This publication has been superseded by SSG-54.

IAEA Safety Standards

for protecting people and the environment

Severe Accident Management Programmes for Nuclear Power Plants

Safety Guide

No. NS-G-2.15

IAEA

International Atomic Energy Agency

SEVERE ACCIDENT MANAGEMENT PROGRAMMES FOR NUCLEAR POWER PLANTS

Safety standards survey
The IAEA welcomes your response. Please see:
http://www-ns.iaea.org/standards/feedback.htm

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
BURUNDI
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
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".

IAEA SAFETY STANDARDS SERIES No. NS-G-2.15

SEVERE ACCIDENT MANAGEMENT PROGRAMMES FOR NUCLEAR POWER PLANTS

SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2009

Printed by the IAEA in Austria
July 2009
STI/PUB/1376

IAEA Library Cataloguing in Publication Data

Severe accident management programmes for nuclear power plants : safety guide. — Vienna : International Atomic Energy Agency, 2008.
p. ; 24 cm. — (IAEA safety standards series, ISSN 1020–525X ; no. NS–G–2.15)
STI/PUB/1376
ISBN 978–92–0–112908–6
Includes bibliographical references.

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

IAEAL 08–00559

FOREWORD

by Mohamed ElBaradei
Director General

The IAEA's Statute authorizes the Agency to establish safety standards to protect health and minimize danger to life and property — standards which the IAEA must use in its own operations, and which a State can apply by means of its regulatory provisions for nuclear and radiation safety. A comprehensive body of safety standards under regular review, together with the IAEA's assistance in their application, has become a key element in a global safety regime.

In the mid-1990s, a major overhaul of the IAEA's safety standards programme was initiated, with a revised oversight committee structure and a systematic approach to updating the entire corpus of standards. The new standards that have resulted are of a high calibre and reflect best practices in Member States. With the assistance of the Commission on Safety Standards, the IAEA is working to promote the global acceptance and use of its safety standards.

Safety standards are only effective, however, if they are properly applied in practice. The IAEA's safety services — which range in scope from engineering safety, operational safety, and radiation, transport and waste safety to regulatory matters and safety culture in organizations — assist Member States in applying the standards and appraise their effectiveness. These safety services enable valuable insights to be shared and I continue to urge all Member States to make use of them.

Regulating nuclear and radiation safety is a national responsibility, and many Member States have decided to adopt the IAEA's safety standards for use in their national regulations. For the contracting parties to the various international safety conventions, IAEA standards provide a consistent, reliable means of ensuring the effective fulfilment of obligations under the conventions. The standards are also applied by designers, manufacturers and operators around the world to enhance nuclear and radiation safety in power generation, medicine, industry, agriculture, research and education.

The IAEA takes seriously the enduring challenge for users and regulators everywhere: that of ensuring a high level of safety in the use of nuclear materials and radiation sources around the world. Their continuing utilization for the benefit of humankind must be managed in a safe manner, and the IAEA safety standards are designed to facilitate the achievement of that goal.

THE IAEA SAFETY STANDARDS

BACKGROUND

Radioactivity is a natural phenomenon and natural sources of radiation are features of the environment. Radiation and radioactive substances have many beneficial applications, ranging from power generation to uses in medicine, industry and agriculture. The radiation risks to workers and the public and to the environment that may arise from these applications have to be assessed and, if necessary, controlled.

Activities such as the medical uses of radiation, the operation of nuclear installations, the production, transport and use of radioactive material, and the management of radioactive waste must therefore be subject to standards of safety.

Regulating safety is a national responsibility. However, radiation risks may transcend national borders, and international cooperation serves to promote and enhance safety globally by exchanging experience and by improving capabilities to control hazards, to prevent accidents, to respond to emergencies and to mitigate any harmful consequences.

States have an obligation of diligence and duty of care, and are expected to fulfil their national and international undertakings and obligations.

International safety standards provide support for States in meeting their obligations under general principles of international law, such as those relating to environmental protection. International safety standards also promote and assure confidence in safety and facilitate international commerce and trade.

A global nuclear safety regime is in place and is being continuously improved. IAEA safety standards, which support the implementation of binding international instruments and national safety infrastructures, are a cornerstone of this global regime. The IAEA safety standards constitute a useful tool for contracting parties to assess their performance under these international conventions.

THE IAEA SAFETY STANDARDS

The status of the IAEA safety standards derives from the IAEA's Statute, which authorizes the IAEA to establish or adopt, in consultation and, where appropriate, in collaboration with the competent organs of the United Nations and with the specialized agencies concerned, standards of safety for protection of health and minimization of danger to life and property, and to provide for their application.

With a view to ensuring the protection of people and the environment from harmful effects of ionizing radiation, the IAEA safety standards establish fundamental safety principles, requirements and measures to control the radiation exposure of people and the release of radioactive material to the environment, to restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation, and to mitigate the consequences of such events if they were to occur. The standards apply to facilities and activities that give rise to radiation risks, including nuclear installations, the use of radiation and radioactive sources, the transport of radioactive material and the management of radioactive waste.

Safety measures and security measures[1] have in common the aim of protecting human life and health and the environment. Safety measures and security measures must be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security.

The IAEA safety standards reflect an international consensus on what constitutes a high level of safety for protecting people and the environment from harmful effects of ionizing radiation. They are issued in the IAEA Safety Standards Series, which has three categories (see Fig. 1).

Safety Fundamentals

Safety Fundamentals present the fundamental safety objective and principles of protection and safety, and provide the basis for the safety requirements.

Safety Requirements

An integrated and consistent set of Safety Requirements establishes the requirements that must be met to ensure the protection of people and the environment, both now and in the future. The requirements are governed by the objective and principles of the Safety Fundamentals. If the requirements are not met, measures must be taken to reach or restore the required level of safety. The format and style of the requirements facilitate their use for the establishment, in a harmonized manner, of a national regulatory framework. The safety requirements use ‘shall’ statements together with statements of

[1] See also publications issued in the IAEA Nuclear Security Series.

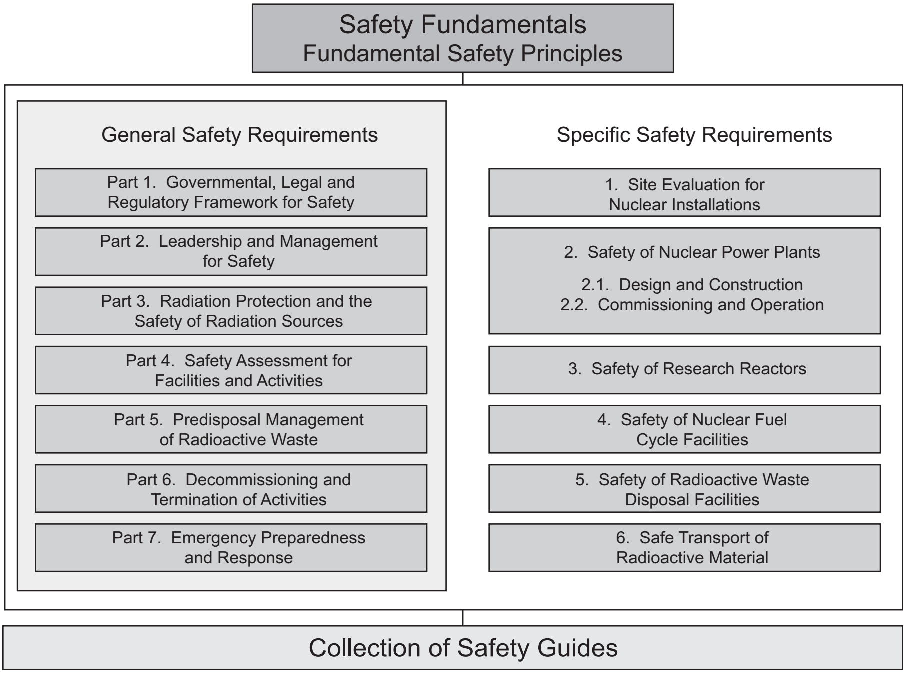

FIG. 1. The long term structure of the IAEA Safety Standards Series.

associated conditions to be met. Many requirements are not addressed to a specific party, the implication being that the appropriate parties are responsible for fulfilling them.

Safety Guides

Safety Guides provide recommendations and guidance on how to comply with the safety requirements, indicating an international consensus that it is necessary to take the measures recommended (or equivalent alternative measures). The Safety Guides present international good practices, and increasingly they reflect best practices, to help users striving to achieve high levels of safety. The recommendations provided in Safety Guides are expressed as ‘should’ statements.

APPLICATION OF THE IAEA SAFETY STANDARDS

The principal users of safety standards in IAEA Member States are regulatory bodies and other relevant national authorities. The IAEA safety standards are also used by co-sponsoring organizations and by many organizations that design, construct and operate nuclear facilities, as well as organizations involved in the use of radiation and radioactive sources.

The IAEA safety standards are applicable, as relevant, throughout the entire lifetime of all facilities and activities — existing and new — utilized for peaceful purposes and to protective actions to reduce existing radiation risks. They can be used by States as a reference for their national regulations in respect of facilities and activities.

The IAEA's Statute makes the safety standards binding on the IAEA in relation to its own operations and also on States in relation to IAEA assisted operations.

The IAEA safety standards also form the basis for the IAEA's safety review services, and they are used by the IAEA in support of competence building, including the development of educational curricula and training courses.

International conventions contain requirements similar to those in the IAEA safety standards and make them binding on contracting parties. The IAEA safety standards, supplemented by international conventions, industry standards and detailed national requirements, establish a consistent basis for protecting people and the environment. There will also be some special aspects of safety that need to be assessed at the national level. For example, many of the IAEA safety standards, in particular those addressing aspects of safety in planning or design, are intended to apply primarily to new facilities and activities. The requirements established in the IAEA safety standards might not be fully met at some existing facilities that were built to earlier standards. The way in which IAEA safety standards are to be applied to such facilities is a decision for individual States.

The scientific considerations underlying the IAEA safety standards provide an objective basis for decisions concerning safety; however, decision makers must also make informed judgements and must determine how best to balance the benefits of an action or an activity against the associated radiation risks and any other detrimental impacts to which it gives rise.

DEVELOPMENT PROCESS FOR THE IAEA SAFETY STANDARDS

The preparation and review of the safety standards involves the IAEA Secretariat and four safety standards committees, for nuclear safety (NUSSC), radiation safety (RASSC), the safety of radioactive waste (WASSC) and the safe transport of radioactive material (TRANSSC), and a Commission on

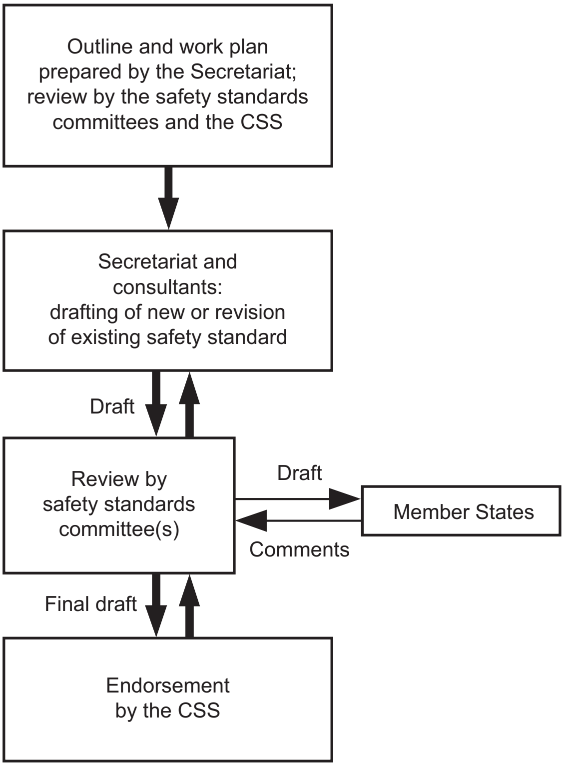

FIG. 2. The process for developing a new safety standard or revising an existing standard.

Safety Standards (CSS) which oversees the IAEA safety standards programme (see Fig. 2).

All IAEA Member States may nominate experts for the safety standards committees and may provide comments on draft standards. The membership of the Commission on Safety Standards is appointed by the Director General and includes senior governmental officials having responsibility for establishing national standards.

A management system has been established for the processes of planning, developing, reviewing, revising and establishing the IAEA safety standards. It articulates the mandate of the IAEA, the vision for the future application of the safety standards, policies and strategies, and corresponding functions and responsibilities.

INTERACTION WITH OTHER INTERNATIONAL ORGANIZATIONS

The findings of the United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR) and the recommendations of international expert bodies, notably the International Commission on Radiological Protection (ICRP), are taken into account in developing the IAEA safety standards. Some safety standards are developed in cooperation with other bodies in the United Nations system or other specialized agencies, including the Food and Agriculture Organization of the United Nations, the United Nations Environment Programme, the International Labour Organization, the OECD Nuclear Energy Agency, the Pan American Health Organization and the World Health Organization.

INTERPRETATION OF THE TEXT

Safety related terms are to be understood as defined in the IAEA Safety Glossary (see http://www-ns.iaea.org/standards/safety-glossary.htm). Otherwise, words are used with the spellings and meanings assigned to them in the latest edition of The Concise Oxford Dictionary. For Safety Guides, the English version of the text is the authoritative version.

The background and context of each standard in the IAEA Safety Standards Series and its objective, scope and structure are explained in Section 1, Introduction, of each publication.

Material for which there is no appropriate place in the body text (e.g. material that is subsidiary to or separate from the body text, is included in support of statements in the body text, or describes methods of calculation, procedures or limits and conditions) may be presented in appendices or annexes.

An appendix, if included, is considered to form an integral part of the safety standard. Material in an appendix has the same status as the body text, and the IAEA assumes authorship of it. Annexes and footnotes to the main text, if included, are used to provide practical examples or additional information or explanation. Annexes and footnotes are not integral parts of the main text. Annex material published by the IAEA is not necessarily issued under its authorship; material under other authorship may be presented in annexes to the safety standards. Extraneous material presented in annexes is excerpted and adapted as necessary to be generally useful.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Consideration of beyond design basis accidents at nuclear power plants is an essential component of the defence in depth approach used in ensuring nuclear safety [1–3]. The probability of occurrence of a beyond design basis accident is very low, but such an accident may lead to significant consequences resulting from the degradation of nuclear fuel.

1.2. A design basis accident is defined as accident conditions against which a facility 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 [4].

1.3. A beyond design basis accident comprises accident conditions more severe than a design basis accident, and may or may not involve core degradation. Accident conditions more severe than a design basis accident and involving significant core degradation are termed severe accidents [4].[1]

1.4. Accident management is the taking of a set of actions during the evolution of a beyond design basis accident:

(a) To prevent the escalation of the event into a severe accident;
(b) To mitigate the consequences of a severe accident;
(c) To achieve a long term safe stable state [4].

The second aspect of accident management (to mitigate the consequences of a severe accident) is also termed severe accident management. Accident management is essential to ensure effective defence in depth at the fourth level [2].[2]

---

[1] See para. 2.1.

[2] The objective of the fourth level of defence in depth is to ensure that both the likelihood of an accident entailing significant core damage (a severe accident) and the magnitude of a release of radioactive material following a severe accident are kept as low as reasonably achievable and, thereby, to reduce risk.

OBJECTIVE

1.5. This Safety Guide provides recommendations on meeting the requirements for accident management, including managing severe accidents, that are established in Section 5 of Ref. [5], in Sections 3 and 5 of Ref. [6] and in Section 4 of Ref. [7].

1.6. This Safety Guide presents recommendations for the development and implementation of an accident management programme.

1.7. This Safety Guide is intended primarily for use by operating organizations of nuclear power plants, utilities and their support organizations; it may also be used by regulatory bodies to facilitate preparation of the relevant national regulatory requirements.

SCOPE

1.8. This Safety Guide includes recommendations for the development of an accident management programme to prevent and to mitigate the consequences of beyond design basis accidents, including severe accidents. This Safety Guide focuses on the severe accident management programme.

1.9. Although the recommendations of this Safety Guide have been developed primarily for use for light water reactors, they are anticipated to be valid for a wide range of nuclear reactors, both existing and new.

1.10. The recommendations of this Safety Guide have been developed primarily for accident management during at-power states, but are intended to be valid also for other modes of operation, including shutdown states.

1.11. For more details, reference is made to other IAEA Safety Guides [8–10]. References [11–13] present elements of accident management programmes, give examples of how to prepare, develop, implement and review accident management programmes and provide useful background material.

STRUCTURE

1.12. This Safety Guide consists of two main sections. Section 2 presents the overall concept of an accident management programme. High level considerations are described in Section 2, while the process of development and implementation of an accident management programme is treated in Section 3. Recommendations for the use of severe accident management guidelines are provided in the Appendix. An example of a categorization scheme for accident sequences is provided in the Annex.

2. CONCEPT OF THE ACCIDENT MANAGEMENT PROGRAMME

REQUIREMENTS

2.1. Reference [5] establishes the following requirements on addressing severe accidents and accident management in the design of nuclear power plants:

> "Certain very low probability plant states that are beyond design basis accident conditions and which may arise owing to multiple failures of safety systems leading to significant core degradation may jeopardize the integrity of many or all of the barriers to the release of radioactive material. These event sequences are called severe accidents. Consideration shall be given to these severe accident sequences, using a combination of engineering judgement 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 shall be addressed in the design.

(3) Potential design changes 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 operational states, 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" (Ref. [5], para. 5.31).

2.2. Reference [6] establishes the following requirements on severe accident management and accident management in the operation of nuclear power plants:

"Plant staff shall receive instructions in the management of accidents beyond the design basis. The training of operating personnel shall ensure their familiarity with the symptoms of accidents beyond the design basis and with the procedures for accident management" (Ref. [6], para. 3.12).

"Emergency operating procedures or guidance for managing severe accidents (beyond the design basis) shall be developed" (Ref. [6], para. 5.12).

2.3. Requirement 13 of Ref. [7] on assessment of defence in depth states:

"It has to be determined in the assessment of defence in depth whether adequate provisions have been made at each of the levels of defence in depth to ensure that the legal person responsible for the facility can:

(a) Address deviations from normal operation or, in the case of a repository, from its expected evolution in the long term;
(b) Detect and terminate safety related deviations from normal operation or from its expected evolution in the long term, should deviations occur;

(c) Control accidents within the limits established for the design;
(d) Specify measures to mitigate the consequences of accidents that exceed design limits;
(e) Mitigate radiation risks associated with possible releases of radioactive material" (Ref. [7], para. 4.45).

CONCEPT OF ACCIDENT MANAGEMENT

2.4. An accident management programme should be developed for all plants, irrespective of the total core damage frequency and fission product release frequency calculated for the plant.

2.5. A structured top-down approach should be used to develop the accident management guidance. This approach should begin with the objectives and strategies, and result in procedures and guidelines, and should cover both the preventive and the mitigatory domains. Figure 1 illustrates the top-down approach to accident management.

2.6. At the top level, the objectives of accident management are defined as follows:

— Preventing significant core damage;
— Terminating the progress of core damage once it has started;
— Maintaining the integrity of the containment as long as possible;
— Minimizing releases of radioactive material;
— Achieving a long term stable state.

To achieve these objectives, a number of strategies should be developed.

2.7. From the strategies, suitable and effective measures for accident management should be derived. Such measures include plant modifications, where these are deemed important for managing beyond design basis accidents and severe accidents, and personnel actions. These measures include repair of failed equipment.

2.8. Appropriate guidance, in the form of procedures and guidelines, should be developed for the personnel responsible for executing the measures for accident management.

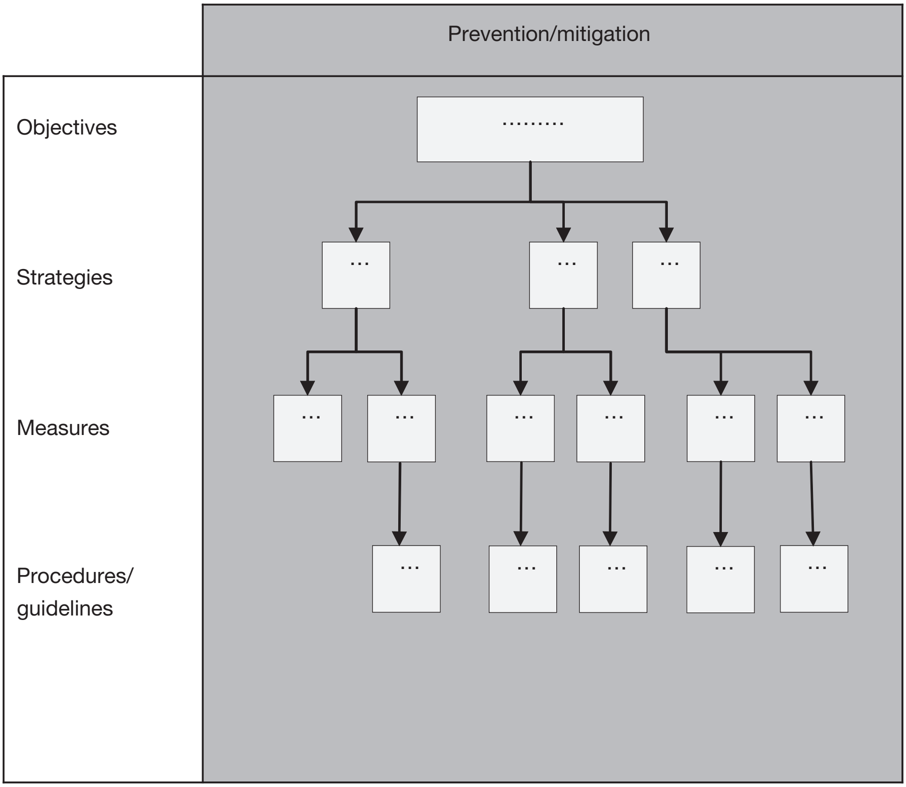

FIG. 1. The top-down approach to accident management.

2.9. When developing guidance on accident management, consideration should be given to the full design capabilities of the plant, using both safety and non-safety systems, and including the possible use of some systems beyond their originally intended function and anticipated operating conditions, and possibly outside their design basis.

2.10. The point at which the transition of responsibility and authority is to be made from the preventive to the mitigatory domain should be specified and should be based on properly defined and documented criteria.

2.11. For any change in the plant configuration or if new results from research on physical phenomena become available, the implications for accident management guidance should be checked and, if necessary, a revision of the accident management guidance should be made.

MAIN PRINCIPLES

2.12. In view of the uncertainties involved in severe accidents, severe accident management guidance should be developed for all physically identifiable challenge mechanisms for which the development of severe accident management guidance is feasible; severe accident management guidance should be developed irrespective of predicted frequencies of occurrence of the challenge.

2.13. Accident management guidance should be set out in such a way that it is not necessary for the responsible staff to identify the accident sequence or to follow some pre-analysed accident in order to be able to execute the accident management guidance correctly.

2.14. The approach in accident management should be based on directly measurable plant parameters or parameters derived from these by simple calculations.[3]

2.15. Development of accident management guidance should be based on best estimate analyses in order to capture the proper physical response of the plant. In the accident management guidance, consideration should be given to uncertainties in knowledge about the timing and magnitude of phenomena that might occur in the progression of the accident. Hence, mitigatory actions should be initiated at parameter levels and at a time that gives sufficient confidence that the protection intended by carrying out the action will be achieved. For example, venting the containment, if necessary to protect the structural integrity of this fission product barrier, should be initiated at a time and at a containment pressure level that gives confidence that the structural integrity of the containment will not be lost.

2.16. Severe accidents may also occur when the plant is in the shutdown state. In the severe accident management guidance, consideration should be given to any specific challenges posed by shutdown plant configurations and large scale maintenance, such as an open containment equipment hatch. The potential damage of spent fuel both in the reactor vessel and in the spent fuel

[3] This is often referred to as a ‘symptom based approach’. The simple calculations are often referred to as ‘computational aids’.

pool or in storage[4] should also be considered in the accident management guidance. As large scale maintenance is frequently carried out during planned shutdown states, the first concern of accident management guidance should be the safety of the workforce.[5]

2.17. Severe accident management should cover all modes of plant operation and also appropriately selected external events, such as fires, floods, seismic events and extreme weather conditions (e.g. high winds, extremely high or low temperatures, droughts) that could damage large parts of the plant. In the severe accident management guidance, consideration should be given to specific challenges posed by external events, such as loss of the power supply, loss of the control room or switchgear room and reduced access to systems and components.[6]

2.18. External events can also influence the availability of resources for severe accident management (e.g. severe droughts can limit available natural cooling water sources, such as rivers and lakes, which are a backup for normal resources; seismic events may damage dams). Such possible influences should be taken into account in the development of the accident management guidance.

EQUIPMENT UPGRADES

2.19. Design features important for the prevention or mitigation of severe accidents should be evaluated. Accordingly, existing equipment and/or instrumentation should be upgraded or new equipment and/or instrumentation should be added, if necessary or considered useful[7] for the development of a meaningful severe accident management programme, i.e. a severe accident management programme that reduces risks in an appreciable way or to an

---

[4] It is prudent also to consider any other potential large source of radiation, although this is not formally a part of severe accident management.

[5] ‘Stop work’ could be one of the first commands in such accident management guidance.

[6] Such limited accessibility could arise from fires, floods or extended area damage caused by, for example, collapse of non-seismically qualified structures in a seismic event.

[7] Equipment may not be necessary, in the strict sense of the word, but can be very useful, for example, passive autocatalytic recombiners remove uncertainties about hydrogen burns.

acceptable level. The decision to add or upgrade equipment may depend on cost–benefit considerations.

2.20. If a decision is taken to add or upgrade equipment or instrumentation, the design specification of such equipment or instrumentation should be such as to ensure appropriate independence from existing systems and preferably appropriate margins with regard to the use of the equipment or instrumentation under accident and/or severe accident conditions. These margins should be such as to provide confidence or, where possible, to enable demonstration that the new equipment or instrumentation will function properly under the anticipated conditions. Where feasible, these conditions should be selected as the design conditions for the equipment under consideration. In that case, proper acceptance criteria for the equipment should be selected that are commensurate with the safety function of the equipment and the level of understanding of the severe accident processes.

2.21. Where existing equipment or instrumentation is upgraded or otherwise to be used outside its normal design basis range, the severe accident management guidance for the use of such equipment should be updated accordingly. Preferably, dedicated operating procedures should be developed for the equipment or instrumentation in the severe accident domain.

2.22. The installation of new equipment or the upgrading of existing equipment should not remove the need for the development of guidance in the case of an equipment malfunction, even if such a malfunction has a low probability.

FORMS OF ACCIDENT MANAGEMENT GUIDANCE

Preventive domain

2.23. In the preventive domain, the guidance should consist of descriptive steps, as the plant status will be known from the available instrumentation and the consequences of actions can be predetermined by appropriate analysis. The guidance for the preventive domain, therefore, takes the form of procedures, usually called emergency operating procedures (EOPs), and is prescriptive in nature. EOPs cover both design basis accidents and beyond design basis accidents, but are generally limited to actions taken before core damage occurs. Further details on EOPs can be found in Refs [10, 11].

Mitigatory domain

2.24. In the mitigatory domain, uncertainties may exist both in the plant status and in the outcome of actions. Consequently, the guidance for the mitigatory domain should not be prescriptive in nature but rather should propose a range of possible mitigatory actions and should allow for additional evaluation and alternative actions. Such guidance is usually termed severe accident management guidelines (SAMGs).

2.25. The guidance should contain a description of both the positive and negative potential consequences of proposed actions, including quantitative data where available and relevant, and should contain sufficient information for the plant staff to reach an adequate decision on the actions to be taken during the evolution of the accident.

2.26. The guidance for the mitigatory domain should be presented in the form of guidelines, manuals or handbooks. The term 'guideline' here is used to describe a fairly detailed set of instructions that describe the tasks to be executed on the plant, but which are still less strict and prescriptive than the procedures found in the EOPs; that is, used in the preventive domain. Manuals or handbooks will contain a more general description of the tasks to be executed and their background reasoning.

2.27. The guidance should be sufficiently detailed to support the responsible members of staff in carrying out deliberations and making decisions in a high stress environment, and should be such as to minimize chances that relevant information is deleted or overlooked.

2.28. The guidance should not be set out in such a form and with such detail that responsible personnel will tend to follow it verbatim, unless that is the intended type of action.

2.29. The overall form of the guidance and the selected amount of detail should be tested in drills and exercises. Based on the outcome of such drills, it should be judged whether the form is appropriate and whether additional detail or less detail should be included in the guidance.

Both preventive and mitigatory domains

2.30. The guidance in both the preventive and mitigatory domains should be supported by appropriate background documentation. This documentation should describe and explain the rationale of the various parts of the guidance, and should include an explanation of each individual step in the guidance, if considered necessary. The background documentation does not replace the guidance itself.

ROLES AND RESPONSIBILITIES

2.31. Accident management guidance should be an integral part of the overall emergency arrangements at a nuclear power plant [14]. The execution of the severe accident management guidance is the responsibility of the emergency response organization at the plant or the utility. Roles and responsibilities for the different members of the emergency response organization involved in accident management should be clearly defined and coordination among them should be ensured.

2.32. Where the members of the emergency response organization are not situated at the same location, a highly reliable communication network between the different locations should be used. The impact of external events, such as extreme weather conditions, seismic events or events that are disruptive to society,[8] should be considered when placing the decision making authority for severe accident management at an off-site location. Guidance should be put in place for measures to be taken if off-site communication fails and only the part of the emergency response organization located at the plant site remains functional.

2.33. The assignment of responsibilities should be compatible with the type of guidance material provided[9] and should be consistent with the other functions described in the documents prepared by the emergency response organization.

2.34. The roles assigned to the members of the emergency response organization may be different in the preventive and mitigatory domains, and where this is the case, transitions of responsibility and authority should be clearly defined.

---

[8] An example of events that would be disruptive to society would be general strikes.

[9] If it has been decided to separate decision making from evaluation, for example, guidance should be available for both functions.

2.35. A specialized team or group of teams (referred to in the following as the technical support centre) should be available to provide technical support by performing evaluations and recommending recovery actions to a decision making authority, in both the preventive and mitigatory domains. The technical support centre should also provide appropriate input to the people responsible for the estimation of potential radiological consequences. For multiple teams, the role of each team should be specified.

2.36. The decision making authority should be placed at an appropriate level commensurate with the complexity of the task and the potential for on-site and off-site releases. In the preventive domain, the control room shift supervisor or a dedicated safety engineer or other designated official should be largely able to carry this responsibility;[10] in the mitigatory domain, decisions should be made by a person at a higher level.

2.37. The operations department should be made responsible for the implementation of the accident management actions that are decided upon.

2.38. Appropriate levels of training should be provided to members of the emergency response organization; training should be commensurate with their responsibilities in the preventive and mitigatory domains.

3. DEVELOPMENT OF AN ACCIDENT MANAGEMENT PROGRAMME

GENERAL REMARKS: PREVENTIVE REGIME

3.1. The preventive accident management guidance should address the full spectrum of credible beyond design basis accident events; that is, all events considered credible on the basis of possible initiating events, and possible complications during the evolution of the event that could be caused by additional hardware failures, human errors and/or events from outside.

[10] Some decisions may be placed at a higher level of authority; for example, where certain actions that are beneficial for accident management may damage components (see also Table 1).

3.2. For determination of the full spectrum of events, useful guidance can be obtained from the probabilistic safety assessment (PSA) Level 1 (if available), or similar studies from other plants, and operating experience from the plant and other plants. A selection of events should be sufficiently comprehensive to provide a basis for guidance for the plant personnel in any identified situation, even if the evolution of the accident would constitute a very unlikely path within the PSA or is not identified in the PSA at all.

GENERAL REMARKS: MITIGATORY REGIME

3.3. The accident management guidance should address the full spectrum of credible challenges to fission product boundaries due to severe accidents, including those arising from multiple hardware failures, human errors and/or events from outside, and possible physical phenomena that may occur during the evolution of a severe accident (such as steam explosions, direct containment heating and hydrogen burns). In this process, issues should also be taken into account that are frequently not considered in analyses, such as additional highly improbable failures and abnormal functioning of equipment.

3.4. For determination of the full spectrum of challenge mechanisms, useful guidance can be obtained from the probabilistic safety assessment (PSA) Level 2 (if available), or similar studies from other plants and insights from research on severe accidents. However, identification of potential challenge mechanisms should be sufficiently comprehensive to provide a basis for guidance for the plant personnel in any identified situation, even if the evolution of the accident would constitute a very unlikely path within the PSA or is not identified in the PSA at all.

3.5. In view of the inherent uncertainties involved in determining credible events, the PSA should not be used a priori to exclude accident scenarios from the development of severe accident management guidance.[11]

3.6. After the accident management guidance has been completed, it should be verified whether indeed all important accident sequences, in particular those obtained from the PSA, are covered and whether risks are reduced accordingly.

---

[11] If such use is considered, very low cut-off levels should be specified so as not to underestimate the scope and nature of scenarios to be analysed.

3.7. Four main steps should be executed to set up an accident management programme:

(1) Plant vulnerabilities should be identified, to find mechanisms through which critical safety functions may be challenged. In the event that these challenges are not mitigated, the core may be damaged and the integrity of fission product barriers may be compromised;
(2) Plant capabilities under challenges to critical safety functions and fission product barriers should be identified, including capabilities to mitigate such challenges, in terms of both equipment and personnel;
(3) Suitable accident management strategies and measures should be developed, including hardware features, to cope with the vulnerabilities identified;
(4) Procedures and guidelines to execute the strategies should be developed.

3.8. Additional important elements that should be considered in the development of an accident management programme include:

(1) Hardware provisions (equipment, instrumentation) for accident management;
(2) The means of obtaining information on the plant status, and the role of instrumentation therein;
(3) Specification of lines of decision making, responsibility and authority in the teams that are in charge of the execution of the accident management measures;
(4) Integration of the accident management programme within the emergency arrangements for the plant;
(5) Verification and validation of procedures and guidelines;
(6) Education and training, drills and exercises;
(7) Supporting analysis for the development of the accident management programme;
(8) A management system for all tasks in the accident management programme;
(9) A systematic approach to incorporating new information and new insights on severe accident phenomena.

3.9. Accident management programmes may be developed first on a generic basis, by a plant vendor or other organization, and may then be utilized by a plant utility for a plant specific accident management programme. Where such a process is followed, care should be taken that the transition from a generic accident management programme to a plant specific accident management programme is handled appropriately. This includes the search for additional vulnerabilities, and strategies to mitigate these.

3.10. To ensure the success of the development of the accident management programme, a 'core development team' of experts with sufficient scope and level of expertise should be assembled.

3.11. The core development team should comprise, apart from any external experts (if an external vendor for accident management guidance is selected), staff responsible for the development and implementation of the accident management programme at the plant, including personnel from the training department (for training operators and engineering staff), operations department, maintenance department and engineering department.

3.12. The staff who will be working in the control room or technical support centre or any other organizational unit responsible for evaluation and decision making in the course of an accident should be involved at an early stage in the development of an accident management programme, as this provides invaluable training for future tasks and feedback. Examples of the composition of a core development team are presented in Ref. [12].

3.13. The development of an accident management programme is a complex task, which requires close cooperation and well organized teamwork among the experts involved. Hence, consideration should be given to the way in which plant personnel will be made available to participate in the development activities of the accident management programme in relation to their normal duties. Sufficient time should be allocated to plant personnel in the core development team in relation to their other obligations.

IDENTIFICATION OF PLANT VULNERABILITIES

3.14. The vulnerabilities of the plant in the case of accidents beyond the design basis should be identified. How specific accidents will challenge critical safety functions should be investigated, and also if these safety functions are lost and not restored in due time, how the core will be damaged and how the integrity of other fission product barriers will be challenged.

3.15. A comprehensive set of insights on the behaviour of the plant during a beyond design basis accident and severe accident should be obtained; these should identify the phenomena that may occur and their expected timing and severity. In the severe accident domain, these insights should be collected and set out in the technical basis[12] for severe accident management.

3.16. The insights should be obtained using appropriate analysis tools. Other inputs should also be used, such as the results of research on severe accidents, insights from other plants and engineering judgement. In developing insights, consideration should be given to uncertainties in severe accident models and in the assumptions made.

IDENTIFICATION OF PLANT CAPABILITIES

3.17. All plant capabilities available to fulfil the safety functions should be investigated, including the use of non-dedicated systems, unconventional line-ups and temporary connections (hoses, mobile or portable equipment) and use of systems beyond their design basis, up to and including the possibility of equipment damage.[13] It should also be considered whether failed systems can be restored to service and, hence, can again contribute to the mitigation of the event. Where unconventional line-ups and temporary connections are identified, consideration should be given to the adaptation of equipment necessary to use these capabilities.

3.18. The severe accident management measures should be robust; that is, they should be defined in such a way that they provide sufficient margin to structural failure of relevant components where such failure can be prevented (e.g. flooding of a steam generator should be done in a timely manner and to such a level that there is ample margin to creep rupture of a steam generator tube,[14] and venting the containment should be done at such a containment pressure level that there is still ample margin to containment failure). Where failure cannot be prevented by the envisaged measures, attempts should be made to delay failure. It should be realized that full control and mitigation of such events may not be possible, despite severe accident management

[12] An example of a generic technical basis that is widely used in Member States is provided in Ref. [15].

[13] An example is the restart of a reactor coolant pump under low pressure, which can enhance core cooling but may damage the pump.

[14] The action to flood the steam generator will effectively protect the steam generator tubes against creep rupture; in addition, however, the action should be initiated well below the threshold above which such creep rupture may occur.

measures and consideration of severe accidents in the design basis of the nuclear power plant.

3.19. The capabilities of plant personnel to contribute to unconventional measures to mitigate plant vulnerabilities, including the behaviour and reliability of personnel under adverse environmental conditions, should also be investigated. Where necessary, protective measures should be provided and training should be specified for the execution of such tasks. It should be noted that work that poses risks to the health or even the life of plant personnel is always voluntary in nature and can never be demanded of the individual; the guidance should be developed accordingly.

DEVELOPMENT OF ACCIDENT MANAGEMENT STRATEGIES

3.20. On the basis of the vulnerability assessment and the understanding of accident phenomena, as well as of the plant capabilities to cope with accidents, suitable accident management strategies should be developed for each individual challenge or plant vulnerability, in both the preventive and mitigatory domains.

3.21. In the preventive domain, strategies should be developed to preserve safety functions that are important to prevent core damage (often called ‘critical safety functions’), such as achieving and maintaining core subcriticality, core cooling, primary inventory and containment integrity. An example of a preventive strategy is ‘feed and bleed’.

3.22. In the mitigatory domain, strategies should be developed to enable:

— Terminating the progress of core damage once it has started;
— Maintaining the integrity of the containment as long as possible;
— Minimizing releases of radioactive material;
— Achieving a long term stable state.

Strategies may be derived from ‘candidate high level actions’, examples of which are given in Appendix II of Ref. [12]. Examples of mitigatory strategies are: filling the secondary side of the steam generator to prevent creep rupture of the steam generator tubes; depressurizing the reactor circuit to prevent high pressure reactor vessel failure and direct containment heating; flooding the reactor cavity to prevent or delay vessel failure and subsequent basemat failure; mitigating the hydrogen concentration; and depressurizing the containment to prevent its failure by excess pressure or to prevent basemat failure under elevated containment pressure.

3.23. The application of a specific mitigatory strategy should be dependent on a single parameter, or on a group of parameters indicative for a certain plant damage state. Plant damage states reflect different phases of increasing severity in the evolution of the accident. They refer to an identification of the state of the core and containment with respect to challenges to the fission product barriers of the plant. Examples are, for the core: in-vessel core cooled and covered, in-vessel core overheated and badly damaged, ex-vessel core cooled and covered, and ex-vessel core overheated; and, for the containment: controlled stable state, controlled not-stable state (i.e. new strategies required but fission product release not imminent), challenged state (new strategies required immediately), and ongoing releases.[15]

3.24. A method for carrying out a systematic evaluation of the possible strategies that can be applied should be developed, taking into consideration the evolution of the accident. Adverse conditions that may hamper the execution of the strategy for that phase of the accident should be considered. In selecting and prioritizing strategies, it should be noted that evaluation is very important owing to the potential for multiple negative impacts of actions, and the increased levels of uncertainty about the plant status and the plant's response to actions.

3.25. Particular consideration should be given to strategies that have both positive and negative impacts in order to provide the basis for a decision about which strategies constitute a proper response under a given plant damage condition. An example is withholding water from the reactor cavity to extend the time to overpressure failure of the containment; this has the negative impact of possible core–concrete interactions that may be irreversible. A further example is flooding the cavity, with the negative impact of possible occurrence of an ex-vessel steam explosion.

[15] Further examples are presented in Appendix I of Ref. [12] and in Refs [15, 20, 26, 27]. Reference [26] also gives an example of a 'single parameter' approach. This approach and the approach based on plant damage states are described in Ref. [27].

3.26. Insights into the plant damage states[16] in the evolution of the accident should be obtained wherever possible. They are helpful, as they can help to select strategies, because some strategies can be effective in one plant damage state, but may be ineffective or even detrimental in another.[17] In addition, such insights are relevant for the estimation of the source term and, if available, should be used for this purpose.

3.27. Priorities should be set between strategies, because possible strategies can have a different weight and/or effect on safety, and because not all strategies can be carried out at the same time. In the preventive domain, the priority of the strategies should be reflected in the priority established for the critical safety functions. In the mitigatory domain, priority should be given to measures that mitigate large ongoing releases or challenges to important fission product barriers (where 'large' means releases with levels of radioactivity that are above the general emergency levels, as defined in the plant emergency plan). The basis for the selection of priorities should be recorded in the background documentation. An example is a set of priorities that follows the evolution of many severe accidents; that is, the first priority is to the first fission product barrier to fail if no mitigatory measures are taken.[18] The setting of priorities should include the consideration of support functions (vital auxiliaries such as AC and DC power and cooling water).

3.28. If strategies are considered that need to be implemented within a certain time window, the possibly large uncertainties in identifying such a window should be taken into account. However, care should be exercised in order not to discard potentially useful strategies.

---

[16] Note the difference between an accident sequence and a plant damage state: the latter is an observable damage condition at the plant, irrespective of the accident sequence that has led to that damage condition.

[17] For example, filling an empty steam generator in a pressurized water reactor is an effective strategy if there is a risk of steam generator tube creep rupture or an existing steam generator tube leak, but is irrelevant if there is no such risk or leak. In a boiling water reactor, it is relevant to know whether the pressure suppression capability still is required. A further example is the recognition of a containment bypass sequence. In all these cases, insights into the plant damage states enhance the execution of an accident management measure.

[18] In high pressure scenarios at pressurized water reactors, these are often the steam generator tubes, by the mechanism of creep rupture. Hence, the first priority then is to prevent such creep rupture by filling the steam generator.

3.29. Where immediate attention and short term actions are needed, there may be no time available for the deliberation of all possible consequences of the actions. The guidance should be developed accordingly. An example is an immediate challenge to a fission product barrier, where ‘immediate’ means that there is no time, or limited time, for evaluation prior to decision making.

3.30. In defining and selecting strategies in the mitigatory domain, it should be noted that safety functions from the preventive domain may remain relevant in the mitigatory domain and, accordingly, the need to maintain these functions should also be incorporated into the mitigatory strategies. For example, subcriticality of the core geometry or core debris configuration should be maintained, and a path should be provided from the core or core debris decay heat to an ultimate heat sink, where possible.[19]

3.31. It should also be noted that actions to fulfil objectives relating to critical safety functions that are adequate in the preventive domain may not be so in the mitigatory domain. For example, it is more difficult to keep the core geometry subcritical when the control rods have melted away but the stack of fuel elements is still intact. Hence, safety functions relating to the emergency operating procedures that are called upon in the mitigatory domain should be reviewed for their applicability and, notably, for limitations and potential negative consequences under the various plant damage states.

DEVELOPMENT OF PROCEDURES AND GUIDELINES

3.32. The strategies and measures discussed in the previous section should be converted to procedures for the preventive domain (EOPs) and guidelines for the mitigatory domain (SAMGs). The procedures contain a set of actions to prevent the escalation of an event into a severe accident. The guidelines contain a set of actions to mitigate the consequences of a severe accident according to the chosen strategies. Procedures and guidelines contain the necessary information and instructions for the responsible personnel, including the use of equipment, equipment limitations, and cautions and benefits. The

[19] The execution of strategies in the mitigatory domain may be different from that in the preventive domain; for example, removal of decay heat may occur through venting the steam from the containment that escapes from a boiling pool covering the melt. Priority is given to an intact containment rather than to the perfect prevention of release of radioactive material.

guidelines also address the various positive and negative consequences of proposed actions and offer options.

3.33. The procedures and guidelines should contain the following elements:

— Objectives and strategies;
— Initiation criteria;
— The time window within which the actions are to be applied (if relevant);
— The possible duration of actions;
— The equipment and resources (e.g. AC and DC power, water) required;
— Actions to be carried out;
— Cautions;
— Throttling and termination criteria;
— Monitoring of plant response.

3.34. The set of procedures and guidelines should include a logic diagram that describes a sequence of relevant plant parameters that should be monitored and which are linked to the criteria for initiation, throttling or termination of the various procedures and guidelines. The sequence should be in line with the priority of associated strategies, procedures and guidelines, as described in paras 3.27 and 3.39.

3.35. In the preventive domain, it may be possible to identify the accident sequence at hand on the basis of an appropriate procedure to diagnose the event. Guidance should be put in place for situations where such a diagnosis cannot be obtained or, when it has been obtained, it later has been found to be incorrect or has been lost in the evolution of the accident. Alternatively, the guidance can be fully linked to the observed physical state of the plant, thus further diagnosis of the accident sequence is not necessary. The guidance should be aimed at preserving or restoring high level safety functions (critical safety functions) on the basis of the selected strategies. The diagnostic procedure should be applied at regular intervals in the evolution of the accident, to make it possible to return to the procedure specifically developed for the observed accident sequence once it has been recognized or recognized again after any initial loss of insight.

3.36. Although in the mitigatory domain it should not be necessary for the responsible staff to identify the accident sequence or to follow a pre-analysed accident scenario in order to be able to use the SAMGs correctly, they should be able to identify the plant damage state for a correct or optimum[20] use of the SAMGs. A temporary loss of insight into the plant damage states should not preclude the execution of the SAMGs.

3.37. In developing the guidance, it should also be recognized that there is a potential for a false diagnosis of scenarios or plant damage states. The potential for such false diagnosis should be minimized, for example, by the use of redundant signals and, possibly, by placing or leaving actions in the guidelines that otherwise would have been removed on the basis of the change in diagnosis.[21] The technical support centre may remove such lower priority items if it has sufficient insight into the evolution of the accident, but should be aware of the possibility of false information.

3.38. Possible positive and negative consequences of proposed strategies should be specified in the guidelines, in cases where the selection of the strategies will need to be done during the evolution of the accident. The technical support centre should check whether additional negative consequences are possible, and should consider their impact.

3.39. Priorities should also be defined among the various procedures and among the various guidelines, in accordance with the priority of the underlying strategies. Conflicts in priorities, if any, should be resolved. The priorities may change in the course of the accident and, hence, the guidelines should contain a recommendation that selection of priorities be reviewed at regular time intervals. The selection of actions should be changed accordingly.

3.40. Interfaces between the EOPs and the SAMGs should be addressed, and proper transition from EOPs into SAMGs should be provided for, where appropriate.[22] Functions and actions from strategies in the EOPs that have

[20] An approach that does not require the recognition of plant damage states will nevertheless benefit from such recognition, as it can delete or deprioritize actions with less relevance for the recognized damage state.

[21] As an example, there are combinations of signals (such a combination is often referred to as a ‘signature’) that resemble vessel failure when in fact the vessel has not failed. Hence, actions that are relevant for an in-vessel phase should still be retained in a guideline developed for the case when vessel failure has been diagnosed, but at a lower priority.

[22] EOPs may contain exits to SAMGs, i.e. if certain steps are not successful, entry into SAMGs is made. An example is a core cooling EOP, where the core exit temperature does not stay below or return below a specified limit (e.g. 650°C).

been identified as relevant in the mitigatory domain should be identified and retained in the SAMGs. Preferably, there should be no formal transition back from the mitigatory domain (SAMGs) to the preventive domain (EOPs), once the EOPs have been exited, although EOPs may still be used as judgement dictates.[23] Where this is nevertheless applied, it should be ensured that the EOPs considered are applicable and valid in the core damage domain, and that the decision making process includes all features necessary in the core damage or mitigatory domain. As EOPs have been designed for a reactor with an intact core, they lose, in principle, their design basis in the mitigatory domain and, hence, should be exited.

3.41. Where EOPs are not exited but are executed in parallel with the SAMGs, their applicability and validity in the mitigatory domain should be demonstrated. In that case, a hierarchy between EOPs and SAMGs should be established, in order to avoid any conflict.

3.42. In addition to entry conditions to the SAMGs, exit conditions and/or criteria to long term provisions should be specified. An example is given in Appendix VII of Ref. [12].

3.43. The transition point from the preventive domain to the mitigatory domain should be set at some time prior to 'imminent core damage' or at the 'beginning of core damage',[24] or at some other well defined point (e.g. the execution of preventive measures has become ineffective or impossible). The selection of the transition point may influence the magnitude and/or sequence of subsequent challenges to fission product barriers. In such cases, this should be taken into account in the selection of the transition point which, therefore, should be placed at a point that is optimal for accident management.[25] Where the transition point is specified on the basis of conditional criteria (i.e. the transition is made if certain planned actions in the EOPs are unsuccessful), the time necessary to identify the transition point and the possible consequences thereof should be taken into account. For example, the rise in core temperature

[23] While transition from the SAMGs back to the EOPs is not recommended, there are cases, such as in-vessel recovery of a degraded core, in which the use of some of the EOPs may be appropriate after use of the SAMGs is finished.

[24] The 'beginning of core damage' can be considered to be, for example, a point at which the calculated molten mass is above 0 kg; this point can be dete rmined using a suitable severe accident computer code.

[25] For some plants, a late transition (i.e. at a high core exit temperature) may invoke an early risk of hydrogen release.

and the associated core damage that will occur during the attempts to prevent core damage should be considered.[26]

3.44. The possibility of transition from EOPs to SAMGs before the technical support centre is operable, that is, before it is ready to make its first recommendation, should be considered in the development of procedures and guidelines. This situation can occur in cases where an event rapidly develops into a severe accident. Any mitigatory guidance provided to control room operators in this case should be presented in a way that makes prompt and easy execution possible and, therefore, should preferably be presented in the same format as operating procedures.

3.45. Procedures and guidelines should be based on directly measurable plant parameters. Where measurements are not available, parameters should be estimated by means of simple computations and/or precalculated graphs. Parameters that can be obtained only after carrying out complex calculations during the accident should not be used as the basis for decisions.[27]

3.46. Procedures and guidelines should be written in a user friendly way and such that they can be readily executed under high stress conditions, and should contain sufficient detail so as to ensure that the focus is on the necessary actions.[28] The procedures and guidelines should be written in a predefined format.[29] Instructions to operators should be clear and unambiguous.

[26] For example, if the transition is to be made when the core exit temperature reaches a certain level and in addition the planned EOP actions fail, the time that is lost in the attempts to prevent core damage should be estimated and the associated core temperature rise should be calculated to determine whether core damage may already have occurred.

[27] The fuel cladding temperature, for example, is not a suitable parameter on which to base decisions, as it can only be determined by carrying out complex calculations.

[28] Where primary injection is recommended, for example, it should be identified whether this should be initiated from dedicated sources (borated water) or alternate sources (possibly non-borated water such as fire extinguishing water). Additionally, the available line-ups to achieve the injection should be identified, and guidance should be put in place to configure unconventional line-ups where these are needed. It should be known how long sources will be available, and what needs to be done either to replace them or to restore them once they are depleted.

[29] A widely used format for a ‘writers’ guide’ for procedures is provided in Ref. [16].

3.47. The SAMGs should be written in such a way that there is provision for sufficient latitude to deviate from an anticipated path where this might be necessary or beneficial. Such flexibility may be necessary owing to the uncertainty in the status of the plant and in the effectiveness and/or outcome of actions, and in order to cover unexpected events and complications. The structure and format of the guidance should be shaped in a way that is commensurate with this uncertainty. Consequently, guidance should not be formulated in such a way that personnel will tend to execute it verbatim.

3.48. Procedures and guidelines should contain guidance for situations where the accident management equipment may be unavailable (e.g. because of equipment failure or equipment lockout). Alternate methods should be explored and, if available, included in the guidance.

3.49. It should be noted that various equipment may start automatically upon certain parameters reaching predefined values ('set points'). Such automatic starts have usually been designed for events in the preventive domain. These automatic actions may be counterproductive in the mitigatory domain. Hence, all automatic actions should be reviewed for their impact in the mitigatory domain and, where appropriate, equipment should be inhibited from automatic start. Manual start of the equipment concerned should then be considered in the SAMG.

3.50. Guidance should be developed to diagnose equipment failure and to identify methods to restore such failed equipment to service. The guidance should include recommendations on the priorities for restoration actions. In this context, the following should be considered:

— The importance of the failed equipment for accident management;
— Possibilities to restore the equipment;
— The likelihood of successful recovery if several pieces of equipment are out of service;
— Dependence on the number of failed support systems;
— Doses to personnel involved in restoration of the equipment.

3.51. Recovery of failed equipment and/or recovery from erroneous operator actions that led to the beyond design basis accident or severe accident should be a primary strategy in accident management, and this should be reflected in the accident management guidance. The time to recover failed equipment may be outside the time window to prevent core damage. If this is the case, an earlier transition to the mitigatory domain can be decided upon than one based on plant parameters.

3.52. Relevant management levels in the operating organization of the plant, as well as outside organizations responsible for the protection of the public, should also be made aware of the potential need for early transition to the mitigatory domain. Late transition to the mitigatory domain can lead to serious degradation of safety and the potential for on-site and off-site releases. Identification of an earlier transition should be covered as such in the emergency plan for the plant.

3.53. In the development of procedures and guidelines, account should be taken of the habitability of the control room and the accessibility of other relevant areas, such as the technical support centre or areas for local actions. It should be investigated whether expected dose rates and environmental conditions inside the control room and in other relevant areas may give rise to a need for restrictions for personnel. It should be determined what the impact of such situations will be on the execution of the accident management programme; the need for replacement of staff for reasons of dose should also be considered.

3.54. In the case where several units are in operation at the same site, the use of a unit that has not been affected should be taken into account in the accident management guidance. It should also be considered whether or not the neighbouring unit has to be shut down. Special care should be taken to identify limitations on non-standard equipment that might be shared between units. For example, a cross-tie of heat removal systems from an unaffected unit may be useful for heat removal from the affected unit but this may require that the unaffected unit will remain at a certain predefined power level.

3.55. As part of the severe accident management guidance and further to the estimation of parameters addressed in para. 3.45, precalculated graphs or simple formulas should be developed, where appropriate, to avoid the need to perform complex calculations during the accident in a potentially high stress situation. These are often called ‘computational aids’ and should be included in the documentation of the SAMGs. Examples are provided in Appendix III of Ref. [12]. Computer based aids should take into account the limited battery life of self-contained computers (laptops) and the potential for loss of AC power during severe accident scenarios.

3.56. Rules of usage should be defined for the application of SAMGs. Such rules define what needs to be done in the actual application of the guidelines. Questions to be answered are, for example:

— If an EOP is in execution but the point of entry to SAMGs is reached, should actions in the EOP then be interrupted, continued if not in conflict with the applicable SAMG, or continued in any case?
— Should restorative actions started in the EOP domain be continued in the SAMG domain?
— If an SAMG is in execution, but the point of entry for another SAMG is also reached, should that other SAMG then be executed in parallel?
— Should the consideration to initiate another SAMG be delayed while parameters that called upon the first one are changing value?

3.57. Adequate background material should be prepared in parallel with the development and writing of individual guidelines. The background material should fulfil the following roles:

— It should be a self-contained source of reference for:
  - The technical basis for strategies and deviations from generic strategies, if any;
  - A detailed description of instrumentation needs;
  - Results of supporting analysis;
  - The basis for and detailed description of steps in procedures and guidelines;
  - The basis for calculations of set points;
— It should provide a demonstration of compliance with the relevant quality assurance requirements;
— It should provide basic material for training courses for technical support staff and operators.

HARDWARE PROVISIONS FOR ACCIDENT MANAGEMENT

3.58. The plant should be equipped with hardware provisions in order to fulfil the fundamental safety functions (control of reactivity, removal of heat from the fuel, confinement of radioactive material), as far as is reasonable for beyond design basis accidents and severe accidents. Dedicated systems and/or design features for managing severe accidents should be put in place, in particular for new plants.

3.59. In new plants there are usually design features present that practically eliminate some severe accident phenomena, and/or dedicated equipment is available for managing beyond design basis accidents and severe accidents. However, for some existing plants, it may be concluded that it is not possible to develop a meaningful[30] severe accident management programme for the plant in its existing hardware configuration and layout.[31] In that case, modification of the plant should be considered accordingly.

3.60. Hardware provision should also be considered where essential functions (e.g. removal of decay heat) need to be available for an extended time[32] and the equipment normally foreseen for this function cannot be anticipated to remain available for such a long time. In estimating the long term availability of components,[33] the limited possibility — or impossibility — of maintenance should be taken into account.

3.61. Changes in design should also be proposed where uncertainties in the analytical prediction of challenges to fission product barriers cannot be reduced to an acceptable level.

3.62. Suitable analysis methods that utilize appropriate safety or risk metrics exist and these should be used to aid in decision making regarding upgrades. Consideration should be given to the fact that analysis in the field of severe accident management is usually not conservative but of best estimate type, and does not in itself create margins.[34]

---

[30] ‘Meaningful’ is to be understood as ‘reducing risk in an appreciable way or to an acceptable level’.

[31] An example is a reactor with a small containment which is vulnerable to hydrogen explosions. Inertization may then be needed.

[32] Active decay heat removal, for example, may need to be provided for many months, before removal by natural processes can be counted on.

[33] This is most relevant for active components, but passive components may also be damaged (e.g. clogging of heat exchangers by debris in the circulating water).

[34] Margins may be conservative in one direction but non-conservative in another. For example, an assumption that hot leg creep failure will not prevent steam generator creep failure may be conservative in defining strategies to prevent steam generator creep failure but it may be non-conservative in addressing the ultimate location of core debris on reactor vessel failure, as hot leg failure may disperse much core debris through the containment, whereas steam generator tube creep rupture will not do so.

3.63. Equipment upgrades aimed at enhancing preventive features of the plant should be considered as tasks with high priority. Examples are qualification of pressurizer valves for feed and bleed operation and additional redundancies on important safety systems (AC and DC power, available cooling water).

3.64. For the mitigatory domain, in upgrading equipment the focus should be placed on preservation of the containment function and, in particular, the following functions should be taken account of:

- Containment isolation in a severe accident, including bypass prevention;
- Monitoring parameters in the containment, allowing an early diagnosis of the unit status including the concentration of fission products and hydrogen;
- Ensuring the leaktightness of the containment, including preservation of the functionality of isolation devices, penetrations and personnel locks, for a reasonable time after a severe accident;
- Management of pressure and temperature in the containment by means of a containment heat removal system;
- Control of the concentration of combustible gases, fission products and other materials released during severe accidents;
- Containment overpressure and underpressure[35] protection;
- Prevention of high pressure core-melt scenarios;
- Prevention of vessel melt through;
- Prevention and mitigation of containment basemat melt through by the molten core;
- Monitoring and control of containment leakages.

3.65. In view of the utmost importance of the integrity of the containment, all measures that can be realized with acceptable costs should be taken to ensure this, unless justified otherwise. Acceptable costs are, as a minimum, to be defined as the cost of radiation dose to the general public in the vicinity of the plant[36] that would be averted by implementation of such measures. The regulatory body should identify acceptable methods of evaluating such averted radiation exposures[37] and should determine the value of the averted dose.[38] In

[35] This refers to subatmospheric pressure after containment venting and subsequent condensation of steam in the containment.

[36] Some countries define the vicinity of a plant as the area within 80 km of the plant.

[37] A suitable method is one whereby the utility proposes such a method, which then is approved (or amended) by the regulatory body.

[38] For example, a value of US $100 000 per man-sievert averted is sometimes used.

defining the value of the averted dose, all costs and other consequences should be considered, including long term effects for public health and safety that, upon the occurrence of a severe accident, would arise from releases that would be averted by these measures.[39] The ultimate goal of this method is to ensure that containment failures are extremely improbable.

3.66. Appropriate measures should be taken to remove the decay heat from the core debris to an ultimate heat sink. Where it is decided to or considered necessary to remove the decay heat by repeated or continuous venting of the containment atmosphere, such venting should, in principle, take place through a pathway that can provide appropriate reduction in the fission product releases, for example, by filtering or scrubbing.

3.67. Examples of possible design changes that can be implemented in existing plants are: a hardened and/or filtered containment vent; passive autocatalytic recombiners; igniters; a passive containment cooling system; reactor cavity flooding; isolation of pathways to the environment that may exist after basemat failure;[40] larger station batteries or alternate power supplies; and enhanced instrumentation (extended scale or new measurements), such as enhanced instrumentation for the steam generator level. A modification can fulfil several functions. For example, a filtered containment vent can be used to prevent containment overpressurization, but also to release hydrogen (or oxygen) to reduce the hydrogen risk, to prevent unfiltered leakage from existing openings or from a containment that has a pre-existing (relatively) large leakage rate, or to prevent basemat failure — if anticipated to occur — at an elevated containment pressure.

3.68. If equipment and systems used to cope with design basis conditions are supplemented by additional equipment to mitigate severe accidents, the latter equipment should preferably be independent.

3.69. For dedicated or upgraded equipment, there should be sufficient confidence in the equipment and, where possible, demonstration of its capability to perform the required actions in beyond design basis and severe

[39] At the discretion of the government, costs and other consequences that are associated with protecting, maintaining and/or restoring the environment may also be included, as such costs can be extremely high.

[40] Some plants have a direct pathway to the environment at melt through of the concrete below the cavity.

accident conditions should be provided. Demonstration of the capability of equipment should be provided where other assessment methods cannot provide sufficient confidence. However, the level of qualification applied to such equipment need not necessarily be the same as that typically required for components and systems that cope with design basis conditions. Similarly, requirements on the redundancy of such systems may also be relaxed compared to the requirements applied in the design basis domain.

3.70. The required accuracy of various instruments used for severe accident management should be recognized in assessing instrumentation capabilities. In many cases, proper instrument indication that permits accurate trending may be more important than the accuracy of the indicated values.

ROLE OF INSTRUMENTATION AND CONTROL

3.71. Since the SAMGs depend on the ability to estimate the magnitude of several key plant parameters, the plant parameters needed for both preventive accident management measures and mitigatory accident management measures should be identified. It should be checked that all these parameters are available from the instrumentation in the plant. Where instruments can give information on the accident progression in a non-dedicated way, such possibilities should be investigated and included in the guidance.[41]

3.72. The existing qualification for relevant instruments should be taken into account, and it should be recognized that such equipment may continue to operate well beyond its qualified range. Alternative instrumentation should be identified where the primary instrumentation is not available or not reliable. Where such instrumentation is not available, alternative means should be developed, for example, computational aids.

3.73. Use of instrumentation that is qualified for the expected environmental conditions is the preferred method to obtain the necessary information.

3.74. The effect of environmental conditions on the instrument reading should be estimated and included in the guidance. It should be taken into consideration that

[41] Ex-core neutron detector readings, for example, are influenced by the location of core debris in the vessel and the amount of remaining water, so these readings could be used to acquire information about the evolution of the accident.

a local environmental condition can deviate from global conditions and, hence, instrumentation that is qualified under global conditions may not function properly under local conditions.[42] The expected failure mode and resultant instrument indication (e.g. off-scale high, off-scale low, floating) for instrumentation failures in severe accident conditions beyond the design basis should be identified.

3.75. Severe accidents may present challenges to instrumentation beyond its design basis where such instruments may operate outside their design operating range. As the indication from instruments then may be in error, all indications used to diagnose plant conditions for severe accident management should be benchmarked against other direct or derived indications in order to reduce the risks associated with faulty readings. In practice, every key instrumentation reading from a non-qualified dedicated instrument that is used for diagnosis or verification should have an alternate method to verify that the primary reading (i.e. the reading from the dedicated instrument) is reasonable.[43] When an alternative means of obtaining a key parameter value cannot be identified, consideration should be given to upgrading or replacing the instruments in order to provide that alternative indication.

3.76. In the development of the SAMGs, the potential failure of important non-qualified instrumentation during the evolution of the accident should be included and, where possible, alternative strategies that do not use this instrumentation should be developed.[44] The ability to infer important plant parameters from local instrumentation or from unconventional means should also be considered. For example, the steam generator level can be inferred from local pressure measurements on the steam line and steam generator blowdown lines.

3.77. The need for development of computational aids to obtain information where parameters are missing or their measurements are unreliable should be

[42] High pressure melt ejection, for example, will spread debris all around the containment and while global conditions may remain within qualification envelopes, the local environment can be quite challenging (e.g. radiation due to locally deposited fission products, excessive heating due to decay heat from deposited fission products).

[43] The recommendation is for the reading to be 'reasonable' rather than 'accurate', since precision is not generally needed.

[44] An example is the steam generator level indication: if this is lost, the policy at some plants is to stop all feedwater and allow the steam generator to empty; at other plants it is assumed that the steam generator is empty and so it will continue to be fed, which includes accepting the risk of overfill of the steam generator. The applicable SAMGs should be developed accordingly.

identified and appropriate computational aids should be developed accordingly.

RESPONSIBILITIES AND LINES OF AUTHORIZATION

3.78. Functions and responsibilities in accident management, in both the preventive and mitigatory domains, should be clearly defined within the documentation of the accident management programme and of the overall emergency response organization. Where off-site organizations have responsibilities in accident management, this should be described. An example of a typical layout of the technical elements of the on-site emergency response organization is shown in Fig. 2.

3.79. The roles of personnel involved in severe accident management should be considered in three categories:

(1) Evaluation/recommendation (assessment of plant conditions, identification of potential actions, evaluation of the potential impacts of these actions, and recommendation of actions to be taken and, after

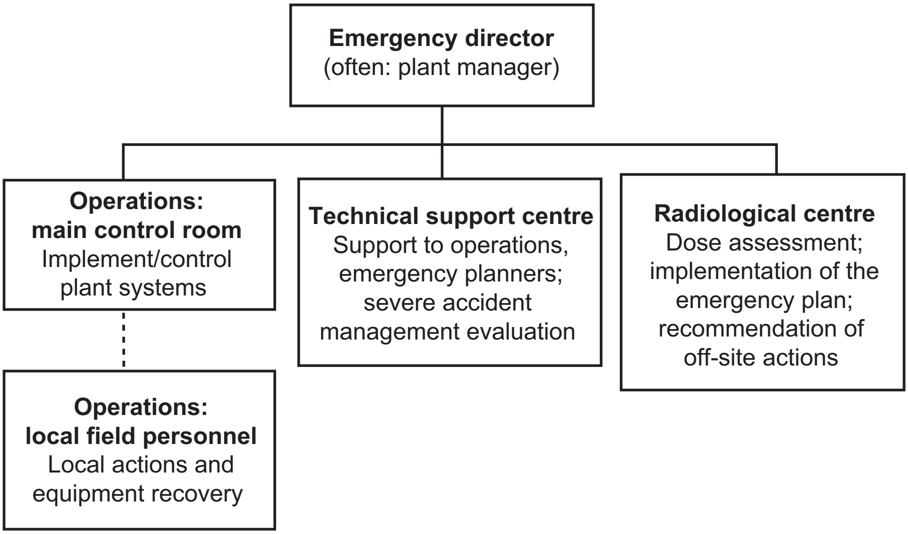

FIG. 2. Typical layout of the technical elements of the on-site emergency response organization.

implementation, assessing the outcome of actions; personnel in charge of these duties are often called ‘evaluators’);

(2) Authorization (decision making: approving the recommended action for implementation; personnel in charge of these duties are often called ‘decision makers’);

(3) Implementation of the actions (operation of the equipment as necessary, including verification of operation; personnel in charge of these duties are often called ‘implementers’).

Further recommendations for the use of SAMGs are given in the Appendix.

3.80. Preventive accident management is characterized by the need to take actions where the priority is on restoring core cooling and maintaining fuel integrity. The primary measures used in preventive accident management are EOPs. Decision making should be carried out by the control room staff (i.e. the shift supervisor or shift manager, or a particular dedicated person such as a safety engineer). For complex situations, where it is deemed appropriate, decision making may be placed at a higher level of authority. In the preventive domain, the technical support centre should be made available to provide technical support to the control room staff.

3.81. In an event that degrades into a severe accident, transfer of responsibilities and decision making authority from the control room staff to a higher level of authority should be made at some specified point in time, as decision making is highly complex in view of the uncertainties involved, and because it may involve actions with consequences that go beyond the information available in the control room or even at the plant.[45] In the mitigatory domain, the technical support centre should be charged with performing evaluations and recommending recovery actions to the decision making authority.

3.82. This decision making authority in the mitigatory domain should lie with a high level manager, here denoted as the emergency director. The emergency director should be granted the authority to decide on the implementation of severe accident management measures proposed by the technical support centre or, if needed, based on the director’s own deliberation. The emergency

[45] For example, the intention to vent the containment at a certain moment and for a certain time on the basis of plant parameters may not be in line at that moment with proposed actions of the off-site emergency response organization.

director should have a broad understanding of the actual status of the plant and of other relevant aspects of the emergency response, including off-site effects.[46]

3.83. In the mitigatory domain, the control room staff should provide input to the evaluations of the technical support centre on the basis of their knowledge of the capabilities of plant equipment and instrumentation, and their other special skills from their training, and given that they may have experienced the early phases of the accident. In principle, consensus should be sought between the observations or assessments of the control room staff and the evaluations or recommendations of the technical support centre. Control room staff should not wait for questions or instructions from the technical support centre, but rather should approach the technical support centre on their own initiative with insights and findings which they consider useful.

3.84. All transfers of authority should be clearly defined where the roles and responsibilities assigned to the members of the on-site emergency response organization are different in preventive and mitigatory domains.

3.85. The severe accident management programme should not assign responsibilities in a way that is inconsistent with the requirements of the operator licence. However, the operator licence should not be restrictive on the required responsibilities and should be adapted where useful or necessary for an adequate severe accident management programme. For example, operators should be allowed to violate limits and conditions for normal operation to mitigate a severe accident, subject to appropriate controls and oversight.

3.86. In transferring authority to the emergency director, the actions and functions that could or should remain in the control room and that can be decided upon by the control room staff independently of the emergency director should also be specified.[47] As the control room staff is also responsible for the execution of the measures decided upon by the emergency director, consistency and a hierarchy between the two groups of actions should be established.

---

[46] The emergency director also has responsibilities for notifying off-site teams. The emergency plan describes this (see Ref. [14], para. 4.23).

[47] These include activities that control room staff can carry out independently, such as maintaining support conditions (e.g. room cooling, service water) and responding to some alarms; activities that the control room staff should not do on their own (e.g. starting up major equipment) should also be specified.

3.87. It should be noted that a transfer of responsibilities in the course of a complex accident in itself poses risks. Hence, such a transfer should take place at a point in time that minimizes such risks and, thus, is optimal from the viewpoint of severe accident management. Ideally, the transfer should not create a ‘vacuum’ in decision making and necessary actions. Hence, formal transfer should not take place until the new decision maker is ready to formulate the first decision. Any transfer of responsibilities should be consistent with the transitions required in the emergency plan (see Ref. [14]).

3.88. Criteria for activation of the technical support centre should be specified, and severe accident management measures should continue to be carried out by the control room staff until the technical support centre is functional. Such measures should be written in a format that is familiar to the control room staff (e.g. in the same format as the EOPs).

3.89. Support from the plant vendor or other equivalent support should be sought for the implementation of additional qualified accident management recommendations, if such support is not already part of the emergency response organization. The mechanisms for calling on support should be well established, and the support capabilities should be tested from time to time. The vendor or equivalent organization providing such support should be kept up to date with all relevant changes at the plant.

3.90. The responsibilities defined in the documentation of the severe accident management programme should be reflected in the emergency plan, since this is the document that defines the overall emergency response organization of a nuclear power plant. A review of the emergency plan should be performed with respect to the actions that should be taken according to the accident management programme, to ensure that conflicts do not exist.

3.91. The technical support centre personnel should have a detailed knowledge of the EOPs and the SAMGs, and they should have access to the information on plant status. They should have a good understanding of the underlying severe accident phenomena dealt with in the SAMGs. Also, they should be made responsible for monitoring the effectiveness of severe accident management measures once these have been initiated. The team of the technical support centre should communicate extensively with the control room staff, to benefit from their expertise in and insight into the capabilities of the plant.

3.92. The decision makers should ensure that they understand the consequences and uncertainties inherent in their decisions; the implementers should ensure that they understand the actions that they may be asked to take; and the evaluators should ensure that they understand the technical grounds upon which they will make their recommendations.

3.93. Rules for information exchange between the various teams of the emergency response organization should be defined. The mechanisms for ensuring the flow of information between the technical support centre and the control room as well as from the technical support centre to other parts of the emergency response organization, including those responsible for the execution of on-site and off-site emergency plans, should be specified. Oral communication between the technical support centre and the control room staff should be undertaken by a member of the technical support centre who is a licensed operator or similarily qualified person. As the occurrence of a severe accident will generate extensive communication between on-site and off-site teams, care should be taken that this communication does not disrupt the management of the accident at the plant.

3.94. If there is to be any involvement of the regulatory body in the decision making,[48] how this is to be done should be defined.

3.95. If there is more than one unit at a site, the site emergency plan should include the necessary interfaces between the various parts of the overall emergency response organization.

3.96. The accessibility and habitability of the physical locations of the teams of evaluators and implementers as well as of the emergency director under severe accident conditions should be checked and maintained.[49] The possible loss of AC power should be considered in providing for communication between the control room and the technical support centre.

---

[48] Some Member States have specific regulations on regulatory body involvement; in other cases, involvement of the regulatory body may not be required but may be prudent (e.g. for containment venting).

[49] A widely applied arrangement is that the team of evaluators is located in the technical support centre room, and the team of implementers is in the control room of the plant. Examples of how this can be organized in accordance with the accident management programme are provided in Ref. [12].

3.97. Information about the performance of the instrumentation and control and other equipment (possibly already summarized in the SAMGs for easy reference) should be made available to the technical support centre. It is advantageous if the technical support centre has direct access to plant information. The availability and use of such information should be considered in the development of SAMGs. The plant information in the technical support centre should be captured and monitored appropriately, for example, by electronic data transfer. Where manual transfer of data is needed, this should preferably be done by a dedicated member of the technical support centre.

3.98. Table 1 presents characteristics of the preventive and mitigatory domains.

VERIFICATION AND VALIDATION

3.99. All procedures and guidelines should be verified. Verification should be carried out to confirm the correctness of a written procedure or guideline and to ensure that technical and human factors have been properly incorporated [10]. The review of plant specific procedures and guidelines in the development phase, in accordance with the quality assurance regulations, forms part of this verification process. In addition, independent reviews should be considered, where appropriate, in order to enhance the verification process.

3.100. All procedures and guidelines should be validated. Validation should be carried out to confirm that the actions specified in the procedures and guidelines can be followed by trained staff to manage emergency events [10].

3.101. Possible methods for validation of the SAMGs are the use of a full scope simulator (if available), an engineering simulator or other plant analyser tool, or a tabletop method. The most appropriate method should be selected. On-site tests should be performed to validate the use of equipment. Scenarios should be developed that describe a number of fairly realistic (complex) situations that would require the application of major portions of the EOPs and the SAMGs. The scenarios encompass the uncertainties in the magnitude and timing of phenomena (both phenomena that result from the accident progression and phenomena that result from recovery actions).

3.102. Members of staff involved in the validation of the procedures and guidelines should not be those who developed the procedures and guidelines.

TABLE 1. CHARACTERISTICS OF THE PREVENTIVE AND MITIGATORY DOMAINS

Subject/Attribute	Preventive domain	Mitigatory domain
Aim	Prevention of core damage, through fulfilment of a set of safety functions of primary importance (‘critical safety functions’)	Limitation of releases of radioactive material to the environment through actions comprising termination of core melt progression, maintenance of reactor pressure vessel integrity, maintenance of containment integrity and control of releases
Establishment of priorities	Establishment of priorities among the various ‘critical safety functions’	Establishment of priorities between mitigatory measures, with the highest priority to mitigation of significant ongoing releases and immediate threats to fission product barriers
Responsibilities	Control room staff or leader of the emergency response organization, if deemed appropriate	Emergency response organization, with control room staff available for advice and execution of measures
Role of emergency response organization	Emergency response organization available for advice to control room, or decision making for complex tasks, if deemed appropriate	Emergency response organization responsible for decision making
Procedures/guidelines	Use of procedures for accident management measures (EOPs) in control room	Use of guidance documents (SAMGs) by emergency response organization or other designated staff

TABLE 1. CHARACTERISTICS OF THE PREVENTIVE AND MITIGATORY DOMAINS (cont.)

Subject/Attribute	Preventive domain	Mitigatory domain
Use of equipment	Use of all systems still available, use of design margins admissible; possible use of beyond design margins upon advice, or decision, by emergency response organization Measures beyond the defined scope require advice, or instructions, by the emergency response organization	Use of all systems still available, also beyond their design limits
Verification of effectiveness	The effectiveness of the accident management measures can be verified with reasonable accuracy	The effectiveness of the accident management measures can be verified in a limited way Positive and negative consequences of proposed actions to be considered in advance and monitored throughout and after implementation of measures

3.103. The findings and insights from the verification and validation processes should be documented and used for providing feedback to the developers of procedures and guidelines for any necessary updates before the documents are brought into force by the management of the operating organization.

EDUCATION AND TRAINING

3.104. For each group involved in accident management, including the management of the operating organization and other decision making levels, and also, where applicable, regulatory personnel, specific objectives and training needs should be defined. The training should be commensurate with the tasks and responsibilities of the functions; hence, in-depth training should be provided for the key functions in the severe accident management programme, that is, the technical support centre evaluators, decision makers and implementers. Regulators, where they participate in utility decisions, should be trained so that they fully understand the basis of proposed utility decisions.

3.105. Training should be developed by professional trainers. Experts in the subject matter can assist in the development of training material and should be called on to review the final training material. Subject matter experts should also be available to respond to student questions that are beyond the capability of the professional trainers.

3.106. Training should be developed using a systematic approach to training (e.g. as defined in Ref. [17]). This includes identifying training needs, defining the training objectives, identifying the technical basis for training material, developing training material, specifying the appropriate venue for delivering training and measuring the effectiveness of training to provide feedback to the training process.

3.107. Training needs and objectives should be specified in due time, preferably already in the development phase of the accident management programme. The training programme should be put in place prior to the accident management programme being implemented. All training material should be developed using a well defined approach to training. More details about training specific to accident management can be found in Refs [18, 19].

3.108. Initial training as well as refresher training should be developed. Refresher training should take place at regular intervals that are compatible with the plant's overall training programme. A maximum interval for refresher training should be defined; depending on the outcome of exercises and drills held at the plant, a shorter interval may be selected.

3.109. Exercises and drills should be based on appropriate scenarios that will require the application of a substantial number of procedures and guidelines. Results from exercises and drills should be fed back into the training programme and, if applicable, into the procedures and guidelines as well as into organizational aspects of accident management.

3.110. The effectiveness of an exercise should not be judged on the basis of the manner in which the responsible team was able to regain control of the plant, but in the way that people were able to understand and follow the events in the plant, could handle complications and unexpected events in a controlled way, were able to reach sound decisions, and initiated a series of well founded actions.

PROCESSING NEW INFORMATION

3.111. For any change in plant configuration, the effect on EOPs and SAMGs as well as on organizational aspects of accident management should be checked. A revision of the documents should be made if it is found that there is an effect on these procedures and guidelines.

3.112. After any revision of background documentation used in the development of the procedures and guidelines, it should be verified whether revision of the procedures and guidelines is necessary. An example is a plant that has based its procedures and guidelines on a reference design or some other generic source of information, where the originator of the procedures and guidelines on the reference design issues a revision of the accident management programme. Another example is an update of the PSA that identifies new accident sequences that were not a part of the basis of the existing accident management guidance.

3.113. International research on severe accident phenomena should be followed actively and new insights should be processed accordingly in the accident management programme.

3.114. Exchange of information with peers should be used to improve the SAMGs for future revision. Such an exchange of information could take the form of peers observing plant drills, and participation in exercises at other plants.

SUPPORTING ANALYSIS

3.115. Analysis of a potential beyond design basis accident or severe accident sequence typically has one of the following objectives: (1) formulation of the technical basis[50] for development of strategies, procedures or guidance; (2) demonstration of the acceptability of design solutions to support the selected strategies, procedures and guidelines in accordance with the established criteria; or (3) determination of the reference source terms for emergency plans. While the basic approach (the use of best estimate analysis) is the same for all three objectives, the scope and assumptions for various applications of the analysis will be different for each objective. Later stages of the analysis aim to provide only analytical support for accident management.

3.116. In order to develop the technical basis documents for the accident management programme, a range of accident sequences should be analysed.

3.117. In the first step of the analysis of a potential beyond design basis accident or severe accident sequence, a set of sequences should be analysed that would, without credit for operator intervention in the beyond design basis accident or severe accident domain, lead to core damage and subsequent potential challenges to fission product barriers. Following the general remarks in paras 3.1–3.4 of this Safety Guide, the full set of core damage sequences typically identified in the PSA, where available, should be considered. Note that selection of sequences that would, without intervention, lead to core damage is an appropriate way of identifying accident scenarios for subsequent investigation of both preventive actions (taken before core damage) and mitigatory actions (taken after core damage).

3.118. In addition, severe accident conditions that result from operator errors prior to core damage should be considered in developing strategies for severe accident management. Severe accident conditions can result from either operator errors of omission or errors of commission.

[50] A technical basis includes analyses, evaluations, assessments and engineering judgement.

3.119. A method to select accident sequences, or classes of sequences, to be analysed should be chosen, since the number of sequences leading potentially to the release of fission products to the environment is virtually limitless. A scheme for categorizing accident sequences is typically based on several plant state designators such as groups of initiating events, the status of emergency core cooling, the status of the secondary heat sink, and the status of the containment heat removal and the containment boundary.

3.120. Every categorization scheme, however, should result in a list of groups of accident sequences that address plant behaviour and response, including core degradation and melting, reactor vessel failure and containment boundary failure, and the associated severe accident phenomena. Different categorization schemes are conceivable.[51] A typical Level 2 PSA will also contain such a categorization scheme.

3.121. The selection of accident sequences should be performed in the following three steps:

(1) A suitable categorization approach and a set of damage states should be developed. One method of achieving this is summarized in the Annex.
(2) The full list of damage states should be screened to identify a limited set, considering contribution to core damage frequency and ensuring that all initiators are represented.
(3) One or more accident sequences per retained damage state should be chosen, considering the total contribution to core damage frequency, the ability of the chosen sequence to represent other sequences in the same damage state, and the amenability of the chosen sequence to preventive accident management measures.

3.122. In the second step of the analysis of a potential beyond design basis accident or severe accident sequence, the effectiveness of proposed strategies and their potential negative consequences[52] should be investigated. The analysis performed at this step should also support development of the actual

[51] Examples of categorization schemes are described in Refs [20–23].

[52] For example, bleed and feed may be an effective countermeasure for loss of decay heat removal along normal ways, but it is sometimes only effective in a certain time window. Another example in the severe accident domain is the restart of a reactor coolant pump, which may be very beneficial at the beginning of an accident, but may greatly increase the risk of creep rupture of the steam generator tube if done later.

procedures and guidelines, since proper set points to initiate, throttle or terminate actions need to be determined. The potential availability and functionality of equipment and instrumentation, as well as the habitability of workplaces under the prevailing accident conditions, should be investigated.

3.123. In the third step of the analysis of a potential beyond design basis accident or severe accident sequence, once the procedures and guidelines have been developed, they should be verified and validated, as described in paras 3.99–3.103. Validation requires the development of suitable scenarios. Analysis is necessary to determine the evolution of the accident and the various phenomena to which the operators and technical support centre may need to respond.

3.124. If a generic technical basis is available, it may be used to obtain the insights mentioned in steps (1) to (3) of para. 3.121, provided it is adapted to the specific plant at hand.

3.125. Generally, analysis should be of a best estimate type, as it is important to retain the best available physical picture of the response of the plant. Best estimate calculations usually yield the mean or median value of a possible range of values. Hence, appropriate consideration should be given to uncertainties in the determination of the timing and severity of the phenomena. This consideration should include the uncertainties in the understanding of phenomena that may occur in both the progression of the accident (e.g. high pressure melt ejection) and the recovery phase (e.g. the generation of steam and hydrogen as a result of adding water to an overheated core).

3.126. Computer codes used for analysis should be validated to the extent possible. However, it should be noted that many codes used in the beyond design basis accident and severe accident cannot be subjected to the same level of validation as the codes used in the design basis domain,[53] due to uncertainty in the understanding of the phenomena. Usually, no single code can cope with the entire range of phenomena, and special purpose codes may also need to be used. The operating organization of the plant should specify the proper codes

[53] For example, subject matter experts are not all in agreement on the coolability of ex-vessel core debris for various possible scenarios, yet most simulation codes contain models that predict either coolability or non-coolability for each scenario. Thus, there is no basis upon which to verify the code models.

and models for the various applications, and should justify their use. Where relevant, the operating organization of the plant should carry out a sensitivity analysis in addition to the uncertainty analysis, to find the relative weight of certain phenomena compared to others.

3.127. Computer code results should be interpreted with consideration given to model limitations and uncertainties. Mechanistic codes should be used where otherwise code limitations would prevent the attainment of trustworthy results. All code results should be evaluated and interpreted with due consideration given to code limitations and the associated uncertainties. For example, many codes have fixed heat transfer correlations (e.g. critical heat flux on a flat plate) based on an assumed geometry, whereas the actual event may involve geometry changes (e.g. shattering of core debris), which create varying heat transfer surfaces that will enhance or degrade heat transfer and, hence, influence the actual temperatures attained.

3.128. In addition to accident analysis in the areas of neutronics, thermo-hydraulics, core degradation, etc., structural analysis should be performed for phenomena that present mechanical loads.[54]

3.129. Analysis should be performed to investigate the effectiveness of the accident management guidance and, where feasible, the associated reduction of risks at the plant (see para. 3.6). Analysis should also be used to demonstrate that dominant scenarios are mitigated.

MANAGEMENT SYSTEM

3.130. Development of an accident management programme should follow the applicable IAEA safety requirements and guidance on this subject [24, 25]. Where these cannot be followed due to the uncertainties in the severe accident domain, the intent of the safety requirements should be followed to the extent practicable.

[54] For example, if hydrogen combustion is calculated to occur, combustion loads should be calculated and it should be investigated whether the containment or other relevant structures will survive the loads. Often, the capability of structures to accommodate the loads is presented as a fragility curve depicting probability of failure.

Appendix

PRACTICAL USE OF THE SAMGs[55]

A.1. Once the main control room staff, while executing the EOPs, has reached the point of entry to the SAMG domain or the emergency director has determined that the SAMGs should be applied, or SAMG entry is reached by some other specified basis (para. 3.40), the transition from the EOP domain to the SAMG domain should be made. The main control room staff should initiate actions under the SAMGs that apply until responsibility for recommending actions shifts to the technical support centre. This occurs when the technical support centre is operable,[56] is informed about the facts, has evaluated the plant status and is ready to give its first recommendation or decision on execution of an SAMG. The main control room staff should continue to work with actions already initiated in the EOP domain, provided they are consistent with the 'rules of usage' (para. 3.56).

A.2. The technical support centre should consult the logic diagram (para. 3.34) at regular time intervals as the accident progresses, on the basis of which priorities for mitigatory actions may change accordingly. Recommendations should be presented by the technical support centre in written form to the decision maker, who will decide on the course of actions to be taken.

A.3. Decisions on actions to be taken should be communicated to control room staff in written form or an equivalent method that prevents misunderstandings. The main control room staff should confirm the actions it is supposed to take and should report back the progress of the actions taken and the impact that these have on the plant. Oral (telephone) communication with the control room staff should be carried out by a technical support centre staff member who is a licensed operator.

A.4. Plant parameters should be shown on a wall board or equivalent that is displayed in the technical support centre. Trends should be noted and recorded on this display. Actions taken should also be recorded on the display, as well as

[55] The Appendix contains some elements that are addressed in some other parts of this Safety Guide, but are repeated here for clarification of the process of working with SAMGs.

[56] This means that the technical support centre has been set up and has started working according to its work procedures.

other relevant information, such as the EOP or SAMG applicable at the time, emergency alerts for the plant and planned releases of radioactive material.

A.5. The technical support centre should, at regular intervals, estimate the timing and magnitude of possible future releases, and should communicate these to the emergency response organization. Such releases may be determined by consulting the PSA for the plant and inferring the relevant scenarios by interpretation of the plant parameters. Alternatively, fast running computer codes may be applied to analyse perceived scenarios and their most probable future evolution.

A.6. The emergency director, with advice from the technical support centre, should ensure that he/she is aware of the large uncertainties that are associated with the process of estimating possible releases, and should include them in statements to the public about possible releases.

A.7. The work at the technical support centre should be well structured. Staff members of the technical support centre should be provided with a clear task description. The technical support centre should convene in session at regular times (e.g. every 30 minutes) and should leave sufficient time for individual staff members to carry out their analysis between these regular meetings.

A.8. The technical support centre should consult external sources where their plans interfere with planned actions by the staff of the emergency response organization. Through such consultations it should be ensured that planned releases correspond with off-site levels of preparedness and, possibly, the times for such releases should be moved to times that better correspond with off-site levels of preparedness.[57] Alternatively, the releases should be delayed to a later time, if such a shift is compatible with the severe accident management actions foreseen.

A.9. A mechanism should be put in place to assign priorities in case of conflict between planned releases and the off-site protection afforded by the emergency arrangements. In principle, priority should be assigned to the actions that prevent major damage to the last fission product barrier still intact.

---

[57] For example, if a particular release is planned for a certain point in time, emergency plan staff should be informed so that they can take appropriate action to protect the lives and property of plant staff and the general public.

For example, prevention of gross containment failure should take priority over delaying planned releases.

A.10. Generally, the decision making process includes deliberation of possible actions and alternatives, and takes account of possibilities to restore systems back to service (i.e. repairs), consequences of possible releases, etc. However, in fast developing scenarios, there may be no time to consider all these aspects (see also para. 3.29). Consequently, in specifying the process for decision making, account should be taken of the fact that decisions may have to be taken in a very short time frame. A basic principle is that the decision making process should always be commensurate with the time frame of the evolution of the accident.[58]

[58] In some approaches, this is addressed by the fact that possible negative aspects of planned actions are disregarded if there are immediate challenges to fission product barriers.

REFERENCES

[1] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

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

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

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna (2007).

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

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

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4, IAEA, Vienna (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment Systems for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.10, IAEA, Vienna (2004).

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

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Review of Plant Specific Emergency Operating Procedures, Safety Reports Series No. 48, IAEA, Vienna (2006).

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

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for the Review of Accident Management Programmes in Nuclear Power Plants, IAEA Services Series No. 9, IAEA, Vienna (2003).

[14] 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 COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).
[15] ELECTRIC POWER RESEARCH INSTITUTE, Severe Accident Management Guidance Technical Basis Report, Vols 1 and 2, TR-101869-V1 and TR-101869-V2, EPRI, Palo Alto, CA (1992).
[16] INSTITUTE OF NUCLEAR POWER OPERATIONS, Emergency Operating Procedures Writing Guideline, INP0 82-017, INPO, Atlanta, GA (1982).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Experience in the Use of Systematic Approach to Training (SAT) for Nuclear Power Plant Personnel, IAEA-TECDOC-1057, IAEA, Vienna (1998).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of Simulation Techniques for Accident Management Training in Nuclear Power Plants, IAEA-TECDOC-1352, IAEA, Vienna (2003).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Overview of Training Methodology for Accident Management at Nuclear Power Plants, IAEA-TECDOC-1440, IAEA, Vienna (2005).
[20] CHEXAL, B., et al., “Update on the technical basis for the Severe Accident Management Guidelines”, Severe Accident Management Implementation (Proc. Specialist Mtg Niantic, CT, 1995), Rep. OECD/NEA/CSNI/R(95)5, OECD, Paris (1995).
[21] SAUVAGE, E.C., et al., “OSSA — An optimized approach to severe accident management: EPR application”, Proc. ICAPP’06, Reno, NV (2006).
[22] NUCLEAR ENERGY INSTITUTE, Severe Accident Issue Closure Guidelines, NEI 91-04, Rev. 1, NEI, Washington, DC (1994).
[23] NUCLEAR ENERGY INSTITUTE, Methodology for Development of Emergency Action Levels, NEI 99-01, Rev. 4, NEI, Washington, DC (2003).
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).
[26] LUTZ, R., et al., “Westinghouse Owners Group approach to severe accident management”, Severe Accident Management Implementation (Proc. Specialist Mtg, Niantic, CT, 1995), Rep. OECD/NEA/CSNI/R(95)5, OECD, Paris (1995).
[27] VAYSSIER, G., et al., SAMIME — Concerted Action on Severe Accident Management and Expertise in the EU, Final Report, AMM-SAMIME (00) – P009, European Commission, Luxembourg (2000).

Annex

AN EXAMPLE OF A CATEGORIZATION SCHEME FOR ACCIDENT SEQUENCES

A–1. Initially, all accident sequences will be chosen that, in the absence of preventive accident management measures, would lead to core damage. This large class of accidents is usually identified from the results of a Level 1 PSA analysis. All accident sequences leading to a core damage condition are of interest in principle. Because of their large number, this class of accidents needs to be subdivided into groups characterized by core damage states, each of which may be characterized by a representative accident sequence. Thus an aim of the classification is to choose suitable attributes and values so that the events leading to core damage will be appropriately subdivided. In this way, it is ensured that accidents within one group can reasonably be represented by a single sequence without creating an unmanageably large number of groups.

A–2. It is proposed to use three core damage state designators: initiating event, emergency core cooling status and secondary heat sink status. An example of a definition of the core damage state is given in Table A–1.

A–3. It should be noted that not all combinations of values for each of the three attributes are meaningful and care should be taken in the selection of a correct matrix of core damage states. For the categorization example given in Table A–1, the number of meaningful core damage states would be 29 (see Table A–2).

A–4. Most nuclear power plants have completed a Level 1 PSA, so that there generally will be enough information available to select categories of accident sequences, which are subsequently analysed to determine plant behaviour until core damage.

A–5. The results of these analyses form the basis for specifying operator actions as well as the necessary (available or additional) equipment to cope with the accident. This part of the process eventually leads to the development and implementation of emergency response guidelines (for groups of plants) and plant specific EOPs.

A–6. Although the existence of a Level 1 PSA for the plant is certainly a prerequisite for the selection of categories of accident sequences, there are additional ways to supplement the selection process:

TABLE A–1. AN EXAMPLE OF A CATEGORIZATION SCHEME

Attribute	Possible values	Symbol
Initiating event	Small loss of coolant accident (LOCA)	S
	Medium LOCA	M
	Large LOCA	A
	Steam generator tube rupture	W
	Secondary break	T_S
	Complete loss of AC power	T_B
	Anticipated transient without scram	T_A
	Transient	T
Status of emergency core cooling system	All failed	1
	High pressure injection successful, high pressure removal failed	2
	High pressure injection successful, high pressure removal successful	3
	Low pressure injection successful, low pressure removal failed	4
	Low pressure injection successful, low pressure removal successful	5
Status of secondary heat sink	Failed	F
	Successful	S

— Research into severe accident phenomena;
— Generic studies and analyses performed for similar (reference) plants;
— Study of operational experience and accident precursors;
— Review of existing procedures;
— Evaluation of existing instrumentation and its capabilities as well as its limitations under the environmental conditions of a severe accident.

A–7. The status of containment systems and the containment boundary become important in the next step, which involves identifying categories of accident sequences for the investigation of mitigatory accident management measures. This refers to mitigating the consequences of core damage should it occur, and in particular controlling and minimizing any release of fission products. The status of containment systems such as sprays, and the response of the containment to the loads presented by a severe accident, become important and need to be included in the definition of categories of accident sequences for mitigatory accident management.

TABLE A–2. AN EXAMPLE OF A MATRIX OF CORE DAMAGE STATES

Initiator	Status of emergency core cooling	Heat sink status
S	1	F
		S
	2	F
		S
	3	F
		S
M	1	X
	2	X
A	1	X
	4	X
W	1	F
		S
	2	F
		S
	3	F
		S
T_S	1	F
		S
	2	F
		S
	3	F
		S
T_B (equivalent to T1F)	X	X
T_A	1	F
		S
	2	F
		S
	3	F
		S
T	1	F
	2	F
	3	F

Note: X means that the attribute is not relevant for that particular combination and may take any assigned value.

A–8. To select and assess accident sequences that could lead to core damage states, and finally to containment damage and the release of fission products to the environment, a Level 2 PSA would be desirable to quantify containment damage states and the contribution of particular accident sequence categories to risks. Even if a Level 2 PSA has not been completed for the plant or is not available at all, there are methods of choosing categories of sequences that contribute significantly to risks at the plant. These include a systematic review of containment systems and containment response to severe accidents, such as:

— Identification of containment systems important to preventing the release of fission products, and their possible status in the event of a severe accident; this process would broaden the definitions of core damage states to definitions of plant damage states;
— Identification of important modes of containment failure and severe accident phenomena that may influence these.

A–9. Two additional attributes may also be used to broaden definitions of core damage states to definitions of plant damage states: the status of the heat removal from the containment and the status of the containment boundary, as outlined in Table A–3.

A–10. Analysing accident sequences and the associated operator actions will lead to the development of generic SAMGs, and eventually to plant specific SAMGs.

TABLE A–3. AN EXAMPLE OF A DEFINITION OF A CONTAINMENT DAMAGE STATE

Attribute	Possible values	Symbol
Status of containment heat removal	Failed	F
	Successful (either spray, high pressure injection or low pressure injection operate in recirculation mode). If the emergency core cooling system has the value 3 or 5 (see Table A–1), containment heat removal status is S.	S
Status of containment boundary	Isolation successful, normal leakage	S
	Isolation failed	I
	Bypassed	B

A–11. The process described in paras A–1 to A–10 is generic in nature and the accident sequences that contribute significantly to risks will need to be chosen for detailed analysis. This involves:

— Identification of accident sequences that contribute significantly to risks;
— Demonstration that the chosen accident sequence represents other sequences leading to the same plant damage state;
— Identification of key operator actions;
— Demonstration that the chosen accident sequence is amenable to preventive and mitigatory accident management measures.

A–12. A completed formalized Level 2 PSA will contain all the necessary analyses of a severe accident. In the absence of a Level 2 PSA it will be necessary to develop by other means an understanding of potential vulnerabilities to severe accidents by performing analyses. To determine which severe accident phenomena are important, a list of potential challenges to fission product barriers needs to be developed using the results of analyses of accident sequences without operator intervention. An example is given in Table A–4.

TABLE A–4. AN EXAMPLE OF SEVERE ACCIDENT PHENOMENA THAT MAY PRESENT SIGNIFICANT CHALLENGES TO FISSION PRODUCT BARRIERS

Containment failure mode	Applicable accident sequences	Associated phenomena	Mitigatory measures
Early failure — hydrogen combustion	Water injection onto an overheated core	Deflagration Accelerated flames Transition from deflagration to detonation Direct detonation	Maintain core in-vessel (reduce hydrogen) Cool debris ex-vessel (reduce hydrogen) Control hydrogen in containment
Early failure — high pressure melt ejection	High pressure in reactor coolant system at reactor vessel failure	Overpressurization of reactor shaft or cavity access doors Vessel rocketing Direct containment heating/ debris dispersal	Prevent vessel failure at high pressure (e.g. primary circuit depressurization)
Early failure — penetration failure	High pressure in reactor coolant system at reactor vessel failure	Debris attack to cavity access doors Overtemperature failure of penetrations	Prevent high temperature debris attack of concrete or cavity access doors
Late failure — overpressurization	Failure of active heat sinks in the containment such as containment spray, containment fan coolers and bubble towers	Steam generation from ex-vessel debris Non-condensable gas and steam generation from molten core–concrete interaction	Reduce pressure by condensing steam or venting

TABLE A–4. AN EXAMPLE OF SEVERE ACCIDENT PHENOMENA THAT MAY PRESENT SIGNIFICANT CHALLENGES TO FISSION PRODUCT BARRIERS (cont.)

Containment failure mode	Applicable accident sequences	Associated phenomena	Mitigatory measures
Late failure — basemat penetration	Failure to flood containment to provide water to cool ex-vessel core debris; or failure to flood reactor cavity prior to reactor vessel failure (depends on coolability arguments)	Long term molten core–concrete interaction	Prevent molten core–concrete interaction
Containment bypass	Steam generator tube rupture or intersystem LOCA		Recover isolation and/or scrub fission products
Containment bypass (induced)	High pressure in reactor coolant system and dry steam generator	Induced tube failure by heat-up of tubes due to natural recirculation in reactor coolant system	Protect steam generator tubes (e.g. refill steam generator)
Containment isolation failure	Containment isolation system malfunction		Recover isolation and/or scrub fission products

CONTRIBUTORS TO DRAFTING AND REVIEW

Aeberli, W.	Beznau Nuclear Power Plant, Switzerland
Gustavsson, V.	SwedPower AB, Sweden
Kersting, E.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Lee, S.	International Atomic Energy Agency
Lutz, R.J., Jr.	Westinghouse Electric Corporation, United States of America
Lundström, P.	Fortum Nuclear Services, Finland
Misak, J.	Nuclear Research Institute, Czech Republic
Prior, R.	ArevaP, France
Réocreux, M.	Institut de radioprotection et de sûreté nucléaire, France
Sonnenkalb, M.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Vayssier, G.L.C.M.	Nuclear Services Corporation, Netherlands

BODIES FOR THE ENDORSEMENT OF IAEA SAFETY STANDARDS

An asterisk denotes a corresponding member. Corresponding members receive drafts for comment and other documentation but they do not generally participate in meetings. Two asterisks denote an alternate.

Commission on Safety Standards

Argentina: González, A.J.; *Australia*: Loy, J.; *Belgium*: Samain, J.-P.; *Brazil*: Vinhas, L.A.; *Canada*: Jammal, R.; *China*: Liu Hua; *Egypt*: Barakat, M.; *Finland*: Laaksonen, J.; *France*: Lacoste, A.-C. (Chairperson); *Germany*: Majer, D.; *India*: Sharma, S.K.; *Israel*: Levanon, I.; *Japan*: Fukushima, A.; *Korea, Republic of*: Choul-Ho Yun; *Lithuania*: Maksimovas, G.; *Pakistan*: Rahman, M.S.; *Russian Federation*: Adamchik, S.; *South Africa*: Magugumela, M.T.; *Spain*: Barceló Vernet, J.; *Sweden*: Larsson, C.M.; *Ukraine*: Mykolaichuk, O.; *United Kingdom*: Weightman, M.; *United States of America*: Virgilio, M.; *Vietnam*: Le-chi Dung; *IAEA*: Delattre, D. (Coordinator); *Advisory Group on Nuclear Security*: Hashmi, J.A.; *European Commission*: Faross, P.; *International Nuclear Safety Group*: Meserve, R.; *International Commission on Radiological Protection*: Holm, L.-E.; *OECD Nuclear Energy Agency*: Yoshimura, U.; *Safety Standards Committee Chairpersons*: Brach, E.W. (TRANSSC); Magnusson, S. (RASSC); Pather, T. (WASSC); Vaughan, G.J. (NUSSC).

Nuclear Safety Standards Committee

Algeria: Merrouche, D.; *Argentina*: Waldman, R.; *Australia*: Le Cann, G.; *Austria*: Sholly, S.; *Belgium*: De Boeck, B.; *Brazil*: Gromann, A.; **Bulgaria*: Gledachev, Y.; *Canada*: Rzentkowski, G.; *China*: Jingxi Li; *Croatia*: Valčić, I.; **Cyprus*: Demetriades, P.; *Czech Republic*: Šváb, M.; *Egypt*: Ibrahim, M.; *Finland*: Järvinen, M.-L.; *France*: Feron, F.; *Germany*: Wassilew, C.; *Ghana*: Emi-Reynolds, G.; **Greece*: Camarinopoulos, L.; *Hungary*: Adorján, F.; *India*: Vaze, K.; *Indonesia*: Antariksawan, A.; *Iran, Islamic Republic of*: Asgharizadeh, F.; *Israel*: Hirshfeld, H.; *Italy*: Bava, G.; *Japan*: Kanda, T.; *Korea, Republic of*: Hyun-Koon Kim; *Libyan Arab Jamahiriya*: Abuzid, O.; *Lithuania*: Demčenko, M.; *Malaysia*: Azlina Mohammed Jais; *Mexico*: Carrera, A.; *Morocco*: Soufi, I.; *Netherlands*: van der Wiel, L.; *Pakistan*: Habib, M.A.; *Poland*: Jurkowski, M.; *Romania*: Biro, L.; *Russian Federation*: Baranaev, Y.; *Slovakia*: Uhrik, P.; *Slovenia*: Vojnovič, D.; *South Africa*: Leotwane, W.; *Spain*: Zarzuela, J.; *Sweden*: Hallman, A.; *Switzerland*: Flury, P.; *Tunisia*: Baccouche, S.;

Turkey: Bezdegumeli, U.; *Ukraine*: Shumkova, N.; *United Kingdom*: Vaughan, G.J. (Chairperson); *United States of America*: Mayfield, M.; *Uruguay*: Nader, A.; *European Commission*: Vigne, S.; *FORATOM*: Fourest, B.; *IAEA*: Feige, G. (Coordinator); *International Electrotechnical Commission*: Bouard, J.-P.; *International Organization for Standardization*: Sevestre, B.; *OECD Nuclear Energy Agency*: Reig, J.; **World Nuclear Association*: Borysova, I.

Radiation Safety Standards Committee

**Algeria*: Chelbani, S.; *Argentina*: Massera, G.; *Australia*: Melbourne, A.; **Austria*: Karg, V.; *Belgium*: van Bladel, L.; *Brazil*: Rodriguez Rochedo, E.R.; **Bulgaria*: Katzarska, L.; *Canada*: Clement, C.; *China*: Huating Yang; *Croatia*: Kralik, I.; **Cuba*: Betancourt Hernandez, L.; **Cyprus*: Demetriades, P.; *Czech Republic*: Petrova, K.; *Denmark*: Øhlenschlæger, M.; *Egypt*: Hassib, G.M.; *Estonia*: Lust, M.; *Finland*: Markkanen, M.; *France*: Godet, J.-L.; *Germany*: Helming, M.; *Ghana*: Amoako, J.; **Greece*: Kamenopoulou, V.; *Hungary*: Koblinger, L.; *Iceland*: Magnusson, S. (Chairperson); *India*: Sharma, D.N.; *Indonesia*: Widodo, S.; *Iran, Islamic Republic of*: Kardan, M.R.; *Ireland*: Colgan, T.; *Israel*: Koch, J.; *Italy*: Bologna, L.; *Japan*: Kiryu, Y.; *Korea, Republic of*: Byung-Soo Lee; **Latvia*: Salmins, A.; *Libyan Arab Jamahiriya*: Busitta, M.; *Lithuania*: Mastauskas, A.; *Malaysia*: Hamrah, M.A.; *Mexico*: Delgado Guardado, J.; *Morocco*: Tazi, S.; *Netherlands*: Zuur, C.; *Norway*: Saxebol, G.; *Pakistan*: Ali, M.; *Paraguay*: Romero de Gonzalez, V.; *Philippines*: Valdezco, E.; *Poland*: Merta, A.; *Portugal*: Dias de Oliveira, A.M.; *Romania*: Rodna, A.; *Russian Federation*: Savkin, M.; *Slovakia*: Jurina, V.; *Slovenia*: Sutej, T.; *South Africa*: Olivier, J.H.I.; *Spain*: Amor Calvo, I.; *Sweden*: Almen, A.; *Switzerland*: Piller, G.; **Thailand*: Suntarapai, P.; *Tunisia*: Chékir, Z.; *Turkey*: Okyar, H.B.; *Ukraine*: Pavlenko, T.; *United Kingdom*: Robinson, I.; *United States of America*: Lewis, R.; **Uruguay*: Nader, A.; *European Commission*: Janssens, A.; *Food and Agriculture Organization of the United Nations*: Byron, D.; *IAEA*: Boal, T. (Coordinator); *International Commission on Radiological Protection*: Valentin, J.; *International Electrotechnical Commission*: Thompson, I.; *International Labour Office*: Niu, S.; *International Organization for Standardization*: Rannou, A.; *International Source Suppliers and Producers Association*: Fasten, W.; *OECD Nuclear Energy Agency*: Lazo, T.E.; *Pan American Health Organization*: Jiménez, P.; *United Nations Scientific Committee on the Effects of Atomic Radiation*: Crick, M.; *World Health Organization*: Carr, Z.; *World Nuclear Association*: Saint-Pierre, S.

Transport Safety Standards Committee

Argentina: López Vietri, J.; **Capadona, N.M.; *Australia*: Sarkar, S.; *Austria*: Kirchnawy, F.; *Belgium*: Cottens, E.; *Brazil*: Xavier, A.M.; *Bulgaria*: Bakalova, A.; *Canada*: Régimbald, A.; *China*: Xiaoqing Li; *Croatia*: Belamarić, N.; **Cuba*: Quevedo Garcia, J.R.; **Cyprus*: Demetriades, P.; *Czech Republic*: Ducháček, V.; *Denmark*: Breddam, K.; *Egypt*: El-Shinawy, R.M.K.; *Finland*: Lahkola, A.; *France*: Landier, D.; *Germany*: Rein, H.; *Nitsche, F.; **Alter, U.; *Ghana*: Emi-Reynolds, G.; **Greece*: Vogiatzi, S.; *Hungary*: Sáfár, J.; *India*: Agarwal, S.P.; *Indonesia*: Wisnubroto, D.; *Iran, Islamic Republic of*: Eshraghi, A.; *Emamjomeh, A.; *Ireland*: Duffy, J.; *Israel*: Koch, J.; *Italy*: Trivelloni, S.; **Orsini, A.; *Japan*: Hanaki, I.; *Korea, Republic of*: Dae-Hyung Cho; *Libyan Arab Jamahiriya*: Kekli, A.T.; *Lithuania*: Statkus, V.; *Malaysia*: Sobari, M.P.M.; **Husain, Z.A.; *Mexico*: Bautista Arteaga, D.M.; **Delgado Guardado, J.L.; **Morocco*: Allach, A.; *Netherlands*: Ter Morshuizen, M.; **New Zealand*: Ardouin, C.; *Norway*: Hornkjøl, S.; *Pakistan*: Rashid, M.; **Paraguay*: More Torres, L.E.; *Poland*: Dziubiak, T.; *Portugal*: Buxo da Trindade, R.; *Russian Federation*: Buchelnikov, A.E.; *South Africa*: Hinrichsen, P.; *Spain*: Zamora Martin, F.; *Sweden*: Häggblom, E.; **Svahn, B.; *Switzerland*: Krietsch, T.; *Thailand*: Jerachanchai, S.; *Turkey*: Ertürk, K.; *Ukraine*: Lopatin, S.; *United Kingdom*: Sallit, G.; *United States of America*: Boyle, R.W.; Brach, E.W. (Chairperson); *Uruguay*: Nader, A.; *Cabral, W.; *European Commission*: Binet, J.; *IAEA*: Stewart, J.T. (Coordinator); *International Air Transport Association*: Brennan, D.; *International Civil Aviation Organization*: Rooney, K.; *International Federation of Air Line Pilots' Associations*: Tisdall, A.; **Gessl, M.; *International Maritime Organization*: Rahim, I.; *International Organization for Standardization*: Malesys, P.; *International Source Supplies and Producers Association*: Miller, J.J.; **Roughan, K.; *United Nations Economic Commission for Europe*: Kervella, O.; *Universal Postal Union*: Bowers, D.G.; *World Nuclear Association*: Gorlin, S.; *World Nuclear Transport Institute*: Green, L.

Waste Safety Standards Committee

Algeria: Abdenacer, G.; *Argentina*: Biaggio, A.; *Australia*: Williams, G.; **Austria*: Fischer, H.; *Belgium*: Blommaert, W.; *Brazil*: Tostes, M.; **Bulgaria*: Simeonov, G.; *Canada*: Howard, D.; *China*: Zhimin Qu; *Croatia*: Trifunovic, D.; *Cuba*: Fernandez, A.; *Cyprus*: Demetriades, P.; *Czech Republic*: Lietava, P.; *Denmark*: Nielsen, C.; *Egypt*: Mohamed, Y.; *Estonia*: Lust, M.; *Finland*: Hutri, K.; *France*: Rieu, J.; *Germany*: Götz, C.; *Ghana*: Faanu, A.; *Greece*: Tzika, F.; *Hungary*: Czoch, I.; *India*: Rana, D.; *Indonesia*: Wisnubroto, D.; *Iran, Islamic*

Republic of: Assadi, M.; *Zarghami, R.; *Iraq*: Abbas, H.; *Israel*: Dody, A.; *Italy*: Dionisi, M.; *Japan*: Matsuo, H.; *Korea, Republic of*: Won-Jae Park; **Latvia*: Salmins, A.; *Libyan Arab Jamahiriya*: Elfawares, A.; *Lithuania*: Paulikas, V.; *Malaysia*: Sudin, M.; *Mexico*: Aguirre Gómez, J.; **Morocco*: Barkouch, R.; *Netherlands*: van der Shaaf, M.; *Pakistan*: Mannan, A.; **Paraguay*: Idoyaga Navarro, M.; *Poland*: Wlodarski, J.; *Portugal*: Flausino de Paiva, M.; *Slovakia*: Homola, J.; *Slovenia*: Mele, I.; *South Africa*: Pather, T. (Chairperson); *Spain*: Sanz Aludan, M.; *Sweden*: Frise, L.; *Switzerland*: Wanner, H.; **Thailand*: Supaokit, P.; *Tunisia*: Bousselmi, M.; *Turkey*: Özdemir, T.; *Ukraine*: Makarovska, O.; *United Kingdom*: Chandler, S.; *United States of America*: Camper, L.; **Uruguay*: Nader, A.; *European Commission*: Necheva, C.; *European Nuclear Installations Safety Standards*: Lorenz, B.; **European Nuclear Installations Safety Standards*: Zaiss, W.; *IAEA*: Siraky, G. (Coordinator); *International Organization for Standardization*: Hutson, G.; *International Source Suppliers and Producers Association*: Fasten, W.; *OECD Nuclear Energy Agency*: Riotte, H.; *World Nuclear Association*: Saint-Pierre, S.

FUNDAMENTAL SAFETY PRINCIPLES
IAEA Safety Standards Series No. SF-1
STI/PUB/1273 (21 pp.; 2006)
ISBN 92–0–110706–4 Price: €25.00

SAFETY OF NUCLEAR POWER PLANTS: OPERATION
SAFETY REQUIREMENTS
IAEA Safety Standards Series No. NS-R-2
STI/PUB/1096 (31 pp.; 2000)
ISBN 92–0–100700–0 Price: €11.50

CONDUCT OF OPERATIONS AT NUCLEAR POWER PLANTS
SAFETY GUIDE
IAEA Safety Standards Series No. NS-G-2.14
STI/PUB/1339 (55 pp.; 2008)
ISBN 978–92–0–105408–1 Price: €19.00

EVALUATION OF SEISMIC SAFETY FOR EXISTING NUCLEAR INSTALLATIONS
IAEA Safety Standards Series No. NS-G-2.13
STI/PUB/1379
ISBN 978–92–0–100409–3 Price: €20.00

AGEING MANAGEMENT FOR NUCLEAR POWER PLANTS
SAFETY GUIDE
IAEA Safety Standards Series No. NS-G-2.12
STI/PUB/1373 (48 pp.; 2009)
ISBN 978–92–0–112408–1 Price: €20.00

A SYSTEM FOR THE FEEDBACK OF EXPERIENCE FROM EVENTS IN NUCLEAR INSTALLATIONS
SAFETY GUIDE
IAEA Safety Standards Series No. NS-G-2.11
STI/PUB/1243 (61 pp.; 2006)
ISBN 92–0–101406–6 Price: €23.00

PERIODIC SAFETY REVIEW OF NUCLEAR POWER PLANTS
Safety Guide
IAEA Safety Standards Series No. NS-G-2.10
STI/PUB/1157 (52 pp.; 2003)
ISBN 92–0–108503–6 Price: €15.50

Safety through international standards

"The IAEA's standards have become a key element of the global safety regime for the beneficial uses of nuclear and radiation related technologies.

"IAEA safety standards are being applied in nuclear power generation as well as in medicine, industry, agriculture, research and education to ensure the proper protection of people and the environment."

Mohamed ElBaradei
IAEA Director General

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–112908–6
ISSN 1020–525X