, is likely/unlikely Ex-vessel: will or will not fail containment, is likely/unlikely
High pressure melt ejection	Will or will not fail containment Is/is not precluded by RPV depressurization
Core concrete interaction	Can/cannot lead to containment overpressurization Can lead to combustible gas (CO) Will/will not continue after flooding of debris
Recriticality	Control rods will/will not melt before fuel rods melt Likely/unlikely during flooding if control rods have melted Debris bed will/will not be critical when flooded
In-vessel debris cooling	Submerging debris will/will not keep debris in-vessel
External vessel cooling	Will/will not keep debris in-vessel Venting of skirt (BWR) is needed/not needed to debris cool in-vessel
Ex-vessel debris cooling	Submerging debris will/will not keep drywell intact (BWR)
Hydrogen generation	Hydrogen deflagration may/may not occur Deflagration may/may not challenge the containment integrity
Pressure suppression (BWR)	Will be lost/not lost at discharge of debris from vessel
Determination of accident progression	Onset of core melting will/will not be observed by the CR Relocation of debris to lower plenum will/will not be identified by the CR Reactor pressure vessel breach will/will not be observed by the CR

identified. A degraded condition is often called a 'plant damage state', for which several approaches exist. Examples are given in Appendix I, where the damage states refer to the core and the containment, or are directly linked to certain parameters that exceed safety thresholds. Sometimes the initiating event and the degraded condition of the safety systems are also considered. A matrix of generic plant states has been developed by the OECD (see Section 4 of Ref. [9]).

Some calculations may be needed to define a particular plant damage state, as measured parameters may need interpretation. In order to avoid the need for such calculations during an actual event, precalculated curves and graphs may be used as CAs. Measuring the containment pressure and reading the hydrogen concentration may, for example, give an immediate insight as to whether or not the containment is challenged. Appendix III contains further information and examples of such CAs.

Strategies are based on actions that are either still available to the operator or are available only after certain systems have been restored to service. These are high level actions, as they are primarily meant to protect FP boundaries (containment, SG tubes) and restore core/debris cooling to the extent possible. For this reason, these actions are sometimes called CHLAs. A list of such CHLAs is given in Appendix II. In general, they provide responses to the plant damage states defined above and are either initiated after recognition of such plant damage states or after certain parameters exceed their safety thresholds, depending on the approach chosen.[7]

As these actions may be executed under a variety of plant damage conditions, it is important to determine beforehand what their effect will be under these conditions. Injecting non-borated water into a PWR vessel may, for example, have profoundly different effects when done on an intact core geometry than when the control rods are already molten, or on a debris bed. Restart of a reactor coolant pump (RCP) may be very beneficial at the beginning of the accident while there is still water in the RCS, but may greatly increase the risk of SG tube creep rupture if done later.

The Electric Power Research Institute (EPRI) has conducted a comprehensive study on the effect of CHLAs during plant damage states [6]. Note that this information is usually not available from the plant PSA or IPE, as these normally do not model the large variety of operator actions during and after the onset of core damage [9, 10].

---

[7] The US Combustion Engineering Owners Group (CEOG) approach is an example of the former and the Westinghouse Owners Group (WOG) approach an example of the latter approach.

As pointed out in Section 2.5 and further explained and illustrated in Appendix II, actions should not be taken before their positive and negative consequences have been carefully considered. In this decision making process, the uncertainties inherent to severe accident phenomena also have to be taken into account. The initiation and execution of actions, with all their side effects, is set forth in the SAMGs. Where quantitative information is needed or useful, use is made of CAs, for example, if it is known beforehand how much water will be needed to remove the debris decay heat as a function of time after shutdown. Appendix III gives examples of such CAs.

As the independent development of suitable SAMGs is a major undertaking, it may be beneficial to use one of the generic approaches available. These have been developed by the industry, mainly by owners' groups or larger utilities.[8] The generic material must then be adapted to meet the needs of individual plants.

4.1.2. Development of severe accident management strategies

The first step in the development of an AMP is to decide on and document the basic severe accident management strategies to be applied to the specific plant. The strategies selected and their implementation may depend on the basic approach chosen based on national requirements. If plant modifications are carried out to enhance the AMP, the degree of confidence in successful accident management actions will be increased.

If the AMP is developed from a generic programme based on the reference plant concept, the development team should check that the differences between the actual plant and the reference plant are not important enough to invalidate the strategies. It may be crucial to the preventive strategies that the reactors, as well as primary and relevant secondary system designs, are similar. The containment designs should also be similar. If this is not the case, the generic actions may still be valid, but they may need to be executed in a different order or initiated from other values of set points.[9]

When developing individual severe accident management strategies, interaction between various strategies may take place. Examples are interaction among primary circuit depressurization, hydrogen management, cavity

---

[8] These include: in the USA, Westinghouse, ABB/Combustion Enginering, Babcock & Wilcox and General Electric; in France, Electricité de France; in Sweden, Vattenfall.

[9] An example is the value of the core exit temperature for entering the WOG SAMG domain at WWER reactors, which is about 100°C lower than for Western PWRs. Another example is the sequence of primary and secondary feed and bleed actions at WWER reactors.

flooding, filtered venting and long term heat removal from the containment. These strategies should therefore not be developed independently. For some plant designs, even slight differences may have a major impact on the interaction of selected strategies. The resulting strategy basis document will be applied for the development of accident management procedures and guidelines. There are various ways to develop the accident management guidance based on the selected strategies (see Fig. 1):

(a) Incorporate preventive strategies into the EOPs and develop separate guidelines for mitigatory strategies,
(b) Include all accident management guidance (i.e. actions related to beyond design basis events) in separate procedures and/or guidelines,
(c) Incorporate accident management guidance as an enveloping symptom based or state oriented part of EOPs.

The following sections describe the process of developing the procedures and guidelines.

4.2. DEVELOPMENT OF ACCIDENT MANAGEMENT PROCEDURES AND GUIDELINES

4.2.1. Development and writing

Development and writing of accident management guidance involves various closely related activities, each influencing the quality of the final product. There are quality assurance (QA) related requirements such as several independent reviews of each EOP by development team members as well as CR staff. There may be a need to assess modifications to strategies or development of new strategies which may influence already written procedures. Clarity of language, consistency of terminology and other style related requirements should also be given proper consideration. Therefore, careful planning of the project with enough control points and effective interface between the individual phases is important.

A critical part of development is feasibility assessment. This may be done while strategies are being developed and the guidelines are being written and includes, but may not be limited to, evaluation of:

(a) The availability of information and instrumentation,
(b) Equipment performance under severe accident conditions,
(c) Accessibility of equipment,

(d) The necessity/possibility of overriding safety related instrumentation and control (I&C).

For each severe accident management strategy, the existing instrumentation should be analysed to check whether information necessary to monitor safety functions, entry criteria to the relevant guideline, execution of the guideline and success criteria for the guideline are available. Another important aspect is the reliability and accuracy of the information in view of environmental conditions of instrumentation and sensors. Procedures should include diversity and redundancy of measurement of some parameters and provide alternative information sources for instruments that may have failed.

A prerequisite to execution of SAMGs is that equipment and instrumentation used in any of these guidelines and strategies will perform as intended under the expected environmental conditions. It should be decided whether the proposed strategy should be implemented if this performance has not been confirmed. If it is decided to implement the strategy even if success cannot be guaranteed, a minimum requirement would be that the information used to initiate and monitor execution and success of the strategy is sufficiently reliable and the fact that equipment performance has not been verified is known to the operator.

One of the major differences between procedures and SAMGs is the increased need for on-site actions in different plant compartments, e.g. restoration of power to active components, repair of malfunctioning driving devices or components, and operation of valves which are not power driven. When such on-site actions are included in the guidelines, a careful examination should be conducted to determine whether the equipment concerned can be accessed without exposing personnel to excessive radiation, temperature and other potential dangers. Such an examination could also result in backfitting measures to reduce hazards and improve physical accessibility.

Since SAMGs are often based on the non-conventional use of existing operating or safety systems, it is possible that the proposed staff intervention will be prevented by the safety related I&C which has priority, or individual component protection I&C. The operator must be able to deactivate these functions without major delays when it is sufficiently clear that they would prevent him or her from executing the required accident management guideline. An important aspect of accident management planning is to ensure that adequate administrative controls are in place to prevent premature or inappropriate execution.

Depending upon the approach adopted, the following guidelines and documents need to be provided in parallel with the development and writing of the SAMGs:

(i) Guidance for the main CR operators during a severe accident.
(ii) Guidance for the TSC (or equivalent support staff), including the chosen methodology for recording implemented strategies and listing and addressing long term concerns.
(iii) Computational aids to allow support staff to understand plant conditions based on the available instrumentation (not necessarily computerized) and to guide them in the selection and execution of suitable strategies; several examples of CAs and their application are given in Appendix III.
(iv) Calculation of the plant specific set points required by the SAMGs.

If the generic procedures and guidelines are written in another language, suitable provisions must be made to prevent confusion arising from language differences.

Based on the severe accident management strategies, procedures are to be as user friendly as possible. Extensive use of flow charts, figures, tables and diagrams should therefore be considered.

4.2.2. Preparation of background material and documentation

Background material is prepared in parallel with the development and writing of the individual procedures as it has to document all the changes, improvements and modifications to generic strategies and procedural steps which were agreed to at the time of writing of the accident management guidance. All grounds and justifications should be recorded to allow for future reviews and for the updating of procedures and guidelines in the light of new knowledge of plant behaviour or modification of plant systems.

Because of the greater complexity of severe accidents compared with DBAs, as well as the continuously increasing knowledge base on plant behaviour under severe accident conditions, consideration should be given to creating background documents in a way that allows easy upgrades and extensions and allows their use as reference and training materials. Background material should include:

(a) The technical basis for strategies,
(b) Detailed description of instrumentation needs,
(c) Results of supporting analyses,
(d) The basis and detailed descriptions of procedure and guideline steps,
(e) Set point calculations and their basis.

The preparation of good background documentation is very important. It has three primary functions:

(1) It is a self-contained source of reference,
(2) It demonstrates compliance with the relevant QA requirements,
(3) It provides support material to be used in training courses for technical support staff and operators.

The reference and training course support functions of a background document may require it to be supplemented by additional analyses for illustration, even though generic preventive and mitigatory strategies have been applied and the assessment did not require a plant specific analysis.

Additionally, a 'deviation document' may be prepared which lists the differences between the plant specific procedures and guidelines developed and the generic ones, and explains the reasons for the differences.

4.3. SUPPORTING ACCIDENT ANALYSIS FOR DEVELOPMENT OF PROCEDURES AND GUIDELINES

Plant specific analysis requirements are discussed in terms of three categories: preliminary analysis, development analysis, and analysis to support verification and validation of procedures and guidelines. This section discusses development analysis and assumes that preventive actions are incorporated into the EOPs and guidance on mitigatory actions is given by the SAMGs.

4.3.1. Development analysis of EOPs

Development analyses are needed for detailed confirmation of the choice of recovery strategies adopted, to provide necessary input to set point calculations (where appropriate), and to resolve other open items identified during the writing of EOPs and the review of draft documents. Phase I of the AMP results in a preliminary list of such analyses. This list will include most of the plant specific analyses needed for the development of EOPs because, provided the information inputs to phase 1 were sufficiently detailed and a good knowledge of design differences between the reference plant and the plant concerned is available, major changes to strategies or additional open items should not arise during phase 2 (the actual developing and writing of procedures). In the case of more substantial design differences, such as those between a PWR (reference plant) and a WWER, several behaviour differences related to plant design can be expected, which will have an effect on generic strategies.

Empirically, four types of open items are identified for this generic approach:

(1) A need for evaluation, usually in terms of a specific system design or capability to perform a certain function (for example, can the auxiliary spray be used during a steam generator tube rupture (SGTR) to depressurize the primary system without adverse thermal fatigue problems to components);
(2) A need for an analysis to be performed (for example, what criterion should be used to initiate primary side feed and bleed cooling);
(3) A possible need for a plant modification (for example, an increase in the range of core exit temperature measurements to allow monitoring of the core cooling safety function);
(4) A need to change the staffing of the plant.

The list of open items defined in this way will therefore include the analysis required to resolve all issues before the detailed procedures are written. Such analysis should ideally be performed before phase 2 is begun, but could in practice be performed in parallel with the writing of the phase 2 procedures. The need for specific analyses will arise from attempts to refine the strategies. Therefore easy availability of computing facilities, preferably with access to a full scope simulator, is very useful.

4.3.2. Analysis for the development of severe accident management guidelines

As in the EOP process, during phase 1 a list of issues or open items which should be resolved prior to or during the early stages in the preparation of plant specific SAMGs will be identified. This list includes the analysis needed to confirm the choice of recovery strategies adopted, to provide necessary input to set point calculations (where appropriate), and to resolve any other open items identified during the development and review of SAMG strategies. These issues or open items can be divided into the following four types:

(1) Evaluation of the capabilities and design of the systems. Based on the experience gained in implementing SAMGs, the type of evaluation needed most at this stage pertains to the performance of systems, and in particular the capability of systems to perform functions other than those for which they were designed, together with assessment of the adequacy of the system to perform that function (for example, it may be possible to align the containment spray system to inject directly into the reactor system; in this case it will be necessary to evaluate the flow rates achievable, system pressure ranges, ability to manually realign systems within the required time, and access to system components following a severe

accident, etc.). Additional evaluations for possible degradation of the designed systems need to be made before any changes to the physical plant are considered. Increasing the failure probability for a system design mode is not acceptable even if it offers an advantage during a severe accident condition because its use for design mode operation is much more likely than for a severe accident mode. Deviations from this principle are acceptable only after careful consideration.

(2) Additional severe accident analyses to support individual severe accident management strategies and their interaction. For example, flooding the reactor cavity prior to vessel failure will enhance steam production and hence influence the time needed for venting the containment.

(3) Analysis needed to support development of CAs, diagnostic tools and guideline set points. For example, hydrogen combustion sensitivity calculations and containment flooding analysis.

(4) Analysis needed to determine the ability of plant personnel to perform the tasks it may be required to perform as part of the accident management strategy under the conditions prevailing during an accident.

(5) Analysis needed to minimize the consequences of accident management actions for the off-site population, including the consideration of provisions to allow off-site officials to implement appropriate protective actions.

(6) A potential need for plant modification. The philosophy of SAMGs is to implement guidance to make the best use of existing plant equipment in mitigating the consequences of a severe accident, and not to generate exaggerated requirements for system changes. However, in certain cases where changes would clearly bring great benefit, they may be recommended at this stage. For example, this approach may be applied mainly to monitoring capability, such as hydrogen concentration measurement for the containment and extension of the range of pressure instrumentation for the containment.

4.4. DETERMINATION OF THE NEEDS FOR PLANT INSTRUMENTATION, EQUIPMENT AND MATERIAL, AND NECESSARY UPGRADES

Following the principles laid down in phase 1, detailed lists of the equipment and instrumentation needed and available and its capabilities must be prepared. Moreover, it needs to be demonstrated that the equipment foreseen in the strategies will meet the requirements.

With regard to the instrumentation, each requirement in the guidelines to monitor a plant condition has to be taken into account. All possible means of

monitoring a particular parameter should be identified and prioritized. For prioritization, consideration should be given to:

(a) The information available regarding the expected environmental conditions to be experienced by the instrument and its likely ability to withstand them,
(b) The qualification of the instrument,
(c) The physical location of the instrument,
(d) The ability of the instrument to perform the required function (its range, accuracy and other capabilities).

Any limitations of the equipment and instrumentation identified need to be specifically listed and included in the SAMGs. These limitations may give rise to requirements for upgrades or new dedicated instrumentation.

If analysis indicates that instruments are beyond their environmental range of accurate operation, it should be determined to what extent they can still function. For instance, if a temperature indicator is not accurate in an environment of high humidity and radiation levels, it may not show the temperature accurately but may still have the ability to indicate whether the temperature is increasing or decreasing.

Protection against radiation in the CR or the central location from which accident management will be co-ordinated and monitored (TSC, on-site emergency control centre), as well as important access routes to and from the plant, needs to be evaluated. Such protection would enable the long term presence of operating personnel in this location, but fulfilling the habitability requirements may necessitate plant upgrades.

4.5. INTEGRATION OF PROCEDURES, GUIDELINES AND THE PLANT'S EMERGENCY ARRANGEMENTS

As stated in Section 3.3.4, a transition from EOPs to SAMGs must be defined. This can be either a fixed and irreversible transition or a parallel execution of both, with a consistency check and priority given to the SAMGs. In the former case EOPs should be formally exited and need to be modified to include such exit conditions.

Paragraph 4.7 of Ref. [7] requires that the transition from normal operation to emergency operation be clearly defined and be effectively made without jeopardizing safety. It is required to designate the responsibilities of all those persons who would be present on the site in an emergency as part of the transition. It is also required to ensure that the transition to emergency response and the performance of initial response actions do not impair the ability of the

operational staff (such as the CR staff) to follow the procedures necessary for safe operations and for taking mitigatory actions.

In addition, the process for the classification of emergencies and the activation of the response, as established in Ref. [7] (paras 4.20, 4.70), should be integrated into the process of activation of and transition to the accident management arrangements.

The actual transition is decided upon either by the CR staff when they reach the exit conditions, or by higher levels in the emergency response organization (ERO) hierarchy once they have taken note of the deteriorating situation of the plant. Appendix VII gives examples of the 'exit criteria' and transition mechanisms for several actual applications.

As a consequence, the ERO should be reorganized to include the activities of the TSC (or equivalent support) with respect to SAMGs. This sometimes entails the establishment of a separate accident analysis team (AAT) whose prime responsibility is to assess the plant state and give recommendations to the responsible management. Principles for dealing with these will have been defined in phase 1, and they must now be implemented. Important issues to be addressed include:

(a) Consistency with the emergency plan and any necessary upgrades to it,
(b) Definition and approval of the responsibility matrix,
(c) Definition of criteria for activation of the TSC and AAT,
(d) TSC equipment for monitoring the current plant status.

The accident management guidance provides a function which has up to now been missing at most plants — that of identifying, evaluating and implementing a set of well-defined recovery actions to terminate or mitigate releases and restore a controlled stable condition in a plant which is experiencing a severe accident. Since this function did not previously exist in any formal way, it has not been reflected in the organization defined by the plant's emergency plan, which in most cases deals primarily with the management of off-site occurrences. The SAMGs must be integrated into the organizational structure defined in the emergency plan and interface with it to ensure a consistent and co-ordinated response to severe accident conditions. Therefore, as part of the plant specific SAMG implementation, the emergency plan needs to be reviewed with respect to the actions that should be taken following the SAMG, to ensure that conflicts do not exist. This review might recommend changes to the emergency plan to eliminate such conflicts.

It needs to be ensured that there are no conflicts with the arrangements made for security, fire fighting and support from off the site, such as the off-site fire brigade or off-site security.

An important part of the integration of the SAMGs with the emergency arrangements is the definition of the matrix of responsibilities for severe accident mitigation actions. Use of the SAMGs will result in recommendations for CR operators to take specific actions in response to decisions made at the appropriate level. If the event has developed to the extent that SAMGs are required at all, which means that there has been a multitude of systems and equipment failures, the availability of equipment needed to perform mitigatory actions needs to be assessed 'on the spot', and continually reassessed during the use of the SAMGs. The guidelines therefore provide a structure for the evaluation of current plant conditions and equipment availability, and a means to determine which of the available courses of action is the most appropriate. Following the evaluation and recommendation of a course of action, the decision must be made to either implement the proposed actions or choose alternative actions, and then act upon that decision. Therefore, in a severe accident situation, the on-site ERO must have three kinds of personnel:

(1) Evaluators: This is a team responsible for evaluating (using the SAMGs) and identifying a relevant accident management strategy. This requires a detailed knowledge of the SAMGs and a good understanding of the underlying severe accident phenomena, as well as access to plant status information. Sometimes this group of people is called the AAT or accident management team (AMT).
(2) Decision makers: These persons have the authority to decide on the implementation of an accident management strategy (as put forth by the evaluators) and have a broader understanding of the status of other aspects of the emergency response, including effects off-site, which he or she takes into consideration when making decisions.
(3) Implementers: This team implements the recommended strategy in the CR.

The above responsibilities are to be defined clearly in the AMP documentation. The emergency plan must reflect these responsibilities since it defines the overall emergency organization.

The guidelines can be structured to separate the evaluators from the implementers. Normally it is suggested that the evaluators be in the TSC and the implementers the CR duty shift.[10] However, during the plant specific implementation phase the accommodation of these different SAMG functions

[10] For example, the generic US SAMG has been written on this basis.

within the plant's emergency organization (as defined in the emergency plan) has to be addressed on a plant specific level.

Apart from the three core functions mentioned above, other support functions are useful or required. For instance, the flow of information between the TSC (or equivalent group) and the CR, as well as from the TSC (or equivalent) to other parts of the ERO, must be well organized. These functions are best assigned to dedicated 'communicators'. However, as a severe accident will generate extensive communication needs, both on-site and off-site, it is desirable that the off-site needs do not interfere with accident management. Section 5 further describes the plant's emergency organization, including the responsibilities of the TSC and AAT.

Reference [7] establishes requirements for performing various emergency response functions, including: establishing emergency management operations; identifying, notifying and activating; taking mandatory action; and protecting emergency workers. These requirements form the foundation of the emergency response arrangements on the site.

4.6. VERIFICATION AND VALIDATION OF PROCEDURES AND GUIDELINES

4.6.1. Verification

Verification is the evaluation which confirms the correctness of a written procedure or guideline and ensures that technical and human factors have been properly incorporated. As such, the review of plant specific guidelines during the development phase, in accordance with QA regulations, forms part of the verification process. It is advisable to perform all implementation activities, including independent review, in accordance with internationally accepted QA guidelines as outlined in Refs [11, 12]. In addition, an independent review and verification by an independent organization which is completely familiar with the AMP (for example, another similar plant) is recommended. Review by the national regulatory body may also be required, though the extent of this review depends on the individual organization's or national requirements.

4.6.2. Validation

Validation is the evaluation which determines that the actions specified in the procedures and guidelines can be followed by trained staff to manage emergency events. Emergency operating procedures can be validated in a number of ways. The best is probably to use a full scope simulator facility. However,

engineering simulators, plant analyser tools, table top exercises, etc., might also be used. The amount of analysis needed beforehand depends on this choice. Validation also provides a 'check' on strategy selection and development and will further confirm that strategies adopted directly from the generic guidelines with no analysis at the phase 1 stage are appropriate.

Validation of SAMGs can be approached in various ways. Although the purpose is the same as for EOP validation, different means will be adopted for various reasons. To date, SAMGs have been successfully validated using table top methods for the TSC staff and full scope simulators to exercise the operator controlled transitions from the EOP [13–17]. Both individual exercises (involving the TSC, the operators or any other part of the plant emergency response team separately) and integrated exercises (involving whole teams) have been performed. In setting up a validation programme for plant specific severe accident management guidance a number of factors must be considered, including:

(a) The general approach: tabletop exercises, use of simulators or plant analysers, integrated versus limited/individual exercises.[11]
(b) The supporting analysis needs: the methods used to provide them, codes to be used, possible use of scenario templates, etc.
(c) The staffing of the validation team: speficially the exercise controllers and technical advisers who are not involved in the exercise but are responsible for running and co-ordinating it. They must be able to define credible plant conditions for the exercise on the spot.

4.6.3. Supporting analysis

The need for supporting analysis for verification and validation of EOPs will largely depend on the validation method. Therefore general guidance cannot be given. However, the following considerations apply:

(a) Verification of the plant specific EOP (i.e. evaluation to confirm the written correctness of the EOP and to ensure that technical and human factors have been properly incorporated) can normally be achieved without additional analysis.
(b) Validation (the real time evaluation performed to determine whether the actions specified in the EOP can be followed by trained operators to manage emergency situations) is achievable in a number of ways.

[11] In a limited exercise only the TSC staff are trained, not the integration of the entire emergency preparedness staff.

Probably the best method is use of a full scope simulator, but other approaches such as engineering simulators, plant analyser tools, tabletop exercises, etc., may also be used. The amount of analysis needed beforehand depends on which method is chosen.

(c) Validation provides a 'check' on strategy selection and further confirms that strategies that were adopted directly from generic guidelines with no analysis during phase 1 are appropriate.

(d) Analysis to support verification and validation of guidelines may be done in order to demonstrate the capabilities and choice of appropriate strategies and optimize them. Such analysis should be done with a suitable and reasonably validated code, and should be carried out on a best estimate basis [18]. The need for this type of analysis will also depend on the type and methodology of the validation process.

(e) At present, most simulators are not capable of modelling system response in a severe accident regime. A SAMG validation programme will instead most likely consist of a combination of simulator (for testing the EOP–SAMG transitions and the early phase of the accident) and table top exercises (to test TSC usage and long term recovery). Tabletop exercises will require some severe accident analysis prior to validation to serve as a basis for simulated plant response. The amount and scope of such analysis must be defined once the detailed approach to validation is finalized.

4.7. SPECIFICATION OF TRAINING NEEDS

During the AMP development phase training needs must be identified in time to allow preparation of the training programme which must be held during the implementation phase. The training plan identifies the staff members who need training, the level and scope of the training and its form for various groups.

Classroom courses can be used for basic familiarization with the accident management guidance. Drills and exercises, possibly using simulators with severe accident modelling capabilities where these exist, are efficient training methods. Implementation of training programmes will be discussed in more detail in Section 5.

4.8. REVIEW OF THE AMP

Regular meetings are to be organized between the core team developing the accident management guidance and the plant personnel who will be required to use it. Information exchange between both groups can contribute

greatly to further development work at a later stage. Recommendations made at these meetings can easily be included in the draft procedures and guidelines before finalization.

Review meetings need to confirm that existing QA rules are being obeyed, including that any requirements set forth by the regulatory body during the first phase of the project have been taken into account. This phase of the project is important because a careful review process can greatly enhance the quality of the work. It can also minimize the time and work needed for completion of the project and implementation of procedures and guidelines. Appendix VI can be used as an example of such a review.

4.9. INVOLVEMENT OF THE REGULATORY BODY

The degree of involvement of the regulatory body varies from State to State. It will always be necessary to understand and check compliance with any requirements.

5. IMPLEMENTATION

5.1. OVERVIEW OF THE PLANT'S EMERGENCY ORGANIZATION

5.1.1. General

Reference [7] establishes specific requirements relating to the infrastructure necessary for implementing and maintaining an emergency response capability. These infrastructural requirements cover: authority; organization; co-ordination of the response; plans and procedures; logistical support and facilities; training, drills and exercises; and quality assurance programmes. These requirements form the basis for the implementation of the emergency response arrangements necessary for accident management. The following text deals with specific issues relating to on-site accident management.

An overview of a typical on-site organization for responding to an emergency is provided here, as the new SAMG functions interface with the existing emergency organization. The emphasis is on those people who are responsible for actually using the EOPs and SAMGs. There are variations between plants and in the details, as each plant's organization is different. The organization described here is typical of many US and Western European NPPs and can be

used as an example of the structure of a specific plant organization. It should be noted that TSCs may not currently be in place for all nuclear utilities. However, technical support should be accessible during an emergency. In the following the abbreviation TSC will be used to describe all such organized support.

5.1.2. On-site emergency organization

The plant's on-site emergency organization and the duties and responsibilities of its members should be defined in the site specific emergency plan and, where appropriate, supported by relevant procedures. The on-site response to an emergency situation will depend on the following key staff:

(a) Paragraph 4.23 of Ref. [7] requires that there be a person on the site at all times with the authority and responsibility to classify a nuclear or radiological emergency and upon classification promptly, without consultation, initiate an appropriate on-site response.
(b) Operations staff: The operating shift is ultimately responsible for implementing recovery strategies. Organizations vary, but the operating shift for a single unit will normally consist of a shift supervisor and two or three operators in the CR, sometimes with an additional shift member out on the plant. The shift staff are supervised by a shift manager. Normally, the shift manager may be responsible for more than one operating shift in multiple unit plants. The shift manager reports to the head of the plant's operations department, who himself reports to the plant manager.
(c) On-site technical support, usually located in a TSC: Before the advent of accident management, the on-site duties of the TSC were to provide, on an as-needed basis during an emergency, technical advice to the operation staff. The EOPs recognize that most plants have a TSC, and in the relatively few cases in which EOPs require an evaluation of plant conditions before a possible action can be chosen, the EOP directs the operators to seek the TSC's advice. However, in the past the role of the TSC has often been somewhat unclear or ill defined. In spite of this, a TSC is part of the emergency organizations of most plants (it is a requirement in many countries), with fixed requirements as to the qualifications of its members, the provision of a location equipped with data acquisition and display systems, plant status boards and communications links with the main CR. The TSC's role has, however, always been more oriented towards the support of operations and on-site plant recovery. Implementation of the SAMGs gives the TSC important new responsibilities. It would, in the event of a severe accident, now play a primary role. Technical support centre staffing varies, but normally consists of a team of plant technical staff from different depart-

ments and with different areas of technical expertise. It is important that the activation of the TSC, including the members who are on call, and the time allowed for the establishment of a functioning team once the CR requests support, be considered for the successful integration of the SAMGs. The TSC normally consists of ten to twenty persons. This number may vary, depending on the evolution of the event and the technical expertise needed. In addition to the TSC, different technical departments are represented (e.g. operations, electrical engineering, systems engieering). A secretary and a team member dedicated to updating plant status boards may be included. Actual repair and maintenance work is carried out by a group of technicians assigned to those tasks which is sometimes called the operations support centre (OSC).

(d) Accident assessment team (AAT)[12]: Most plants do not yet have an AAT. With implementation of SAMGs, a small team is required to actually use the guidelines and develop the recommended recovery strategies. This team is part of the TSC but retains a separate identity because it needs specific training. The AAT would normally consist of three to four TSC members reporting to the TSC leader (not himself an AAT member). It comprises the evaluators described in Section 4.5 plus their support staff who provide data on trends and communicate with the CR and the emergency response team.

(e) Emergency response team (ERT): The ERT is responsible for assessing the off-site consequences of an event and recommending off-site actions. The functions of the ERT are defined in the emergency plan. They include communication with local authorities, declaration of the emergency status of the plant, assessment of radioactive releases and prediction of likely radiological consequences as the event evolves. The team leader, usually called the emergency director or emergency controller, is specially trained for these duties, and will often be the plant manager or one of his deputies, or the manager of one of the other plant departments (such as operations). The emergency director will perhaps have the best overall view of the event's evolution. Usually, one of the tasks of the TSC is to supply the ERT with FP source term projections for use in predicting possible off-site exposure, or the ERT might do everything itself. A typical TSC organization is depicted in Annex III.[13] Extensive guidelines have been developed for some applications.[14] These are intended to structure and guide the work of the TSC.

---

[12] This group is sometimes referred to as the AMT.

[13] This is an example from a typical BWR in the USA.

[14] Notably with the US BWR Owners Group (BWROG).

5.1.3. Organizational aspects of implementation

Organizational aspects of EOP implementation are quite limited since they primarily involve the operations department, with support from other departments as needed. However, SAMG implementation has more organizational implications which should be given initial consideration at this stage. These include:

(1) Definition of the lines of responsibility for the actions contained in the SAMGs, especially with regard to who is responsible for the evaluation, decision making and implementation of guidelines (see Section 4.5).
(2) Definition of the responsibility matrix must consider the organizational aspects at the plant, the qualifications and expertise of the staff, and any legal and licensing implications.
(3) The team charged with actually using the SAMGs, i.e. those responsible for evaluating plant conditions and recommending actions, should be defined. Normally, this will be the AAT.

5.1.4. Involvement of the regulatory body

The development of an EOP/SAMG programme by the core team at the plant should involve a frequent dialogue with the regulatory body. The need for this will vary from country to country, but in all cases it will be necessary to understand the requirements (if any) and expectations of the regulator at an early stage and to develop an understanding of the likely approval process (if required) for the final EOP/SAMG package. It is therefore recommended that meetings be organized between the core team and representatives of the regulatory body at the end of each phase of the programme. It is also recommended that the severe accident sequences to be considered, the acceptance criteria, and the analysis methodology be discussed with the regulatory body at an early stage in the preparation of the AMP.

5.2. TRAINING

5.2.1. General

All personnel and groups which are required to respond to an accident should be clearly identified and their training needs well defined.

5.2.2. Scope and means

Classroom training or exercises and drills can be used. In the latter, a severe accident scenario is acted out by teams from the CR and the TSC. The focus is on correct execution of the EOPs in the pre-core damage state, the transition from the EOP domain to the SAMG domain, and the proper execution of the SAMGs applying to the TSC (if any). Specific training is needed where responsibility is passed on, e.g. from the CR to the TSC when an 'exit' condition is reached in the EOPs. Although the focus is on the correct execution of the severe accident management guidance by the CR personnel and the TSC, training on the overall emergency plan should also be provided at regular intervals.

Training should be based on an appropriate 'template' consisting of a scenario plus all the ramifications needed to act out the scenario in a drill. In developing this template it is important to include a wide spectrum of SAMGs so that the TSC and/or CR do not have only one or a small number of guidelines to choose from. The template should be 'dynamic' in nature; as the various actions taken by the TSC and CR cannot be predicted in much detail, a range of possible responses should be considered. Time constraints will usually prevent the template from covering a complete core damage scenario, necessitating 'jumps' or 'skips' in the scenario. These interruptions should not receive undue attention from the teams being trained since their working methods should reflect changes to parameters.

Drills have to include all team members. Too much emphasis on certain team members (e.g. the decision maker(s)) should be avoided. Training will be most realistic if the pre-core damage and transition phases are executed on a plant simulator.

The exercises and drills need to be observed by a team that assesses performance. The teams involved should also give a self-assessment/critique of their performance. Assessments are documented and filed, and the lessons learned are incorporated in the procedures and guidelines and in the training itself.

It should be emphasized that the success of the actions in terms of controlling the simulated accident is, by itself, not the proper criterion to measure team performance. The drill/exercise is a success if the teams have worked together, have followed their working procedures, and have established the proper level of communication, evaluation and decision making.

5.2.3. Skills of staff members

The following should be used as an aid to identify the individuals and groups requiring training and the level of training needed:

(a) SAMG users: The members of the on-site emergency team who are given the task of actually using the SAMGs, evaluating plant status and recommending the appropriate recovery strategy (see 'Evaluators' in Section 4.5) will require the most thorough training.

(b) Control room staff and supervisors: As discussed, most SAMG approaches are organized in such a way that those responsible for evaluating the plant status and selecting the recommended recovery strategy will not be the operators themselves, but a separate and perhaps remote (though still on-site) team, most likely the TSC. Operators will still be responsible for implementing the strategies recommended by this team (see 'Implementers' in Section 4.5). It is therefore extremely important for the operators to have confidence in the TSC and SAMGs and to understand that actions may be required of them which appear to be in conflict with their established EOP training. The level of training provided must ensure this without becoming an excessive burden on operating staff to the detriment of training in the use of EOPs.

(c) Emergency director/controller (see 'Decision makers' in Section 4.5): The emergency director (or emergency controller) heads the on-site ERT. He or she usually works at the plant management level and may be the plant manager or the manager of operations. For SAMGs, this person is likely to have the final say as to whether the TSC's recommendations are to be implemented by the CR. He or she must be completely familiar with the SAMGs and what they are based on. The personnel interfacing with SAMG users include:

— Emergency response staff: Those members of the ERT not directly involved with SAMG implementation;
— Technical support staff not using SAMGs: Those members of the TSC not directly involved with SAMG implementation;
— Off-site technical centre (if applicable): Members of off-site technical support teams, often from the operating organization or the plant vendor;
— The regulatory body.

In practice, there is considerable overlap between the different functions. The training needs of the various members of the organization can be evaluated individually and personnel can, for example, be placed in one of the following two groups:

(1) Staff needing detailed training in both the CR and TSC aspects of the SAMGs. This includes all operating shift staff and shift managers (including members of the TSC AAT), and all TSC leaders.

(2) Staff requiring an overview of the SAMG. This includes TSC members who are not part of the AATs, such as emergency controllers and other members of the emergency organization.

The level and content of classroom courses on severe accidents and accident management needs, means and practices may differ for these groups. Plant specific training should also be tailored according to the chosen approach to severe accident management and the function of the staff being trained, i.e. the training given to TSC members will differ from that given to emergency planners, etc. In some cases this training forms part of a formal licensing process (for example, EOP training of operators), in which case recipients must comply with strict requirements for updating, refresher training and testing. Plant specific training will normally be provided by operating organization or vendor staff.

Once the plant specific SAMGs are in place, the detailed training programme is implemented by the operating organization's training department, the vendor, or both. Training must consider:

— The participants and their individual needs (TSC staff, emergency planners, engineering support staff, operators, etc.);
— The professional level of the participants;
— Requalification/refresher needs;
— Drills and exercises.

A technique known as the 'systematic approach to training' is being used more and more. This method adopts a structured approach which defines the objectives, means and testing requirements of all aspects of the training in advance [19].

Training must take place at regular intervals which are compatible with the plant's overall operator and technical staff training programme. It must be frequent enough to keep the responsible staff well informed and prepared.

5.3. STAFFING AND QUALIFICATION

The capabilities of the TSC (or that part of the emergency organization responsible for the SAMG) need to be reviewed to ensure appropriate staffing and the qualifications of the staff to carry out their new SAMG duties [20].

5.4. REVISIONS TO THE AMP

It is important to upgrade the guidelines when new information which has an impact on accident management becomes available from severe accident research or from other sources. The operating organization is advised to actively follow such developments. The lessons learned from drills and exercises also have to be fed back into the programme.

Appendix I

PLANT DAMAGE STATES

The term 'plant damage state' is used to describe the degree of damage to the reactor core, the RPV and the containment. Under the US severe accident management programme, EPRI developed a technical database for use by all US owners groups (Babcox & Wilcox, Combustion Engineering ABB, General Electric and Westinghouse) in the development of guidelines to combat these conditions. At about the same time or a little later the PSA community used a description of plant damage states for scenario development in level 2 PSAs or interfaces between level 1 and level 2 PSAs.

Following are definitions of the EPRI technical database plant damage states:

Damage states of the core and the RPV:

- OX: The core is overheated and significantly oxidized but retains its intact configuration;
- BD: The core is badly damaged and sufficient overheating has occurred in it to melt and liquefy the reactor fuel and cladding;
- EX: The accident has progressed to failure of the RPV, and debris has accumulated in the containment.

Damage states of the containment:

- CC: Containment isolation is complete and containment heat removal systems are available;
- CH: Containment isolation is complete but containment integrity is challenged, either by loss of heat removal or hydrogen conditions which, if left unchecked, could cause containment damage;
- I: The containment is impaired, i.e. the isolation function is not complete;
- B: The containment is bypassed and may have no significant role in preventing or mitigating a release to the environment.

When discussing SAMGs and their content, the plant damage states are referred to as those plant damage conditions for which mitigatory strategies should be developed. Plant damage states can be presented as a matrix. In the following sample matrix, used by the Combustion Engineering ABB reactors, the OX condition has been dropped since the EOPs can deal with this condition if their configuration remains the same.

Conditions	CC	CH	I	B
BD	BD/CC	BD/CH	BD/I	BD/B
EX	EX/CC	EX/CH	EX/I	EX/B

The matrix is used as a guide for the response organization to understand what damage has occurred and gives a simplified graphical representation of what barriers, if any, remain intact and therefore the most urgent action needing to be taken to prevent any of the fission produced radiation from reaching the general public.

The plant damage states are defined through a logical process in which parameters for determining the condition of the core and the containment are checked and the availability of important systems is assessed. Both RCS and containment damage states are defined in this way, each having its own logic tree. An example is given in Fig. 2.

A group of CHLAs is defined for each of the plant damage states which are used to respond to that particular damage state (see Appendix II). These are then formatted into guidelines, i.e. groups of actions that can be executed by plant personnel. These guidelines contain initiation, throttling and termination criteria, cautions and benefits, and are basically the main vehicles used by plant personnel to respond to the degraded conditions.

A simple example of their use would be if the conditions were BD/I. This would mean that the reactor core is badly damaged and the containment is impaired. Therefore it is understandable that use of strategies developed for keeping the damaged core in the RPV should be considered first because, if the badly damaged core causes a vessel failure and the containment is impaired, some or all the FPs now in the RPV will be released from the containment.

Additional presentation methods have been used for identifying the severe accident plant damage conditions. These will aid the response organization in choosing a mitigating strategy.

A method developed by the WOG uses a diagnostic flow chart and a severe challenge status tree which groups plant equipment or parameters needed to evaluate plant damage states. These can be used to lead the response organization in the selection of strategies that may be more beneficial for the present accident situation. The diagnostic flow chart and severe challenge status trees look at the core damage condition and the containment conditions. Therefore they consider all the plant damage states described earlier, but do so in a different format (Fig. 2).

Other methods can be used to present strategies to the response organization. Their format usually allows integration into the plant's EOPs.

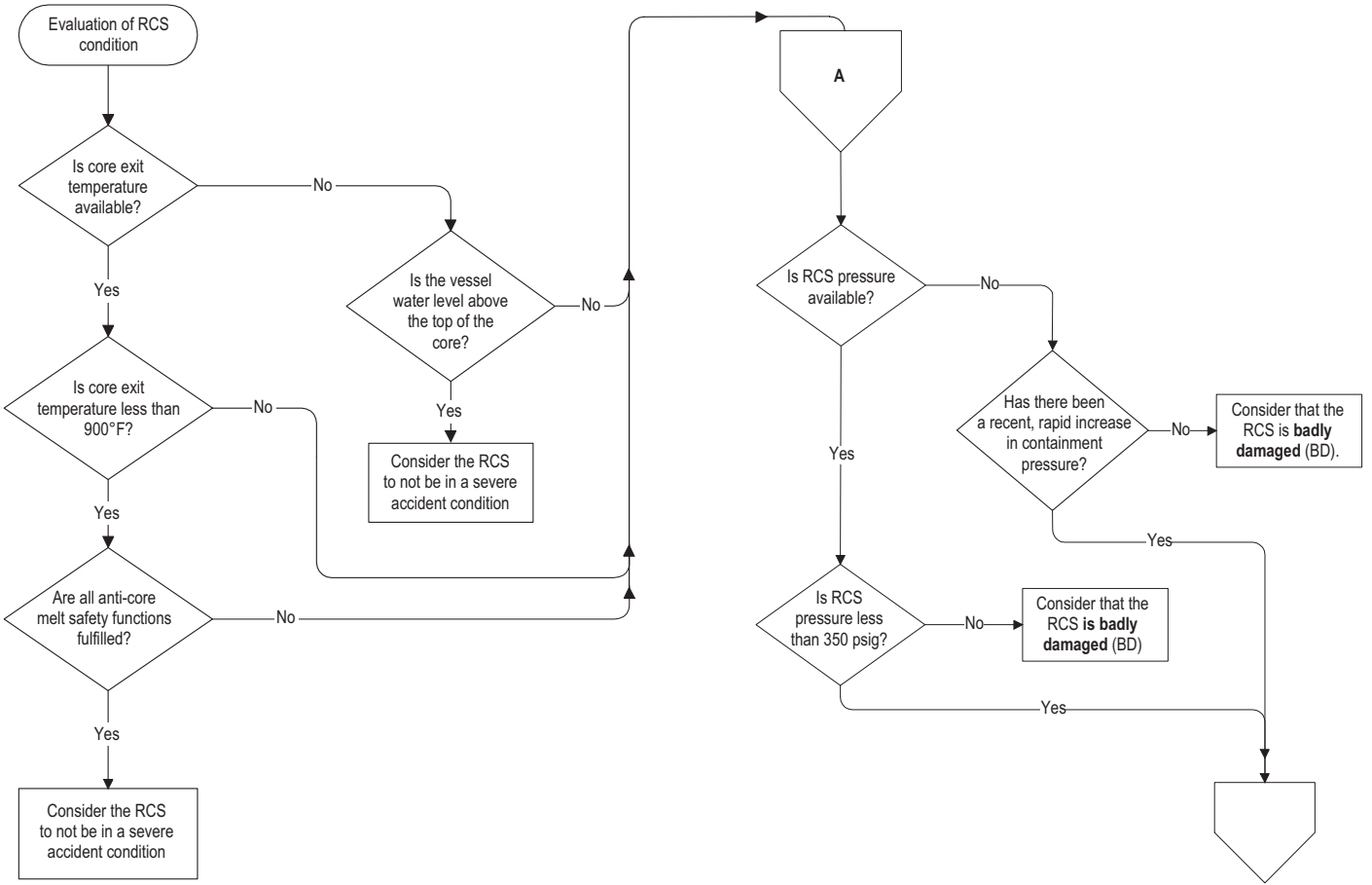

FIG. 2. Example of a CEOG logic tree to determine plant damage states (1 psi = 6.8946 kPa, ˚C = $\frac{5}{9}$ (˚F–32)).

The US BWROG has grouped its CHLAs into three guidelines which respond to deteriorating conditions in the vessel and the containment. The major guideline is an integrated RPV and containment flooding guideline that defines responses to the core degradation process in its increasing severity until vessel melt-through, while keeping track of the degree of damage to the containment with emphasis on protection of the pressure suppression function. In European approaches the distinction between the different plant damage states is less explicit, but the countermeasures envisaged fulfil the same basic objectives.

Appendix II

CANDIDATE HIGH LEVEL ACTIONS

Appendix I provides a structure to define a limited number of plant damage states. The appropriate responses to these states are sometimes called CHLAs (mainly in US approaches).

The following is a list of CHLAs, as used in various programmes:

(a) Inject into the RPV/RCS/RCP seal,
(b) Depressurize the RPV,
(c) Spray within the RPV (BWR),
(d) Restart RCPs,
(e) Depressurize the SGs (PWR),
(f) Inject into (feed) the SGs,
(g) Spray into the containment,
(h) Inject into the containment,
(i) Operate fan coolers,
(j) Operate recombiners,
(k) Operate igniters,
(l) Inert the containment with non-condensables,[15]
(m) Vent the containment,
(n) Spray the secondary containment,
(o) Flood the secondary containment.

Additional considerations:

(p) External cooling of RPV,
(q) Steam inerting of the containment.

The actual list depends on the plant's characteristics and actual application will vary from plant to plant.

Normally both the positive and negative consequences of the CHLAs should be considered. This should be done for each plant damage state to which the CHLAs are applied or for each of the guidelines that have been derived from the CHLAs. Whether the CHLA/guideline is actually executed depends

[15] This primarily applies to BWRs; it could also include dilution of PWR containment with non-condensables with the aim of suppressing flame acceleration.

on the balance of these two. The following are examples of CHLAs and some of their positive and negative effects.

(1) Injection into the RCS

Positive effects:
(a) A medium is provided to transfer heat away from the core.
(b) It may help collapse the upper head steam void which enables better RCS pressure control via the pressurizer.

Negative effects:
(a) A possible high pressure spike is generated when water is added to an overheated core.
(b) Hydrogen may be generated as a result of the zirconium–water reaction.
(c) Injection of unborated water may lead to a return to criticality.
(d) A steam explosion is possible if the injection rate is too fast.

(2) Injection into SGs

Positive effects:
(a) Heat removal from the secondary side is provided, which could lower the primary pressure and promote primary side water injection.
(b) The tubes are protected from over temperature conditions and the possibility of tube creep rupture is reduced.
(c) Fission products are scrubbed if SG tube leakage has occurred.

Negative effects:
(a) Thermal shock from feeding a dry SG could cause the tubes to fracture.
(b) Creep rupture of tubes could occur when a hot, dry SG is fed by lowering the pressure on the secondary side of the tubes.

(3) Depressurization of the SGs

Positive effects:
(a) Lower pressure water pumps can be used to feed the SG.
(b) Heat is removed from the primary side of the SG.

Negative effects:
(a) Creep rupture of the SG is possible due to depressurization of the secondary side of the SG and promotion of circulation on the primary side of the tubes.
(b) If low pressure water pumps are sufficiently low in pressure, SG dryout may be necessary to reduce the pressure enough to allow feed.

(4) Restart of RCPs

Positive effects:

(a) Any water volume in the crossunder pipe will be sent to the core, which removes heat and offers some temporary retardation of core melt.
(b) A recirculation path with the SG for reflux cooling could be established.

Negative effects:

(a) A recirculation pathway to the SG can be started and, if any SGs are dry, tube creep potential is increased.

(5) Flooding of the reactor cavity

Positive effects:

(a) Vessel failure can be prevented or delayed (to avoid creep rupture of the vessel) if the water level inundates the vessel sufficiently.
(b) A heat sink for the RPV is provided and reactor coolant boil-off is reduced, provided the RPV insulation does not prevent the submerged vessel from steaming.
(c) The corium–concrete interaction is reduced if the RPV fails, even if the cavity is covered by only a small amount of water.

Negative effects:

(a) If flooding is accomplished by containment spray, de-inerting the steam atmosphere may cause a hydrogen burn.
(b) Extended water injection into the containment could submerge safety related equipment.
(c) Extended injection of external water sources into the containment could cause long term corrosion cracking concerns.
(d) A steam explosion is possible.

(6) Depressurization of the RCS

Positive effects:

(a) A low pressure water make-up system is allowed to supply water to the RCS.
(b) Stress in the primary system is reduced, thereby decreasing the probability of creep rupture of SG tubes or reactor coolant system piping.
(c) The effect of high pressure RPV failure is reduced, i.e. DCH concerns and corium relocation outside the RPV.
(d) A steam explosion or at least an energetic corium–water reaction is possible.

Negative effects:

(a) If pressure is reduced too soon the heat removal capability of the coolant could be reduced.

(7) Spraying into the containment

Positive effects:

(a) The pressure and temperature in the containment is reduced, thereby reducing the challenge of containment failure and leakage.
(b) The airborne fission products are washed out, thereby reducing their release through any containment leakage.
(c) Cavity flooding is promoted.

Negative effects:

(a) Containment of a steam atmosphere can be 'de-inerted', which can increase the possibility of a hydrogen burn.

(8) Operation of containment fan coolers

Positive effects:

(a) The pressure and temperature in the containment is reduced, thereby reducing the challenge of containment failure and any leakage.

Negative effects:

(a) Containment of a steam atmosphere can be de-inerted, which can increase the possibility of a hydrogen burn.

(9) Operation of hydrogen recombiners

Positive effects:

(a) The hydrogen concentration in the containment atmosphere is reduced.

Negative effects:

(a) Some hydrogen recombiners may become ignition sources under high hydrogen concentrations.

Reference [6] provides a complete description of both the positive and negative effects of all CHLAs during all plant damage states. Some CHLAs were studied further in the late 1990s and equipment was developed for some plants to enhance their execution. For example, catalytic recombiners were developed that are able to remove hydrogen without combustion. Also, filtered vents were developed for a number of containments. Work is continuing to give further insight into the mechanism of cooling the RPV from outside by flooding the cavity. Utilities may consider upgrading their existing programmes on the basis of this work and regulatory bodies may consider upgrading their national requirements.

Appendix III

COMPUTATIONAL AIDS

During BDBAs all the activities performed by the response organization should be evaluated for ease of application. The stress level of all personnel will be high during such events. Therefore by reducing the potential for human error, ease of application will increase the overall success of the response organization. One of the possible ways of accomplishing this is to develop calculation methods that may be used by the implementers in combating plant damage. Some of these could be developed before they are needed. Therefore CAs could be developed for the response organization prior to an actual event. Such CAs are obtained using simplified assumptions and typically are presented graphically (with parameter graphs, diagrams, nomographs, tables, etc.). Several plants which have developed SAMPs have such CAs. These CAs are all plant specific but can be calculated by individual NPPs as part of the development process of their SAMPs. Some examples of CAs follow:

(a) The coolant injection rate needed for the removal of decay heat from the core, plus heat from metal oxidation and accumulated heat of the RPV structural material;
(b) Hydrogen production due to a steam metal oxidation reaction.

The following two examples are described in more detail:

(1) Containment water level and volume (Fig. 3): The purpose of this CA is to provide a correlation between the injected water volume and the containment water level so that flooding levels in the containment can be evaluated. This allows the response organization to estimate when the RPV has been sufficiently flooded to be an effective external heat sink which might possibly prevent an RPV failure. It also informs the response organization as to what equipment will be ineffective due to flooding. One NPP used multiple parameters to estimate the flood level of the containment. Figure 3 shows this graphically for a Westinghouse plant. The vertical axis is the containment water level and the horizontal axis is the injected water volume. The line representing the increase in the containment level also shows the level which represents a full volume of one or more refuelling water storage tanks (RWSTs). This line also shows which equipment would be submerged as the water level in the containment increases.

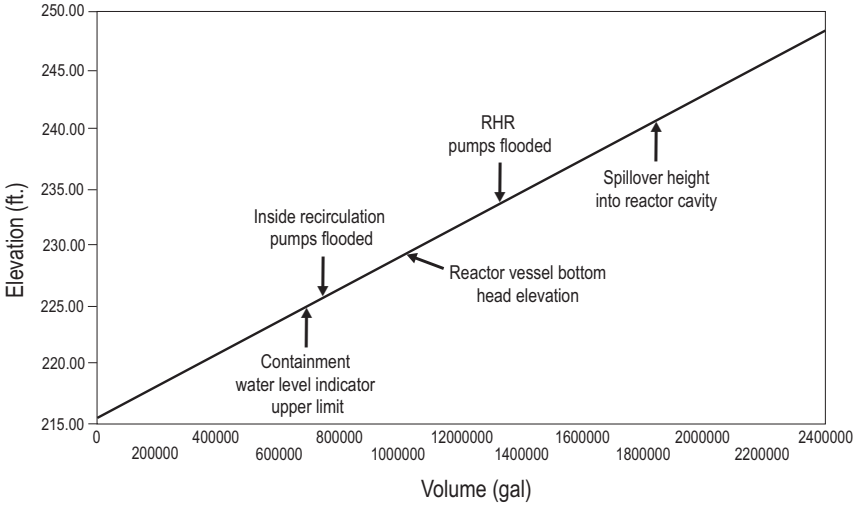

FIG. 3. Containment water level and volume (1 gal = 0.003785 m^3 , 1 ft = 0.3048 m).

(2) Hydrogen flammability in an open type of containment[16] (Fig. 4): This CA will help the response organization to determine whether the hydrogen in the containment atmosphere is flammable. Additionally, in some applications (notably in the WOGSAMG) it is used to show the amount of hydrogen present in the containment atmosphere if a specific amount of zirconium reaction has occurred. A predetermined value of hydrogen can be calculated for a 50% or a 75% zirconium reaction. (However, use of a measuring device is preferable). In the example given in Fig. 4, which applies to a Combustion Engineering plant, the vertical axis represents the hydrogen concentration in the containment as a percentage of volume and the horizontal axis represents containment pressure. If the resulting co-ordinates fall within the combustion region but below the constant pressure burn line equal to the design pressure, the containment pressure is not threatened. As the hydrogen concentration increases or the steam pressure decreases, the combustibility of the mixture increases and the risk associated with the post-burn hydrogen pressure increases. The containment failure challenge increases as post-burn pressures approach the median containment failure pressure. The situation changes if the containment is vented. Figure 5 shows the situation when 30% of the containment has been vented. All these CAs will be plant specific and should be evaluated according to each plant's determination of the predeveloped strategies needed for its SAMP.

[16] As opposed to some containments with many subcompartments.

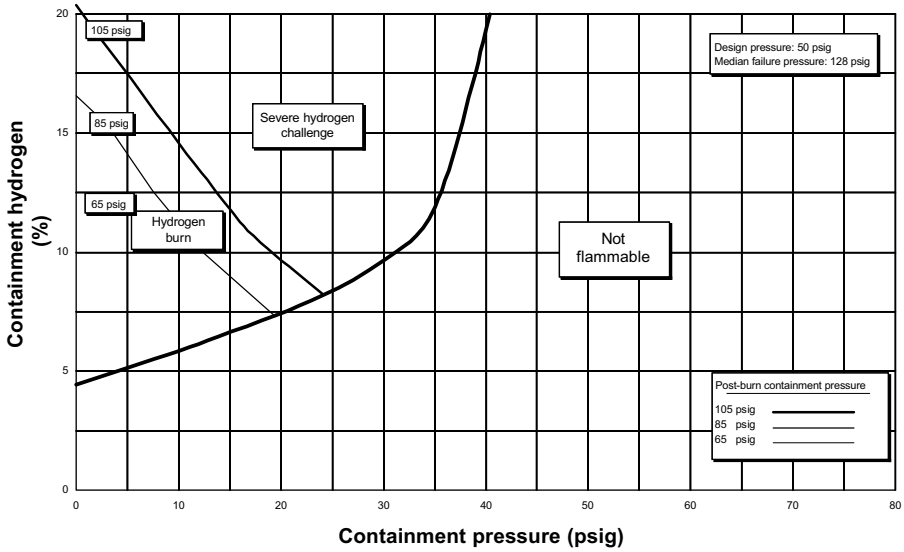

FIG. 4. Hydrogen combustibility based on measurement of wet hydrogen.

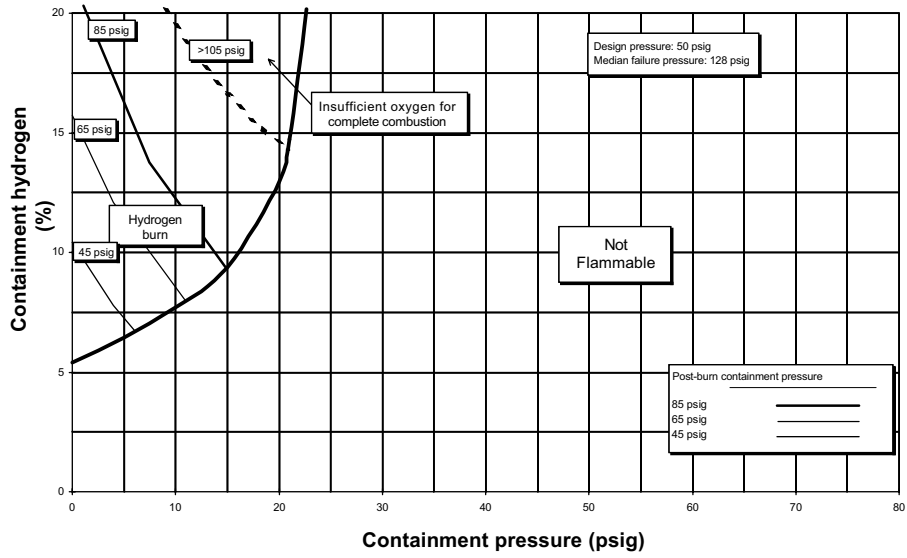

FIG. 5. Hydrogen combustibility based on measurement of wet hydrogen (30% of containment vented).

Appendix IV

TYPICAL PARAMETERS AND MECHANISMS USED FOR INITIATION OF PREVENTIVE AND MITIGATORY ACTIONS

The following general approach is proposed for the selection of instrumentation and parameters needed to diagnose and monitor those conditions which cause the initiation of accident management strategies:

(a) The existing instrumentation of an NPP has to allow monitoring and control of all the important parameters of any accident which does not exceed the NPP's design basis envelope. Such control is necessary to keep the event within the design basis envelope, possibly by means of operator intervention in accordance with existing EOPs.
(b) In the case of a BDBA, some parameters exceed design basis values. Some extension of existing instrumentation is necessary to enable the operator to monitor the current status of the plant and evaluate its safety margins. Because the operator is expected to take preventive accident management actions in compliance with symptom based EOPs (both event oriented and the function oriented parts), instrumentation showing all the parameters used as symptoms for starting preventive actions or monitoring their efficiency in a BDBA environment has to be provided or upgraded to survive adverse environmental conditions.
(c) In severe accidents which may involve very harsh environmental conditions in the containment, reliable information on symptoms which start mitigatory measures is needed. This information is characterized by various measurements of the containment and on-site parameters.

According to the above grouping, three classes of instrumentation can be introduced for the purpose of this report: the DBA group, the BDBA group (core damage prevention) and the severe accident group (mitigation of consequences). Examples of the instrumentation needed for diagnosis and monitoring are given below:

Design basis accidents:

— Design instrumentation;

— A CSF display system[17] showing such parameters as neutron flux, RCS temperature and pressure, SG level and pressure, containment pressure and water level (requirements differ from country to country).

Beyond design basis accidents:

— The core exit temperature up to the value indicating severe core cooling inadequacy but not above a level at which application of preventive actions can prevent core degradation (typically in a range of 400–700°C at core exit, measured by several thermocouples);
— A CSF display system (with the same parameters as above);
— A post-accident monitoring system (an example of requirements specified by NUREG is given in Ref. [21]).

Severe accidents:

The set of parameters given as examples are generic PWR SAMG symptoms (for evaluation of a diagnostic flow chart), but are also applicable for WWER NPPs:

— The SG water level (wide range SG level, narrow range SG level);
— The RCS pressure (wide range RCS pressure, pressurizer pressure, accumulator pressure, safety injection header pressure, emergency core cooling system (ECCS) flow rates);
— The core temperature (RCS temperature or RPV temperature, core exit temperatures, hot/cold leg temperature difference, subcooling margin monitor, RPV level, source range monitor, power range monitor);
— The water level in the containment (containment recirculation sump level, RWST water level);
— Site release (site area emergency levels);
— The containment pressure (containment pressure, wide range containment pressure, water levels that use the containment as a reference leg);
— The hydrogen concentration in the containment (containment hydrogen monitor);
— The water level in the reactor cavity;
— The neutron flux monitor current (for RPV breach signature).

Some approaches also use parameter trends which add information to the values at a specific point in time. This is shown in Table II.

[17] Often known as a safety parameter display system (Westinghouse plants).

TABLE II. EXAMPLE OF A DATA TABLE FOR AMGs (Source: ABB Combustion Engineering)

Time started
Core exit temperature (°F)
Vessel water level above core? (Y/N)
RCS pressure (psi)
Rapid increase in containment pressure? (Y/N)
Radiation level in containment — high range CTMT area rad monitors (rad/h) (1 rad = 1.00×10^{-2} Gy)
Rapid increase in the ex-core power range detector current (pico-amps)? (Y/N)
Was a SGTR diagnosed (Use flow chart A)? (Y/N)
If a SGTR was diagnosed, is the affected S/G isolated (Use flow chart B)? (Y/N)
Was a LOCA outside containment diagnosed (Use flow chart C)? (Y/N)
If there is a LOCA outside containment, has it been isolated (Use flow chart D)? (Y/N)
Rapid drop in containment pressure? (Y/N)
If there is a drop in containment pressure is it due to heat removal? (Y/N)
If there is a drop in containment pressure is it due to controlled or uncontrolled venting? (CV/UV)
Radiation level outside containment (mrad/h)
Is containment threatened based on a containment challenged calc. aid? (Y/N)
Containment pressure (psig)

Note: If data are unavailable or unreliable write ‘not available’ or ‘unreliable’ in the data cell (DO NOT leave a cell blank).

Appendix V

PREVENTIVE ACCIDENT MANAGEMENT ACTIONS

The objective of preventive accident management actions is to prevent or terminate core degradation as early as possible. Prevention of reactor core degradation should be the primary goal of any AMP. Preventive accident management actions should be distinguished from mitigatory ones.

Generic strategies and approaches can be used as examples of preventive accident management strategies for WWER NPPs. An additional example of a possible preventive accident management action (secondary feed and bleed) used in Sweden has also been included.

The Westinghouse generic approach to preventive accident management uses six CSFs — subcriticality, core cooling, heat removal, RCS integrity, containment integrity and inventory — which are monitored on-line using CSF status trees while the operators follow the event oriented (symptom based) part of the EOPs. When a CSF is severely challenged the operators switch to function restoration guidelines, which are the function oriented part of EOPs. Although all EOP actions or activities are meant in principle to prevent core damage, the term preventive accident management action seems to be more appropriate for activities that are considered in the function restoration guidelines, i.e. activities initiated by the operator to recover from a severe challenge to core safety. These preventive accident management actions are sometimes referred to as recovery actions. In part, accident management preventive actions are based on a philosophy similar to that of previous activities (restoring cooling, restoring safety injection, restoring level, restoring concentration, decreasing cooling, attempting to utilize other sources of water, power, etc.); only the priority of the actions to be taken is adapted and less stringent safety limitations are applied.

Some preventive accident management actions from the start include actions that are qualitatively different from previous activities. Good examples are initiation of feed and bleed in loss of heat removal conditions, RCS and SG depressurization in loss of core cooling conditions. These specific preventive accident management actions are discussed below with the aim of providing sufficient insight into their logic but not dealing with them in detail.

Plant specific EOPs were developed for several WWER-440/213 NPPs by adapting generic Westinghouse guidelines, as described in Sections 3 and 4. Some of the generic preventive accident management measures and entry symptoms were reassessed as part of PHARE project 4.2.7a/93, on Beyond Design Basis Accident Analysis and Accident Management, sponsored by

the European Union from 1996 to 1998. As a main computational tool, the MAAP4/WWER code with a specific input file from the Bohunice NPP (Slovakia) was used. The results of the preventive accident management measures are summarized below.

V.1. SUBCRITICALITY

Entry condition (symptom): The reactor is not shut down as a result of neutron flux measurement.

Preventive accident management measures:

(a) Attempt to shut down the reactor by manually positioning the control rods in all possible ways;
(b) If the actions taken in (a) are not successful, stop heat removal (including manual turbogenerator trip) and provide feedwater flow by means of at least one auxiliary feedwater pump;
(c) Let the reactor stabilize power by means of moderator temperature feedback effects at the equilibrium with the feedwater RHR capability;
(d) Borate RCS using any available means.

A technical problem in the application of these preventive actions is the shut-off head pressure of the pumps which are available for injecting boric acid into the RCS. Therefore depressurization of the RCS through pressurizer relief valves (possibly an automatic action) may in some cases be a precondition for effective boric acid injection.

V.2. CORE COOLING

In the following only the highest priority challenge to CSF core cooling is considered. Less 'drastic' preventive actions (secondary depressurization at a lower rate) will have been performed already before the onset of the inadequate core cooling condition.

Entry condition (symptom): 650°C at the core exit.

The following preventive accident management measures are to be applied sequentially:

(1) Attempt to restore safety injection;

(2) If (1) is not successful, depressurize the SGs as quickly as possible to allow injection of low pressure water sources into the RCS (hydroaccumulators, low pressure ECCS pumps);
(3) If (2) is not successful, attempt to restart RCPs, even if damage to them is to be expected, to inject residual water trapped in lower parts of the RCS into the core and to restore cooling;
(4) If (3) is not successful, depressurize the RCS by any available means (through pressurizer relief and safety valves) to allow low pressure sources to be injected into the RCS.

V.3. HEAT REMOVAL

The basic preventive accident management action is primary feed and bleed.

Generic entry conditions (symptoms) for starting primary feed and bleed are:

- The minimum SG level allowing recovery of core cooling,
- An RCS temperature allowing recovery of core cooling.

During the development of an EOP for WWER V-213 NPPs, the following primary feed and bleed entry conditions were considered feasible:

- The minimum SG level effective for heat removal;
- An RCS temperature of 320°C (corresponding to this minimum SG level in conservative analysis of feedwater flow transients);
- A feedwater flow less than the minimum necessary for a safe RHR when the RCS temperature cannot be stabilized by the secondary side.

In the validation phase of the EOP the third entry condition was found too difficult for the operators to evaluate and therefore the temperature symptom will probably be used in the future.

Preventive accident management measures:

- Attempt to restore feedwater flow to at least one SG by all available means and minimize heat production in the RCS (tripping all RCPs);
- Establish primary feed and bleed by:
  (a) Starting high pressure safety injection (HPSI) pump(s),
  (b) Manually opening pressurizer relief and/or safety valve(s),

(c) Cooling down RCS and transferring injection to low pressure safety injection (LPSI) pumps as soon as the RCS parameters allow (giving adequate consideration to maintaining RCS subcooling in all situations).

V.4. REMAINING CSFs

Three CSFs remain:

(1) Integrity of the RCS (safety of the RPV in relation to brittle fracture phenomena in subcooling transients);
(2) Integrity of the containment (challenge to the containment safety function from high pressure, low pressure, flooding and high radiation levels);
(3) Inventory of the RCS water volume (abnormal pressurizer level).

In contrast to the first three CSFs, a violation of any of those listed above is not directly related to core damage (not taking into account catastrophic failure of the RPV due to transients). Therefore they do not require drastic preventive accident management measures. The actions taken in EOPs are basically 'parameter recovery' or 'parameter stabilization' in nature.

V.5. STATION BLACKOUT

A station blackout is an event combining a loss of heat removal accident (loss of feedwater flow) with a potential LOCA (through pressurizer safety/relief valves and the RCP's seals). Recovery from a blackout is complicated by the concurrent loss of non-vital instrumentation and controls and later, when the batteries are depleted, even the loss of vital I&C. The only way to prevent core damage is to restore the power supply to at least some of the systems needed for decay heat removal which, in most situations, takes time. Therefore some of the preventive accident management measures concentrate on winning time to allow for restoration of power sources. Some PWRs have a secondary feed and bleed capability which is basically a mitigatory system preventing vessel failure. Secondary feed and bleed, if applied early enough, can also be useful in the prevention of core damage.

Entry condition (symptom): Blackout of the station.

Preventive accident management measures:

(a) Actions aimed at delaying depletion of batteries.
(b) Actions minimizing any loss of RCS coolant (such as seal leakage of the RCP) or secondary side coolant (such as SG blowdown).
(c) Secondary side depressurization aims at reducing the temperature and pressure in the RCS to delay failure of the RCP seals and/or minimize leakage when they fail due to overheating or overpressurization. The drawback of this preventive action is the loss of secondary water and the jeopardizing of heat removal in a later phase. Therefore use of this preventive measure requires the availability of a feedwater source (turbine driven feedwater pump). The presence of large volumes of secondary water in horizontal SGs could also, in principle, justify use of this preventive action.
(d) Primary depressurization is not used in the generic Westinghouse guidelines because it accelerates uncovering of the core. After the core has been partially uncovered, but before significant core damage can occur, primary depressurization may be useful to allow the hydroaccumulators to inject and delay further damage. This action can also be considered to be a mitigatory accident management action because it prevents high pressure RPV failure.

In the EOPs for the WWER-440/213 NPP, secondary side depressurization alone was implemented after approximately two hours of power recovery activities, in view of limited knowledge of the specific behaviour of the plant under core damage conditions. Recent experiments devoted to assessment of the vulnerability of RCP seals have shown that long term survival of the seal is possible if the temperature is maintained below ~250°C. Primary side depressurization has not been implemented in V-213 plant specific EOPs due to insufficient analytical knowledge at the time of their development.

Secondary feed and bleed consists of feeding one or two SGs with fire extinguishing water (other sources are also possible) and relieving steam by means of SG relief valves. A negative aspect of this strategy is the thermal stress on the SG tubes.

The PHARE 4.2.7a project analysed preventive accident management actions applicable in conditions of inadequate core cooling, loss of heat removal and station blackout in more detail. The main conclusions for inadequate core cooling were:

(1) The condition for starting preventive actions (650°C) should be reassessed because the core is already considerably degraded at this temperature and the rate of further degradation is too high. Based on analytical data, a value of between 550 and 600°C is preferable.

(2) Restart of RCPs is effective for WWER reactors, similarly to PWR reactors, and core damage can be delayed for several hours (for example, more than 3 hours for a 10 mm LOCA).
(3) The effectiveness of secondary depressurization of V-213 plants has not been confirmed if the preventive action is started at a temperature of 650°C. Secondary depressurization is better started at a temperature below 600°C. However, this finding may be dependent on specific MAAP4/WWER modelling, and additional analyses with improved modelling of certain phenomena are suggested.
(4) Consideration should be given to reversing the priority of secondary and primary depressurization if the MAAP4/WWER results are confirmed (see point (3)).
(5) Primary depressurization proved to be effective in all situations analysed.
(6) The availability of an LPSI system is necessary for long term prevention of core degradation.

The main conclusions for loss of heat removal were:

(a) If the entry condition for primary feed and bleed is the temperature, a value considerably higher than 320°C is acceptable (up to the temperature used as a symptom of inadequate core cooling — currently 650°C).
(b) The limitations on the time of initiation of primary feed and bleed, which are known for PWRs and which depend on parameters like reactor rated power, relief capacity and RCS volume, have not been proven for WWER V-213 reactors.
(c) Use of secondary depressurization as a preventive accident management action to support primary feed and bleed under certain conditions was not found to be beneficial because:
    (i) If HPSI is not available, secondary depressurization does not bring the RCS pressure below the shut-off head pressure of the LPSI pumps and therefore primary feed and bleed cannot be established with LPSI pumps. This leads to earlier uncovering of the core.
    (ii) If HPSI is available, secondary depressurization accelerates the development of the accident and the primary feed and bleed entry conditions are reached earlier. This leaves less time for attempts to restore the feedwater system.

The main conclusions for station blackout were:

TABLE III. GENERAL PREVENTIVE ACCIDENT MANAGEMENT MEASURES FOR PWRs

Plant status	Challenge	Preventive action	Symptom for initiating preventive accident management action	Parameter(s) needed for diagnosis	Positive impact	Possible negative impact
No core damage	Inadeaquate subcriticality	RCS heat-up Borating	Reactor not subcritical after scram	Neutron flux		None
	Inadequate core cooling	Secondary depressurization Start of RCP Primary depressurization	650°C	Core exit temperature		RCS depletion None
	Inadequate heat removal	Primary feed and bleed	Hot leg temperature or SG level	Hot leg temperature or SG level	Core cooling	None
	Blackout	Secondary depressurization	650°C	Electric power distribution system	Hydroaccumulator injection into RCS	RCS depletion
		Primary depressurization		Annunciators		None

(1) Secondary depressurization: If there is no leakage through RCP seals, depressurization accelerates uncovering of the core and core damage.
(2) Primary depressurization: Start of primary depressurization at 650°C has a beneficial effect in all analysed cases because hydroaccumulators inject water into the RCS, delaying subsequent core degradation. The pressure is also lower during core melt and vessel attack.

The analyses helped to find an optimum rate of relief flow at which the positive effect of depressurization is optimally balanced with RCS inventory loss. In the Bohunice NPP this flow corresponds to the combination of one pressurizer safety valve plus a relief valve. Table III summarizes general preventive accident management measures for PWRs.

Appendix VI

REVIEW OF AN AMP

VI.1. METHODOLOGY

At various stages in the development and implementation of an AMP and, in particular, prior to its implementation, the AMP should be reviewed from the point of view of its completeness and quality. Suggestions and good practices are given in this publication and in Refs [3, 9], which describe in detail the basic components of and approaches used in the preparation, development and implementation of AMPs. The review can be carried out either by the NPP personnel or by an external review team, possibly an IAEA review team. This appendix describes one of the possible methodologies for reviewing whether an AMP is sufficiently comprehensive and whether all relevant issues have been adequately addressed.

The methodology refers to an IAEA publication on Basic Safety Principles for Nuclear Power Plants [1]. Safety principles are shared safety concepts indicating how to achieve safety objectives at different levels of defence in depth. As stated in Ref. [1], "The safety principles do not guarantee that NPPs will be absolutely free of risk, but, when the principles are adequately implemented, the plants should be very safe…". The principles do not differentiate between new and existing plants, but do of course consider necessary differences in implementation.

The major part of level 4 of defence in depth, which covers the control of severe conditions, including prevention of accident progression and mitigation of the consequences of a severe accident, is included in the AMP. Reference [1] gives guidance on how to specify relevant safety principles for each level of defence in depth, including level 4. The principles for level 4 have been selected and grouped as follows:

Group 1: Strategies for accident management

(a) Strategy for accident management.

Group 2: Performance of equipment in accident management

(a) Equipment qualification,
(b) Automatic shutdown systems,
(c) Preservation of control capability,

(d) Station blackout,
(e) Achievement of quality,
(f) Verification of design and construction,
(g) Pre-operational plant adjustment,
(h) Engineered features for accident management,
(i) Quality assurance in operation,
(j) Maintenance, testing and inspections.

Group 3: Response of personnel in accident management

(a) Validation of operating and functional test procedures,
(b) Training and procedures for accident management.

Group 4: Operational excellence and physical protection of the plant

(a) Operational excellence,
(b) Physical protection of the plant.

Group 5: Interface with off-site emergency planning

(a) Emergency arrangements,
(b) Assessment of accident consequences and radiological monitoring,
(c) The radiological impact on the public and the local environment,
(d) Off-site support.

Group 6: Emergency heat removal and ultimate heat sink provisions

(a) Emergency heat removal,
(b) Ultimate heat sink provisions.

Group 7: Protection of the containment structure

(a) Protection of the containment structure.

Group 8: Confinement of radioactive material

(a) Confinement of radioactive material.

The safety principles show the complexity of the issue on the one hand but, on the other hand, allow for a comprehensive review of the AMP aimed at evaluating whether all aspects are being adequately considered.

Practical guidance for the review of an AMP can use an 'objective tree' technique. This technique, as demonstrated in Fig. 6, is used to relate the objectives of each level of defence to the necessary provisions in design and operation. The objectives of each level of defence clearly state what is to be achieved. The safety principles show how to achieve it and give an indication of which relevant safety functions should be maintained. Challenges causing the deterioration of each safety function can be specified, various mechanisms induced by these challenges can be identified, and adequate provisions for prevention or control of these mechanisms can be made. The safety principles also indicate how to select and evaluate the adequacy of individual provisions which need to be implemented to prevent mechanisms which could prevent the safety functions from occurring. The provisions reflect measures applicable to all structures, systems, components and procedures important to safety during all the stages of design and operation of an NPP. Figure 7 shows the basic elements of the technique for level 4 of defence in depth. This technique has been used to construct full objective trees, including specification of provisions for each of the relevant safety principles. The entire set of objective trees for all safety principles can be used afterwards as a checklist ('reminder') for completeness (adequate consideration of all aspects) of the AMPs. References [1, 3, 9], as well as the main part of this report, explain the contents of the provisions in objective trees in more detail.

For practical reasons, in the development of objective trees, safety principles have been combined into several groups. The main basis for such combinations was similarity of provisions which are relevant to several safety principles. One objective tree has been developed for each group of safety principles. More details of the provisions will be given in the following sections.

VI.2. SPECIFIC GUIDELINES FOR REVIEW AREAS

VI.2.1. Strategies for accident management (group 1)

Strategies are a key aspect of an AMP. Figure 8 illustrates the main steps needed to set up a complete, adequate and workable set of recovery strategies for a specific plant in terms of the various elements that must be addressed.

The first steps involve doing the necessary work to provide a complete and balanced understanding of the plant's specific response to different severe accidents which may occur, including identifying and ranking the various mechanisms which can challenge the FP retention boundaries and the vulnerability of the plant to these different mechanisms.

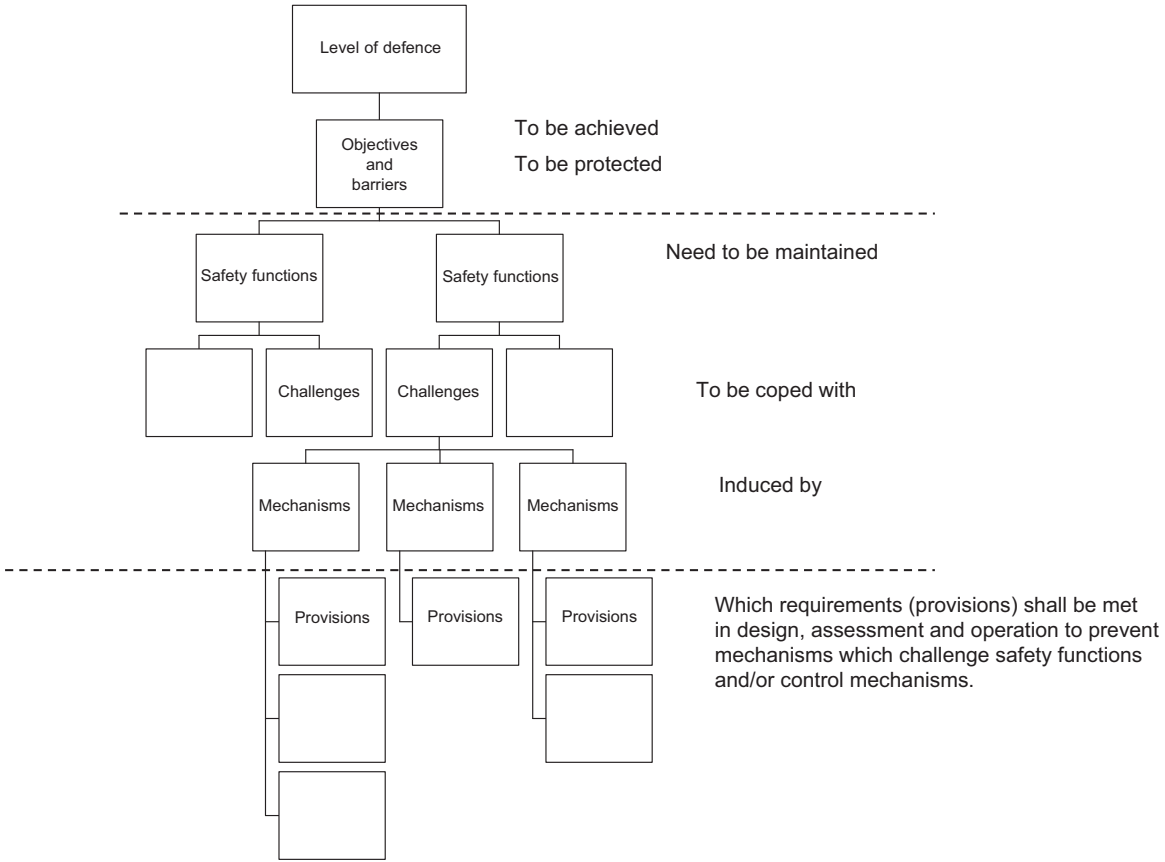

FIG. 6. Objective trees — logical structure and approach.

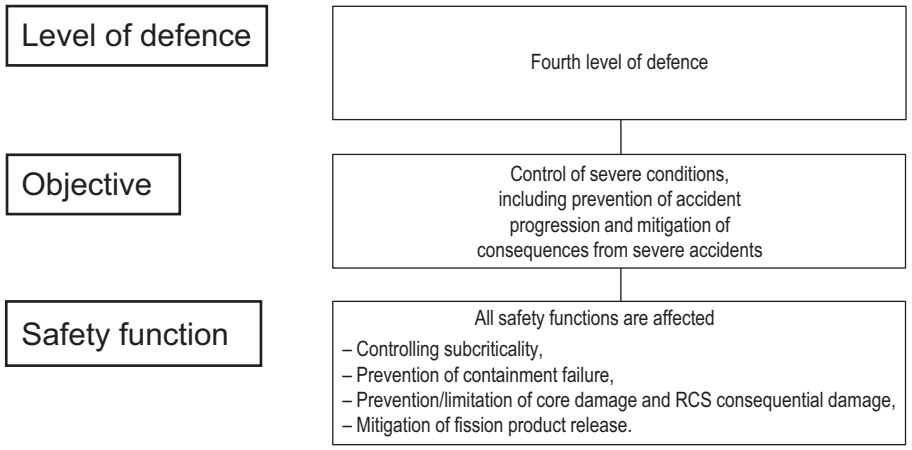

FIG. 7. Objectives and safety functions of accident management.

To ensure a balanced understanding it is important to systematically define the range of accident scenarios and the initial conditions to be investigated, taking into account both the likelihood and the expected severity of a given scenario. An existing plant specific PSA study provides valuable input. In the absence of a PSA, other techniques are also feasible. Efforts should be made to demonstrate broad coverage of the potential range of severe accident sequences for the plant in question. Accident sequences need to be analysed and the challenges to FP boundaries identified on a best estimate basis.

The specific plant's capabilities to implement basic severe accident recovery strategies (secondary side feed, RCS injection, RCS depressurization, containment water addition and depressurization, hydrogen control, etc.) should be reviewed in order to identify all possible means of achieving safety objectives, even those involving use of equipment outside its original design envelope. At the same time, major equipment limitations (for example shut-off heads for injection systems, maximum achievable flow rates, depressurization capacity, etc.) should be identified. The identification of possible requirements to bring in equipment from outside the plant ('external needs' in Fig. 8) should also be addressed.

Definition of symptoms and of the associated plant process parameters which must be monitored in order to detect and prioritize potential challenges is an important next step. It represents the formulation of the basic objectives of the strategies in terms of the safety functions to be protected (or challenges to be met). Strategies must then be developed which provide all practical means to protect the safety functions. During this phase it is important to define clearly and unambiguously specific criteria such as entry and exit conditions,

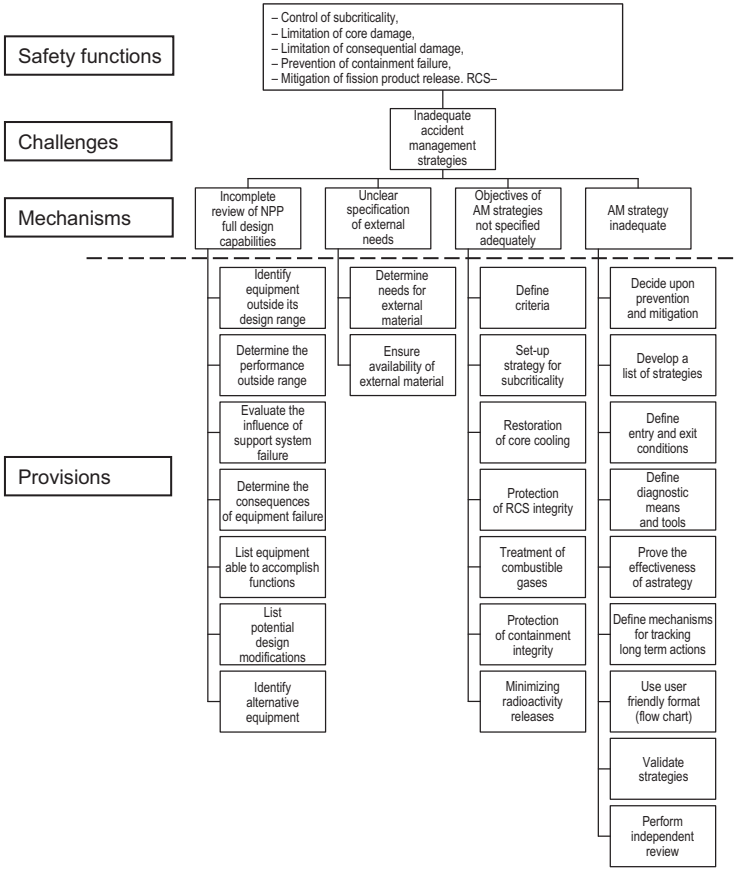

FIG. 8. Objective trees for the accident management. Safety principle: strategy for accident management.

diagnostic symptoms, etc. Efforts should also be made to demonstrate that the list of strategies developed is complete. The 'correctness' and the usability of the various strategies must be checked by an appropriate verification and validation programme. A severe accident will lead to the need to monitor and control various plant parameters in the very long term, even after the event has been controlled and the structured guidance terminated. A means should be defined for identifying, tracking and monitoring these long term concerns.

VI.2.2. Performance of equipment in accident management (group 2)

A major part of accident management is associated with assessing the availability of equipment and instrumentation, and recovering failed equipment. The ability of equipment and instrumentation to operate outside its design basis depends on many factors but should be assessed during the development of the AMP (Fig. 9).

Environmental conditions which will be experienced by equipment will be known from previous analyses and should be used to assist in evaluating the likely response of the equipment and the survivability of instrumentation. Where possible, the operability margin of equipment beyond its design basis can be estimated and factored into the evaluation. For instrumentation, the number of plant parameters which need to be monitored should be clearly defined (and minimized, consistent with achieving the aims of the AMP), together with an assessment of all available means to measure those parameters and their likely survivability under severe accident conditions.

There is no single approach to addressing the need for new equipment for accident management. In general, while the implementation of an AMP may generate requirements for limited upgrades (for example extending the ranges of certain instruments), the requirement for major equipment changes will not normally be generated here. Level 1 PSA, for example, offers a means of deciding on the need for equipment upgrades. However, the assumed plant configuration basis, together with any resulting recommendations for upgrades, must be clearly stated in the AMP.

Figure 9 presents a framework to help in reviewing the equipment aspects of an AMP. It is presented under the main categories of quality and maintenance of equipment, instrumentation availability, equipment availability, and actuation ('initiation') and control of systems and equipment.

VI.2.3. Response of personnel in accident management (group 3)

Figure 10 illustrates the key aspects of defining the roles and responsibilities of personnel, of developing and implementing procedures and guidelines

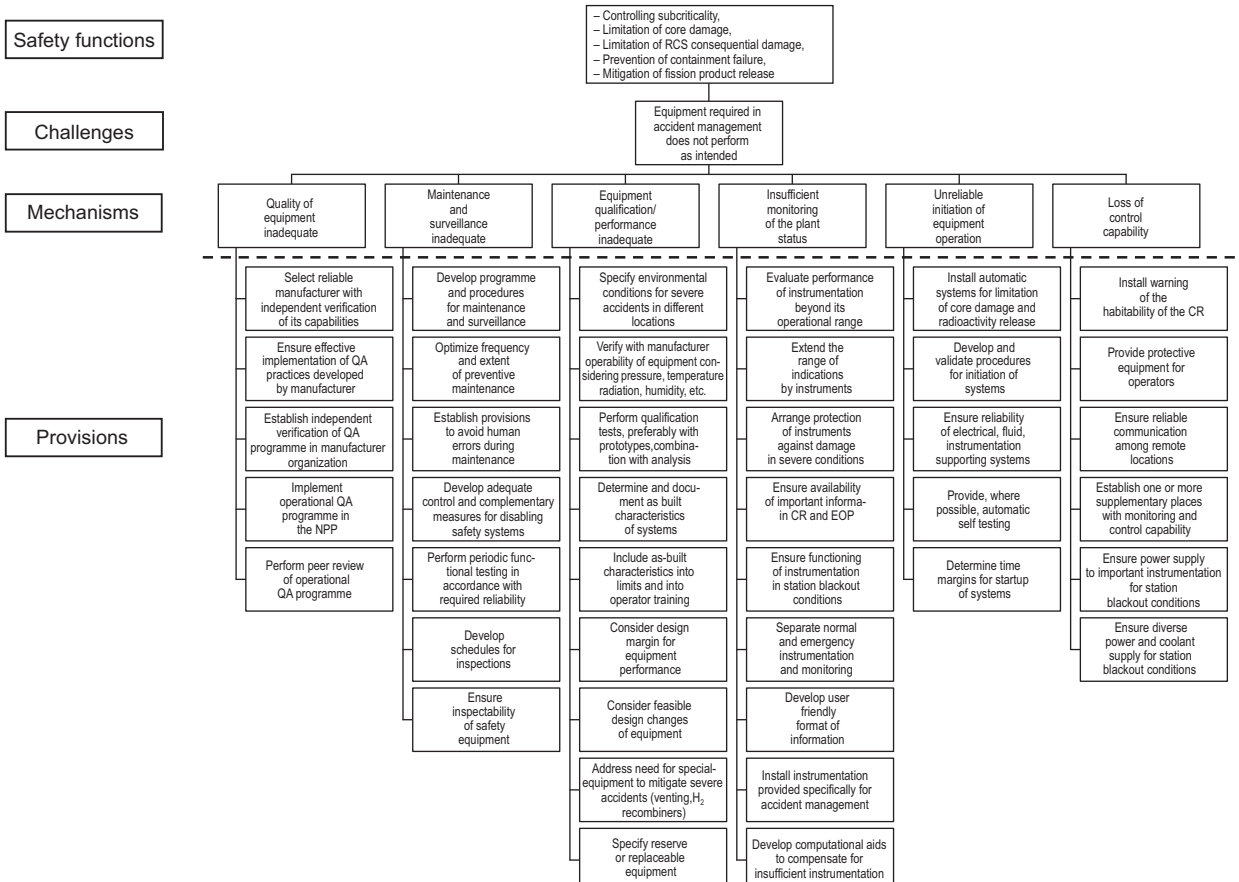

FIG. 9. Objective trees for accident management. Safety principles: automatic shutdown system, preservation of control capability, station blackout, achievement of quality, quality assurance in operation, maintenance, testing and inspection, equipment qualification, verification of design and construction, pre-operational plant adjustment, engineered features for accident management.

for accident management, and of training on-site emergency staff responsible for using the tools in case of an accident.

Organizational aspects of accident management are extremely important and very plant specific. It is important to define the roles of the different parts of the emergency organization early in the programme development (primarily operations, technical support, emergency planning and response), and how these roles may be modified by changes or enhancements to the emergency response capability. Responsibility for evaluation, decision making and implementation must be assigned to the various accident management functions. It can be helpful to develop a matrix showing which member(s) of the organization are responsible for each of the different accident management functions. Defining decision making responsibility (i.e. responsibility for final authorization of a given course of action) is particularly important. It is generally recommended that, at least in severe accident situations, those responsible for performing plant evaluations and recommending recovery strategies be a different group from those responsible for implementing them.

The development of EOPs, SAMGs or similar systems entails the conversion of high level strategies into easily usable procedures or guidelines. Emergency operating procedures and SAMGs should be fully symptom based. They may or may not address specific accident scenarios in addition to protecting the core by preserving safety functions or plant states. In general, SAMGs do not attempt to diagnose the specific sequence under way (a difficult task which is of little benefit), but rather provide a symptom based, structured way of determining which actions are needed to prevent challenges to the barriers to FP release and finally allow a controlled, stable plant state to be achieved. The procedures and guidelines must be usable and workable (the main purpose of validation being to check these aspects), and they must be presented in a user friendly and consistent format which emergency staff can become fully familiar with and feel comfortable using.

The last column in Fig. 10 deals with various aspects of training which will be required for the emergency staff. The development of an AMP must include a systematic identification of the training needs of personnel carrying out each function of the emergency response team. The development of the required training material and the schedule for the training, re-training and testing of staff must also be defined. In the case of SAMGs, the phenomenology of the severe accident should be covered during the training of operating organization personnel, but the topics covered and the level of detail devoted to each should be chosen carefully, always keeping the overall objective of the training in mind.

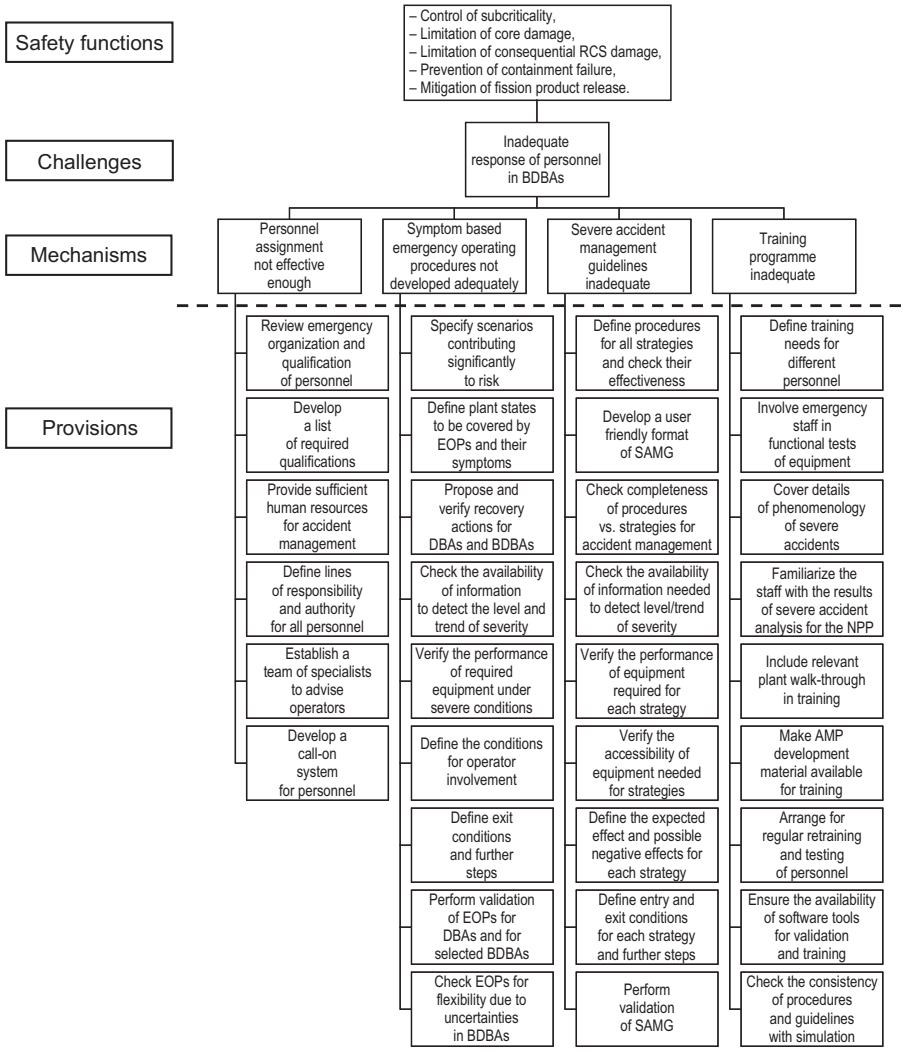

FIG. 10. Objective trees for accident management. Safety principles: validation of operating and functional test procedures, training and procedures for accident management.

VI.2.4. Operational excellence and physical plant protection (group 4)

The objective tree for these two safety principles is shown in Fig. 11. In this particular case, the two principles have nearly no connection and have been combined only to optimize the use of space.

As described in Ref. [1], operational excellence includes augmenting the safety culture, defence in depth, improving human performance, using self-assessment and peer reviews, exchanging operational experience and other information worldwide, increasing application of probabilistic safety assessment and augmenting the implementation of severe accident management. Many aspects of operational excellence have already been reflected in other objective trees. Several remaining aspects are presented here.

Effective feedback of operating experience is essential for all levels of defence in depth. This is also true for the majority of provisions shown in Fig. 11. Special attention should be given to lessons learned from analysis or consideration of severe accidents or their precursors which have occurred in similar plants. The results of emergency drills and exercises should also be utilized for updating the AMP.

Insufficient physical protection of the plant (plant security issues) can provide possibilities of illegal acts against plant safety. On the other hand, physical protection should not jeopardize accessibility of the plant and/or its locations to authorized personnel.

VI.2.5. Interface with off-site emergency planning (group 5)

All aspects of accident management related to off-site emergency planning are reflected in Fig. 12. The organization, facilities, tools, staffing, responsibilities, qualification and training of the on-site emergency centre staff must all be established and described in the emergency plan, and may be modified when the AMP is updated or enhanced.

It is wise to keep a clear distinction between the responsibilities and duties of personnel responsible for the off-site implications and personnel dealing with recovery of the plant, although the on-site emergency centre will normally be the focal point of both activities.

The emergency plan itself should be reviewed to ensure that the required institutional arrangements are clearly laid out, including definition of the organization, responsibilities, staffing, qualification, etc. of the ERT. The emergency plan must also clearly specify the interfaces between the on-site recovery actions (for example, between the EOPs and the SAMGs), and between on-site and off-site activities. This should address the arrangements for promptly informing and co-ordinating with off-site officials in the event that

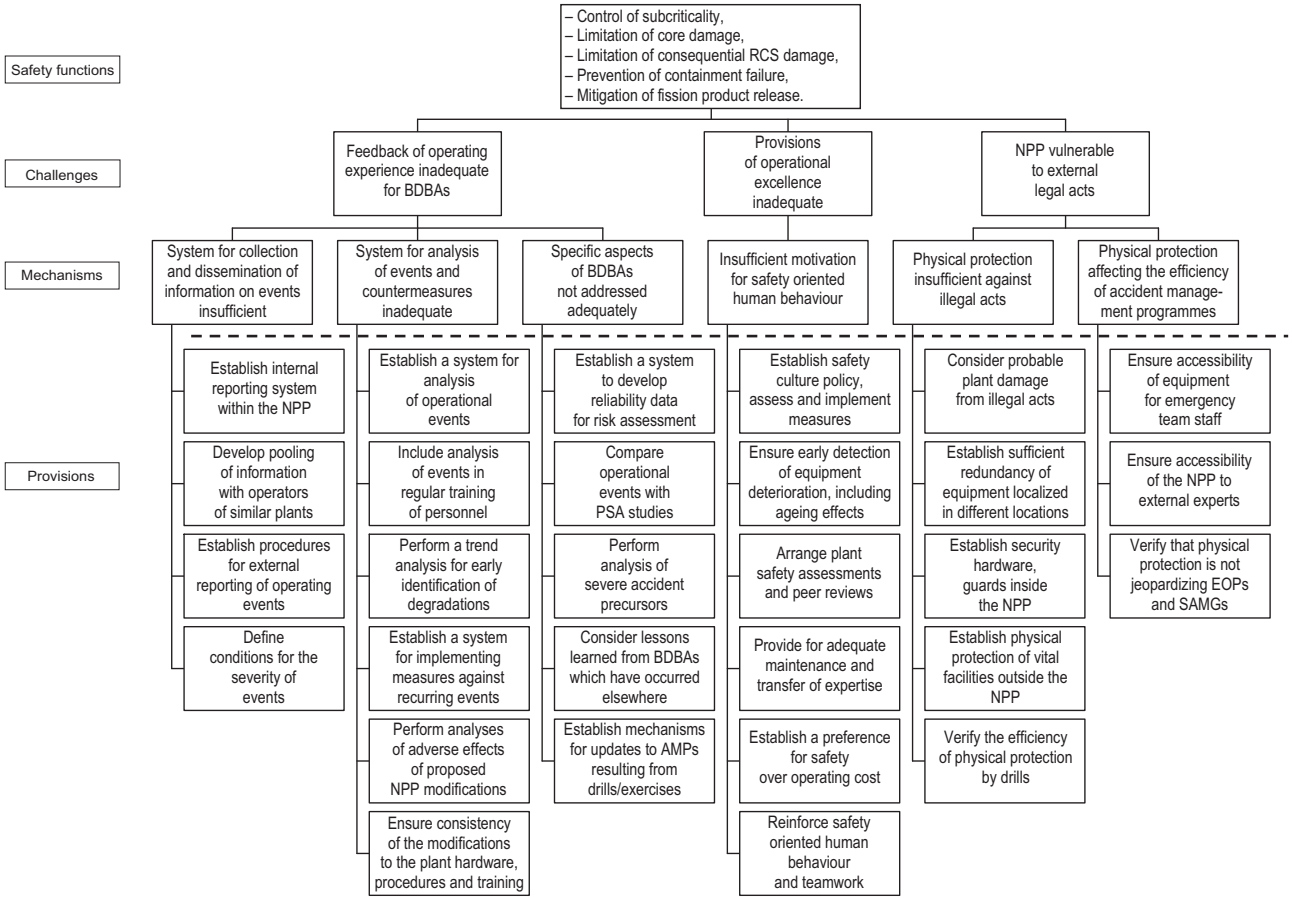

FIG. 11. Objective trees for accident management. Safety principles: operational excellence, physical plant protection.

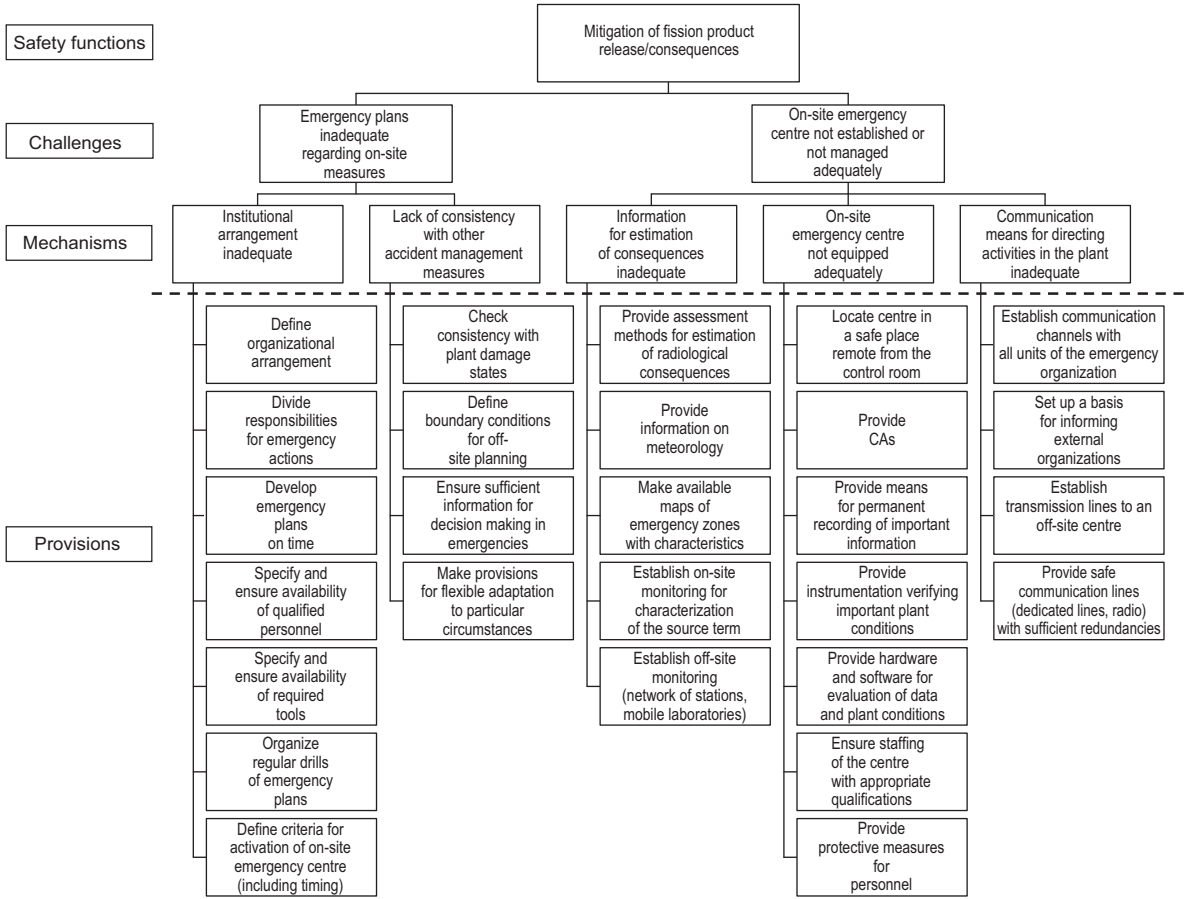

FIG. 12. Objective trees for accident management. Safety principles: emergency plans, emergency response facilities, assessment of the consequences of accidents and radiological monitoring, the radiological impact on the public and the local environment.

any accident management action may result in either an increased off-site risk or an actual radioactive release. The interface with the off-site arrangements for providing support on the site (e.g. for fire fighting) also needs to be addressed. In assessing the consistency of the emergency plan, systematic consideration of all such interfaces is essential.

The adequacy of the on-site emergency centre can be assessed by means of three key aspects: information needs, tools, and communications. The second half of the figure suggests important elements to be considered when reviewing each of these.

VI.2.6. Emergency heat removal and ultimate heat sink provisions (group 6)

Technical and procedural means to ensure emergency heat removal and transfer to the ultimate heat sink are reviewed by applying the objective tree shown in Fig. 13. These strategies play a crucial role, first in preventing the accident from progressing to core degradation and later in preventing the RCS (lower head failure and induced SG tube ruptures) and containment failure which this would induce.

These strategies are challenged by recriticality, since emergency systems are designed only for decay heat removal, and by inadequate operation of emergency systems to remove the decay heat. The AMP should address all these challenges and mechanisms.

The principal strategy for preventing core heat-up is to ensure secondary side bleed and feed by any available means and, if this is not successful, to try to ensure coolant injection into the reactor circuit. However, care should be taken not to cause recriticality by injection of non-borated water after melting out of the control elements from the core region. Reactor circuit depressurization plays a crucial role, as it presents an interface between preventive accident management and the mitigation of the consequences if injection to the reactor is not successful.

VI.2.7. Protection of the containment structure (group 7)

The objective tree in Fig. 14 describes technical and procedural means of preventing containment failure during a severe accident. This safety function plays a crucial role in mitigating the environmental consequences if core has not been successfully prevented.

The integrity of the containment integrity is challenged by pressure and temperature loadings and missiles created by explosive severe accident phenomena. The AMP should address all the challenges and mechanisms.

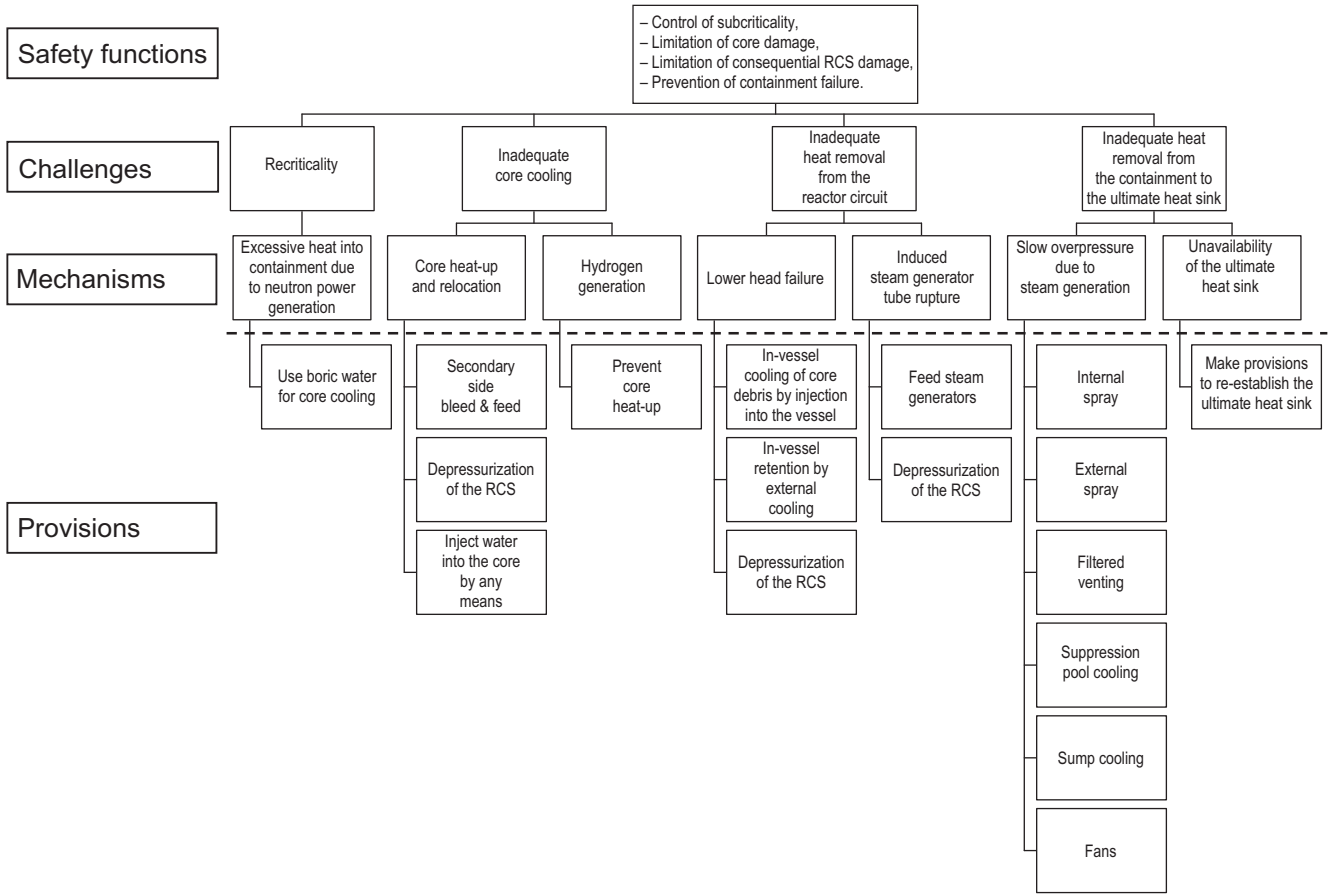

FIG. 13. Objective trees for accident management. Safety principles: emergency heat removal, ultimate heat sink provisions.

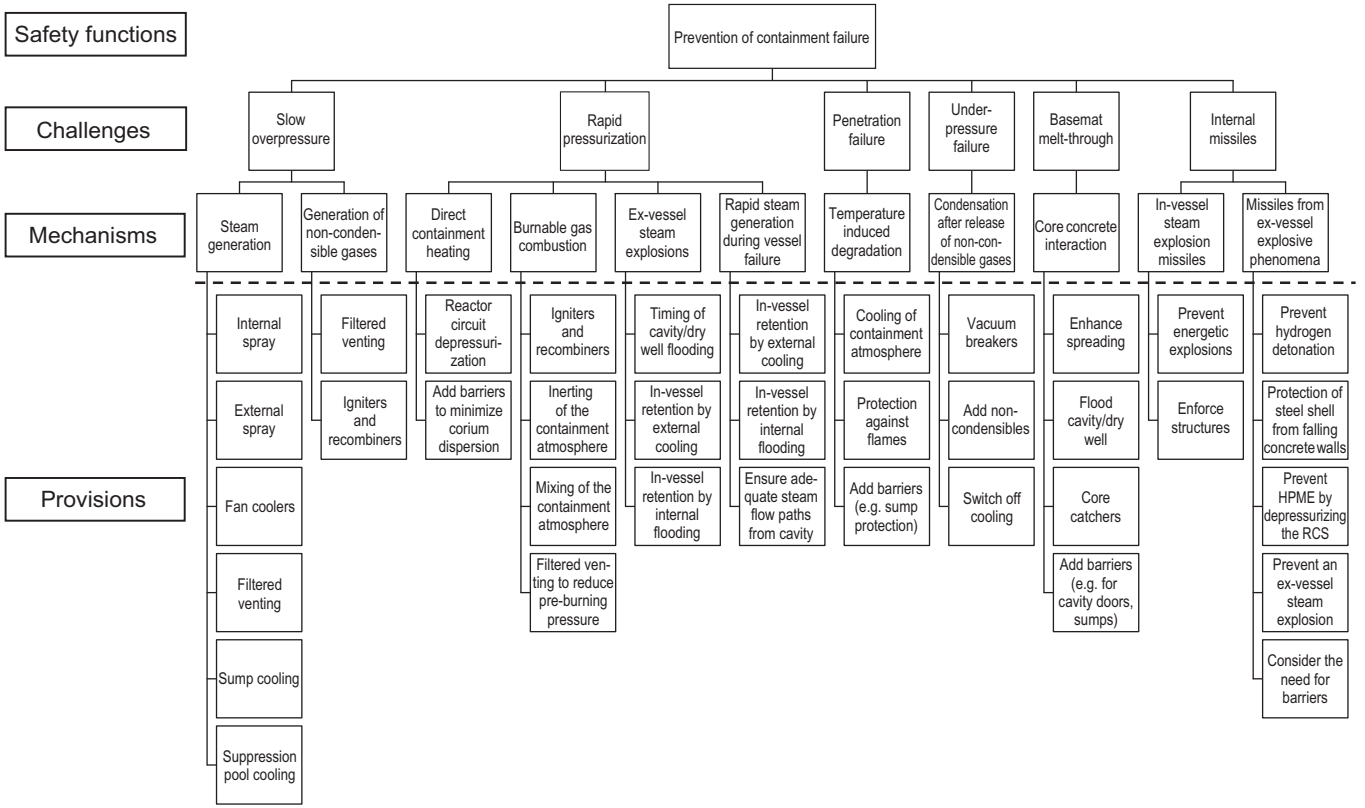

FIG. 14. Objective trees for accident management. Safety principles: protection of the containment structure.

The provisions to be applied should be defined consistently to eliminate the challenges to the containment integrity. Figure 14 gives a structured overview of the possible strategies for protecting the containment. Which provisions will be applied by the AMP depends on national requirements, on the specific plant and on the operating organization. The review should examine the basis for the selected accident management provisions and assess their overall adequacy for protection of the containment.

VI.2.8. Confinement of radioactive material (group 8)

The safety function for mitigation of FP releases is reviewed by considering the risks of FP dispersion (i.e. source term into the containment and source term into the environment), FPs in the containment atmosphere and eventual release from the sump water.

Most FPs are released in aerosol form, with the exception of noble gases and some forms of iodine. There are various aerosol retention mechanisms on the release route from the reactor to the containment, in the containment atmosphere and finally on the release route from the containment to the environment. The most effective retention mechanisms are scrubbing effects when aerosols pass the water pool and the sprays. In some cases deposition in pipes may be efficient, and in the case of hygroscopic aerosols gravitational settling from the containment will quickly approach saturation conditions. Chemical additives to the spray also help in washing the iodine from the containment atmosphere. The effect of noble gases is greatest if they are released to the environment early in the accident.

Two classes of provisions are listed in Fig. 15. Most of them aim at enhancing the inherent aerosol retention and iodine scrubbing mechanisms and are therefore helpful in mitigating releases. The main task of accident management is to prevent containment failure due to physical phenomena which are reviewed by a separate objective tree, shown in Fig. 14. When a major containment failure has been prevented, releases due to normal leakage, as well as from major leakages (resulting from an impaired containment function, i.e. isolation failure, or pre-existing opening) and containment bypass sequences should have been mitigated. Level 2 PSA studies should also give special emphasis on minimizing the releases from such sequences.

VI.3. REVIEW PROCEDURE

The objective tree approach is intended to be used for self-assessment by the plant operators or for an independent assessment by another reviewer. The

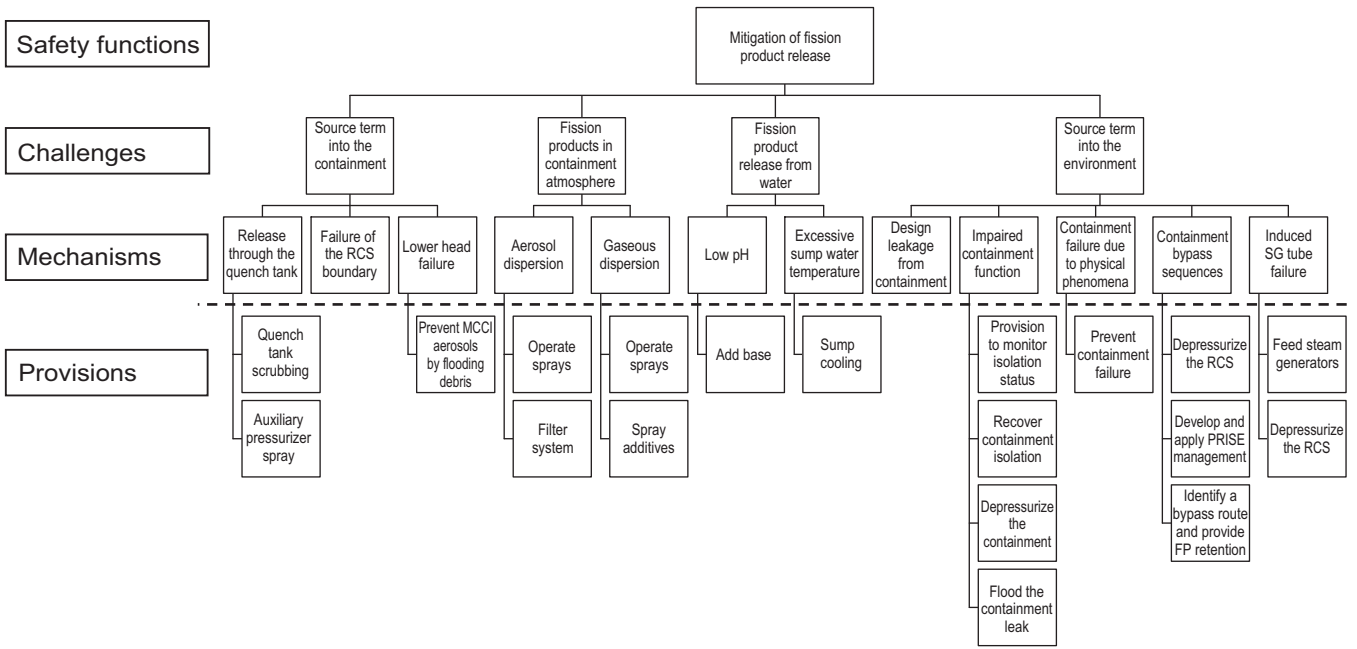

FIG. 15. Objective trees for accident management. Safety principles: confinement of radioactive material.

reviewer is expected to compare provisions identified in the objective trees to the capabilities and provisions of the plant, to evaluate whether they exist and how they are being implemented. The bottom-up method of screening individual provisions is used. A judgment should be made of the level of implementation of each particular provision in design, assessment and operation to prevent mechanisms from challenging safety functions and/or control mechanisms. If a satisfactory answer to the implementation of each provision belonging to the specific mechanism has been given, the relevant mechanism can be considered to be prevented from occurring.

As mentioned previously, not all of the provisions shown in the objective trees should be considered absolutely necessary for the completeness of the AMP; in fact, some of the provisions are optional. It is up to the reviewer to judge whether or not the absence of a provision actually leads to a weakness in defence in depth.

The approach described in this appendix cannot be used as a standalone document. More explanations can be found in Refs [1, 3, 9].

Appendix VII

TRANSITION FROM THE EOP DOMAIN TO THE SEVERE ACCIDENT MANAGEMENT GUIDANCE DOMAIN

Once conditions of existing or imminent core damage exist, a transition from the EOP domain to the severe accident management guidance domain takes place. Several approaches to this transition are possible. Some of the US and European approaches are described below.

VII.1. THE WOG SAMG

In this approach the EOP domain is left when certain conditions exist and an irreversible transition to the SAMG occurs. Conditions indicating actual or imminent core damage are included in the EOP and once they exist, the EOP domain is left.

In the EOP domain the operator follows the functional restoration guidelines (FRGs). One of the major FRGs is C1. It directs the operator to respond to a high core temperature. Several levels are identified, with increasing levels of response. A temperature above 650°C plus notification that no ECCS is available is defined as the exit condition from FRG C1. A similar exit condition exists for the subcriticality safety function. An exit condition from event oriented procedures also exists. If the operator notices the loss of all alternating current (AC) power, he or she must leave the EOP domain. Table IV gives an overview of the different exit conditions from the EOP domain. The actual exit conditions are incorporated in the EOPs.

Whether or not the SAMGs are actually followed depends on the ability of the TSC to function since it assumes all responsibility according to the WOG SAMG approach. The CR operators follow their instructions to execute the SAMGs. As long as the TSC is not available, operators have specific guidance as to how to control the accident by the best possible means. These instructions are contained in separate guidelines, called severe accident control room guidelines (SACRGs). Guideline SACRG1 describes the actions to be taken as long as the TSC is not functional, SACRG2 directs operator actions once the TSC is functional. Once the shift supervisor determines that the TSC is functional (i.e. present and capable of making evaluations and decisions), responsibility is transferred.

VII.2. THE CEOG ACCIDENT MANAGEMENT GUIDELINES (AMGs)

In contrast to the WOG approach, the CEOG does not formally close its EOPs. The purpose of the AMGs is to provide continuing guidance on the mitigation of a severe accident once the site director (or another high level authorized person) has decided that the EOPs are no longer sufficient to control the event. There are no specific entry conditions into the AMGs. The site emergency director (or an equivalent authorized person) decides when the AMGs are to become the controlling document in the event. This decision will be based on many factors, including the current plant emergency action level, the type of accident in progress, the readiness of the TSC, and input from the plant shift supervisor and other CR personnel. Appendix I describes the method used to determine whether the plant is in one of the predefined plant damage states.

The CEOG's generic AMGs are structured as guidance material to be utilized solely by the TSC personnel. However, to better integrate the entire emergency staff during a severe accident the CR personnel as well as key managers at most plants possess a basic working knowledge of the AMGs. This enhances effective communication. In practice, attempts are made to reach a consensus between the main CR and the TSC as to the decisions to be taken.

While the AMGs are being executed, continuous monitoring takes place for any conflict with the EOP being executed. In the case of such a conflict, priority is given to the AMG and the EOP will be closed.

VII.3. THE BWROG SAMGs

The original emergency procedure guidelines (EPGs) of the BWROG went quite far into the severe accident domain. It was, however, decided to

TABLE IV. MODIFICATIONS REQUIRED TO WOG EMERGENCY PROCEDURES TO INCORPORATE SAMG INTERFACE (EXAMPLES ONLY)

Emergency procedure	Modification
FR-S.1 (Response to inadequate shutdown)	Exit to SAMGs
FR-C.1 (Response to inadequate core cooling)	Exit to SAMGs
ECA-0.0 (Loss of all AC power)	Exit to SAMGs

decouple the severe accident phase and give the associated guidance in a set of separate SAMGs. The EPGs contain a set of procedures, including contingencies, for cases when normally available systems are not operable. If, for example, the water level in the RPV cannot be maintained using the normal EOPs, a contingency is entered called 'alternate level control', which makes use of a variety of sources, including unconventional ones. If, even using this contingency, the level cannot be kept above a certain minimum (called the minimum steam cooling water level, i.e. the level at which the core, although already partly uncovered, is still cooled by upflowing steam), it becomes clear that core damage is imminent. This is the moment when the EPGs are exited and the SAGs are entered. The transition, therefore, formally takes place when SAG-1, the integrated RPV and containment flooding guideline, is entered. At this time total responsibility shifts to the TSC. The EPGs will no longer be used.

VII.4. EMERGENCY GUIDELINES AT SIEMENS REACTORS, GERMANY

Siemens NPPs have two sets of manuals, the operations manual (OM) and the accident management manual (AMM). The AMM includes BDBAs not necessarily associated with core damage, e.g. bleed and feed is a major procedure in the AMM. Use of the AMM commences when the safety functions can no longer be controlled using the OM procedures.

VII.5. ELECTRICITÉ DE FRANCE REACTORS, FRANCE

As stated in Appendix I, French reactors employ a family of procedures, called I, A, H and U, for increasing severity of an event (i.e. with an increasing number of failed safety functions).

When the core exit temperature exceeds 1100°C or the radiation level in the containment goes beyond a predefined level, the transition to the SAMGs occurs. The transition is decided upon by the safety engineer, a person whose dedicated function is to oversee CR operations. A separate organization becomes active in the case of severe accidents. This consists of a number of crisis teams, both on-site and off-site. Responsibility is shifted to this crisis organization.

Appendix VIII

USE OF PSA IN SAMG DEVELOPMENT

VIII.1. USE OF PSA IN SEVERE ACCIDENT MANAGEMENT

Probabilistic safety assessment plays an important role in the development of severe accident management. It is used in the preparatory part, the selection of suitable strategies, the development of the actual severe accident management guidance, and in drills and training. In addition, it serves the needs of the on- and off-site emergency organizations by giving an indication of the potential releases caused by severe accidents. The following sections deal with these roles in greater detail. A detailed picture of the use of PSA in severe accident management guidance is given in Ref. [22].

VIII.2. PREPARATION OF SEVERE ACCIDENT MANAGEMENT

As discussed in the main text, the development of a SAMG starts with an investigation of the plant's vulnerabilities to identify those scenarios for which such guidance should be developed. It may also be determined at this time for which very low probability scenarios no guidance needs to be developed as they belong to the area of acceptable residual risk. Level 1 and level 2 PSAs will identify the core damage and core melt phenomena that are relevant for the particular plant or group of plants.

VIII.3. THE STRATEGY SELECTION PROCESS

VIII.3.1. Derivation of the severe accident insights needed for SAMG development

Depending on the analysis outlined in Section 1, those processes which are relevant for the specific plant should be selected and those which are irrelevant should be discarded, e.g. it may appear that steam explosions have a very low probability or that hydrogen deflagration will not pose a challenge to the containment. Consequently, these phenomena need not be considered further in the selection of suitable strategies unless certain operator actions will make them relevant again. For example, if the scenario predicts that an ex-vessel

steam explosion will not occur if the cavity is dry, the situation may change if the operator floods the cavity.

VIII.3.2. Technical basis for candidate strategies

Based on the insights gained from Sections 2 and 3, candidate strategies can be defined which are in essence derived from the CHLAs discussed in Section 4 (and in Appendix II). Thus, if it is known from the preparatory analysis that a high pressure melt ejection may lead to failure of the containment, depressurization of the RPV becomes an important strategy. Similarly, if it is found that flooding the cavity or the dry well may cool the debris in the vessel, such flooding becomes a candidate strategy.

This study should investigate the effects of the different CHLAs on the various plant damage descriptors (see Appendix I) to either predict the positive outcome of the potential action or the negative consequence of it. Theoretically, the effect of all CHLAs during all plant damage descriptors can be studied. In practice, the number of studies is limited as not all actions are relevant for all plant damage states. The phenomenological part of the PSA is mainly used for this. Dedicated mechanistic severe accidents codes (MAAP, MELCOR, etc.) can also be used.

VIII.3.3. Selection of strategies

Based on the insights gained from Sections 4.1 and 4.2, strategies can be developed to mitigate the relevant accident scenarios. The strategies could eventually be fed back into the PSA to estimate their benefit and, thus, verify the usefulness of the proposed action. A severe limitation of this is that a real event has many uncertainties, many decision points and many ramifications, making such feedback complicated and its result highly uncertain.

VIII.4. DEVELOPMENT OF SAMGs

VIII.4.1. Entry and exit set points

After the strategies have been defined, the actual guidelines need to be developed. They have entry and exit conditions. Probabilistic safety assessment may serve to find the conditions both to enter the SAMG domain and to leave the EOP domain as the only or the dominant accident management tool. Insights from PSA can be used to obtain such set points; for example the entry into SAMGs may occur at a core exit temperature of 650°C. This value must be

such that the SAMG actions which follow make sense and attain their objectives. For example, an empty SG must be flooded at a rate at which SG tube creep rupture will be prevented. Such insights are obtained from PSA type analyses.

VIII.4.2. Computational aids

Quantitative information to support the TSC (or related group) can also be obtained from PSA, such as the amount of water that will prevent vessel meltthrough (for BWRs, the minimum debris retention injection rate), the amount of water needed to effectively spray the containment, or the effect of containment venting on the flammability of hydrogen in the containment.

VIII.4.3. Priorities

A severe accident may easily lead to a situation calling for simultaneous execution of all available guidelines. However, some guidelines are more important in such situations and these can be identified with PSA.

VIII.5. DRILLS AND TRAINING

Drills are usually based on suitable templates. They should cover the relevant scenarios and call for many of the SAMGs to be executed. A PSA is an excellent tool to develop those templates.

VIII.6. DETERMINATION OF SOURCE TERM/DOSE RATE TO THE ENVIRONMENT

A level 3 PSA gives estimates of the source term and its external consequences. As the execution of the SAMG during the severe accident will have a great influence on the outcome of the accident in terms of releases, a reliable prediction using PSA is not possible. However, it may appear that the initiating event with its initial complications is fairly well known. The associated PSA source term may then serve as an upper estimate of the potential release.

REFERENCES

[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

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

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

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants, Safety Reports Series No. 23, IAEA, Vienna (2002).

[6] ELECTRIC POWER RESEARCH INSTITUTE, Severe Accident Management Guidance, Technical Basis Report, Vols 1 & 2, Rep. EPRI TR-101869, EPRI, Palo Alto, CA (1992).

[7] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, 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, Safety Requirements, Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[8] NUCLEAR REGULATORY COMMISSION, Assessment of Candidate Accident Management Strategies, Rep. NUREG/CR 5474, US Govt Printing Office, Washington, DC (1992).

[9] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS, Implementing Severe Accident Management in Nuclear Power Plants, Rep. OECD/GD(97)198, OECD, Paris (1997).

[10] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS, Specialist Meeting on Severe Accident Management Implementation, Rep. OECD/NEA/CSNI/R(95)5, OECD, Paris (1995).

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Quality Management and Quality Assurance, Rep. ISO 9000/1-4, ISO, London (1994).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations: Code and Safety Guides, Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[13] LUTZ, R.J., Westinghouse Owners Group — Severe Accident Management Guidance Validation, Rep. WCAP-14213, Westinghouse Electric Corporation, Pittsburgh (1994).

[14] HOLDERBAUM, D.F., Koeberg Nuclear Plant — Severe Accident Management Guidance Validation, Rep. WCAP-14603, Westinghouse Electric Corporation, Pittsburgh, PA (1996).

[15] NORTH ANNA POWER STATION, Severe Accident Management Guideline Demonstration Programme, Virginia Power, Richmond, VA (1997).
[16] DUANE ARNOLD ENERGY CENTER, Technical Support Guidelines (TSGs), Training Material, IES Utilities Inc., Cedar Rapids, MI (1998).
[17] HENRY, S.A., Assessment of Severe Accident Management Training Drill, Calvert Cliffs Nuclear Power Station, Rep. NEU 98-130, Baltimore Gas & Electric Corporation, Cusby, MD (1998).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for the Review of Accident Management Programmes in Nuclear Power Plants, Services Series No. 9, IAEA, Vienna (2003).
[19] INSTITUTE OF NUCLEAR POWER OPERATIONS, A Systematic Approach to Training, Training Program Handbook DOE-HDBK-1078-94, INPO, Atlanta (1994).
[20] HODGSON, C.D., "The management of severe accidents — Eskom position", Severe Accident Management (Proc. Expert Mtg Lyon, 1996), WANO, London (1996).
[21] NUCLEAR REGULATORY COMMISSION, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, Rep. NUREG 1.97, Rev. 3, US Govt Printing Office, Washington, DC (1983).
[22] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS, Implementing Severe Accident Management in Nuclear Power Plants, Rep. OECD/GD(97)198, OECD, Paris (1997).

Annex I

SUMMARY OF INTERNATIONAL ACTIVITIES IN SEVERE ACCIDENT MANAGEMENT

The subject of accident management programmes (AMPs) has already been covered by a number of IAEA publications. The IAEA has sponsored work on the development of operating procedures for accident conditions and on the practical implications of source term reassessment. In 1985 and 1988, the IAEA convened advisory groups on accident management. The results of this work were published in Refs [I–1, I–2]. In 1985, the IAEA sponsored a symposium on Source Term Evaluation for Accident Conditions and in 1988, together with the OECD Nuclear Energy Agency (OECD/NEA), a symposium on Severe Accidents in Nuclear Power Plants [I–3]. A number of Technical Co-operation meetings were held on the following topics:

(a) Use of PSA results for accident management (1989),
(b) Symptom oriented emergency operating procedures (1990),
(c) Containment performance (1990),
(d) Containment filtering and venting (1991),
(e) Severe accident management (1997, 1998).

Co-ordinated Research Projects on accident management and containment integrity and effectiveness for accident conditions were also sponsored in the period from 1994 to 1996. Additional information on the subject can be found in Refs [I–4 to I–6].

Information on the efforts being made, particularly in OECD Member Countries, and on typical strategies implemented to prevent or mitigate the consequences of core melting, is available, for example, from a report entitled Implementing Severe Accident Management in Nuclear Power Plants [I–7]. That report summarizes the situation in representative OECD Member Countries and can be used as a starting point for the development of further plant specific AMPs.

The European Commission (EC) has contracted a study[1] on severe accident management, entitled SAMIME, with the objective of determining the status and the extent of severe accident management development in European Union (EU) countries and developing a consensus among the partners as to which elements are needed or useful, as well as defining what further research work is needed to support severe accident management development [I–8]. The project was completed in 2000 [I–9].

[1] Formally called a 'concerted action' under the Fourth Framework Programme.

In 1994 the IAEA published a report on Accident Management Programmes in Nuclear Power Plants [I–10], which was designed as a guidebook to provide a systematic, structured approach to the development and implementation of an AMP. The main emphasis of this guidebook, which was developed by a consortium of consultants during the early 1990s, is on generic accident management guidance, including evaluation of vulnerabilities, accident management strategies, symptom oriented EOPs, training and organization. Since that IAEA report was published, a great effort has been made to implement plant specific AMPs in a large number of LWR plants. Accident management programmes have been implemented in all US NPPs and corresponding work is at an advanced stage in many European countries. The present report can be understood, to a certain extent, as an update of the previous report [I–10], reflecting knowledge gained from the implementation process of AMPs.

REFERENCES TO ANNEX I

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Developments in the Preparation of Operating Procedures for Emergency Conditions of Nuclear Power Plants, IAEA-TECDOC-341, Vienna (1985).

[I–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Some Practical Implications of Source Term Reassessment, IAEA-TECDOC-451, Vienna (1988).

[I–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accidents in Nuclear Power Plants (Proc. Symp. Sorrento, 1988), IAEA, Vienna (1988).

[I–4] OECD NUCLEAR ENERGY AGENCY, Specialist Meeting on Severe Accident Management Programme Development, Rep. NEA/CSNI/R(91)16, ENEA, Rome (1992).

[I–5] OECD NUCLEAR ENERGY AGENCY, Instrumentation to Manage Severe Accidents (Proc. Specialist Mtg Cologne, 1992), Gesellschaft für Reaktorsicherheit, Cologne (1992).

[I–6] NUCLEAR REGULATORY COMMISSION, Summary of a Workshop on Severe Accident Management, Rep. NUREG/CR-5780/5781, US Govt Printing Office, Washington, DC (1991).

[I–7] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS, Implementing Severe Accident Management in Nuclear Power Plants, Rep. OECD/GD(97)198, OECD, Paris (1997).

[I–8] EUROPEAN UNION, Concerted Actions on Severe Accident Management Implementation and Expertise in the European Union, SAMIME, Contract F145-CT98-0652 (1998).

[I–9] EUROPEAN COMMISSION, FISA '99 — EU Research in Reactor Safety (Proc. Symp. Luxembourg, 1999), EC, Luxembourg (1999).

[I–10] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Management Programmes in Nuclear Power Plants: A Guidebook, Technical Reports Series No. 368, IAEA, Vienna (1994).

Annex II

OVERVIEW OF THE SEVERE ACCIDENT MANAGEMENT GUIDANCE APPROACH AND IMPLEMENTATION IN SOME MEMBER STATES

This annex gives an overview of approaches to SAMGs as they exist to date, with emphasis on developments in the USA and Europe. Greater attention is given to the US approach as the USA has developed an extensive set of SAMGs which has now been implemented in all operating US NPPs and is being implementated in many NPPs in other countries. The information on the European countries has been collected in Ref. [II–1] and has been made available to the IAEA by the European Commission. It has been updated where additional information has become available from Member States. Separate information was provided by Japan. A wider but less recent overview, with more technical detail, is available in Ref. [II–2].

II.1. UNITED STATES OF AMERICA

II.1.1. Early developments

Following the completion of actions to ensure correction of safety and emergency response issues experienced during the Three Mile Island (TMI) accident, both the industry and the regulatory body took the initiative to analyse and evaluate generic issues related to the accident. One of these issues concerned radiological source terms; the actual releases during the TMI accident did not reflect what existing accident scenarios had predicted.

The process that followed led to the development of revised design basis scenarios, revised design basis source terms addressed by the Nuclear Regulatory Commission (NRC) [II–3], the development of symptom based EOPs and, ultimately, to the recognition of the need for severe accident management.

In August 1985 the NRC published its policy statement regarding severe reactor accidents [II–4]. This statement recognized the industry effort in severe accident risk management and essentially supported this ongoing effort. This was followed in 1988 by Report SECY-88-147 [II–5], which described the NRC plan for development and implementation (closure) of severe accident issues. This document also supported the approach of the NUMARC/(NEI) Nuclear Energy Institute programme. In 1989, Report SECY-89-012 [II–6] was issued describing the NRC approach to closure of the accident management guidelines portion of the integration plan for severe accident management.

The industry process, which included international co-operation, was managed by the NEI, with significant interaction among operating organizations, the Institute of Nuclear Power Operations, the Electric Power Research Institute (EPRI), owners groups, the NRC and recognized experts. Application was seen mostly outside the formal regulatory environment and the focus was on developing severe accident management guidance for the existing stations, i.e. without consideration of other than minor hardware modifications. In December 1994, Report NEI 91-04, Rev.1 [II–7] was published, with an agreement among all US operating organizations to follow through with implementation of these guidelines. The NRC concurred with this industry approach in January 1995.

II.1.2. The US industry position

The goal of US severe accident management, as defined in Ref. [II–7], was to enhance the capabilities of the emergency response organization (ERO) to mitigate severe accidents and prevent or minimize any off-site releases. The objective was to establish core cooling and ensure that any current or immediate threats to the FP barriers were being managed. To accomplish this, the ERO was to make full use of existing plant capabilities, including standard and non-standard uses of plant systems and equipment. The position, which was binding for all NPPs in the country, reads as follows:

"Each licensee will:

- Assess current capabilities to respond to severe accident conditions using Section 5 of NEI 91-04, Rev. 1, 'Severe Accident Issue Closure Guidelines';
- Implement appropriate improvements identified in the assessment, within the constraint of existing personnel and hardware, on a schedule to be determined by each licensee and communicated to the NRC, but in any event no later than December 31, 1998."

II.1.3. The severe accident management closure process

Section 5 of Ref. [II–7] specifies the closure process for a given licensee in the following four steps:

(1) Evaluate industry developed and owners group SAMGs along with the individual plant examination (IPE) for external events and the plant's current capabilities, to develop SAMGs for significant accidents and

screened with pre-specified criteria, and consider other generic and plant specific information (e.g. NRC and industry studies, PSA results, etc.) where appropriate.

(2) Interface the SAMG with the plant's emergency plan.

(3) Incorporate severe accident material into appropriate training programmes.

(4) Establish a means to consider and possibly adopt new severe accident information from self-assessments by licensees, applicable NRC generic communications, PSA studies, etc.

Screening criteria were used which basically state that for sequences with a relatively large core damage frequency (CDF) or containment bypass frequency, measures should be taken (i.e. administrative, procedural or hardware modification) which are mainly directed towards reducing the likelihood of the source of the accident sequence initiator; for sequences with a relatively small CDF or containment bypass frequency, SAMGs should be in place. Below 1×10^{-6} per reactor-year for the CDF and below 1×10^{-7} per reactor-year for containment bypass frequency, no actions were required (i.e. no SAMGs would be required).

Since the development of these criteria, the US industry has gone beyond this threshold and implemented severe accident management irrespective of event or sequence probability. Severe accident management is bounded solely by the physical phenomena arising from severe accidents, i.e. all mechanistically possible conditions are considered.

II.1.4. Development of SAMG strategies

The industry developed a technical basis for the selection and determination of potential countermeasures. This was done by EPRI and documented in the technical basis report (TBR). The purpose of the TBR was to provide an industry-wide common technical basis, from which the owners' groups and individual operating organization could develop their vendor and plant specific accident management guidance. The TBR uses various plant damage conditions to describe a severe accident progression, along with their anticipated symptoms and related phenomena. The report is symptom, not event oriented. Hence, no event sequences were studied with their consequences and potential ramifications, but severe accident symptoms were sought and their sensitivity to a spectrum of potential countermeasures, the candidate high level actions (CHLAs), was investigated.

The different damage conditions of the core were summarized in three major core damage states. A similar concept was followed for the containment.

Fifteen CHLAs were defined and the TBR investigated the response of each of the core and containment damage states to each of the CHLAs. Later, three additional actions were considered: external cooling of the (RPV/RCS), steam inerting of the containment and in-vessel cooling. It was recommended that these should also be considered when developing plant specific guidance. The process is described in further detail in Appendices I and II, where the individual CHLAs and the plant damage states are identified.

The actual development of SAMGs was not attempted. This was left to the owners groups and the individual operating organizations. These considered the TBR results plus information from their probabilistic safety studies, i.e. IPEs or PSAs, and identified the areas which were of relevance for their stations. From this material they developed generic strategies which were to be the essence of the plant's methodology. Individual plants then transformed this generic material into their plant specific procedures and guidelines.

II.1.5. Status of implementation

As already discussed, the US effort is based on the approaches of the owners groups. Hence, four groups of generic SAMGs have been developed, which have been transformed to plant specific guidance by the individual operating organizations. Extensive verification and validation was done, partly with the help of simulators, for the pre-severe accident management phase. Drills and exercises were held which included peer review, i.e. personnel from other stations was involved in review and assessment. The NRC oversaw the programme but did not formally approve the implementation of SAMGs. As of 31 December 1998, all operating US stations had implemented SAMGs.

More detailed elements of the US Owners Groups guidance are contained in other parts of this report, such as the plant damage states, the transition from the EOP-to the severe accident management domain, the list of CHLAs, the logical diagrams used by the WOG and the CEOG among others, and computational aids where these elements appear as examples of industrial applications of certain more general SAMG principles.

II.2. EUROPE

Developments in Europe have been more hardware oriented. Filtered containment vents were designed and installed in several countries; in some countries, catalytic hydrogen recombiners were also installed. Equipment such as power operated relief valves (PORVs) was requalified or replaced to make it capable of withstanding loads from bleed and feed, etc. From a software point of view, many plants performed PSAs or upgraded existing PSAs. However,

many countries have not yet established a formal severe accident management programme, i.e. a full and comprehensive inclusion of core melt scenarios with all their associated phenomena in the procedures. This section highlights the approaches in a number of European countries.

II.2.1. Belgium

Belgium has no uniform programme for development of SAMGs. Some stations follow US developments and have started development and implementation of the WOG guidelines at the request of the regulatory body. The methodology and lines of authority also follow the WOG approach. The WOG SAG is not used in those stations which have catalytic recombiners. Generally, strategies were selected based on level 1 and 2 PSA results, systems analysis and instrument analysis.

Some older stations have developed SAMGs independently, not in response to a request by their regulatory body. In these cases the EOPs are not closed, but enhanced by additional SAGs. An example is the continuous monitoring of water and power sources. Equipment that has failed is also brought back into service. Core damage is not addressed as such in the procedures.

II.2.2. Netherlands

Since only one plant (Siemens design) is still in operation, its situation is the only relevant one. Its management voluntarily elected to follow the WOG approach since the regulatory body had requested severe accident procedures but had left the choice of method and vendor to the licensee. The plant decided to not just follow the WOG, but to enhance this method with useful features of other US approaches, with the CEOG's diagnostic tools and the BWR Owners Group's technical support guidelines as the candidates. This will be done in an iterative process, i.e. after implementation of the WOG method as such.

II.2.3. Sweden

Sweden completed its severe accident management programme in 1988. It contained several hardware features (e.g. a filtered vent on the containment), procedures and training. Westinghouse beyond emergency response guidelines (BERGs) were developed and implemented in Sweden's three PWRs. In contrast to the modern WOG approach, they require the recognition of vessel failure. More recently, handbooks on severe accidents were developed that are intended to be used in the TSC. These handbooks

contain severe accident insights plus some guidance. Exercises are limited; they are not focused on the use of SAGs, but more on communication paths and effectiveness.

II.2.4. France

French reactors have a family of procedures, called I, A, H and U, for increasing severity of an event (i.e. with an increasing number of failed safety functions). I stands for 'incidents', A for 'accidents', H for 'outside design' and U for 'ultimate procedures'. Examples of U procedures are U2, restoring the containment function and U5, containment venting. In recent years, state oriented procedures have been added, replacing event oriented EOPs in order to support the operators. There is no need for them to diagnose the initiating event.

For conditions indicating core damage, a set of SAGs is entered which basically centres around depressurization and feeding of the RPV, depressurization and feeding of the steam generator, and restoring containment integrity using U2 and, ultimately, U5 procedures. French procedures do not explicitly address plant damage states (i.e. possible combinations of core and containment damage states), but are oriented towards restoring critical safety functions (CSFs) on the basis of observed parameters and the availability of safety systems. Severe accidents are handled by on-site and off-site crisis teams which decide on the actions to be taken.

II.2.5. Spain

Spanish operating organizations follow the rules and regulations of the country of origin. Plants of US origin therefore follow the SAMG approach. No decision has yet been taken for the single Siemens plant, as Siemens in Germany have not yet taken such steps. It may follow the general philosophy of SAMG as it is applied by the other Spanish NPPs. The Spanish regulatory body, Consejo de Seguridad Nuclear (CSN), has not explicitly required SAMGs.

In 1994 the Spanish PWR owners group presented a 'common basis report' to the regulatory body, addressing SAMGs. Similarly, the BWR owners group did the same in 1995. These documents are comparable to the US industry's position. The association of Spanish operating organizations, Asociación Española de la Industria Eléctrica (UNESA), presented the case to the CSN in 1996. A programme calling for SAMGs to be in place by the end of 2000 was developed and presented. For the Siemens plant, a later date may well be possible.

II.2.6. United Kingdom

Severe accident prevention and mitigation strategies have been developed and implemented at the single operating PWR, Sizewell B, and the advanced gas cooled reactors (AGRs). The detailed design development of Sizewell B was undertaken in the period immediately following the TMI accident, which highlighted the importance of dealing with beyond design basis scenarios. The decision was therefore taken to produce a suite of operating procedures to cover all operating states from normal operation to severe accidents. In addition, the design benefited from insights derived from plant specific level 3 PSAs.

Examples of design changes made include a 'wet' reactor cavity to mitigate basemat failure and the incorporation of additional isolation valves in the RHR suction lines to reduce interfacing systems LOCA (so-called V sequence) frequency. Included in the Sizewell B station operating instructions (SOIs) are a set of symptom based procedures (SOI 8) which are extended to severe accident mitigation. The actions included in the severe accident mitigation procedures are associated with the use of existing plants in different modes and with relaxed limits applied. Because severe accidents were considered in the plant design, it has not proved necessary to provide additional equipment for severe accident management. Current international developments in severe accident management are closely monitored for any future upgrade of the SOIs.

In the case of the AGRs, the plants are equipped with an accident management capability to deal with BDBAs. It includes a set of symptom based emergency response guidelines (SBERGs) designed primarily to prevent core damage. In the unlikely event that the SBERGs should fail, the emergency controller will refer to a set of advisory guidelines, the severe accident management guidelines, designed with the objective of mitigating activity release to the environment.

II.2.7. Germany

With respect to accident management, in Germany a distinct line is drawn between the design basis area and the beyond design basis area. Accidents within the design basis area are dealt with by so-called 'event oriented procedures' when the event is clearly identifiable by use of a decision tree. If this is not the case or if the selected procedure is not successful, a set of 'symptom oriented procedures' is employed. Both sets of procedures comprise the operations manual (OM).

Accidents which have been identified as BDBAs are dealt with by using the so-called 'beyond design basis operations manual' (BDBOM). The

BDBOM is structured along the same lines as the symptom oriented part of the OM, i.e. it is based on the CSF concept.

The BDBOM includes preventive (core intact) as well as mitigatory procedures (core damaged). The emphasis is, however, on the prevention side and limited guidance is available for the core damage situation. Use is made not only of existing hardware. Extensive new hardware has been installed to be able to carry out both preventive and mitigatory accident management. Bleed and feed of the secondary and/or primary side are examples of the former; filtered containment venting, catalytic recombiners and a sampling system including H_2 sampling are examples of the latter. Care has been taken that such components (e.g. PORVs) are fully qualified for their functions.

In order to implement accident management actions correctly, a clear set of criteria based on directly measurable physical quantities has to exist. Precise criteria are available to the shift leader as to when to use event oriented procedures, when to switch to symptom oriented procedures, and when to begin using the beyond design basis operating manual. Precise criteria for mitigatory actions such as containment venting are also defined.

It should be noted that the efforts made by the German operating organizations in the beyond design basis area are voluntary. Operating organizations and the Federal Government have, however, agreed that the recommendations made by the Reactor Safety Commission (RSK) in this area will be followed.

II.2.8. Slovakia

A major activity in Slovakia has been the transition from event based to symptom based EOPs by means of emergency response guidelines (ERGs), which is being done with support from Westinghouse. It has included a critical review of the ERG strategies, which had to be adapted to the configuration and characteristics of WWERs (e.g. the generic EOP exit criterion of 650°C had to be changed to 550°C). From there, SAMG development was initiated under a PHARE contract. A detailed investigation of WWERs under severe accident conditions was carried out using MAAP4, which included characteristics of the WOG SAMG strategies for the WWERs.

The project has proceeded to the definition of logic trees, i.e. the decision flow chart (DFC) and the severe challenge status tree (SCST) (see Appendix I) plus high level strategies and a proposal to upgrade instrumentation and control (I&C) for severe accidents. This includes a requalification of selected I&C equipment to severe accident conditions, i.e. it will be qualified for beyond design basis conditions, including some margin where appropriate (for example, core exit thermocouples up to 1000°C).

In addition to ERGs, which are in use at NPPs, a set of severe accident management documents has been prepared for the emergency response centre of the Nuclear Regulatory Authority of the Slovak Republic (UJD SR). At the present time, the emergency procedure for evaluation of severe accidents in the emergency response centre of UJD is being developed for the Mochovce NPP by the technical staff of the department for safety analysis and technical support at the UJD SR.

A set of accident scenarios representing a spectrum of postulated severe accidents for the Mochovce NPP has been analysed using the MELCOR severe accident computer code. The analyses performed include thermal-hydraulic core damage, FP release, FP transport and containment response during the postulated accident conditions. The accident source term has been evaluated to estimate the radiological consequences. In the final phase, based on the analysis results, the emergency procedure for the emergency response centre of the UJD SR will be developed and used during emergency drills or real emergency situations at units 1 and 2 of the Mochovce NPP.

The emergency procedures for the Jaslovske Bohunice NPP have been completed. Depending on the progress of reconstruction of the V-1 Jaslovske Bohunice NPP, the emergency procedures for this plant will be updated.

II.2.9. Finland

In Finland two nuclear operating organizations independently operate two plants based on different concepts, a WWER-440 and an ABB BWR. Teollisuuden Voima Oy, the owner and operator of the Olkiluoto ABB BWRs, carried out a severe accident management project at the end of the 1980s, which included several plant modifications and integration of SAMGs into the ultimate EOP. Fortum Engineering Ltd (formerly IVO) has developed a complete severe accident management approach applying the integrated risk oriented accident analysis methodology for the Loviisa WWER-440 units. Following this approach, Fortum is in the process of developing SAMG documents in parallel with plant modifications.

II.3. ASIA

II.3.1. Japan

Symptom based EOPs were developed in Japan in the 1980s after the TMI-2 accident. Conventional accident operating procedures (AOPs) were installed, as well as hardware, e.g. wide range monitors. Level 1 and 2 PSAs have been extensively applied in Japan, both by the regulatory body and the

industry, and accident management measures have been developed which address, for example, utilization of conventional systems, electric power supply from an adjacent unit, alternate measures for reactivity control, water injection, heat removal and recovery of failed components. These measures were identified on the basis of PSA results. The industry was to have implemented these accident management countermeasures around the year 2000.

For accident management at some plants in Japan AOPs, EOPs and severe accident operating procedures (SOPs) have been prepared for use in the CR, and AMG and recovery procedures for RHR and D/G have been prepared for use in the TSC, which is set up during an accident. The AMG is applied after detection of core damage. The AMG makes use of figures and graphs of analytical results and shows the technical bases and criteria for identifying plant conditions, selecting proper accident management countermeasures and making evaluations. For the CR, SOPs which contain the most important aspects of the AMG used by the TSC are prepared using a flow chart format to allow quick responses. These accident management procedures are reviewed periodically and improved to reflect the progress of knowledge in PSA and severe accident research. Similar approaches are being considered for other plants.

REFERENCES TO ANNEX II

[II–1] EUROPEAN COMMISSION, FISA '99 — EU Research in Reactor Safety (Proc. Symp. Luxembourg, 1999), EC, Luxembourg (1999).

[II–2] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS, Implementing Severe Accident Management in Nuclear Power Plants, Rep. OECD/GD(97)198, OECD, Paris (1997).

[II–3] NUCLEAR REGULATORY COMMISSION, Severe Accident Risk: An Assessment of Five US Nuclear Power Plants, Rep. NUREG-1150, US Govt Printing Office, Washington, DC (1990).

[II–4] NUCLEAR REGULATORY COMMISSION, Policy Statement on Severe Accidents Regarding Future Designs and Existing Plants, NRC Policy Statement 50FR 32138, Federal Register, US Govt Printing Office, Washington, DC (1985).

[II–5] STELLO, V., Integration Plan for Closure of Severe Accident Issues, Rep. SECY-88-147, Nuclear Regulatory Commission, US Govt Printing Office, Washington, DC (1988).

[II–6] STELLO, V., Staff Plans for Accident Management Regulatory and Research Programs, Rep. SECY-89-012, Nuclear Regulatory Commission, US Govt Printing Office, Washington, DC (1989).

[II–7] NUCLEAR ENERGY INSTITUTE, Severe Accident Issue Closure Guidelines, Rep. NEI 91-04, Rev. 1, NEI, Washington, DC (1994).

Annex III

TYPICAL TSC ORGANIZATION AT A BWR IN THE USA

At Alliant Energy's Duane Arnold Energy Center NPP, the TSC has been organized as depicted in Fig. III–1. The accident management team (AMT) or accident assessment team (AAT) has been added to the original TSC, as can be seen from Fig. III–1. In this scheme, the operations supervisor holds a reactor operator licence and is the prime contact between the AMT and the CR in order to facilitate communications between the TSC and the CR.

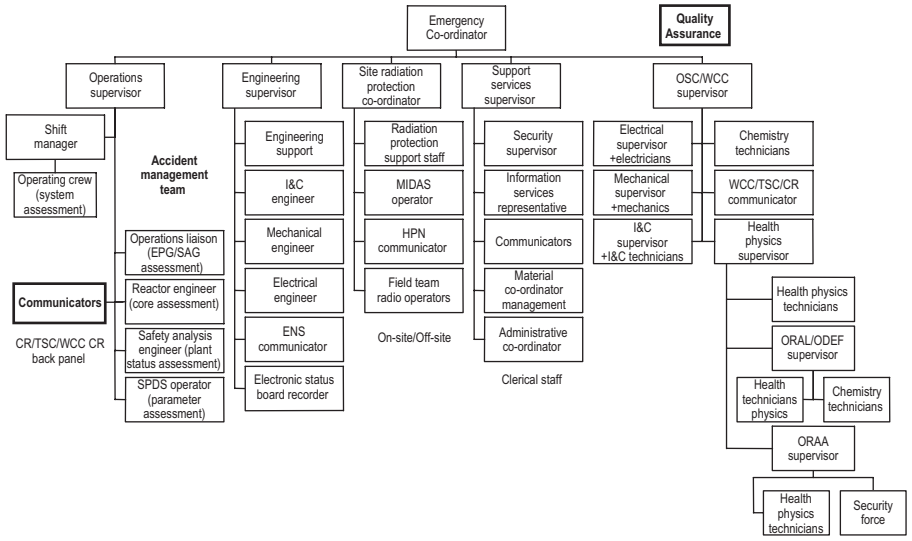

FIG. III.1. Emergency response organization scheme of the Duane Arnold NPP (USA). ENS: emergency notification system (the primary means of communicating reactor safety related information throughout an emergency from the licensee to the NRC); EPG: emergency procedure guidelines; HPN: health physics notification (the primary means of communicating radiological data from the licensee to the NRC); MIDAS: meteorological equipment; SAG: severe accident guidelines; SPDS: safety parameter display system; ODEF: off-site decontamination facility; ORAA: off-site relocation and assembly area; ORAL: off-site radiological and analytical laboratory; OSC: operational support centre; WCC: work control centre (where the OSC is established during an emergency and responsible for establishing and controlling in-plant assessment and repair teams).

DEFINITIONS

The definitions were compiled solely for the purpose of the present report. The list does not represent a consensus or an endorsement by the IAEA.

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

accident management programme. Plans and actions undertaken to ensure that the plant and the personnel with responsibilities for accident management are adequately prepared to take effective on-site actions to prevent or to mitigate the consequences of a severe accident.

arrangements (for emergency response). The integrated set of infrastructural elements necessary to provide the capability for performing a specified function or task required in response to a nuclear or radiological emergency. These elements may include authorities and responsibilities, organization, co-ordination, personnel, plans, procedures, facilities, equipment or training.

beyond design basis accident (BDBA). Accident conditions more severe than a design basis accident. (A BDBA may or may not involve core degradation.)

computational aid. Pre-calculated analyses, nomographs or easily used computer software available for use by plant staff during a severe accident: (1) to support plant staff guidance, (2) to predict accident phenomena and timing, and (3) to evaluate the effectiveness of specific candidate strategies.

containment. Methods or physical structures designed to prevent the dispersion of radioactive substances.

design basis accident (DBA). 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.

emergency. 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. This includes nuclear and radiological emergencies and conventional emergencies such as fires, release of hazardous chemicals, storms or earthquakes. It includes situations for which prompt action is warranted to mitigate the effects of a perceived hazard.

emergency operating procedures. Plant specific procedures containing instructions to operating staff for implementing measures to prevent core degradation in both DBAs and BDBAs.

emergency plan. A description of the objectives, policy and concept of operations for the response to an emergency and of the structure, authorities and responsibilities for a systematic, co-ordinated and effective response. The emergency plan serves as the basis for the development of other plans, procedures and checklists.

emergency procedure. A set of detailed written instructions describing the actions to be taken by response personnel in an emergency.

emergency response. The performance of actions to mitigate the consequences of an emergency for human health and safety, quality of life, property and the environment.

event specific procedure. A procedure containing actions which are appropriate only for a specific accident sequence (or set of sequences) which must be diagnosed before applying the procedure. An event specific procedure may or may not be symptom based.

guideline. A text setting out actions to mitigate or stabilize accident conditions.

mitigatory action. Immediate action by the operator or another party: (1) To reduce the potential for conditions to develop that would result in exposure or a release of radioactive material requiring emergency actions on or off the site; or (2) To mitigate source conditions that may result in exposure or a release of radioactive material requiring emergency actions on or off the site.

probabilistic safety assessment (PSA). A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk. Three levels of PSA are generally recognized. Level 1 comprises the assessment of plant failures leading to the determination of core damage frequency. Level 2 includes the assessment of containment response leading, together with level 1 results, to the determination of containment release frequencies. Level 3 includes the assessment of off-site consequences leading, together with the results of level 2 analysis, to estimates of public risks.

procedure. A set of detailed written instructions to direct actions. The actions should be carried out in the sequence laid down in the procedure unless otherwise indicated in the procedure body or by the rules for use of a document.

response organization. An organization designated or otherwise recognized by a State as being responsible for managing or implementing any aspect of an emergency response.

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

severe accident management guidelines. A set of guidelines for actions for severe accident management.

strategy. A group of activities developed at a plant with the common objective of preventing and/or mitigating the effects of severe accidents.

symptom based procedure/guideline. A procedure or guideline for actions to be taken depending on the values of directly measurable plant parameters.

validation. The process of determining whether a product or service is adequate to perform its intended function satisfactorily. (The evaluation is performed to determine whether the actions specified in the instructions of an accident management programme can be executed by trained staff to manage emergency events.)

verification. The process of determining whether the quality or performance of a product or service is as stated, as intended or as required. (The evaluation is performed to confirm the correctness of a written procedure or guideline to ensure that technical and human factors have been properly taken into account.)

vulnerability. Any combination of plant design features and operations which could lead to a severe accident or could inhibit the ability to prevent or mitigate a severe accident.

CONTRIBUTORS TO DRAFTING AND REVIEW

Fagula, L.	Bohunice NPP, Slovakia
Gustavsson, V.	Vattenfall Energisystems AB, Sweden
Misak, J.	International Atomic Energy Agency
Prior, R.	Westinghouse Energy Systems Europe S.A., Belgium
Sonnenkalb, M.	Gesellschaft für Anlagen- und Reaktorsicherheit, Germany
Tuomisto, H.	Fortum Engineering Ltd, Finland
Vayssier, G.	NSC–Nuclear Safety Consultancy, Netherlands
Walsh, L.A.	Seabrook NPP, United States of America

Consultants Meetings

Vienna, Austria: 3–7 November 1997, 18–22 May 1998,
19–23 October 1998,
26–30 July 1999, 15–19 November 1999