This publication has been superseded by SSG-2 (Rev. 1).

IAEA Safety Standards

for protecting people and the environment

Deterministic Safety Analysis for Nuclear Power Plants

Specific Safety Guide

No. SSG-2

IAEA

International Atomic Energy Agency

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

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

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

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

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

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

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

OTHER SAFETY RELATED PUBLICATIONS

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

Reports on safety and protection in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications. Security related publications are issued in the **IAEA Nuclear Security Series**.

DETERMINISTIC SAFETY ANALYSIS
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
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
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
LESOTHO
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. SSG-2

DETERMINISTIC SAFETY ANALYSIS FOR NUCLEAR POWER PLANTS

SPECIFIC SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2009

COPYRIGHT NOTICE

Sales and Promotion, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
December 2009
STI/PUB/1428

IAEA Library Cataloguing in Publication Data

Deterministic safety analysis for nuclear power plants : safety guide. — Vienna : International Atomic Energy Agency, 2009.
p. ; 24 cm. — (IAEA safety standards series, ISSN 1020–525X ; no. SSG-2)
STI/PUB/1428
ISBN 978–92–0–113309–0
Includes bibliographical references.

1. Nuclear power plants — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL 09–00614

FOREWORD

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.

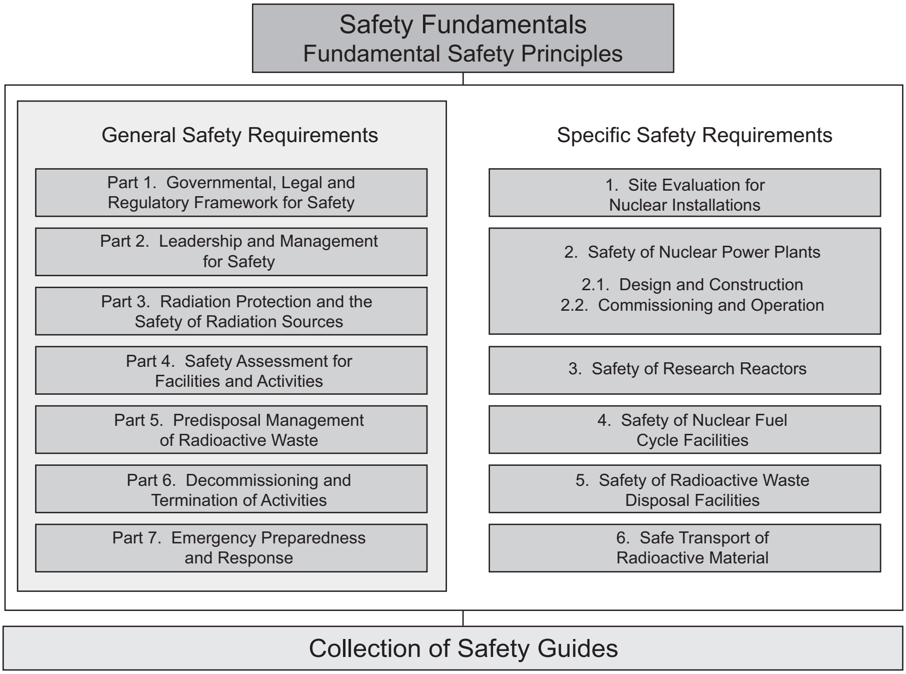

FIG. 1. The long term structure of the IAEA Safety Standards Series.

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

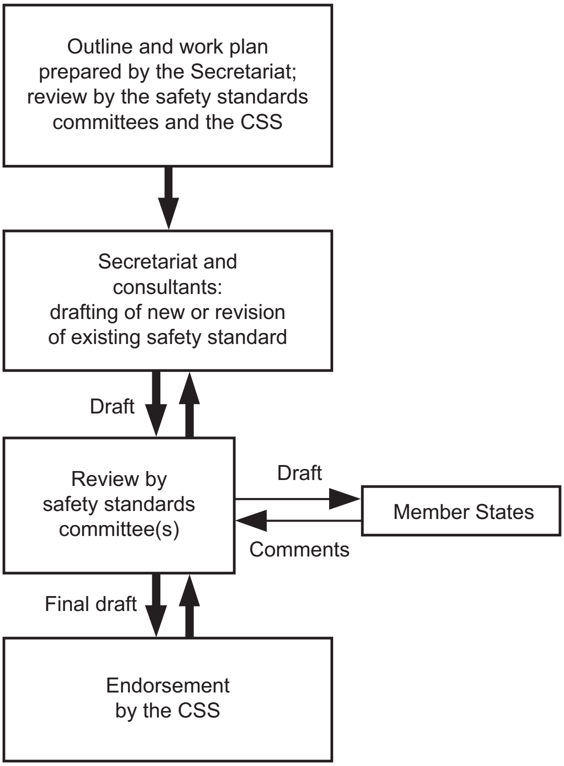

FIG. 2. The process for developing a new safety standard or revising an existing standard.

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 1

    Background (1.1–1.10). 1
    Objective (1.11) 3
    Scope (1.12–1.15) 3
    Structure (1.16) 4

2. GROUPING OF INITIATING EVENTS AND ASSOCIATED TRANSIENTS RELATING TO PLANT STATES (2.1–2.10) 5

3. DETERMINISTIC SAFETY ANALYSIS AND ACCEPTANCE CRITERIA 7

    Deterministic safety analysis (3.1–3.14) 7
    Acceptance criteria (3.15–3.22). 12

4. CONSERVATIVE DETERMINISTIC SAFETY ANALYSIS 14

    Conservative approach (4.1–4.3) 14
    Initial and boundary conditions (4.4–4.6) 15
    Availability of systems and components (4.7–4.9) 15
    Operator actions (4.10). 16
    Nodalization and plant modelling (4.11) 16

5. BEST ESTIMATE PLUS UNCERTAINTY ANALYSIS 16

    Best estimate approach (5.1–5.14). 16
    Best estimate computer codes (5.15–5.24) 19
    Sensitivity analysis and uncertainty analysis (5.25–5.34) 21
    Initial and boundary conditions (5.35–5.37) 23
    Availability of systems: Single failure criterion and loss of off-site power (5.38) 24
    Nodalization and plant modelling (5.39) 25

6. VERIFICATION AND VALIDATION OF COMPUTER CODES. . . 25

Process management (6.1–6.8) 25
Plan for code verification and its implementation (6.9–6.10) 27
Verification of the code design (6.11–6.14). 27
Verification of the source code (6.15–6.17). 28
Errors and corrective actions (6.18–6.19) 28
Code validation (6.20–6.41). 28

7. RELATION OF DETERMINISTIC SAFETY ANALYSIS TO ENGINEERING ASPECTS OF SAFETY AND PROBABILISTIC SAFETY ANALYSIS 32

Relation of deterministic safety analysis to engineering aspects of safety (7.1–7.12) 32
Relation of deterministic safety analysis to probabilistic safety analysis (7.13–7.16) 36

8. APPLICATION OF DETERMINISTIC SAFETY ANALYSIS 37

Areas of application (8.1–8.2) 37
Application of deterministic safety analysis to the design of nuclear power plants (8.3) 38
Application of deterministic safety analysis to the licensing of nuclear power plants (8.4–8.8). 39
Application of deterministic safety analysis to the assessment of safety analysis reports (8.9) 40
Application of deterministic safety analysis in plant modifications (8.10–8.14) 40
Application of deterministic safety analysis to the analysis of operational events (8.15–8.17). 41
Application of deterministic safety analysis to the development and validation of emergency operating procedures (8.18–8.20) . . . 42
Application of deterministic safety analysis to the development of guidelines for the management of severe accidents (8.21–8.26) 43
Application of deterministic safety analysis to periodic safety reviews (8.27) 44

9. SOURCE TERM EVALUATION FOR OPERATIONAL STATES AND ACCIDENT CONDITIONS 44

Use of the source term in design and regulation (9.1–9.11) 44
Normal operational states (9.12–9.18) 47
Accident conditions (9.19–9.35) 49

REFERENCES 55
CONTRIBUTORS TO DRAFTING AND REVIEW 57
BODIES FOR THE ENDORSEMENT OF IAEA SAFETY STANDARDS 59

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide provides recommendations and guidance on the use of deterministic safety analysis and its application to nuclear power plants in compliance with the IAEA's Safety Requirements publications on Safety of Nuclear Power Plants: Design [1] and Safety Assessment for Facilities and Activities [2].

1.2. Current developments for ensuring the stable, safe and competitive operation of nuclear reactors are closely related to the advances that are being made in safety analysis. Deterministic safety analyses for anticipated operational occurrences, design basis accidents (DBAs) and beyond design basis accidents (BDBAs), as defined in Ref. [1] and in the IAEA Safety Glossary [3], are essential instruments for confirming the adequacy of safety provisions.

1.3. Initially, rigorous conservative approaches to anticipated operational occurrences and design basis accidents were used in deterministic safety analyses. Licensing calculations used conservative codes with conservative input data, mostly owing to the difficulty of modelling complicated physical phenomena with limited computer capacity and a lack of adequate data. As more experimental data have become available, and with advances in code development, for loss of coolant accidents (LOCAs) in particular, the practice in many States has moved towards a more realistic approach together with an evaluation of uncertainties. This is termed a best estimate approach.

1.4. There are three ways of analysing anticipated operational occurrences and design basis accidents to demonstrate that the safety requirements, which are currently used to support applications for licensing, are met:

(1) Use of conservative computer codes with conservative initial and boundary conditions (conservative analysis).
(2) Use of best estimate computer codes combined with conservative initial and boundary conditions (combined analysis).

(3) Use of best estimate computer codes with conservative and/or realistic input data but coupled with an evaluation of the uncertainties in the calculation results, with account taken of both the uncertainties in the input data and the uncertainties associated with the models in the best estimate computer code (best estimate analysis). The result, which reflects conservative choice but has a quantified level of uncertainty, is used in the safety evaluation.

1.5. For beyond design basis accidents, best estimate calculations are used in several States, together with an evaluation of the uncertainties associated with the relevant phenomena. However, in determining what measures should be taken to mitigate the consequences of beyond design basis accidents, an uncertainty analysis is not usually performed.

1.6. The use of best estimate analysis together with an evaluation of the uncertainties is increasing for the following reasons:

(a) The use of conservative assumptions may sometimes lead to the prediction of an incorrect progression of events or unrealistic timescales, or it may exclude some important physical phenomena. The sequences of events that constitute the accident scenario, which are important in assessing the safety of the plant, may thus be overlooked.
(b) In addition, the use of a conservative approach often does not show the margins to the acceptance criteria that apply in reality, which could be taken into account to improve operational flexibility.
(c) A best estimate approach provides more realistic information about the physical behaviour of the plant, assists in identifying the most relevant safety parameters and allows more realistic comparison with acceptance criteria.

1.7. For accident scenarios with large margins to the acceptance criteria, it is appropriate for simplicity, and therefore economy, to use a conservative analysis (with no evaluation of uncertainties). For scenarios in which the margin is smaller, a best estimate analysis is necessary to quantify the conservatism.

1.8. For anticipated operational occurrences, the use of a best estimate approach together with an evaluation of the uncertainties may avoid the selection of unnecessarily restrictive limits and set points, and may provide a more precise evaluation of actual margins relating to the limits and set points. In turn, this may provide additional operational flexibility and reduce unnecessary reactor scrams or actuations of the protection systems.

1.9. Changes that require the plant to be modified, such as power uprating and achieving a higher burnup, longer fuel cycles and life extension, necessitate comprehensive analysis to demonstrate compliance with acceptance criteria. Special care has to be taken when a combination of changes is planned.

1.10. This Safety Guide addresses both conservative and best estimate approaches to deterministic safety analysis, and provides recommendations and guidance on the use of deterministic safety analysis and its applications.

OBJECTIVE

1.11. The objective of this Safety Guide is to provide recommendations and guidance on deterministic safety analysis for designers, operators, regulators and technical support organizations. It also provides recommendations on the use of deterministic safety analysis in:

(a) Demonstrating or assessing compliance with regulatory requirements;
(b) Identifying possible enhancements of safety and reliability;
(c) Obtaining increased operational flexibility within safety limits for nuclear power plants.

The recommendations are based on current good practices at nuclear power plants around the world and derive mainly from experience in performing transient analyses and accident analyses for nuclear power plants.

SCOPE

1.12. This Safety Guide applies to nuclear power plants. It addresses safety analyses that are required to be performed to demonstrate that barriers to the release of radioactive material will prevent an uncontrolled release to the environment for all plant states (Ref. [1], paras 5.71, 5.72). It therefore addresses the ways in which deterministic methods are used to verify that the defence in depth concept has been properly implemented. This includes demonstrating that the fission process is controlled within the design limit, that the reactor core can be cooled and that the heat generated can be removed to heat sinks of sufficient size.

1.13. The Safety Guide also addresses applications of deterministic safety analysis for the development and validation of emergency operating procedures and the determination of safety margins for modifications to nuclear power plants. Furthermore, it addresses the analysis of transients that have occurred in operating plants and analysis in support of accident management and planning for emergency preparedness and response.

1.14. The Safety Guide focuses on thermohydraulic, neutronic and source term analysis. Other types of analysis, such as structural mechanical analysis or analysis of electrical transients, are important aspects of demonstrating the safety of a plant; however, they are outside the scope of this Safety Guide. Information on other types of analysis can be found in specific engineering guides.

1.15. Safety analyses play an important role throughout the lifetime of a nuclear power plant. The stages of and occasions in a plant's lifetime in which the use of safety analyses is relevant include:

(a) Design;
(b) Commissioning;
(c) Operation and shutdown;
(d) Modification of design or operation;
(e) Periodic safety review;
(f) Life extension, in States where licences are issued for a limited duration.

STRUCTURE

1.16. Section 2 addresses the plant states and the classification of conditions that should be considered. Deterministic safety analysis and acceptance criteria are described in Section 3, and conservative deterministic safety analysis is explained in Section 4. Best estimate plus uncertainty analysis is discussed in Section 5. The quality of the analysis of computer codes and their verification and validation are described in Section 6. The relationship of deterministic safety analysis to engineering aspects of safety and to probabilistic safety analysis is presented in Section 7. The application of deterministic safety analysis is described in Section 8. Source term evaluation for operational states of and accident conditions for nuclear reactors is described in Section 9.

2. GROUPING OF INITIATING EVENTS AND ASSOCIATED TRANSIENTS RELATING TO PLANT STATES

2.1. Plant states for nuclear power plants are specified in Ref. [1], as shown in Table 1. The plant states are divided into operational states and accident conditions. Operational states include normal operation as well as anticipated operational occurrences. Accident conditions include conditions within design basis accidents and conditions beyond design basis accidents. Beyond design basis accident conditions include severe accident conditions, which are characterized as states with significant core degradation in which, for example, core components start to melt.

2.2. For the plant states listed in Table 1, as specified in Ref. [1], normal operation is defined as operation within specified operational limits and conditions. An anticipated operational occurrence is an operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions (it may result in a reactor scram, however). Design basis accidents are 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 (see Ref. [3]).

TABLE 1. PLANT STATES [1, 3]

Operational states		Accident conditions			
		Within design basis accidents		Beyond design basis accidents	
Normal operation	Anticipated operational occurrences	a	Design basis accidents	b	Severe accidents
				Accident management	

a *Accident conditions* that are not *design basis accidents* as explicitly considered but which are encompassed by them.

b *Beyond design basis accidents* without significant core degradation.

2.3. For all plant states, a comprehensive listing of postulated initiating events (PIEs) should be prepared for ensuring that the analysis of the behaviour of the plant is complete. An initiating event is an event that leads to anticipated operational occurrences or accident conditions. This includes operator errors and equipment failures (both within and external to the facility), human induced or natural events, and internal or external hazards that, directly or indirectly, challenge one or more of the systems required to maintain the safety of the plant.

2.4. Postulated initiating events and the consequential transients should be specified to ensure that all possible scenarios are being addressed. When performing deterministic safety analyses for anticipated operational occurrences, design basis accidents and beyond design basis accidents, all postulated initiating events and associated transients should be grouped into categories. There are different sets of criteria for grouping initiating events and transients into categories, and each set of criteria will result in a different event list. One approach is to group events according to the principal effects that could result in the degradation of safety systems.

2.5. Anticipated operational occurrences typically include loss of normal power, turbine trip, failure of control equipment and loss of power to the main coolant pump.

2.6. The categories of postulated initiating events for design basis accidents typically include the following transients:

(a) Increase or decrease of the removal of heat from the reactor coolant system;
(b) Increase or decrease of the flow rate for the reactor coolant system;
(c) Anomalies in reactivity and power distribution;
(d) Increase or decrease of the reactor coolant inventory;
(e) Release of radioactive material from a subsystem or component.

2.7. Computational analysis of all possible design basis accident scenarios may not be practicable. A reasonable number of limiting cases, which are referred to as bounding or enveloping scenarios, should be selected from each category of events. These bounding or enveloping scenarios should be chosen so that they present the greatest possible challenge to the relevant acceptance criteria and are limiting for the performance parameters of safety related equipment. In addition to design basis accidents, anticipated transients without scram (ATWS) have traditionally been analysed for light water reactors. It is becoming increasingly common for the analysis of other beyond design basis accidents to be required.

2.8. A different grouping of initiating events and transients is more useful when calculating potential releases of radioactive material to the environment. In particular, accidents in which major barriers such as the containment may be ineffective should be identified, and it should be ensured that analyses are performed for these transients. Examples of such cases include steam generator tube ruptures as postulated initiating events or consequential events, loss of coolant accidents in the auxiliary building and faults that occur when the containment is open during shutdown.

2.9. There are two alternative approaches to grouping postulated initiating events and their associated transients. Currently, the most common approach is to group initiating events and their associated transients according to the expected frequency of the initiating events, as indicated in Table 2. The second approach is to group according to the frequency of the accident scenarios. One way of quantifying the frequency of each accident scenario is to perform a probabilistic safety analysis. Probabilistic safety analysis identifies not only the sequences that lead to core degradation, but also the more frequent sequences that do not lead to plant damage or that lead to limited damage.

2.10. Beyond design basis accidents, including severe accidents, are typically treated separately in deterministic safety analyses, although some initiating events may be the same as for design basis accidents. The results help to determine the necessary measures to prevent severe accidents and to mitigate their radiological consequences if they do occur.

3. DETERMINISTIC SAFETY ANALYSIS AND ACCEPTANCE CRITERIA

DETERMINISTIC SAFETY ANALYSIS

3.1. Safety analyses are analytical evaluations of physical phenomena occurring at nuclear power plants, made for the purpose of demonstrating that safety requirements, such as the requirement for ensuring the integrity of barriers against the release of radioactive material and various other acceptance criteria,

TABLE 2. POSSIBLE SUBDIVISION OF POSTULATED INITIATING EVENTS

Occurrence (1/reactor year)	Characteristics	Plant state	Terminology	Acceptance criteria
10^{-2}–1 (expected over the lifetime of the plant)	Expected	Anticipated operational occurrences	Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions	No additional fuel damage
10^{-4}–10^{-2} (chance greater than 1% over the lifetime of the plant)	Possible	Design basis accidents	Infrequent incidents, infrequent faults, limiting faults, emergency conditions	No radiological impact at all, or no radiological impact outside the exclusion area
10^{-6}–10^{-4} (chance less than 1% over the lifetime of the plant)	Unlikely	Beyond design basis accidents	Faulted conditions	Radiological consequences outside the exclusion area within limits
$<10^{-6}$ (very unlikely to occur)	Remote	Severe accidents	Faulted conditions	Emergency response needed

are met for all postulated initiating events that could occur over a broad range of operational states, including different levels of availability of the safety systems. There are two basic types of safety analysis: deterministic safety analysis and probabilistic safety analysis.

3.2. Deterministic safety analyses for a nuclear power plant predict the response to postulated initiating events. A specific set of rules and acceptance criteria is applied. Typically, these should focus on neutronic, thermohydraulic, radiological, thermomechanical and structural aspects, which are often analysed with different computational tools. The computations are usually carried out for predetermined operating modes and operational states, and the events include anticipated transients, postulated accidents, selected beyond design basis accidents and severe accidents with core degradation. The results of computations are spatial and time dependences of various physical variables (e.g. neutron flux; thermal power of the reactor; pressure, temperature, flow rate and velocity of the primary coolant; stresses in structural materials; physical and chemical compositions; concentrations of radionuclides) or, in the case of an assessment of radiological consequences, radiation doses to workers or the public.

3.3. Deterministic safety analyses for design purposes should be characterized by their conservative assumptions and bounding analysis. This is achieved by an iterative process in the design phase, when the limiting case(s) in terms of the minimum margin to the acceptance criteria is (are) determined for each group of postulated initiating events and sequences. To determine the limiting case for a given transient or set of transients, the consequential failures that are caused by the initiating event (internal or external) should be taken into account.

3.4. In addition, an adequate set of conservative or best estimate assumptions for the initial and boundary conditions should be used. A limited number of coincident independent failures (including operator error) should also be addressed. However, the frequency of occurrence will decrease significantly as each coincident independent failure is taken into account. Only those combinations of transients whose frequency remains within the design basis should be analysed.

3.5. The time span of any scenario that is analysed should extend up to the moment when the plant reaches a safe and stable end state. What is meant by a safe and stable end state should be defined. In some cases it is assumed that a safe and stable end state is achieved when the core is covered and long term heat removal from the core is achieved, and the core is subcritical by a given margin. However, the safety analysis may also address provisions for safely removing the fuel from the core and storing it elsewhere in cooled conditions.

3.6. Some approaches consider specific acceptance criteria for each of the groups of postulated initiating events and associated transients discussed in Section 2, and address the availability of systems and the initial plant conditions.

3.7. To guarantee an adequate degree of defence in depth, all credible failure mechanisms of the different barriers should be analysed. Certain limiting faults (e.g. large break loss of coolant accidents, secondary breaks, rod ejection in pressurized water reactors or rod drop in boiling water reactors) should also be part of the deterministic safety analysis and should not be excluded merely on the grounds of their low frequency. However, the leak before break criterion in best estimate analysis may be used to better define certain requirements for structures, systems and components. Other considerations relate to risk informed regulation, and include the need to better define requirements associated with applying the single failure criterion[1] and the loss of off-site power following a loss of coolant accident.

3.8. Although conservative assumptions and bounding analyses should be used for design purposes (see para. 3.3), more realistic analyses should be used to evaluate the evolution and consequences of accidents, for the reasons given in para. 1.6. For the development of emergency procedures and for the analysis of beyond design basis accidents, including severe accidents, several States use best estimate methods and codes. When determining what actions should be taken to prevent core melt, the range of uncertainties associated with the relevant phenomena should be determined. An uncertainty analysis is not always practicable or even possible, and should not necessarily be performed when determining what measures should be taken to mitigate the consequences of beyond design basis accidents.

3.9. Table 3 lists different options for performing deterministic safety analyses. Option 1 is a conservative approach:

(a) The code is conservative, as it is intended to produce pessimistic results.
(b) The selected initial and boundary conditions, including the time available for the operator to act, are assumed to have pessimistic values.
(c) No credit is taken for non-safety-grade equipment unless it is conservative to do so.
(d) The most severe single failure of the safety systems that are designed to mitigate the consequences of the accident is assumed.

3.10. Currently, Option 2 is being used for safety analyses in many States, that is, the use of a 'best estimate' computer code instead of a conservative code. However, conservative initial and boundary conditions are used, as well as conservative assumptions with regard to the availability of systems. Conservative initial and boundary conditions should be used to ensure that all uncertainties associated with the code models and plant parameters are bounded. The complete analysis requires a combination of validation of the code, use of conservatism in the data and use of sensitivity studies.

---

[1] A single failure is a failure which results in the loss of capability of a system or component to perform its intended safety function(s), and any consequential failure(s) which result from it. The single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

TABLE 3. OPTIONS FOR COMBINATION OF A COMPUTER CODE AND INPUT DATA

Option	Computer code	Availability of systems	Initial and boundary conditions
1. Conservative	Conservative	Conservative assumptions	Conservative input data
2. Combined	Best estimate	Conservative assumptions	Conservative input data
3. Best estimate	Best estimate	Conservative assumptions	Realistic plus uncertainty; partly most unfavourable conditions[a]
4. Risk informed	Best estimate	Derived from probabilistic safety analysis	Realistic input data with uncertainties[a]

[a] Realistic input data are used only if the uncertainties or their probabilistic distributions are known. For those parameters whose uncertainties are not quantifiable with a high level of confidence, conservative values should be used.

3.11. Option 3 allows the use of best estimate models in the code instead of conservative models, together with more realistic initial and boundary conditions. However, uncertainties should be identified so that the uncertainty in the calculated results can be estimated. A high probability that acceptance criteria would not be exceeded should be demonstrated (see Section 5). The uncertainties associated with the use of a best estimate computer code and realistic assumptions for the initial and boundary conditions should be combined statistically. Any dependence between uncertainties, if present, should be taken into account. In addition, it should be verified that the ranges of parameters that are applied are realistic. Sensitivity studies should be performed, especially to detect any 'cliff edge effect'[2].

3.12. In principle, Options 2 and 3 in Table 3 are distinctly different types of analysis. However, in practice, a mixture of Options 2 and 3 is employed. This is because whenever extensive data are available, the tendency is to use realistic input data, and whenever data are scarce, the tendency is to use conservative input data. The difference between these two options is the statistical combination

[2] A cliff edge effect in a nuclear power plant is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

of uncertainties. In Options 1, 2 and 3, conservative assumptions are made about the availability of safety and control systems. Currently, the acceptance criteria depend on the frequency of the initiating event.

3.13. Options 1 and 2 are described in more detail in Section 4. Option 3 is explained in Section 5.

3.14. Option 4 is not yet widely used. It includes a realistic analysis, on the basis of a probabilistic safety analysis, to quantify the availability of systems that are significant for safety and the success of mitigatory actions. Option 4 is also relevant to the development of risk informed decision making, and it may be used as a means of verifying the deterministic design basis envelope. This, however, is not intended to be part of the risk informed decision making.

ACCEPTANCE CRITERIA

3.15. Basic acceptance criteria are usually defined as limits and conditions set by a regulatory body, and their purpose is to ensure the achievement of an adequate level of safety. These criteria are supplemented by other requirements known as acceptance criteria (sometimes termed derived acceptance criteria) to ensure defence in depth by, for example, preventing the consequential failure of a pressure boundary in an accident.

3.16. To demonstrate the safety of the plant, the following basic acceptance criteria should be fulfilled:

(a) The individual doses and collective doses to workers and the public are required to be within prescribed limits and as low as reasonably achievable in all operational states by ensuring mitigation of the radiological consequences of any accident (see Ref. [1], para. 2.4).
(b) The integrity of barriers to the release of radioactive material (i.e. the fuel itself, the fuel cladding, the primary and/or secondary reactor coolant system, the primary and/or secondary containment) should be maintained, depending on the categories of plant states for the accidents for which their integrity is required.
(c) The capabilities of systems that, and operators who, are intended to perform a safety function, directly or indirectly, should be ensured for the accidents for which performance of the safety function is required.
(d) In some designs, it is required that early large releases of radioactive material be practically excluded.

3.17. Basic acceptance criteria such as radiation dose criteria should be commensurate with the frequency of the initiating event or the frequency of the sequence, depending on the approach adopted.

3.18. Acceptance criteria should be established for the entire range of operational states and accident conditions. Acceptance criteria may be related to the frequency of the event. Events that occur frequently, such as anticipated operational occurrences, should have acceptance criteria that are more restrictive than those for less frequent events such as design basis accidents.

3.19. Acceptance criteria should be set in terms of the variable or variables that directly govern the physical processes that challenge the integrity of a barrier. Nevertheless, it is a common engineering practice to make use of surrogate variables to establish an acceptance criterion that, if not exceeded, will ensure the integrity of the barrier. Examples of surrogate variables are: peak cladding temperature, departure from nucleate boiling ratio or fuel pellet enthalpy rise. When defining these acceptance criteria, a sufficiently high degree of conservatism should be included to ensure that there are adequate safety margins beyond the acceptance criterion to allow for uncertainties.

3.20. Each safety related structure, system or component should be assessed to demonstrate that it will perform according to its design function during the course of a design basis accident. In addition to demonstrating that the acceptance criteria for the surrogate variables are met, it should be shown that the acceptance criteria for each safety related component are also met. For example, for a small break loss of coolant accident, it should be demonstrated that the design criteria for the diesel powered pumps are not exceeded. Compliance with the single failure criterion should be evaluated for each safety system in the plant, where practicable. The presence of a single failure should always be taken into account in the limiting case, in terms of addressing an acceptance criterion for safety systems. Typical acceptance criteria are:

(a) Numerical limits on the values of calculated variables (e.g. peak cladding temperature, fuel cladding oxidation);
(b) Conditions for plant states during and after an accident (e.g. limitations on power depending on the coolant flow through the core, achievement of a long term safe state);
(c) Performance requirements for structures, systems and components (e.g. injection flow rates);

(d) Requirements for operator actions, with account taken of the specific accident environment (e.g. the reliability of the alarm system and habitability of the control areas).

3.21. Compliance with acceptance criteria should always be demonstrated in licensing applications.

3.22. Acceptance criteria for design basis accidents may be supplemented by criteria that relate to severe accidents. These are typically core damage frequency, prevention of consequential damage to the containment, large early release frequency, probability of scenarios requiring emergency measures off the site, limitation of the release of specific radionuclides such as ^{137}Cs, dose limits and/or risks to the most exposed individual.

4. CONSERVATIVE DETERMINISTIC SAFETY ANALYSIS

CONSERVATIVE APPROACH

4.1. A conservative approach usually means that any parameter that has to be specified for the analysis should be allocated a value that will have an unfavourable effect in relation to specific acceptance criteria. The concept of conservative methods was introduced in the early days of safety analysis to take account of uncertainties due to the limited capability of modelling and the limited knowledge of physical phenomena, and to simplify the analysis.

4.2. In a traditional conservative analysis, both the assumed plant conditions and the physical models used are set conservatively. The reasoning is that such an approach would demonstrate that the calculated safety parameters are within the acceptance criteria and would ensure that no other transient of that category would exceed the acceptance criteria. This is Option 1 in Table 3. Option 2 is also considered to be a conservative approach, as described in para. 3.10.

4.3. However, for both Options 1 and 2, it should also be demonstrated that the calculated results are conservative for each application. The interaction with the set points for activation of the relevant safety systems or the plant control systems should be reviewed to ensure that the conservatism of the results is adequate.

INITIAL AND BOUNDARY CONDITIONS

4.4. The initial conditions are the assumed values of plant parameters at the start of the transient to be analysed. Examples of these parameters are reactor power level, power distribution, pressure, temperature and flow in the primary circuit.

4.5. The boundary conditions are the assumed values of parameters throughout the transient. Examples of boundary conditions are conditions due to the actuation of safety systems such as pumps and power supplies, leading to changes in flow rates, external sources and sinks for mass and energy, and other parameters during the course of the transient.

4.6. For the purpose of conservative calculations, the initial and boundary conditions should be set to values that will lead to conservative results for those safety parameters that are to be compared with the acceptance criteria. One set of conservative values for initial and boundary conditions does not necessarily lead to conservative results for every safety parameter. Therefore, the appropriate conservatism should be selected for each initial and boundary condition, depending on the specific transient and the associated acceptance criterion.

AVAILABILITY OF SYSTEMS AND COMPONENTS

4.7. In conservative analyses, the single failure criterion should be applied when determining the availability of systems and components. This criterion stipulates that the safety systems should be able to perform their specified functions when any single failure occurs. A failure should be assumed in the system or component that would have the largest negative effect on the calculated safety parameter.

4.8. All the common cause and consequential failures associated with the postulated initiating event should also be included in the analysis, in addition to the single failure. Furthermore, unavailability due to on-line maintenance should be considered if this is tolerated in plant operating procedures (see para. 5.37 of Ref. [1]).

4.9. In addition to the postulated initiating event itself, a loss of off-site power should be considered, as appropriate, when analysing design basis accidents. For such cases, the assumption that gives the most negative effect on the margin to the acceptance criterion should be chosen. Likewise, equipment that is not qualified for specific accident conditions should be assumed to fail unless its continued operation results in more unfavourable conditions. The malfunction of control systems and delays in the actuation of protection systems and safety systems should be taken into account in the analysis. For such systems, the issue of whether their continued functioning leads to more unfavourable conditions than does their non-availability should be addressed.

OPERATOR ACTIONS

4.10. For design purposes, credit should not be taken for operator action to limit the evolution of a design basis accident within a specified time. Exceptionally, the design may take credit for earlier operator action, but in these cases the actuation times should be conservative and should be fully justified. Conservative assumptions should be made with respect to the timing of operator actions. It should be assumed that in most cases post-accident recovery actions would be taken by the operator.

NODALIZATION AND PLANT MODELLING

4.11. In some cases, the results produced by conservative analysis are sensitive to decisions that are made by the user, such as the number and structure of nodes that are used. Such user effects could be particularly large for a conservative analysis whose results cannot be compared with plant data or experimental data. The procedures, code documentation and user guidelines should be carefully followed to limit such user effects. Procedures include issues such as the way to compile the input data set and the means of selecting the appropriate models in the code (discussed in Section 6).

5. BEST ESTIMATE PLUS UNCERTAINTY ANALYSIS

BEST ESTIMATE APPROACH

5.1. Conservative hypotheses were introduced in the early days of safety analysis to address the uncertainties that prevailed in the 1970s. Since then, for thermohydraulic issues, extensive experimental research has resulted in a considerable increase of knowledge, and the development of computer codes has improved the ability to achieve calculated results from simulations that correspond more accurately to experimental results.

5.2. The use of a conservative methodology may be so conservative that important safety issues may be masked. For example, the assumption of a high core power level may lead to high levels of steam–water mixture in the core in the case of a postulated small break loss of coolant accident. Consequently, the calculated peak cladding temperature may not be conservative. As another example, the assumption that reduced interfacial shear between water and steam may lead to higher cladding temperatures in the upper core region is conservative. However, this conservative assumption will lead to an optimistic estimate for the refilling/reflooding time, as it will appear that more water remains in the primary cooling system than is actually the case. In cases where a realistic analysis could demonstrate that important safety issues may be being masked, the conservative licensing calculations should be accompanied by a best estimate analysis, without an evaluation of the uncertainties, to ensure that important safety issues are not being concealed by the conservative analysis.

5.3. In addition, a conservative approach often may not show margins to acceptance criteria which, in reality, could be used to obtain greater operational flexibility.

5.4. To overcome these deficiencies, it may be preferable to use a best estimate approach together with an evaluation of the uncertainties to compare the results of calculations with acceptance criteria. This type of analysis is referred to as a best estimate plus uncertainties approach. A best estimate approach provides more realistic information about the physical behaviour of the reactor, identifies the most relevant safety issues and provides information about the existing margins between the results of calculations and the acceptance criteria. A best estimate approach may be used for accident scenarios in which the margin to the acceptance criterion is not very large. For scenarios with large margins to the acceptance criteria, it is more practical to use a conservative analysis in which detailed evaluation of the uncertainties is not performed.

5.5. For a best estimate analysis, a best estimate code (discussed below) or other tools that realistically describe the behaviour of physical processes in a component or system should be used. This requires sufficient data to be able to ensure that all important phenomena have been taken into account in the modelling or that their effects are bounded (see para. 5.9). Establishing that all important phenomena have been taken into account in the modelling or that their effects are bounded should be part of the validation programme (see Section 6).

5.6. Because the results of best estimate codes are not designed to bound experimental data, best estimate codes are not intended to provide conservative results. Uncertainties in the results due to unavoidable approximations in the modelling should therefore be quantified using experimental results. The trend in several States is to use best estimate plus uncertainty analysis, which is Option 3 in Table 3. This is especially important when values of safety parameters approach acceptance criteria, for example, 1200°C for peak cladding temperature in a pressurized water reactor. An evaluation of the uncertainties on the basis of one calculation that is selected on the basis of expert opinion to bound uncertainties in the modelling for the code may not be adequate in these cases.

5.7. Option 3 uses a combination of a best estimate computer code and realistic assumptions for the initial and boundary conditions. Such an approach should be based on statistically combined uncertainties for plant conditions and code models to establish, with a specified high probability, that the calculated results do not exceed the acceptance criteria. It is common practice to require that assurance be provided of a 95% or greater probability that the applicable acceptance criteria for a plant will not be exceeded. A probability of 100% (i.e. certainty) cannot be achieved because only a limited number of calculations can be performed. The 95% probability level is selected primarily to be consistent with standard engineering practice in regulatory matters. However, national regulations may require a different level of probability that the applicable acceptance criteria will not be exceeded.

5.8. Some parameters, such as the departure from nucleate boiling ratio in pressurized water reactors or the critical power ratio in boiling water reactors, have been found to be acceptable at the 95% probability level. Techniques may be applied that use additional confidence levels, for example, 95% confidence levels, with account taken of the possible sampling error due to the fact that a limited number of calculations have been performed.

5.9. The uncertainty in parameters associated with the results of a computer code may be determined with the assistance of a phenomena identification and ranking table (PIRT) for each event that is analysed. This is a process in which several experts perform evaluations to rank the importance of different phenomena for the scenarios that are being considered. The ranking should identify the most important phenomena for which the suitability of the code has to be assured and should be based to the extent possible on available data. The important parameters should be varied randomly in accordance with their respective probability distributions to determine the overall uncertainty. The same process can be applied to evaluate the applicability of a computer code or a computational tool to simulate a selected event.

5.10. A specific phenomena identification and ranking table should be developed for each event for which a computer code or methodology is used. Accidents of different types, such as large break loss of coolant accidents, small break loss of coolant accidents and transients, progress as a result of different phenomena and therefore require specific phenomena identification and ranking tables.

5.11. An alternative to relying completely on expert judgement in an analysis made on the basis of a phenomena identification and ranking table is to use a statistical method. Statistical methods are increasingly being used to provide information on the ranking of parameters.

5.12. Methods for quantifying uncertainties are mature and have been used for licensing purposes as well as in research on reactor safety.

5.13. The procedures, code documentation and user guidelines should be followed carefully to limit the influence of the user in performing 'best estimate plus uncertainties' analyses as well as in performing conservative analyses. Code validation and diversity also protect against user effects, as discussed in Section 6.

5.14. For severe accidents, the operator emergency procedures and severe accident management guidelines should be assessed in addition to the objective of showing compliance with the acceptance criteria. These analyses should include the use of all the systems or components that are available to mitigate the consequences of the accident, and they should be based on the best available knowledge. Some regulatory authorities require the licensee to demonstrate that a release criterion for a severe accident is met under the assumption that within a prescribed time period the operator does not take any action.

BEST ESTIMATE COMPUTER CODES

5.15. A best estimate calculation uses modelling in an attempt to describe realistically the physical processes that occur in a nuclear power plant. The key issue in using a best estimate approach, therefore, is the availability of computer codes that can be used to model realistically the important phenomena in and to simulate the behaviour of the plant systems. The codes that are capable of meeting these requirements are termed best estimate computer codes.

5.16. Best estimate computer codes have various levels of qualification, owing to, for example, the different levels of availability of experimental data or operational data, and the extent of independent assessment of such data. An extensive database is therefore needed to promote confidence in the use of best estimate computer codes and tools. The results obtained by using the code should be compared with the data in the database. This will also help to identify the uncertainties that are associated with best estimate calculations.

5.17. For best estimate analyses, the following classes of codes are available:

(a) System thermohydraulic codes;
(b) Core physics codes;
(c) Component specific or phenomenon specific codes;
(d) Computational fluid dynamics codes;
(e) Coupled codes.

5.18. System thermohydraulic codes include those computer codes (computational tools) that are capable of modelling, even separately, the primary system, the interface with the secondary system, the containment or the confinement system and other plant systems that are important to safety.

5.19. Core physics codes include computational tools that are specialized for performing detailed core physics calculations, including calculations of the neutron flux; calculations of the detailed power distribution (two dimensional or three dimensional); and criticality, long term burnup, fuel management and refuelling calculations.

5.20. Component specific or phenomenon specific codes include computational tools that are specialized for the evaluation of the steady state or transient performance of components of the nuclear steam supply system, such as fuel rods, the reactor core, pumps, valves or heat exchangers, or of individual phenomena, such as critical heat flux, fuel heat-up following reactivity excursions, dynamic loads on components associated with the occurrence of breaks and pressure wave propagation.

5.21. Computational fluid dynamics codes are used to solve equations for the conservation of mass, momentum and energy for different media with a high level of detail. The codes are typically used to model multicomponent distribution and mixing phenomena. Although these codes were originally developed to model one-phase flow in non-nuclear applications, there are many examples of their use in safety analyses. Development to extend computational fluid dynamics codes to two-phase flow regimes is ongoing.

5.22. Coupled codes include those computational tools that are formed by the combination of codes belonging to two or more classes. Examples of coupled codes are codes that combine three dimensional neutron kinetics and system thermohydraulics, and pressurized thermal shock codes, which combine thermohydraulics, stress analysis and fracture mechanics.

5.23. All the types of computational tool identified in para. 5.17 can be used to address issues and to provide results in a best estimate approach to licensing. Full application of the best estimate plus uncertainties method has been performed for evaluation of the acceptance criteria for the emergency core cooling system following design basis accidents and for evaluation of thermal margins for the core.

5.24. The quality of best estimate codes should be ensured when they are used for licensing. Validation and verification are essential steps in qualifying any computational method. They are the primary means of assessing the accuracy of computational simulations, as discussed in Section 6.

SENSITIVITY ANALYSIS AND UNCERTAINTY ANALYSIS

5.25. A sensitivity analysis includes systematic variation of the individual code input variables and of the individual parameters that are used in models, to determine their influence on the results of the calculations.

5.26. An uncertainty analysis should be performed to address the uncertainties in the code models, in the plant model and in plant data, including uncertainties in measurements and uncertainties in calibration, for the analysis of each individual event. The overall uncertainty in the results of a calculation should be obtained by combining the uncertainties associated with each individual input. Studies to quantify the scaling effect between an experimental arrangement and the actual plant size should also be considered.

5.27. Uncertainties of two different kinds, epistemic uncertainties and aleatory uncertainties, should be distinguished, and they should be treated separately.

5.28. Epistemic uncertainty derives from imperfect knowledge or incomplete information. The parameters that are uncertain have a definite but not precisely known value. Furthermore, in any model or analysis of a physical phenomenon, simplifications and assumptions are made. Even for relatively simple situations, a model may not include some aspects that are judged to be unimportant. Thus, simplifications contribute to the epistemic uncertainty, in addition to the uncertainty associated with the state of knowledge.

5.29. Epistemic uncertainty is directly addressed by uncertainty analysis and sensitivity analysis of the results obtained by using deterministic as well as probabilistic computational models. Such analyses quantify the uncertainty associated with the result of a computation and identify the principal sources of this uncertainty.

5.30. Aleatory uncertainty represents the unpredictable random performance of the system and its components and the associated values of plant parameters (e.g. the primary circuit pressure and temperature). The random failure of equipment is an example. Variables that are subject to aleatory uncertainty are random in nature. Aleatory uncertainty is addressed in a probabilistic safety analysis to quantify the ‘chance of occurrence’ of a system failure; that is, to express probabilistically how reliable the system is. Aleatory uncertainty also applies to operator actions.

5.31. Methods for performing uncertainty analysis have been published (e.g. in Ref. [4]). They include:

(a) Use of a combination of expert judgement, statistical techniques and sensitivity calculations;
(b) Use of scaled experimental data;
(c) Use of bounding scenario calculations.

5.32. For licensing purposes, sensitivity analyses are performed to identify the conditions that lead to the smallest margin to acceptance criteria. Subsequently, uncertainty analyses should be performed for the most limiting conditions.

5.33. Usually, a large number of parameters are used in performing safety analyses, contributing to the uncertainties in the results of calculations. Most methods for quantifying the uncertainty of results rely on identifying the input parameters that are considered to be uncertain. The input uncertainties are quantified by determining the range and distribution of possible values of model parameters. If this is not feasible, conservative values should be used. This should be performed for each phenomenon that is important to the analysis.

5.34. The evaluation of uncertainties is an essential element of using best estimate calculations to understand accident scenarios. The need to quantify the uncertainties in predictions made by using computer codes comes from the unavoidable approximations that are made in the modelling, including inadequate knowledge of the magnitude of a number of input parameters. The uncertainties in the results should therefore always be provided when a best estimate approach is used for a deterministic analysis. This evaluation of the uncertainties should include the uncertainties due both to the models and to the numerical methods used. The combined effect of both uncertainties can be evaluated using experimental data or by comparison with validated codes, as discussed in Section 6.

INITIAL AND BOUNDARY CONDITIONS

5.35. A plant input model should be used to define the status of the initial conditions and boundary conditions of the plant and the availability and performance of equipment. These conditions include the initial power, the pump performance, the valve actuation times and the functioning of the control systems. Uncertainties associated with the initial conditions and boundary conditions and with the characterization and performance of equipment should be taken into account in the analysis. It is acceptable to limit the variability to be considered by setting the values of the initial conditions and boundary conditions to conservative bounds. Setting the variability to conservative bounds is one way of not combining uncertainties of two different kinds, namely epistemic uncertainties and aleatory uncertainties, as discussed in paras 5.27–5.30.

5.36. In a deterministic safety analysis, the most limiting initial conditions that are expected over the lifetime of the plant should be used, and these are usually based on sensitivity analyses. As an example, the initial conditions for the safety analysis of a loss of coolant accident are presented below. The following unfavourable deterministic requirements may also be valid in a ‘best estimate’ approach:

(a) Most unfavourable single failure.
(b) Unavailability due to preventive maintenance during operation, if allowed, should be included in the analysis.
(c) Most unfavourable break location.
(d) Range of break sizes that results in the highest peak cladding temperature or other limiting values of the relevant safety variables that are to be compared with acceptance criteria.

(e) Range of longitudinal splits in the largest pipes that results in the highest peak cladding temperature or other limiting values of the relevant safety variables that are to be compared with acceptance criteria; the area of the maximum split is equal to twice the cross-sectional area of the pipe.
(f) Range of break sizes should be sufficiently broad that the system response as a function of break size is defined so that unreasonable results at any point in the range of break sizes can reliably be excluded; for this range, the break sizes should be evaluated in increments that are fine enough to resolve trends and peaks in the safety related variables that are of interest.
(g) Loss of off-site power.
(h) Initial core power should be specified for the most unfavourable conditions and values that may occur in normal operation, with account taken of the set points for integral power and power density control.
(i) Conservative values for the reactivity feedback coefficients.
(j) Time within the fuel cycle (i.e. beginning of cycle, end of cycle, burnup).
(k) Values of thermohydraulic parameters such as pressure, temperature, flow rates and water levels in the primary circuit and secondary circuit that result in the shortest time to uncovering of the core.
(l) Temperature conditions for the ultimate heat sink.
(m) The rod that has the greatest effect on reactivity is assumed to be stuck (in certain reactor designs).

5.37. Initial conditions that cannot occur in combination should not be considered when performing a realistic analysis. For example, the limiting decay heat and the limiting peaking factors cannot physically occur at the same time. For conservative analyses, the limiting values are combined. In the case of realistic analyses, the appropriate combination of decay heat and peaking factor may be used.

AVAILABILITY OF SYSTEMS: SINGLE FAILURE CRITERION AND LOSS OF OFF-SITE POWER

5.38. The licensing requirements with regard to the availability of systems should be the same regardless of whether a conservative approach or a best estimate approach is to be used. These licensing requirements are discussed in Section 4. They are currently the ‘most unfavourable single failure’ criterion and the assumption of a coincident loss of off-site power in the analysis of design basis accidents. With improvements in the development of methods for realistic analyses, these traditional assumptions might not always be applied in the future; for example, the most unfavourable single failure criterion might be relaxed by introducing probabilistic arguments for the availability of systems. This is governed by risk informed safety analysis, using Option 4 in Table 3, and is beyond the scope of this Safety Guide.

NODALIZATION AND PLANT MODELLING

5.39. The nodalization should be sufficiently detailed that all the important phenomena of the scenario and all the important design characteristics of the nuclear power plant that is being analysed are represented. Different input data sets may be necessary for different scenarios. A qualified nodalization that has successfully achieved agreement with experimental results for a given scenario should be used as far as possible for the same scenario when performing an analysis for a nuclear power plant. When scaled tests are used to assess a computer code, a consistent nodalization philosophy should be used for the test and for the full scale analysis of the plant. Sufficient sensitivity analyses should be performed on the nodalization to ensure that the calculated results are free from erratic variations.

6. VERIFICATION AND VALIDATION OF COMPUTER CODES

PROCESS MANAGEMENT

6.1. All activities that affect the quality of computer codes should be managed. This will require procedures that are specific to ensuring the quality of software [5, 6]. The best available software engineering practices that are applicable to the development and maintenance of software critical to safety should be applied. More specifically, formalized procedures and instructions should be put in place for the entire lifetime of the code, including code development, verification and validation, and a continued maintenance process with special attention to the reporting and correction of errors.

6.2. Code developers should ensure that the planned and systematic actions that are required to provide confidence that the code meets the functional requirements have been taken. The procedures should address, as a minimum, development control, document control, configuration of the code and testing, and corrective actions.

6.3. Procedures should be implemented to ensure that the code correctly performs all the intended functions and does not perform any unintended function.

6.4. The necessary activities can be categorized as follows:

(a) Preparation and upgrading of code manuals for developers and users;
(b) Verification and validation activities and their documentation;
(c) Error reporting and corrective actions and their documentation;
(d) Acceptance testing and installation of the code and upgrading of code manuals;
(e) Configuration management;
(f) Control of interfaces.

6.5. To minimize human errors in code development, only properly qualified personnel should be involved in the development, verification and validation of the code. Similarly, in user organizations, only suitably qualified personnel should use the code.

6.6. The quality management for the development of the code should be independent of the code developers. Audits of the development of the code should be conducted. Similarly, in user organizations, audits should be performed to ensure that the code is implemented and used correctly.

6.7. If some tasks of code development, verification or validation are delegated to an outside organization, those tasks should be managed to ensure quality within the outside organization. The parent organization should review arrangements within the outside organization and should audit their implementation.

6.8. As new versions of codes are developed, an established set of test cases should be simulated. Such simulations should be performed by the code developers and users, as appropriate.

PLAN FOR CODE VERIFICATION AND ITS IMPLEMENTATION

6.9. The plan for code verification should be prepared early in the development of the code. This should preferably be done when the functional requirements of the code are being written. The plan should include the objectives, approach, plan for testing, schedule, and arrangements for organization and management. The plan should be reviewed and updated as necessary.

6.10. Verification tasks should be assigned to the code developers. An independent verification process may be desirable and should be considered. The results of all verification activities should be documented and preserved as part of the system for quality management.

VERIFICATION OF THE CODE DESIGN

6.11. Verification of the code design should be performed to demonstrate that the code design conforms to the design requirements. In general, the verification of the code design should ensure that the numerical methods, the transformation of the numerical equations into a numerical scheme to provide solutions, and user options and their restrictions are appropriately implemented in accordance with the design requirements.

6.12. The verification of the code design should be performed by means of review, inspection and audit. Checklists should be provided for review and inspection. Audits should be performed on selected items to ensure quality.

6.13. The verification of the code design should include a review of the design concept, basic logic, flow diagrams, numerical methods, algorithms and computational environment. If the code is run on a hardware or software platform other than that on which the verification process was carried out, the continued validity of the code verification should be assessed.

6.14. The code design may contain the integration or coupling of codes. In such cases, verification of the code design should ensure that the links and/or interfaces between the codes are correctly designed and implemented to meet the design requirements.

VERIFICATION OF THE SOURCE CODE

6.15. Verification of the source code should be performed to demonstrate that it conforms to programming standards and language standards, and that its logic is consistent with the design specification.

6.16. The basic tools of verification of the source code are review, inspection and audit. Checklists should be provided for review and inspection. Comparisons with independent calculations should be carried out where practicable to verify that the mathematical operations are performed correctly. Audits should be performed on selected items to ensure quality.

6.17. A review and inspection of the entire code may not be practicable for verification purposes owing to its large size. In such cases, verification of individual modules or parts of the code should be conducted, and this should include a careful inspection of all interfaces between the modules.

ERRORS AND CORRECTIVE ACTIONS

6.18. An error is a non-compliance of the code or its documentation with the design requirements. All errors should be reported to and should be corrected by the code developer.

6.19. The tracking of errors and reporting of their correction status should be a continuous process and should be a part of code maintenance. The impacts of such errors on the results of analyses that have been completed and used as part of the safety assessment for a plant should be assessed.

CODE VALIDATION

Validation process

6.20. Validation should be performed on all computer codes that are used for the deterministic safety analysis of nuclear power plants. The purpose of validation (also referred to elsewhere as code qualification or code assessment) is to provide confidence in the ability of a code to predict, realistically or conservatively, the values of the safety parameter or parameters of interest. It should also quantify the accuracy with which the values of parameters can be calculated.

6.21. The major sources of information that should be used to assess the quality of computer code predictions are analytical solutions, experimental data, nuclear power plant transients and benchmark calculations (code to code comparisons).

6.22. For complex analysis, the validation process should be performed in two phases: the development phase, in which the assessment is done by the code developer, and the independent assessment phase, in which the assessment is performed by someone who is independent of the developer of the code. Both phases are necessary for an adequate assessment. If possible, the data that are used for the independent validation of the code and the data that are used for the validation by the code developers should be derived from different experiments.

6.23. The validation process should ideally include four different types of test calculation:

(1) *Basic tests.* Basic tests are simple test cases that may not be directly related to a nuclear power plant. These tests may have analytical solutions or may use correlations or data derived from experiments.
(2) *Separate effect tests.* Separate effect tests address specific phenomena that may occur at a nuclear power plant but do not address other phenomena that may occur at the same time. Separate effect tests should ideally be performed at full scale. In the absence of analytical solutions or experimental data, other codes that are known to model accurately the limited physics represented in the test case may be used to determine the accurate solution.
(3) *Integral tests.* Integral tests are test cases that are directly related to a nuclear power plant. All or most of the relevant physical processes are represented. However, these tests may be carried out at a reduced scale, may use substitute materials or may be performed at low pressure.
(4) *Nuclear power plant level tests and operational transients.* Nuclear power plant level tests are performed on an actual nuclear power plant. Validation through operational transients together with nuclear power plant tests are important means of quantifying the plant model.

6.24. The validation tests should ideally cover the entire range of values of parameters, conditions and physical processes that the code is intended to cover.

6.25. The scope of the independent validation exercise performed by the code user should be consistent with the intended purpose of the code and the range of experimental data available. The scope of validation should also be in accordance with the complexity of the code and the complexity of the physical processes that it represents. The code user should also evaluate the accuracy of the results of the calculations.

6.26. For complex applications, a validation matrix should be developed for code validation, because a code may predict one set of test data with a high degree of accuracy but may be extremely inaccurate for other data sets.

6.27. The validation matrix should include test data from different experimental facilities and different sets of conditions in the same facility, and it should ideally include basic tests, separate effect tests, integral tests and nuclear power plant level tests. If sufficient data from full scale experiments are not available, data from reduced scale experiments should be used, with appropriate consideration of scaling. The number and the selection of tests in the test matrix should be justified as being sufficient for the intended application of the code.

6.28. The range of validity and the limitations of a computer code, which are established as a result of validation, should be documented in a validation report which should be referenced in licensing documentation. However, code users may perform additional validation to demonstrate that the code satisfies the objectives for their specific application.

Assessment of validation calculations

6.29. The results of a validation should be used to determine the uncertainty of the results obtained by a code calculation. In assessing the uncertainty of a code, user effects should be minimized. Different methods are appropriate for assessing the uncertainty of the results from the methods used for validation test calculations.

6.30. For point data, the difference between values calculated using the code and experimental results may be determined directly or, in the case of a set of experimental results, by using the concept of mean and variance. For time dependent data, as a minimum a qualitative evaluation of the uncertainty should be performed.

6.31. As a result of the validation process, the uncertainty of the code and the range of validation should be known and should be considered in any results of safety analysis calculations.

6.32. It should be demonstrated that the conservative code bounds the experimental data and the uncertainties associated with the computer code models. The result of a conservative code should always be closer to the acceptance criterion than is the realistic value. This realistic value may come either from experimental results with the uncertainties taken into account or from a best estimate plus uncertainty calculation.

Qualification of input data

6.33. The input data for a computer code include some form of model that represents all or part of the nuclear power plant. There is usually a degree of flexibility in how the plant is modelled or nodalized. The input data that are used to perform safety assessment calculations should conform to the best practice guidelines for using the computer code (as in the user manual) and should be independently checked. The input data should be a compilation of information found in as-built and valid technical drawings, operating manuals, procedures, set point lists, pump performance charts, process diagrams and instrumentation diagrams, control diagrams, etc.

6.34. Users who prepare input data to model validation tests should be suitably qualified and should make use of all available guides. These include the specific code user guide, generic best practice guides for the type of code and guidance from more experienced users.

6.35. The validation process itself often enables the determination of best practices. This may include nodalization schemes, model options, solution methods and mesh densities. The best practice guidelines established during the validation process should be used by those who generate input data sets for safety analysis calculations.

Use of experimental databases

6.36. Although validation tests may be used to compare the code results with analytical solutions, or occasionally with results obtained by other codes, most validation tests should be based on experimental data. It therefore follows that the uncertainty in the code is directly related to the uncertainty in the experimental data. Care should therefore be exercised when planning an experiment to ensure that the measured data are as suitable as possible for the purposes of code validation.

6.37. The safety parameters that will ultimately be calculated using the code should be considered when the experiment and its instrumentation are planned.

6.38. To ensure that the code is validated for conditions that are as close as possible to those in a nuclear power plant, it should be ensured that the boundary conditions and initial conditions of the test are appropriate. Consideration should be given to scaling laws. A scaled experimental facility cannot be used to represent all the phenomena that are relevant for a full size facility. Thus, for each scaled facility that is used in the assessment process, the phenomena that are correctly represented and those that are not correctly represented should be identified. The effects of phenomena that are not correctly represented should be addressed in other ways.

6.39. The uncertainty in the experimental data should be reported in the documentation of the experiment. When performing a validation against experimental data, allowance for errors in the measurements should be included in the determination of the uncertainty of the computer code.

Role of benchmarks

6.40. Benchmarking consists of code to code comparisons that can be used for validation purposes provided that at least one of the codes has been validated.

6.41. Where possible, users should simulate validation tests without having any prior knowledge of the experimental results to preclude any deliberate tuning of code calculations to yield better agreement with experimental results.

7. RELATION OF DETERMINISTIC SAFETY ANALYSIS TO ENGINEERING ASPECTS OF SAFETY AND PROBABILISTIC SAFETY ANALYSIS

RELATION OF DETERMINISTIC SAFETY ANALYSIS TO ENGINEERING ASPECTS OF SAFETY

7.1. A key element of the safety analysis for a nuclear power plant is the demonstration that defence in depth is adequate, and deterministic safety analyses play a vital role in this demonstration. In accordance with Principle 8, para. 3.32 of Ref. [7], “Defence in depth is provided by an appropriate combination of:

—An effective management system with a strong management commitment to safety and a strong safety culture.
—Adequate site selection and the incorporation of good design and engineering features providing safety margins, diversity and redundancy….
—Comprehensive operational procedures and practices as well as accident management procedures.”

7.2. The second point above includes an “appropriate combination of inherent and engineered safety features” (Ref. [7], para. 3.32) in “a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available” (Ref. [7], para. 3.31). It is therefore necessary to identify the various accident scenarios in which each barrier could be threatened. The objective of deterministic safety analyses is to demonstrate that, in normal operational conditions and accident conditions, a sufficient number of barriers are retained. The transients during normal operation and the accident scenarios that are analysed should be the bounding scenarios within each frequency band, as discussed in Section 2. They should all be considered in the engineering design of the barriers and of other safety structures, systems and components. Possible internal and external initiating events should be considered when identifying the accident scenarios that should be analysed. These initiating events should include all those that may challenge the barriers for confining radioactive fission products and that may challenge the performance of systems that are intended to perform a safety function under all operational conditions. These possible internal and external initiating events are often referred to as postulated initiating events. All operational modes of the plant (full power, low power, hot and cold shutdown states, etc.) should be considered as initial conditions in the safety analyses.

7.3. The following approach should be taken to identify postulated initiating events, and examples are given:

(a) Identification of all mechanisms of barrier failure:
   (i) Fuel: swelling, cracking, fragmentation, melting, dispersion;
   (ii) Cladding: thermomechanical stress, mechanical interactions of pellet cladding, ballooning, thermal shock;
   (iii) Pressure boundary of the reactor coolant system: hot and cold overpressure, leaks and breaks, pressurized thermal shock, high energy break effects; jet effects such as dynamic pipe whip; isolation failure, crack propagation, bypass of the coolant system barrier;

(iv) Containment: overpressure (or underpressure for some designs of water moderated, water cooled energy reactor), high energy break effects; jet effects such as dynamic pipe whip; isolation failure, containment bypass;
(v) Secondary containment, if provided: impact loads, containment bypass, isolation failure.

(b) Identification of all processes that could cause the failure mechanisms to initiate:
(i) Thermal overpower: cooldown, rod withdrawal and/or ejection, dilution by fast boron, rod drop;
(ii) Mechanical loads: water hammer, seismic events;
(iii) Power to coolant mismatch: flow reduction or inventory reduction, heat flux increase, coolant heat-up, pressure reduction;
(iv) Crack growth: thermal fatigue, induced corrosion;
(v) Overpressure: inventory increase (hot and cold conditions), inventory expansion.

(c) Grouping of these processes by means of phenomenology:
(i) Increase and/or decrease of heat removal by the secondary system;
(ii) Decrease of flow in the reactor coolant system;
(iii) Anomalies in reactivity and power distribution;
(iv) Increase and/or decrease of reactor coolant inventory;
(v) Release of radioactive material from a subsystem or component.

(d) Identification of scenarios for each of the above groups, such as:
(i) Increase of heat removal by the secondary system:
— Decrease of feedwater temperature;
— Increase of feedwater flow;
— Increase of steam flow;
— Inadvertent opening of a steam generator relief valve or a safety valve;
— Failure of steam system piping inside and outside the containment.

(e) Postulated initiating events that lead to the above scenarios, such as:
(i) Increase of steam flow:
— Steam bypass opening;
— Increase of flow demand.
(ii) Decrease of feedwater temperature:
— Preheater bypass;
— Loss of preheating efficiency (intake of air, low steam flow).

(f) Determination of original cause:
  (i) Internal events:
    — Failures of structures, systems or components, including generated hazards, missiles, fire;
    — Operational and maintenance errors: inoperable safety systems.
  (ii) External events, including their possible combinations:
    — Natural events: earthquakes, flooding, winds, landslides;
    — Human induced events: air crashes, events in other industries;
    — Possible combinations: earthquake and flooding; fire and flooding.

7.4. A comprehensive functional analysis should be performed as a basis for the deterministic safety analysis. The requirements for each safety system and its supporting systems to fulfil its safety function, including their reliability, and the safety classification should be determined in accordance with the requirement to provide defence in depth.

7.5. To determine the adequacy of the initial conditions and boundary conditions that are assumed, a careful analysis should be made of the process that links the original cause, all the consequential failures and the initiating event itself. For example, an electrical short circuit in the switchyard may propagate a perturbation in the plant network that may make unavailable some specific safety systems that are needed to protect against a consequential loss of off-site power.

7.6. To demonstrate that safety margins are adequate for design basis accidents, analyses should be performed for each category of postulated initiating event. Regulatory requirements that include a frequency and/or dose relationship for design basis accidents may accept the failure of some barriers for less frequent accidents, provided that any release of radioactive material to the environment is acceptably low. An example is the failure of the fuel cladding as a result of a large loss of coolant accident.

7.7. Where there are acceptance criteria for beyond design basis accidents, including severe accidents, it should be demonstrated that the consequences would be acceptably low.

7.8. In the deterministic analysis, account should be taken of the redundancy that is provided for in the design of safety systems and support systems that are designed to prevent, limit or mitigate the consequences of an initiating event. Account should also be taken of the independence, diversity and physical separation that have been incorporated into the design to avoid possible common cause failures.

7.9. The time period that is assumed in the analysis for temporary inoperability should be based on the maintenance and repair activities that have been specified.

7.10. For each plant modification that may have an impact on safety, an analysis should be performed to demonstrate compliance with the acceptance criteria.

7.11. This process should follow the credited industry standards that are accepted by the regulatory body and should meet the requirements of the regulatory body. Any deviations from the standards should be justified.

7.12. Deterministic safety analyses are also performed to develop a set of rules, namely, the operational limits and conditions, which are commonly called technical specifications. These reflect the limiting conditions of operation in terms of values of process variables, system requirements, system operability, surveillance and testing requirements, etc., as well as the necessary actions to take when the conditions of the plant are degraded or are not covered by the safety analysis. The technical specifications should cover all the initial conditions and boundary conditions that will subsequently be used in the deterministic safety analyses that are performed to demonstrate the safety of the plant.

RELATION OF DETERMINISTIC SAFETY ANALYSIS TO PROBABILISTIC SAFETY ANALYSIS

7.13. A major part of the process of designing and licensing a nuclear power plant is the safety analysis. Reference [1] states that both deterministic methods and probabilistic methods are required to be applied. The objectives are to identify issues that are important to safety and to demonstrate that the plant is capable of meeting any authorized limits on the release of radioactive material and on the potential exposure to radiation for each plant state. Thus a deterministic safety analysis alone does not demonstrate the overall safety of the plant, and it should be complemented by a probabilistic safety analysis.

7.14. While deterministic analyses may be used to verify that acceptance criteria are met, probabilistic safety analyses may be used to determine the probability of damage for each barrier. Probabilistic safety analysis may thus be a suitable tool for evaluation of the risk that arises from low frequency sequences that lead to barrier damage, whereas a deterministic analysis is adequate for events of higher frequency for which the acceptance criteria are set in terms of the damage allowed. To verify that defence in depth is adequate, certain very low frequency design basis accidents, such as large break loss of coolant accidents or rod ejection accidents, are evaluated deterministically despite the low frequency of the initiating event. Thus deterministic analysis and probabilistic analysis provide a comprehensive view of the overall safety of the plant for the entire range of the frequency–consequence spectrum.

7.15. Deterministic safety analyses have an important part to play in the performance of a probabilistic safety analysis because they provide information on whether the accident scenario will result in the failure of a fission product barrier. Deterministic safety analysis should be used to identify challenges to the integrity of the physical barriers, to determine the failure mode of a barrier when challenged and to determine whether an accident scenario may challenge several barriers. Best estimate codes and data, as for Option 3 in Table 3, should be used to be consistent with the objectives of probabilistic safety analysis, which include providing realistic results. It should be recognized that the results of the supporting analyses are usually bounded by the results of conservative deterministic analyses.

7.16. A probabilistic safety analysis fault tree is a powerful tool that can be used to confirm assumptions that are commonly made in the deterministic calculation about the availability of systems; for example, to determine the potential for common cause failures or the minimum system requirements, to identify important single failures and to determine the adequacy of technical specifications.

8. APPLICATION OF DETERMINISTIC SAFETY ANALYSIS

AREAS OF APPLICATION

8.1. Deterministic safety analyses should be carried out for the following areas:

(a) *Design of nuclear power plants*. Such analyses require either a conservative approach or a best estimate analysis together with an evaluation of uncertainties.

(b) *Production of new or revised safety analysis reports for licensing purposes, including obtaining the approval of the regulatory body for modifications to a plant and to plant operation*. For such applications, both conservative approaches and best estimate plus uncertainty methods may be used.
(c) *Assessment by the regulatory body of safety analysis reports*. For such applications, both conservative approaches and best estimate plus uncertainty methods may be used.
(d) *Analysis of incidents that have occurred or of combinations of such incidents with other hypothetical faults*. Such analyses would normally require best estimate methods, in particular for complex occurrences that require a realistic simulation.
(e) *Development and maintenance of emergency operating procedures and accident management procedures*. Best estimate codes together with realistic assumptions should be used in these cases.
(f) *Refinement of previous safety analyses in the context of a periodic safety review to provide assurance that the original assessments and conclusions are still valid*.

8.2. Only 'frozen' (i.e. fixed) versions of codes should be used for the applications that are identified in para. 8.1. This is to ensure that concurrent piecemeal modifications will not be made. During the period of the analysis, the frozen version should be maintained as described in Section 6, and the only changes would be corrections. To ensure that the deterministic safety analysis is consistent and auditable, enhancements of the model and improvements to the code should not be permitted during an application.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE DESIGN OF NUCLEAR POWER PLANTS

8.3. The design basis for items that are important to safety is required to be established and confirmed by means of a comprehensive safety assessment (Ref. [1], paras 3.10, 3.11). With reference to the deterministic safety analysis, "The applicability of the analytical assumptions, methods and degree of conservatism used shall be verified" (Ref. [1], para. 5.72). The design basis comprises "design requirements for structures, systems and components important to safety that must be met for safe operation of a nuclear power plant, and for preventing or mitigating the consequences of events that could jeopardize safety" (Ref. [1], para. 1.5).

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE LICENSING OF NUCLEAR POWER PLANTS

8.4. Compliance with all applicable regulations and standards and other relevant safety requirements is essential for the safe and reliable operation of a nuclear power plant. This should be demonstrated by means of an initial or an updated safety analysis report.

8.5. "The safety analysis of the plant design … shall be consistent with the current or 'as built' state" (Ref. [1], para. 5.72). The safety analysis examines (Ref. [1], para. 2.7):

(a) All planned modes of the plant in normal operation;
(b) Plant performance in anticipated operational occurrences;
(c) Design basis accidents;
(d) Event sequences that may lead to beyond design basis accidents.

8.6. On the basis of this analysis, the robustness of the engineering design in performing its safety functions during postulated initiating events and accidents should be established. In addition, the effectiveness of the safety systems and safety related systems should be demonstrated, and guidance for emergency response should be provided.

8.7. Analyses should be performed for transients that can occur in all planned modes of the plant in normal operation, including operations during shutdown. This plant state was sometimes neglected in early safety analyses. For this mode of operation, the contributors to risk include: the inability to start some safety systems automatically; equipment in maintenance or in repair; reduced amounts of coolant in the primary circuit as well as in the secondary circuit for some modes; instrumentation switched off or non-functional and measurements not made; open primary circuit; and open containment. Where appropriate, the specific features of a best estimate analysis of shutdown transients should include thermal stratification of coolant in the reactor pressure vessel, low power, low inventory conditions, the presence of non-condensable gases and long term evolution of a transient. Every configuration of shutdown modes should be analysed. The main objectives of the analysis are to evaluate the ability of plant systems to perform safety functions and to determine the time available for the operators to establish safety functions. These safety functions include controlling the reactivity of the fuel, maintaining the ability to remove heat from the fuel, and maintaining the inventory of reactor coolant, the containment integrity and the availability of the power supply.

8.8. The range of scenarios should be evaluated to determine whether abrupt changes in the results of the analysis occur for a realistic variation of inputs (usually termed bifurcation or cliff edge effects; see footnote 2).

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE ASSESSMENT OF SAFETY ANALYSIS REPORTS

8.9. "The operating organization shall ensure that an independent verification of the safety assessment is performed by individuals or groups separate from those carrying out the design, before the design is submitted to the regulatory body" (Ref. [1], para. 3.13). Additional independent analyses of selected aspects may also be carried out by or on behalf of the regulatory body.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS IN PLANT MODIFICATIONS

8.10. A nuclear power plant may be modified on the basis of feedback from operating experience, the findings of periodic safety reviews, regulatory requirements, advances in knowledge or developments in technology. To comply with the requirements established in Ref. [1], para. 5.72, a revision of the safety analysis of the plant design should be made when major modifications or modernization programmes are implemented, when advances in technical knowledge and understanding of physical phenomena are made, when changes in the described plant configuration are implemented or when changes in operating procedures are made owing to operating experience.

8.11. The modification of existing nuclear power plants is normally undertaken to counteract the ageing of the plant, to justify the continued operation of the plant, to take advantage of developments in technology or to comply with changes to the applicable rules and regulations.

8.12. Other important applications of deterministic safety analysis are aimed at the more economical utilization of the reactor and the nuclear fuel. Such applications encompass uprating of the reactor power, the use of improved types of fuel and the use of innovative methods for core reloads. Such applications often imply that the safety margins to operating limits are reduced and special care should be taken to ensure that the limits are not exceeded.

8.13. All the effects of plant changes should be considered, and the analysis should cover all possible aspects of the plant changes. In addition, it should be demonstrated that the cumulative effects of the changes are acceptable.

8.14. Deterministic safety analyses should be used for safety improvements and to support modifications to improve the economy of the plant. In all cases, safe operation of the plant in accordance with the assumptions and intent of the design should be verified, and this should be the main focus of the deterministic safety analyses.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE ANALYSIS OF OPERATIONAL EVENTS

8.15. Accident analyses may be used as a tool for obtaining a full understanding of events that occur during the operation of nuclear power plants and should form an integral part of the feedback from operating experience. Operational events may be analysed with the following objectives:

(a) To check the adequacy of the selection of postulated initiating events;
(b) To determine whether the transients that have been analysed in the safety analysis report bound the event;
(c) To provide additional information on the time dependence of the values of parameters that are not directly observable using the plant instrumentation;
(d) To check whether the plant operators and plant systems performed as intended;
(e) To check and review emergency operating procedures;
(f) To identify any new safety issues and questions arising from the analyses;
(g) To support the resolution of potential safety issues that are identified in the analysis of an event;
(h) To analyse the severity of possible consequences in the event of additional failures (such as severe accident precursors);
(i) To validate and adjust the models in the computer codes that are used for analyses and in training simulators.

8.16. The analysis of operational events requires the use of a best estimate approach. Actual plant data should be used. If there is a lack of detailed information on the plant state, sensitivity studies, with the variation of certain parameters, should be performed.

8.17. The evaluation of safety significant events is a very important aspect of the feedback from operating experience. Modern best estimate computer codes make it possible to investigate and to gain a detailed understanding of plant behaviour. Conclusions from such analyses should be incorporated into the plant procedures that address the use of feedback from operating experience.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE DEVELOPMENT AND VALIDATION OF EMERGENCY OPERATING PROCEDURES

8.18. Best estimate deterministic safety analyses should be performed to confirm the strategies that have been developed to restore normal operational conditions at the plant following transients due to anticipated operational occurrences and design basis accidents. These strategies are reflected in the emergency operating procedures that define the actions that should be taken during such events. Deterministic safety analyses are required to provide the input that is necessary to specify the operator actions to be taken in response to some accidents, and the analyses should be an important element of the review of accident management strategies. In the development of the recovery strategies, to establish the available time period for the operator to take effective action, sensitivity calculations should be carried out on the timing of the necessary operator actions, and these calculations may be used to optimize the procedures.

8.19. After the emergency operating procedures have been developed, a validation analysis should be performed. This analysis is usually performed by using a qualified simulator. The validation should confirm that a trained operator can perform the specified actions within the time period allowed and that the reactor will reach a safe end state. Possible failures of plant systems and possible errors by the operator should be considered in the sensitivity analyses.

8.20. When the predictions of a computer code that has been used to support or to verify an emergency operating procedure do not agree with observed plant behaviour during an event, the code and the procedure should be reviewed. Any changes that are made to the emergency operating procedure should be consistent with the observed plant behaviour.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO THE DEVELOPMENT OF GUIDELINES FOR THE MANAGEMENT OF SEVERE ACCIDENTS

8.21. Deterministic safety analyses should also be performed to assist the development of the strategy that an operator should follow if the emergency operating procedures fail to prevent a severe accident from occurring. The analyses should be carried out by using one or more of the specialized computer codes that are available to model relevant physical phenomena. For light water reactors, these phenomena include thermohydraulic effects, heating and melting of the reactor core, retention of the molten core in the lower plenum, interactions between molten core and concrete, steam explosions, hydrogen generation and combustion, and fission product behaviour.

8.22. The analyses should be used to identify what challenges can be expected during the progression of accidents and which phenomena will occur. They should be used to provide the basis for developing a set of guidelines for managing accidents and mitigating their consequences.

8.23. The analysis should start with the selection of the accident sequences that, without intervention by the operator, would lead to core damage. A grouping of accident sequences with similar characteristics should be used to limit the number of sequences that need to be analysed. Such a categorization may be based on several indicators of the state of the plant: the postulated initiating event, the shutdown status, the status of the emergency core cooling systems, the coolant pressure boundary, the secondary heat sink, the system for the removal of containment heat and the containment boundary.

8.24. The measures can be broadly divided into preventive measures and mitigatory actions. Both categories should be subject to analysis.

8.25. Preventive measures are recovery strategies to prevent core damage. They should be analysed to investigate what actions are possible to inhibit or delay the onset of core damage. Examples of such actions are: various manual restorations of systems; primary and secondary feed and bleed; depressurization of the primary or secondary system; and restarting of the reactor coolant pumps. Conditions for the initiation of the actions should be specified, as should criteria for when to stop the actions or to change to another action.

8.26. Mitigatory measures are strategies for managing severe accidents to mitigate the consequences of core melt. Such strategies include: coolant injection into the degraded core; depressurization of the primary circuit; operation of containment sprays; and use of the fan coolers, hydrogen recombiners and filtered venting that are available in the reactors of different types that are in operation or being constructed. Possible adverse effects that may occur as a consequence of taking mitigatory measures should be taken into account, such as pressure spikes, hydrogen generation, return to criticality, steam explosions, thermal shock or hydrogen deflagration or detonation.

APPLICATION OF DETERMINISTIC SAFETY ANALYSIS TO PERIODIC SAFETY REVIEWS

8.27. New deterministic analyses may be required to refine previous safety analyses in the context of a periodic safety review, to provide assurance that the original assessments and conclusions are still valid. In such analyses, account should be taken of any margins that may have become reduced and that continue to be reduced owing to ageing over the period under consideration. Best estimate analyses together with an evaluation of the uncertainties may be appropriate to demonstrate that the remaining margins are adequate.

9. SOURCE TERM EVALUATION FOR OPERATIONAL STATES AND ACCIDENT CONDITIONS

USE OF THE SOURCE TERM IN DESIGN AND REGULATION

Nature of the evaluation

9.1. To evaluate the source term from a nuclear power plant, it is necessary to know the sources of radiation, to evaluate the inventories of radionuclides that may occur at the plant and to know the mechanisms by means of which radioactive material can be transmitted through the plant and released to the environment.

Purpose of the evaluation

9.2. Source terms should be evaluated for operational states and accident conditions for the following reasons:

(a) To ensure that the design is optimized so that the source term will be reduced to a level that is as low as reasonably achievable;
(b) To demonstrate that the design ensures that requirements for radiation protection, including restrictions on doses, are met;
(c) To provide a basis for the emergency planning arrangements that are required to protect the public in the vicinity of the reactor;
(d) To demonstrate that the qualification of equipment that is required to survive design basis accidents, including instruments and gas treatment systems, is adequate.

9.3. In addition, source terms may be evaluated to support software for use in emergency planning that employs theoretical source terms related to the damage to the plant to provide an early indication of what emergency measures are required. This allows decisions to be made early, before measurements of the activity levels of released radioactive material outside the plant can be made.

Optimization of the design

9.4. An evaluation of the behaviour of fission products, radioactive corrosion products, activation products in coolant and impurities, and actinides following possible accidents of each type at the plant should be carried out early in the design stage. This is required to identify the most important phenomena that affect their behaviour and to identify the possible design features that could increase their retention in the plant. Subsequent analyses should be made to determine the effectiveness of each of the design options so that all those that are effective and that can be engineered at a reasonable cost may be included in the design. Thus, development of the design of the reactor and evaluation of the behaviour of radioactive material and its potential release to the atmosphere after possible accidents should be an iterative process. This is essential to ensuring that the design is optimized.

Regulatory compliance and siting

9.5. Safety criteria should be defined for the safety analysis, and these criteria should be sufficient to meet the fundamental safety objective and fundamental principles established in Ref. [7], the radiation protection requirements established in Ref. [8] and the requirements of the regulatory body. In addition, detailed criteria may be developed to assist in assessing compliance with these higher level principles and requirements, including risk criteria, which relate to the probability of accidents with significant radiological consequences occurring, as discussed in paras 3.15 and 3.16.

9.6. In addition, para. 2.12 of Ref. [9] requires that “For each proposed site the potential radiological impacts in operational states and in accident conditions on people in the region, including impacts that could lead to emergency measures, shall be evaluated with due consideration of the relevant factors, including population distribution, dietary habits, use of land and water, and the radiological impacts of any other releases of radioactive material in the region.”

9.7. Thus, the levels of dose or of risk that should not be exceeded following design basis accidents should be specified in the regulatory regime under which a nuclear power plant is licensed or in the requirements of the associated environmental assessment (Ref. [1], para. 2.4). Such regulatory requirements usually become less restrictive as the frequency of the postulated accidents decreases. There are also requirements that refer to beyond design basis accidents. These may be expressed in terms of the total risk to an individual or the total probability of all accidents that would lead to an impact that is greater than would be acceptable for a design basis accident. This impact may be defined in terms of the dose to a reference person and/or a surrogate measure, such as the total frequency of core damage or of the release of radioactive material above a specified threshold level for specific key radionuclides or groups of radionuclides. Requirements that are expressed in terms of the release of radioactive material allow concerns about the level of impacts on people collectively and on the environment, rather than just on the individual most at risk, to be taken into account in the regulatory requirements. This may have important consequences for the acceptability of nuclear power plants to the public.

9.8. Where requirements are expressed in terms of releases of radioactive material, they include the most radiologically important radionuclides, namely, the isotopes of the noble gases, iodine and caesium.

9.9. To demonstrate compliance with regulatory numerical limits that are expressed in terms of dose, the evaluation of the source terms should be followed by an evaluation of the radiological consequences, as described in Ref. [10]. To demonstrate compliance with a risk target, Level 1, 2 and 3 probabilistic safety analyses should be carried out.

9.10. As well as achieving compliance with regulatory limits and targets, the design should ensure that there is not a rapid increase in the source term for those faults that are considered that have frequencies just beyond those for the design basis. This is sometimes referred to as a cliff edge effect (see footnote 2). It should be part of the regulatory requirements to demonstrate that such an effect does not occur.

Emergency planning

9.11. For every reactor, there should be an emergency plan that is based on a reference accident or reference accidents, and this or these may be subject to approval by the regulatory body [11]. For these accidents, the radiological consequences should be evaluated for conservative weather conditions and for a range of wind directions that could potentially lead to impacts on the local population and on the environment.

NORMAL OPERATIONAL STATES

9.12. The evaluation before a plant is operated of the source terms for normal operational states should include all the radionuclides that, owing to either liquid discharges or gaseous discharges, may make a significant contribution to doses. The derivation of source terms for normal operational states is discussed in annex II of Ref. [12].

Corrosion products

9.13. The evaluation of the full power activity of the reactor coolant should be made on the basis of the best operational data that are available for the particular type of nuclear power plant, the materials of the primary circuit and the chemical regime under which the plant is operated. The data should be relevant to the fuel cycles for which the activity of the primary coolant is expected to be greatest, which is normally after five years, when the activity of ^{60}Co has reached equilibrium.

9.14. Because the range of activity of the primary coolant in similar reactors is so large, there is a danger that using a bounding case value may be unnecessarily conservative. The source term should thus be based on a reasonably conservative value. However, a reactor will be shut down periodically for refuelling and maintenance, and may experience some unplanned trips during a fuel cycle. During these transients, the activity of the primary coolant will increase by about two orders of magnitude. The cumulative release of corrosion products during these transients should be derived on the basis of operational data, and this release should be taken into account when evaluating the quantity of corrosion products that may enter the primary coolant.

9.15. The annual release of radioactive material to the environment can be evaluated by using an average value for the activity of the primary coolant, the fraction of the primary coolant that enters the management system for liquid waste and the decontamination factors that are appropriate for each of the components through which each waste stream passes. Both the planned letdown of primary coolant and leakages should be taken into account in the calculation of the amount of primary coolant that enters the waste management system. Both the amount of primary coolant that is predicted to leak and the decontamination factors should be calculated on the basis of operating experience.

Fission products

9.16. Operating experience in all nuclear power plants shows that the levels of activity of fission products in the coolant vary considerably with time over the fuel cycle, even for the same reactor. The evaluation of the full power activity of the reactor coolant should therefore be based on the best operational data that are available for the same types of reactor, fuel, burnup rate, letdown flow rate and cleanup efficiency as in the case that is being evaluated. The data should be relevant to the fuel cycles for which the activity of the primary coolant is expected to be greatest, which is normally an equilibrium fuel cycle. Again, the source term should be calculated on the basis of a reasonably conservative value of the primary coolant activity, which may be the operational limit for the activity of the primary coolant.

9.17. During the shutdown transient and any unplanned reactor trips, unless the fuel cladding provides a perfect seal, which is rarely the case, the levels of non-gaseous fission products in the reactor coolant will increase sharply. This phenomenon is known as spiking. Again, operational data show that there are large variations in the enhanced release due to spiking and the rate at which the release occurs. Values for the effect of spiking on the activity of the primary coolant should be derived from the relevant operational data in the same way as is discussed for the equilibrium activity of fission products in para. 9.16. This may be related to the operational limit for the activity of the primary coolant, which in turn is related to the level of fuel failures.

9.18. Once the annual average activity of fission products in the reactor coolant has been evaluated, the source term due to liquid discharges should be derived in the same way as that due to corrosion products.

ACCIDENT CONDITIONS

Scope of the analysis

9.19. The consequences associated with all identified fault conditions or accident conditions should be addressed in the safety analysis of a nuclear power plant [13]. The safety analysis should identify all internal and external events and processes that may have an impact on physical barriers for containing radioactive material or that may otherwise give rise to radiological risks. The selection of events and processes to be considered in the safety analyses should be made on the basis of a systematic, logical and structured approach, and should provide justification that the identification of all scenarios relevant to safety is sufficiently comprehensive.

9.20. The starting point for the safety analysis should thus be the identification of the set of postulated initiating events that should be addressed. These will include both internal events and external events. Typical categories of internal events are specified in Section 2; however, for the purpose of deriving source terms, the following categories are more useful.

Releases into the containment

9.21. For many types of postulated accident, the important release of radionuclides would be from the reactor core into the primary circuit and, for power reactors, from the core into the containment or the confinement system. Evaluation of the source term should thus involve determining the behaviour of the radioactive species along this route; their retention in the containment or the confinement system; their release to the secondary containment, if one is provided; and their subsequent release to the atmosphere.

9.22. Separate analyses of the source term should be carried out for each type of fault for which the phenomena that would affect the source term would be different. For example, for a light water reactor, the following design basis faults should be included in the analysis:

(a) Reactivity faults for which the rapid increase in reactivity would result in an increase in the release of fission products from the fuel matrix to the fuel–cladding gap and in the failure of some of the fuel cladding. For faults of this type, the extent to which there would be a departure from nucleate boiling or the critical power ratio, or an excess of energy built up in the fuel and the degree of fuel failure that would occur as a result should be determined.
(b) Large loss of coolant accidents in which the severe transient would also lead to an increase in the release of fission products from the fuel matrix to the fuel–cladding gap and failure of some of the fuel cladding.
(c) Small loss of coolant accidents in which the transient would be less severe and the release of fission products from the fuel matrix to the fuel–cladding gap would not be significantly increased, but some of the fuel cladding might fail.
(d) Very small loss of coolant accidents in which the loss of coolant is less than the make-up flow, no fuel failures would occur and the release of fission products into the containment would be limited to the radioactive material that is in the primary coolant.

9.23. A similar range of different types of fault should be considered in the evaluation of the source terms that would result from severe accidents that involve significant core degradation. In this case, the very small loss of coolant accident would not apply.

Bypass accidents

9.24. The evaluation of source terms should also include a comprehensive analysis of postulated accidents in which the release of radioactive material would occur outside the containment. For example, a loss of reactor coolant might involve a break in a system such as the secondary circuit that is outside the containment, and there would be a potential for the containment to be bypassed if there were a leakage path between the primary and secondary circuits. Accidents in which the release of radioactive material could bypass the containment form a very important category, because a bypass accident with a relatively small release of radioactive material from the fuel may have the same radiological consequences as an accident with a large release into the intact containment. Moreover, such bypass accidents do not allow much time for taking action to protect the public in the vicinity of the plant.

9.25. Examples of bypass accidents in pressurized water reactors include:

(a) Leaks or pipe breaks in the secondary circuit accompanied by rupture of a steam generator tube;
(b) Leaks or pipe breaks in systems that are connected directly to the primary circuit, such as residual heat removal systems and chemical and volume control systems if these systems are outside the containment.

9.26. As well as potentially being design basis accidents, these faults could be either the cause or the consequence of a severe accident, and the appropriate source terms should be evaluated.

9.27. Handling accidents with irradiated fuel and spent fuel should also be evaluated. Such accidents can occur both inside and outside the containment. A fuel handling accident outside the containment may provide the bounding scenario, because if a loss of power resulted in a loss of ventilation in the fuel building, the radioactive material that would be released from the damaged fuel would leak directly to the atmosphere.

9.28. In addition, there are a number of other different types of accident that would result in a release of radioactive material outside the containment and whose source term should be evaluated. Such accidents include:

(a) A reduction in or loss of cooling of the fuel in the spent fuel storage pond;
(b) A criticality accident in the spent fuel building;
(c) A leak or pipe break in any of the other auxiliary systems that carry liquid or gaseous radioactive material;
(d) A failure in systems or components such as filters or delay tanks that are intended to reduce the level of discharges of radioactive material during normal operation;
(e) Fires or other hazards that may cause radioactive material to be released from accumulations outside the containment such as storage facilities for radioactive waste and components in treatment systems for radioactive waste.

External events

9.29. All postulated initiating events that could originate outside the plant should also be identified in the safety analysis. Examples are earthquakes, fires, floods, extreme weather conditions, volcanic eruptions, aircraft crashes, nearby industrial activities and sabotage [14]. In general, these would result in accidents similar in nature to those arising from internal events that might lead to a release of radioactive material, but the magnitude of the release may be different. For example, a release following a fire due to an aircraft crash might be much greater than releases resulting from internal fires. The main design requirements associated with protecting against external events involve designing structures, systems and components to perform their safety functions if such events were to occur.

Reactor states and plant states

9.30. All relevant states of the reactor, including full power, shutdown and transitional states, should be considered in the identification of postulated initiating events. Major changes to the state of important plant systems that are intended to retain radioactive material should also be identified. For example, in a pressurized water reactor, the containment will be open for part of the time during a shutdown for refuelling or maintenance.

Consequential and coincident failures

9.31. In addition to the postulated initiating events, the potential consequential or coincident failures that may occur should also be identified in the safety analysis. Failures of systems that would increase the retention of radioactive material in the plant, such as the spray system in the containment or the ventilation system in auxiliary buildings, fuel buildings or buildings for the management of radioactive waste, are of particular importance in the evaluation of the source term.

Grouping

9.32. A comprehensive identification of all possible accident sequences will result in a large number of possible sequences, and it would be impracticable to perform a separate evaluation of the source term for each sequence. The sequences should therefore be grouped, and a bounding scenario should be chosen for each group. The source term should be evaluated for this bounding scenario, and this source term should be considered to encompass the source terms for the other accidents in the same group.

9.33. The basis for the grouping should be accidents that are in the same frequency band and which are similar in terms of the associated phenomena that will affect the behaviour of radioactive material.

9.34. For each frequency band, the source term should be evaluated for the types of accident that would result in the greatest radiological consequences. Source terms may be evaluated for other accidents of the same type that have higher frequencies and lower radiological consequences if this is necessary to demonstrate compliance with a combined target for frequency of accidents and radiological consequences in terms of doses.

9.35. For severe accidents, source terms should be evaluated for accidents of each type in which different phenomena that affect the behaviour of radioactive material will occur.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).
[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4, IAEA, Vienna (2009).
[3] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2007 Edition), IAEA, Vienna (2007).
[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants, Safety Reports Series No. 23, IAEA, Vienna (2002).
[5] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).
[6] 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).
[7] 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).
[8] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANISATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, IAEA Safety Series No. 115, IAEA, Vienna (1996).
[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3, IAEA, Vienna (2003).
[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Generic Models for Use in Assessing the Impact of Discharges of Radioactive Substances to the Environment, Safety Reports Series No. 19, IAEA, Vienna (2001).
[11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE CO-ORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).
[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.13, IAEA, Vienna (2005).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Control of Radioactive Discharges to the Environment, IAEA Safety Standards Series No. WS-G-2.3, IAEA, Vienna (2000).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

CONTRIBUTORS TO DRAFTING AND REVIEW

D'Auria, F.	University of Pisa, Italy
Dusic, M.	International Atomic Energy Agency
Dutton, L.M.C.	Committee on Radioactive Waste Management, United Kingdom
Fry, C.	Serco Assurance, United Kingdom
Glaeser, H.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Kim, I.G.	Korea Institute of Nuclear Safety, Republic of Korea
Lee, S.H.	International Atomic Energy Agency
Mavko, B.	Jožef Stefan Institute, Slovenia
Pelayo, F.	Consejo de Seguridad Nuclear, Spain
Petruzzi, A.	University of Pisa, Italy
Sandervag, O.	Swedish Nuclear Power Inspectorate, Sweden

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.

No. 21, July 2006

IAEA
International Atomic Energy Agency

Where to order IAEA publications

In the following countries IAEA publications may be purchased from the sources listed below, or from major local booksellers. Payment may be made in local currency or with UNESCO coupons.

Australia
DA Information Services, 648 Whitehorse Road, Mitcham Victoria 3132
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

Belgium
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Telephone: +32 2 538 43 08 • Fax: +32 2 538 08 41
Email: jean.de.lannoy@infoboard.be • Web site: http://www.jean-de-lannoy.be

Canada
Bernan Associates, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: order@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Telephone: +613 745 2665 • Fax: +613 745 7660
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

China
IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

Czech Republic
Suweco CZ, S.R.O. Klecakova 347, 180 21 Praha 9
Telephone: +420 26603 5364 • Fax: +420 28482 1646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

Finland
Akateeminen Kirjakauppa, PL 128 (Keskuskatu 1), FIN-00101 Helsinki
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

France
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90 • Email: formedit@formedit.fr

Lavoisier SAS, 14 rue de Provigny, 94236 Cachan Cedex
Telephone: + 33 1 47 40 67 00 • Fax +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

Germany
UNO-Verlag, Vertriebs- und Verlags GmbH, August-Bebel-Allee 6, D-53175 Bonn
Telephone: +49 02 28 949 02-0 • Fax: +49 02 28 949 02-22
Email: info@uno-verlag.de • Web site: http://www.uno-verlag.de

Hungary
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472 • Email: books@librotrade.hu

India
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Telephone: +91 22 22617926/27 • Fax: +91 22 22617928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell, 24/4800, Ansari Road, Darya Ganj, New Delhi 110002
Telephone: +91 11 23268786, +91 11 23257264 • Fax: +91 11 23281315
Email: bookwell@vsnl.net • Web site: http://www.bookwellindia.com

Italy
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-20146 Milan
Telephone: +39 02 48 95 45 52 or 48 95 45 62 • Fax: +39 02 48 95 45 48

Japan
Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Telephone: +81 3 3275 8582 • Fax: +81 3 3275 9072
Email: journal@maruzen.co.jp • Web site: http://www.maruzen.co.jp

Korea, Republic of
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Telephone: +02 589 1740 • Fax: +02 589 1746
Email: sj8142@kins.co.kr • Web site: http://www.kins.co.kr

Netherlands
Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Telephone: +31 793 684 400 • Fax: +31 793 615 698 • Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Telephone: +31 252 435 111 • Fax: +31 252 415 888 • Email: infoho@swets.nl • Web site: http://www.swets.nl

New Zealand
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

Slovenia
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.cankarjeva-z.si/uvoz

Spain
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Telephone: +34 91 781 94 80 • Fax: +34 91 575 55 63 • Email: compras@diazdesantos.es
carmela@diazdesantos.es • barcelona@diazdesantos.es • julio@diazdesantos.es
Web site: http://www.diazdesantos.es

United Kingdom
The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Telephone (orders): +44 870 600 5552 • (enquiries): +44 207 873 8372 • Fax: +44 207 873 8203
Email (orders): book.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

On-line orders:
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Email: info@profbooks.com • Web site: http://www.profbooks.com

Books on the Environment:
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Telephone: +44 1438748111 • Fax: +44 1438748844
Email: orders@earthprint.com • Web site: http://www.earthprint.com

United Nations (UN)
Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
Telephone: +800 253-9646 or +212 963-8302 • Fax: +212 963-3489
Email: publications@un.org • Web site: http://www.un.org

United States of America
Bernan Associates, 4611-F Assembly Drive, Lanham, MD 20706-4391
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: order@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Telephone: +888 551 7470 (toll-free) • Fax: +888 568 8546 (toll-free)
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders and requests for information may also be addressed directly to:

Sales and Promotion Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 (or 22530) • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

09-48241

RELATED PUBLICATIONS

FUNDAMENTAL SAFETY PRINCIPLES
IAEA Safety Standards Series No. SF-1
STI/PUB/1273 (37 pp.; 2006)
ISBN 92–0–110706–4 Price: €25.00

SAFETY ASSESSMENT FOR FACILITIES AND ACTIVITIES
IAEA Safety Standards Series No. GSR Part 4
STI/PUB/1375 (40 pp.; 2009)
ISBN 978–92–0–112808–9 Price: €48.00

SAFETY OF NUCLEAR POWER PLANTS: DESIGN SAFETY REQUIREMENTS
IAEA Safety Standards Series No. NS-R-1
STI/PUB/1099 (65 pp.; 2000)
ISBN 92–0–101900–9 Price: €14.50

THE MANAGEMENT SYSTEM FOR FACILITIES AND ACTIVITIES
IAEA Safety Standards Series No. GS-R-3
STI/PUB/1252 (39 pp.; 2006)
ISBN 92–0–106506–X Price: €25.00

APPLICATION OF THE MANAGEMENT SYSTEM FOR FACILITIES AND ACTIVITIES
IAEA Safety Standards Series No. GS-G-3.1
STI/PUB/1253 (142 pp.; 2006)
ISBN 92–0–106606–6 Price: €31.00

THE MANAGEMENT SYSTEM FOR NUCLEAR INSTALLATIONS
IAEA Safety Standards Series No. GS-G-3.5
STI/PUB/1392 (139 pp.; 2009)
ISBN 978–92–0–103409–0 Price: €35.00

This publication has been superseded by SSG-2 (Rev. 1).

Safety through international standards

The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.

This fundamental safety objective of protecting people — individually and collectively — and the environment has to be achieved without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks.

— Fundamental Safety Principles: Safety Fundamentals,
IAEA Safety Standards Series No. SF-1 (2006)

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–113309–0
ISSN 1020–525X