IAEA-TECDOC-801

Development of safety principles for the design of future nuclear power plants

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The originating Section of this publication in the IAEA was:

Engineering Safety Section
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

DEVELOPMENT OF SAFETY PRINCIPLES FOR THE DESIGN OF FUTURE NUCLEAR POWER PLANTS
IAEA, VIENNA, 1995
IAEA-TECDOC-801
ISSN 1011–4289

Printed by the IAEA in Austria
June 1995

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

FOREWORD

In September 1991 the General Conference of the IAEA, in its Resolution GC(XXXV)/RES/553, having noted with appreciation the results of the International Conference on the Safety of Nuclear Power — Strategy for the Future, held in Vienna, from 2 to 6 September 1991, invited the Director General "to set up a small group of experts to develop safety principles for the design of future reactors, using a step-by-step approach based — inter alia — on the work of INSAG and taking into account the characteristics of various reactor types".

Safety objectives, requirements and features of future reactor designs were discussed at a Technical Committee Meeting held at the IAEA in Vienna from 11 to 15 November 1991. During the meeting desirable safety enhancements and topics relevant to the development of new principles and criteria were identified. As a follow-up to this meeting a small group of experts prepared a background paper on the development of safety principles for future nuclear power plants (NPPs).

The Advisory Group which met in Vienna from 29 June to 3 July 1992 considered the material prepared by the group of experts to be a useful starting point. Items for further investigation were identified. The Advisory Group reaffirmed that the development of safety principles for future NPPs should be based on existing recommendations, including those made by the International Nuclear Safety Advisory Group (INSAG), with any necessary additions and refinements, and suggested that this task might be carried out by a further small group of experts drawn — inter alia — from the membership of the Advisory Group.

The next step was the preparation, with the help of these experts, of a technical document on safety principles for the design of future NPPs. In December 1992 a group of consultants compiled material for the TECDOC. In April 1993 a Technical Committee reviewed the aforementioned material and prepared a draft of the present publication.

The Technical Committee considered that relatively minor modifications to some of the main safety objectives and safety principles in Safety Series No. 75-INSAG-3 could, with the addition of a small number of further principles and significant new amplifying text, result in a comprehensive set of safety objectives and safety principles for the design of future NPPs. This could then serve as a bridge between the IAEA's Safety Fundamentals and more detailed safety related publications. It could also serve as a framework for the development by Member States of comprehensive criteria and guidance, or as input to INSAG for their consideration in further updates to their documents. This was a challenging task, given the diverse views and existing standards and practices around the world. Ultimately, the publication of this TECDOC was seen as a major step forward in harmonizing these various views.

According to the recommendations of the IAEA Board of Governors in September 1993, INSAG reviewed the draft version of the TECDOC and concluded that it would be 'a useful first step' in the development of such principles, but that 'wide-ranging discussion and consultations' would be necessary before its finalization.

In April 1994 an Advisory Group prepared a new version of the present TECDOC, taking into account the comments of INSAG and of experts in various Member States. In October 1994 a group of consultants reviewed the comments received and prepared a further version which was finally edited by a small group of consultants in November 1994.

The IAEA is grateful to the many experts who contributed to this publication, either as participants at the meetings or with their comments on the drafts. The officers of the IAEA responsible for the TECDOC were L. Kabanov and M. Gasparini of the Division of Nuclear Safety, and C. Goetzmann of the Division of Nuclear Power.

EDITORIAL NOTE

CONTENTS

1. INTRODUCTION AND SUMMARY

1.1. BACKGROUND

A comprehensive set of safety principles for nuclear power plants (NPPs), such as those stated in INSAG-3 [1], helps ensure that NPPs achieve a consistently high level of safety, provided all the principles are observed and correctly implemented. Even though the majority of currently operating plants have an impressive safety record, and can thus be kept in operation without undue risk to the general public, efforts are being undertaken worldwide to enhance the safety of plants even further.

These efforts at enhancement are prompted by several factors. First is the tendency for industrial activities to become safer and more efficient as they are developed with time. For the nuclear industry this results in the desire to incorporate lessons learned from the many accumulated reactor-years of operating experience to date, and to address additional safety issues identified through R&D, testing, and other analysis, such as probabilistic safety analysis. Second is the desire to maintain the current low level of risk to the public from nuclear power, even in the event that the number of nuclear reactors is greatly increased in the future. Third is the desire to limit the likelihood and consequences of severe accidents in future plants so as to minimize the potential for large off-site radiological consequences and the impact on public health and safety, regardless of where the nuclear power plant is located.

There are different ways and means of enhancing safety: design, operation, culture, etc. For existing plants enhanced safety is usually achieved through culture operation, feedback of experience. For future plants, enhanced safety can be achieved "in addition" at the design stage. The aim of this TECDOC is to propose principles and guidelines for such a design stage of future plants.

The Safety Conference held in September 1991 [2] reviewed the status of the next generation of NPPs and after considering the discussions held on topics related to these plants, declared in its major findings "The IAEA should set up a small group of experts to establish safety criteria for the design of future reactors, using a step by step approach which would begin with the development of safety principles and evolve, in the long term, into a comprehensive set of criteria. INSAG documents could provide an important input to the process."

Subsequently, the General Conference, after taking into consideration the major findings of the Safety Conference, invited the Director General "to set up a small group of experts to develop safety principles for the design of future reactors, using a step-by-step approach based — inter alia — on the work of INSAG and taking into account the characteristics of various reactor types". This more limited scope (i.e. design principles only) is the focus of this publication.

Accordingly, a series of meetings involving many experts from different countries were organized by the IAEA. Although directed toward the development of safety principles, these meetings were jointly organized by IAEA's Divisions of Nuclear Safety and Nuclear Power and included attendees representing both regulatory and development perspectives. Such joint organization, cooperation and attendance was intended to help ensure different and diverse views were considered and that the resulting suggested updates to safety principles were developed in a balanced fashion. It is important to note here that, as a practical matter,

safety, reliability and economics must be considered together at the design stage so as to achieve an optimum plant design. Unless a future design with improved safety also results in the reliable and economic production of electricity it will not be utilized.

1.2. PURPOSE

The main purpose of this TECDOC is to propose updates to existing safety principles which could be used as a basis for developing safety principles for the design of future NPPs. Accordingly, this document is intended to be useful to reactor designers, owners, operators, researchers and regulators. It is also expected that this document can contribute to international harmonization of safety approaches, and that it will help ensure that future reactors will be designed worldwide to a high standard of safety. As such, these proposed updates are intended to provide general guidance which, if carefully and properly implemented, will result in reactor designs with enhanced safety characteristics beyond those currently in operation. This enhancement results from the fact that the proposals are derived from the lessons learned from more recent operational experience, R&D, design, testing, and analysis developed over the past decade or so, as well as from attempts to reflect the current trends in reactor design, such as the introduction of new technologies.

1.3. SUMMARY

The Proposed Safety Principles for Future Reactors (Appendix II) represent a contribution to the growing international consensus on what constitutes an appropriate set of technical principles for the design of future reactors. This document has been developed and extensively reviewed by a large and diverse group of experts with knowledge of regulatory, utility and design requirements for future plants. The starting point for this document was the well-established set of principles for nuclear plants laid down in INSAG-3. The experts concluded that the key principles for today's plants formed a very good basis for future designs. Nevertheless, some new principles and objectives were needed, and also new explanatory text for many of the existing principles to reflect the current state of knowledge.

The key proposal of this TECDOC is that severe accidents beyond the existing design basis will be systematically considered and explicitly addressed during the design process for future reactors. Much of the work of the group was focused on agreeing to the best evaluation tools and decision processes to accomplish this task, while remaining cognizant of the many other important performance objectives that designers must consider, such as constructability, reliability, and economic performance.

Particular attention was paid to meeting higher expectations for even lower risks of any serious radiological consequences than has been attained by most current designs, and assurance that the potential need for prompt off-site protective actions would be reduced or even eliminated. In order to achieve this, it is proposed that the Technical Safety Objective of INSAG-3 is made more demanding for future plants, and a Complementary Design Objective is introduced to minimize the potential for significant off-site consequences. This objective is challenging but the group believes that it is achievable for many future designs.

2. SCOPE AND APPROACH

2.1. SCOPE

The proposals presented in Appendix II are intended to be applicable to the design of future NPPs, including evolutionary and advanced designs, regardless of the reactor type (LWR, HWR, HTGR, LMR, etc.). It is recognized that the emphasis is on LWR technology as it dominates the current reactor population, and much of the advanced reactor development efforts. Finally, the proposals are intended to further reduce the accidental release of radioactive material for all modes of reactor operation.

The focus of this publication is on safety principles related to reactor design. Therefore, topics such as quality assurance, siting, operation, maintenance, construction, emergency planning, safeguards and security and those related to the fuel cycle are only addressed as they directly affect the design. In this context, it is important to point out that even though these non-design related topics are not addressed in this TECDOC, they are, however, important and the reader should refer to existing publications, such as INSAG-3 [1], INSAG-5 [3] and the IAEA Safety Fundamentals [4] for further guidance.

2.2. APPROACH

The initial efforts in the development of this TECDOC were focused on identifying those topics where the extensive experience, R&D, design and analysis developed over the past decade or so has indicated that revisions to certain existing safety principles should be considered. A list of these topics was developed and documented by the Consultants Services Meeting to Prepare Working Material for the Advisory Group Meeting on the Development of Safety Principles and Criteria for Future Nuclear Power Plants held in Vienna, 1–5 June 1992, building upon the results of the Technical Committee Meeting to Review Safety Features of New Reactor Design held in Vienna, 11–15 November 1991 and other sources, and covered the following:

- an expanded consideration of severe accidents in the design, including additional attention to prevention and mitigation,
- maintaining defence in depth, including the balance between accident prevention and mitigation,
- reducing the potential releases of radioactive material arising from accidents, by, for example, improving containment performance,
- improving the man–machine interface to reduce the risk of operator errors,
- reducing dependence upon operator actions and active safety systems,
- consideration of siting aspects,
- treatment of external events.

In addition, the report of the Advisory Group Meeting on the Development of Safety Principles and Criteria for Future NPPs (Vienna, 29 June–3 July 1992) suggested that the following topics should be considered:

- Standardization, mainly from the point of view of safety,
- Startup, shutdown and low power operation,
- Spent fuel storage facilities at nuclear power plant sites,
- Decommissioning aspects.

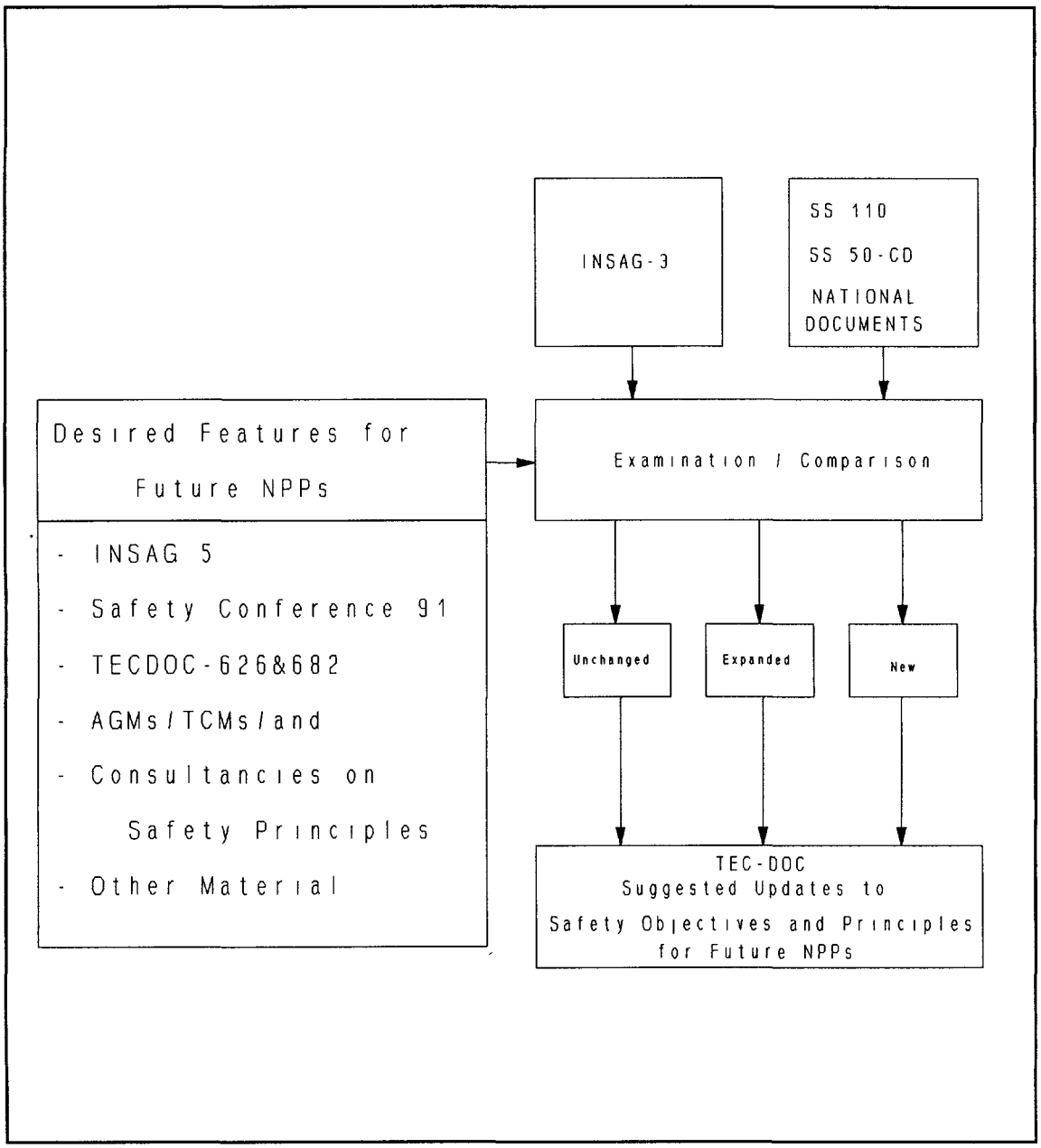


FIG. 1. Approach followed.

The approach taken was to survey existing safety principles documents, and then to use as much previously published and accepted material as possible which address the above topics. Following the General Conference Resolution, the first step was, therefore, to review relevant INSAG publications [1, 3 and 5], the IAEA Safety Fundamentals [4] and the internationally agreed NUSS design code [6].

The next important step was a decision to use, as the main basis for developing proposed new principles, the basic safety principles and explanatory text of INSAG-3. This was a logical approach, since INSAG-3 addresses the safety aspects of the worldwide application of civilian nuclear power plants in a concise, integrated and selfstanding fashion; is applicable to all reactor types; is balanced between regulation and development, and has received wide distribution and acceptance among member states.

The third step was to identify where the above topics were not considered to be adequately addressed for future plants. During this stage, many other documents were reviewed, to ensure consistency and completeness. These included other IAEA-TECDOCs [7, 8] as well as national standards and other documents dealing with the topic of safety principles.

The final step was to develop new safety principles, or amendments to existing principles, and also to provide revised explanatory material to take account of the implications of the new and revised principles.

It should be pointed out that very few new principles were proposed. This confirms that the current principles are essentially adequate. Not only have they served nuclear safety experts very well, but that they are an excellent basis for the future. Substantial updates were made, however, in the section on safety objectives, and to the explanatory text to the principles to accommodate the worldwide moves towards improved safety in future plants.

Figure 1 shows in pictorial form the process described above that was followed in the review of INSAG-3 and other documents, leading to the suggested updates of objectives and principles contained in Appendix II. The description of terms used in this document is given in Appendix I. Even though this publication is intended to be applicable to all reactor types, its main emphasis is on LWR technology, and therefore may in some places use terminology unique to LWRs.

3. PERSPECTIVE ON IMPLEMENTATION OF SAFETY PRINCIPLES

In developing this TECDOC it became apparent that it would be useful to further explain the practical aspects associated with utilizing the objectives and principles, and to ensure that the intent of the proposals is fully understood and considered in their application. This is particularly important in the area of severe accidents, and also where safety limits, targets or goals are concerned. In addition, it is important to note that responsibility for decisions regarding implementation of the principles depends upon the individual Member States national authorities.

Severe accidents

Two groups of severe accident sequences have been defined: those that need to be addressed in the design, referred to in this document as "severe accidents addressed in the design" and those that, either because of their extremely low likelihood, or their being based upon hypothetical assumptions, do not need to be addressed. The selection of which accidents belong in which category is based on a combination of best estimate deterministic analyses, probabilistic considerations, including the application of numerical safety targets, and engineering judgement. The radiological consequences from severe accidents are re-classified by introducing a new term "no significant radiological consequences", in addition to the terms "minor radiological consequences" and "serious radiological consequences" currently used in INSAG-3. The relationship of these terms is discussed in Appendix I and in the suggested updates contained in Appendix II. Finally, the Technical Safety Objective has been revised to differentiate clearly between the two classes of severe accidents and to establish a more demanding design objective to prevent them. The Technical Safety Objective is now accompanied by a related "Complementary Design Objective" aimed at further reducing potential off-site consequences of these low-probability sequences. The key factors associated with the implementation of the suggested updates in the area of severe accidents are discussed below.

(a) Design approach

The analysis of design basis accidents and the design of the related safety equipment is done using conservative assumptions, design rules and acceptance criteria. However, the suggested expansion of the Technical Safety Objective to ensure a more comprehensive consideration of severe accident prevention and mitigation is not meant to imply that the same conservative design basis rules should apply to severe accident analyses or equipment. For those accidents which need to be addressed, due to the extremely low likelihood, it is more appropriate to use engineering judgement, best estimate analyses and acceptance criteria in implementing these principles in the design. Likewise, redundancy, diversity and the quality of equipment can be different from that applied to design basis equipment. Therefore, the suggested updates relating to severe accident prevention and mitigation are formulated in a general form to allow an appropriate degree of engineering judgement and flexibility in the implementation of design measures.

(b) Selection of accidents to be addressed in the design

It should be emphasized here that both deterministic and probabilistic analysis methods and criteria are intended to be employed by designers to aid in the selection of those accidents, including severe accidents, which are to be addressed in the design, and in decisions on the need for severe accident design features. National authorities would make the final decision on which severe accident scenarios and/or phenomena are to be addressed, and in what fashion, for assuring adequate protection of public health and safety and the environment.

Factors such as eliminating accident phenomena or scenarios which lead to early containment failure or bypass, or eliminating phenomena or scenarios which lead to either the need for urgent or long-term off-site protective actions, are examples of the types of considerations which could help guide this selection.

(c) Radiological consequences

The explicit consideration of severe accidents leads to a need for a graded approach to describing the radiological consequences of accidents. This TECDOC defines the terms 'minor radiological consequences', 'no significant radiological consequences' and 'serious radiological consequences', but does not specify numerical values for each. (See Appendix I for these definitions.) The selection of values appropriate to these classifications, considering such factors as the health and safety of people in the vicinity of the plant and the desirability of minimizing the necessity for off-site protective actions, remains the responsibility of national authorities.

(d) Use of probabilistic targets

INSAG-3 and similar documents contain probabilistic targets for events such as core damage frequency and release of radioactive material. Such targets are useful in making design decisions, and have been retained in this TECDOC as an example. While there are many advantages offered by the systematic approach of probabilistic safety analysis, there are also many uncertainties associated with such calculations, especially in the domain of events of very low likelihood. Therefore it is important to discuss the methodology and assumptions to be used to establish the scope of the analysis and level of confidence in such calculations. The following items are examples of what would need to be considered in establishing the calculation methodology:

(i) the scope of what is to be considered in calculating whether or not such a target is met, for example:

- internal events including common mode and common cause failure;
- external events;
- full power, low power, shutdown/refuelling operations;
- common mode failures;
- human error;
- ageing implications;

(ii) the confidence level to which the calculated value must be known, for example:

- the acceptability of the failure/error rates;
- the meteorology conditions assumed in off-site risk calculations;
- the extent of the uncertainty analysis carried out;
- how uncertainties are treated in judging whether or not the target is met.

Documents which contain such numerical probabilistic targets should provide guidance regarding the methods and assumptions to be used in their calculation and interpretation. This TECDOC provides some guidance at a high level, but more work in this area is needed.

Other numerical targets

Other numerical targets useful for designers include the grace period available before operator action is necessary in responding to accident situations, and the length of time which the plant is capable of withstanding a station blackout (i.e., loss of all normal off-site and on-site AC power) situation. An example of current capability for grace period has been

included in this TECDOC, but this should not be regarded as definitive since it is possible that future designs could move to longer periods of elapsed time following a fault before operator intervention is necessary.

Classification of systems, structures and components

The safety principles call for systems, structures and components to be classified according to their safety function. It should be recognized that such classification would require, in addition to establishing various categories of classification, defining what standards would be acceptable for each category. Other considerations which are taken into account include:

- independence
- redundancy
- diversity
- automatic vs. manual actuation, including grace period if applicable
- design rules (e.g. best estimate, conservative)
- acceptance criteria (i.e. what dose criteria, fuel damage criteria, etc. apply)
- environmental conditions
- quality assurance.

Those design features incorporated as a result of severe accident considerations should be addressed in the classification scheme, taking into account that best estimate approaches are acceptable for this category of equipment.

Single failure criterion

The interpretation of the principles contained in this document require the application of the single failure criterion to systems which perform a safety function for coping with the design basis accidents of the plant. The application of this criterion has generally been well understood to include all active systems and components, but its application to passive systems and components is less well understood. The TECDOC discusses this and some other issues related to passive features.

Accident management

It is likely that operating personnel at future NPPs will need to rely less on complex or demanding accident management actions. This is not to suggest that accident management is less important or that it should be reduced for future plants, but that there is an expectation that it may become a less demanding regime with future plants. Nevertheless, accident management should continue to be viewed as a prudent component of the defence in depth concept for future plants that will be applied as needed, even before a potential severe accident condition actually develops.

Appendix I

DESCRIPTION OF TERMS

This appendix contains a description of terms used in this document. It is divided into two sections: the first provides existing descriptions and definitions extracted from other IAEA documents; the second provides new descriptions developed specifically for this document. Figure 2 shows the different plant states and Figure 3 helps convey the relationship between accidents and consequences for the proposed principles.

DESCRIPTIONS OF STANDARD TERMS FROM IAEA DOCUMENTS

The following definitions are derived from Safety Series No. 50-C-D (Rev. 1) "Code on the Safety of Nuclear Power Plants: Design" [6] and No. 110 "The Safety of Nuclear Installations" [4].

The relationships between the following eight definitions and the defined term "severe accidents addressed in the design" are illustrated by Figure 3.

Operational states

States defined under Normal Operation or Anticipated Operational Occurrences.

Normal operation

Operation of a nuclear power plant within specified Operational Limits and conditions including shutdown, power operation, shutting down, starting, maintenance, testing and refuelling.

Anticipated operational occurrences[1]

All operational processes deviating from Normal Operation which are expected to occur once or several times during the operating life of the plant and which, in view of appropriate design provisions, do not cause any significant damage to items important to Safety nor lead to Accident Conditions.

Accident (or accident state)

A state defined under Accident Conditions or Severe Accidents.

Accident conditions

Departure[2] from Operational States in which the releases of radioactive materials are kept to acceptable limits by appropriate design features. These deviations do not include severe accidents.

Design basis accident

Accident Conditions against which the nuclear power plant is designed according to established design criteria.

---

[1]Examples of Anticipated Operational Occurrences are loss of normal electric power and faults such as a turbine trip, malfunction of individual items of a normally running plant, failure to function of individual items of control equipment, loss of power to a main coolant pump.

[2]A departure may be a loss of coolant accident (LOCA), etc.

Severe accidents

Nuclear power plant states beyond Accident Conditions including those causing significant core degradation.

Accident management

Accident management is the taking of a set of actions

- during the evolution of an event sequence, before the design basis of the plant is exceeded, or
- during Severe Accidents without core degradation, or
- after core degradation has occurred

to return the plant to a controlled safe state and to mitigate any consequences of the accident.

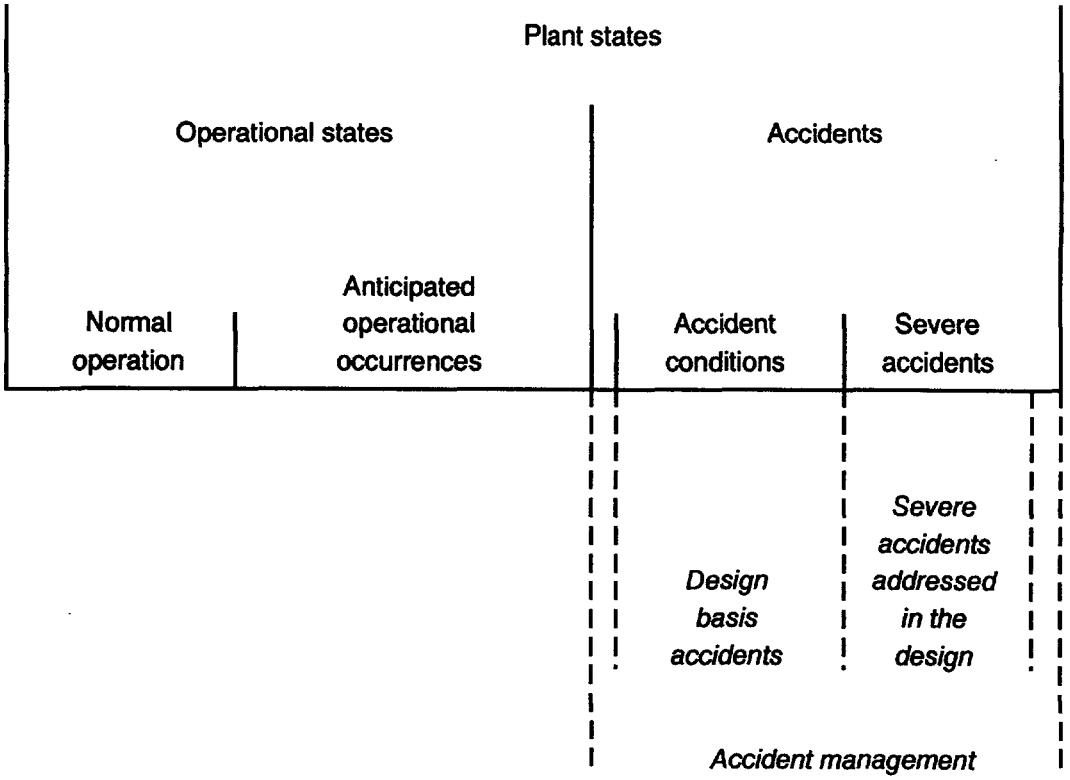


FIG. 2. Plant states ('Severe accidents addressed in the design' has been added to the figure from IAEA Safety Series No. 50-C-D (Rev. 1), p. 2).

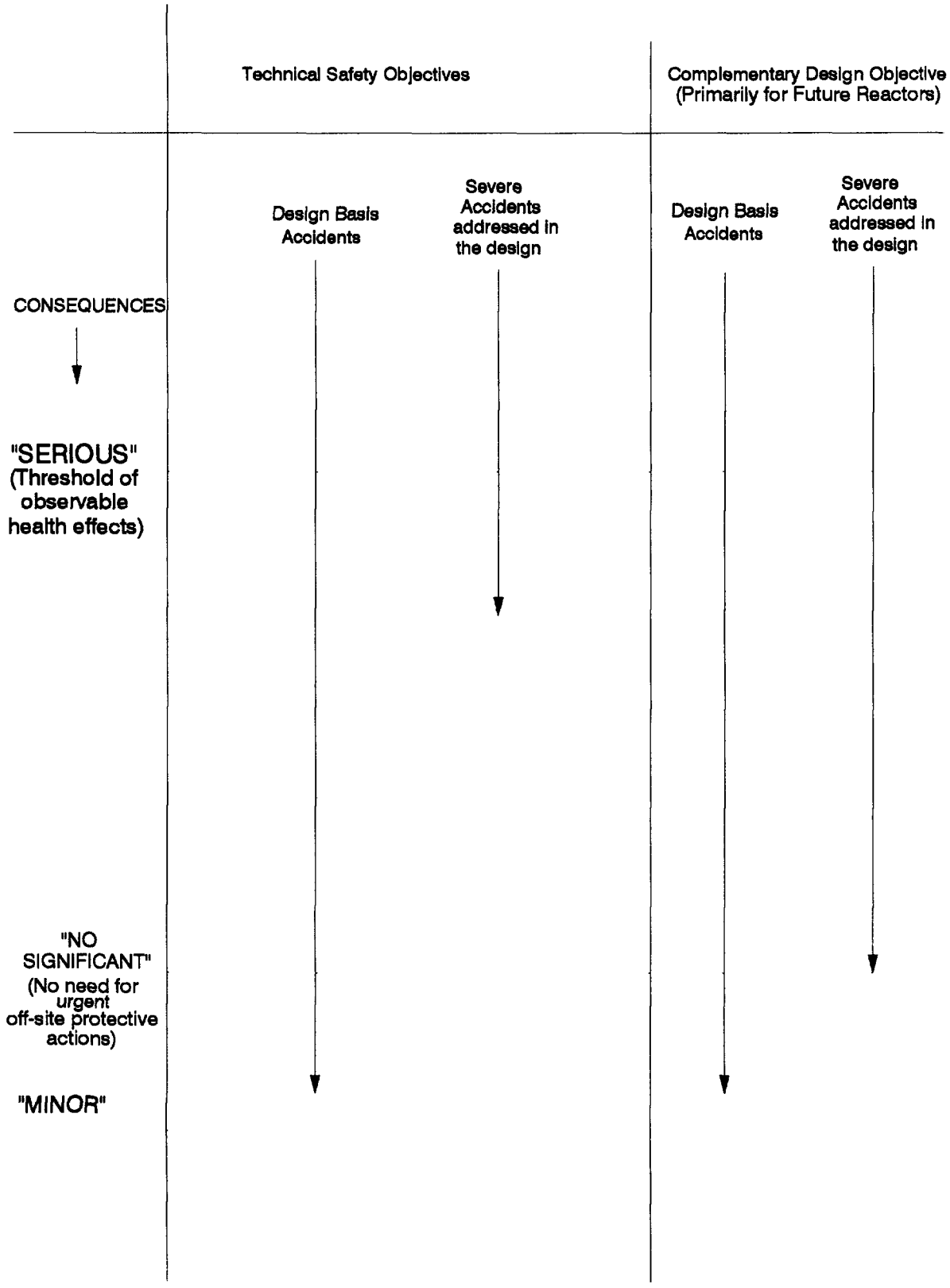


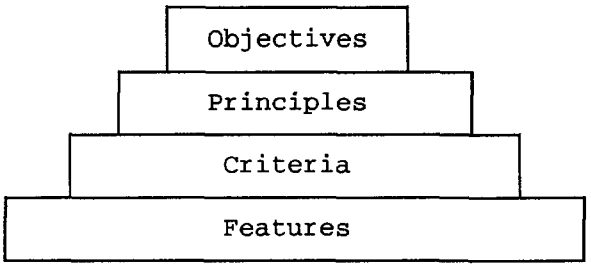
FIG. 3. Relationship between types of accidents addressed in the design and the relative radiological consequences.

NEW TERMS USED IN THIS DOCUMENT

Best estimate analysis:	Analysis that is conducted using actual operating experience, research data and results and realistic assumptions that do not include arbitrary, conservative or bounding assumptions.
Future reactors:	a primarily time-related term that generally refers to reactors that are not currently operating or under construction, and that will comply with objectives and principles of this TECDOC.
Severe accidents addressed in the design:	Those severe accident sequences beyond the design basis of a plant that are systematically taken into account in the design of a plant. The detailed basis for the selection of which severe accidents are addressed, and the general attributes of these design features are discussed in Appendix II. The term "severe accidents addressed in the design" and the term "addressed severe accidents" will be used interchangeably to mean those sequences that have not been excluded in this selection process.
Serious radiological consequences:	This corresponds to the highest level of off-site consequences and is associated with preventing dose levels that exceed the threshold of observable, prompt off-site health effects.
No significant radiological consequences:	This is more restrictive than "serious radiological consequences", and corresponds to a very low level of off-site consequences following events with core damage. It is associated with minimizing small environmental and societal doses that are below those that would create observable health effects. Even though dose limits associated with "no significant radiological consequences" are typically well below those associated with observable health effects, they are nevertheless set administratively as precautionary intervention levels to trigger protective actions. For future plants, the complementary design objective of ensuring "no significant radiological consequences" has the effect of eliminating the need for urgent actions such as emergency notification and rapid evacuation, and permanent actions such as relocation, outside the immediate vicinity of the plant.
Minor radiological consequences:	This is the most restrictive of the consequence terms. (It may correspond to the dose limits stipulated for design basis accidents.)

Safety criteria[3] :	A yardstick statement of acceptance for measuring compliance with a safety principle or safety principles
Safety features[3] :	Plant hardware which represents implementation of safety objectives, safety principle and safety criteria
Safety objectives[3] :	A statement of what is to be achieved.
Safety principles[3] :	A statement of a general rule or rules to be used as a guide for actions (how to achieve what is stated in the safety objectives).

[3]Hierarchical relationship between objectives, principles, criteria and features:



Examples of:

Objective - to prevent with high confidence, accidents in NPPs.
Principle - automatic systems are provided that would safely shut down the reactor if operational conditions were to exceed predetermined setpoints.
Criterion - two independent reactor shutdown systems of different design principles shall be provided, each capable of shutting down the reactor under design basis accident conditions prior to exceeding fuel damage limits.
Feature - two independent shutdown systems in the plant design.

Appendix II

PROPOSED SAFETY PRINCIPLES FOR THE DESIGN OF FUTURE NUCLEAR POWER PLANTS

This appendix contains suggested updates to the design objectives and principles contained in INSAG-3 for application to future nuclear power plants. These proposals result from the lessons learned from recent operation experience, R&D, safety analysis and new design efforts. The most important of these and their basis are summarized below, and are identified in the main text of this appendix.

CONSIDERATION OF SEVERE ACCIDENTS

A number of suggested modifications and additions to the INSAG-3 objectives and principles have been made with respect to the consideration of severe accidents in the design, in particular, to Technical Safety Objective No. 19 and its supporting paragraphs. These suggested modifications introduce a defined term "severe accidents addressed in the design" or "addressed severe accidents", which specify that certain, but not all, severe accidents should be addressed in the design and that the selection of those to be addressed should be based on a combination of best estimate deterministic analysis, probabilistic considerations and engineering judgement. This expansion also implies further efforts directed toward prevention as well as mitigation.

The term "no significant radiological consequences" is also introduced to be used in conjunction with the existing terms in INSAG-3 "minor radiological consequences" and "serious radiological consequences". The intent of introducing this terminology is to define radiological consequences associated with going beyond the Technical Safety Objective of preventing and mitigating severe accidents addressed in the design, keeping in mind the "good neighbour" concept of further reducing the need for off-site protective measures. Accordingly, the Technical Safety Objective has been updated to clearly differentiate between the two groups of severe accidents and to explicitly establish a more demanding objective for designing to prevent them. The Technical Safety Objective is now accompanied by a related "Complementary Design Objective" that is intended to further reduce potential off-site consequences of these low-probability sequences.

OTHER CHANGES

In addition to the suggestion of enhancing severe accident prevention and mitigation, there are other areas in INSAG where modifications or additions to existing principles have been suggested because they reflect lessons learned from operational experience, R&D, testing, analysis and new design initiatives. All of the areas affected are listed below, along with a brief statement as to the nature of the suggested changes.

(a) Accident prevention — the INSAG-3 specific design principles associated with accident prevention (paras 121–170 and 180–188 of INSAG-3) are, for the most part, retained; with the suggestion that certain of these principles be supplemented to address severe accidents consistent with the modified technical objectives. In addition, some new principles or discussion have been suggested in the areas of:

- use of probabilistic safety analysis (from INSAG-5)
- consideration of modes of operation other than full power
- spent fuel handling and storage
- multiple units sharing equipment.

These are the areas where an update of INSAG-3 was judged appropriate, considering that these areas have been prominent in other nuclear safety documents and/or represent new emerging technical issues.

(b) Accident mitigation — the INSAG-3 specific design principles associated with accident mitigation, accident management, and emergency preparedness (paras 56–58, 171–179, 260–265, 268–270, and 271–278 of INSAG-3) are, for the most part, retained; with the suggestion that certain of these principles be supplemented with additional material related to the ability of confinement to mitigate addressed severe accidents. In addition, some consolidation of principles on confinement is suggested.

(c) Proven engineering practices — the INSAG-3 specific design principles associated with proven engineering practices (paras 60–64, 97, 103–104, 110–119, 151–155 of INSAG-3) are retained and supplemented by suggested additions of new principles or discussion paragraphs in the areas of:

- classification of safety systems (from INSAG-3, para. 68)
- standardization
- the consideration of passive systems (from INSAG-5)
- plant security.

(d) Quality assurance — the INSAG-3 fundamental principles on QA (paras 65–67 and 70–72 of INSAG-3) have been retained unchanged.

(e) Human factors — the INSAG-3 specific design principles associated with human factors (paras 73, 76, 180–185, 189–191 of INSAG-3) are retained and supplemented by suggested modifications of principles or discussion paragraphs in the areas of:

- designing to be user friendly and to avoid complexity (from INSAG-5)
- designing to reduce dependence on operator action (from INSAG-5)
- considering operating and maintenance procedures in the design.

(f) Radiation protection — the INSAG-3 specific design principle on radiation protection (paras 144–145 of INSAG-3) is retained and supplemented by a suggested new principle on minimizing exposures during decommissioning (from the Safety Fundamentals document "The Safety of Nuclear Installations", Safety Series No. 110). Although this new principle on decommissioning is not directed at the prevention or mitigation of accidents, it has been suggested here for completeness.

(g) Advanced instrumentation and control — with the increasing use of computer systems in safety applications, as well as for control and information systems, additional descriptive material has been suggested to address the important subject of software and hardware reliability and qualification.

Guide to reading Appendix II

The proposals contained in this appendix are shown in bold face type as suggested changes or additions to the design related objectives and principles contained in INSAG-3. Where the original INSAG principle has been modified by the removal of part of the principle, the omission has been indicated by **[...]**. In addition, for ease of comparing to INSAG-3, the section numbers and the paragraph numbers corresponding to those in

INSAG-3 are retained. Where new principles or paragraphs have been added, these have been allocated the prefixes (a), (b), (c), etc. to the existing, preceding INSAG-3 paragraph number. However, since this appendix only addresses design related principles, INSAG-3 paragraphs addressing non-design related topics are not included, and some reorganization of the remaining design related INSAG-3 material has been made to help consolidate similar subject matter. Therefore, in some parts of this appendix, original INSAG-3 paragraphs are missing or are out of numerical sequence.

It should also be noted that throughout the document the principles and their accompanying discussion are stated, not in the form of requirements, but, to be consistent with INSAG, on the assumption that the practices are in current use, or will be put into use for future reactors.

The structure of this appendix is as follows:

II.1. INTRODUCTION

105. The primary objective of nuclear power plant designers is to provide **an excellent** design. They ensure that the components, systems and structures of the plant have the appropriate characteristics, specifications and material composition, and are combined and laid out in such a way as to meet the general plant performance specifications. Designers also provide a system for recording the safety design basis of the plant and for maintaining conformity to the design basis throughout the design changes that occur in construction and commissioning. At the design stage, consideration is given to the needs and performance capabilities of the personnel who will eventually operate the plant, and to the requirement that the designer will supply information and recommended practices for incorporation into operating procedures. Design choices are made which facilitate the achievement of the first safety priority, accident prevention. Special attention is also given to the prevention and mitigation of the consequences of accidents which could lead to a major release of radioactive materials from the plant.

105.a To assure safety, the plant designers consider both nuclear and conventional (non nuclear) safety. Designers assure conventional safety by complying with laws, regulations, standards and practices that are generally applicable to industrial features that pose similar non radiological hazards (such as high pressure steam, high voltage electricity, etc.). However, since the focus of this document is nuclear safety, principles associated with conventional safety are not included.

106. **Nuclear** safety in reactor design is concerned with controlling the location, movement and condition of radioactive materials inside the plant so that they are confined in a safe state. In a solid fuel reactor, almost all the radioactive materials are confined in fuel pellets sealed within an impervious barrier, usually metallic fuel cladding. Nuclear safety is ensured for these reactors if the radioactive materials are kept inside the fuel and within other barriers provided by design.

107. Safety designers analyze the behaviour of the plant under a wide range of conditions. These include normal operation and variable conditions encountered in manoeuvering. They also include anticipated abnormal occurrences and unusual occurrences that the plant is required to withstand without unacceptable damage by virtue of its normal characteristics and engineered safety features. Advantage is taken of inherent safety characteristics of the design. Consideration is also given in design to accidents beyond the design basis to ensure that the more important ones can be **prevented or** mitigated effectively by means of **design features,** accident management **features** and measures available through emergency preparedness.

108. Most aspects of safety design are connected closely with the three functions that protect against the release and dispersal of radioactive materials:

- controlling reactor power;
- cooling the fuel; and
- confining radioactive materials within the appropriate physical barriers.

II.2. SAFETY OBJECTIVES

12. Three safety objectives are defined for nuclear power plants. The first is very general in nature. The other two are complementary objectives that interpret the general objective,

dealing with radiation protection and technical aspects of safety respectively. The safety objectives are not independent; their overlap ensures completeness and adds emphasis.

13. *Objective: To protect individuals, society and the environment by establishing and maintaining in nuclear power plants an effective defence against radiological hazard.*

14. Each viable method of production of electricity has unique advantages and possible detrimental effects. In the statement of the general nuclear safety objective, radiological hazard means adverse health effects of radiation on both plant workers and the public, and radioactive contamination of land, air, water or food products. It does not include any of the more conventional types of hazards that attend any industrial endeavour. The protection system is effective as stated in the objective if it prevents significant addition either to the risk to health or to the risk of other damage to which individuals, society and the environment are exposed as a consequence of industrial activity already accepted. In this application, risk is defined as the arithmetic product of the probability of an accident or an event and the adverse effect it would produce. These health risks are to be estimated without taking into account the countervailing and substantial benefits which the nuclear and industrial activities bestow, both in better health and in other ways important to modern civilization. When the objective is fulfilled, the level of risk due to nuclear power plants does not exceed that due to competing energy sources, and is generally lower. If another means of electricity generation is replaced by a nuclear plant, the total risk will generally be reduced. The comparison of risks due to nuclear plants with other industrial risks to which people and the environment are exposed makes it necessary to use calculational models in risk analysis. To make full use of these techniques and to support implementation of this general nuclear safety objective, it is important that quantitative targets are formulated.

15. It is recognized that although the interests of society require protection against the harmful effects of radiation, they are not solely concerned with the radiological safety of people and the avoidance of contamination of the environment. The protection of the resources invested in the plant is of high societal importance and demands attention to all the safety issues with which this report is concerned.

16. *Objective: To ensure in normal operation that radiation exposure within the plant and due to any release of radioactive material from the plant is kept as low as reasonably achievable and below prescribed limits, and to ensure mitigation of the extent of radiation exposures due to accidents.*

17. Radiation protection is provided in nuclear power plants under normal conditions and separate measures would be available under accident circumstances. For planned plant operating conditions and anticipated operational occurrences, compliance with radiation protection standards based on ICRP recommendations[4] ensures appropriate radiation protection. That is, the ICRP's system of dose limitation provides appropriate protection for planned situations anticipated to occur once or more in the lifetime of a plant.

18. The aforementioned radiation protection standards have been developed to prevent harmful effects of ionizing radiation by keeping exposures sufficiently low that non-stochastic effects are precluded and the probability of stochastic effects is limited to levels deemed

[4]For example INTERNATIONAL ATOMIC ENERGY AGENCY, **International** Basic Safety Standards for **Protection Against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1994).**

tolerable. This applies to controlled circumstances. **For current plants,** in the event of any accident that could cause the source of exposure to be not entirely under control, safety provisions in the plant are planned and countermeasures outside the plant are prepared to mitigate harm to individuals, populations and the environment. **For future NPPs, even more stringent design and safety objectives are established, which will further minimize potential off-site consequences.**

18a. Two complementary technical objectives are proposed for future NPPs. The first applies to all plants, the second is intended primarily for future NPPs. The first objective addresses prevention and mitigation of accidents, both within and beyond the traditional deterministic design basis, with its critical focus on the objective of protecting public health and safety — thus the title "Technical Safety Objective". The second objective also addresses prevention and mitigation of accidents, both within and beyond the traditional deterministic design basis, but with its critical focus on the minimization of off-site effects, beyond those that could affect public health and safety. The Technical Safety Objective includes explicit consideration of certain severe accident scenarios as defined later. The Complementary Design Objective accommodates the desire of many countries to demonstrate that "no significant radiological consequences" would occur outside the immediate vicinity of the plant, and thus, no stringent off-site emergency response actions (such as prompt notification and/or evacuation, resettlement, etc.) would be necessary, for designs that meet this objective.

19. TECHNICAL SAFETY OBJECTIVE: To prevent with high confidence accidents in nuclear plants; to ensure that, for all ***design basis accidents,*** *radiological consequences, if any, would be minor*** ***and within prescribed limits; to ensure that for all "severe accidents addressed in the design"* there are no "serious radiological consequences"**; and to ensure that the likelihood of any severe accident that could have serious radiological consequences** is extremely small.*

In addition, primarily for future plants, the following objective is introduced:

19a. COMPLEMENTARY DESIGN OBJECTIVE: To ensure, in addition to meeting the Technical Safety Objective, that "severe accidents addressed in the design"* have "no significant radiological consequences"**.

19b. The following are key definitions that support these objectives:

*** The term "severe accidents addressed in the design" [or "addressed severe accidents"] refers to those severe accident sequences beyond the design basis of a plant that are systematically taken into account in the design of a plant. The detailed basis for the selection of which severe accidents are addressed, and the general attributes of these design features are discussed later. The term "severe accidents addressed in the design" and the term "addressed severe accidents" will be used interchangeably to mean those sequences that have not been excluded by this selection process.**

**** The terms "minor radiological consequences", "no significant radiological consequences", and "serious radiological consequences" refer to off-site consequences and their relationships as follows:**

- **The term "serious radiological consequences" corresponds to the highest level of consequences and is associated with preventing dose levels that exceed the threshold of observable, prompt off-site health effects.**
- **The term "no significant radiological consequences" is more restrictive than "serious radiological consequences", and corresponds to a very low level of off-site consequences following events with core damage. It is associated with minimizing environmental and societal doses. Even though dose limits associated with "no significant radiological consequences" are typically well below those associated with observable health effects, they are nevertheless set administratively as precautionary intervention levels to trigger protective actions. For future plants, the complementary design objective of ensuring "no significant radiological consequences" has the effect of eliminating the need for urgent actions such as emergency notification and rapid evacuation, and permanent actions such as relocation, outside the immediate vicinity of the plant.**
- **The term "minor radiological consequences" is the most restrictive one. (It may correspond to the dose limits stipulated for design basis accidents.)**

20. Accident prevention is the first safety priority of both designers and operators. It is achieved through the use of reliable structures, components, systems and procedures in a plant operated by personnel who are committed to a strong safety culture.

21. However, in no human endeavour can one ever guarantee that the prevention of accidents will be totally successful. Designers of nuclear power plants therefore assume that component, system and human failures are possible, and can lead to abnormal occurrences, ranging from minor disturbances to highly unlikely accident sequences. The necessary additional protection is achieved by the incorporation of many engineered safety features into the plant. These are provided to halt the progress of an accident in the specific range of accidents considered **in the deterministic** design **basis** and, when necessary, to mitigate their consequences. The design parameters of each engineered safety feature are defined by a deterministic analysis of its effectiveness against the accidents it is intended to control. The accidents in the spectrum requiring the most extreme design parameters for the safety feature are termed the design basis accidents for that feature. **For future plants, accidents beyond the deterministic design basis are systematically considered, and addressed in the design as necessary to meet safety and design objectives. To some practical degree, current plants also consider accidents beyond the deterministic design basis, consistent with paragraph 25. Design features are provided to prevent and mitigate addressed severe accidents as defined in paragraph 21.a; but these features, while reliable and capable of performing their safety function, need not meet the conservative deterministic requirements applied to safety systems provided for DBAs.**

21.a Severe accidents addressed in the design (as referred to in the Technical Safety Objective and the Complementary Design Objective) are any accidents beyond the design basis, even of very low probability, that are physically, mechanistically or technically justified in being addressed explicitly in the design of future plants. Although all severe accident sequences are very low in probability, they are nevertheless a possible source of remaining risk that is considered in an appropriate way. For future plants, those low probability severe accident sequences that are shown by safety analysis to merit further attention are identified and taken into account through specific features during the design of the plant. Safety objectives for future plants are more demanding than for current plants, and thus will generally result in a more stringent process for

selecting those sequences to be addressed. The final decision on which severe accidents are to be addressed in the design is based on a combination of best estimate deterministic analyses, probabilistic considerations, including the application of numerical safety targets, and a certain amount of engineering judgment. The features that address these severe accidents may be chosen for their prevention capability, their mitigation capability, or both. It is recognized that as a result of this process, a decision will be made to exclude some severe accidents of extremely remote likelihood from the set of severe accidents to be explicitly addressed in the design. Reaching this final decision is an iterative process, with initial judgments made by the designer, based on experience, and careful analysis and then review by utilities and regulators to confirm that the proper decisions have been made, and who may impose further requirements on the design to meet their requirements.

21.b The Complementary Design Objective of limiting the consequences of addressed severe accidents to the objective of "no significant radiological consequences" is to ensure with a high degree of confidence that the need for urgent protective actions would in effect be limited to the immediate vicinity of a plant, and possibly to the plant site boundary, thus minimizing societal and environmental impact. It is expected that many advanced reactor designs could demonstrate this capability. This will enable simplification of the emergency planning for such designs, i.e., to eliminate, from a technical point of view, the need for both urgent and long term off-site protective actions, such as rapid evacuation and permanent relocation. If off-site protective action is still deemed necessary to meet this objective, it should be very restricted in duration and area. However, even if the need for offsite emergency action is eliminated, some emergency planning for contingencies may still remain, as part of an overall public protection policy. The determination of what constitutes "no significant radiological consequences" is the responsibility of national authorities, and takes into account local conditions and national or international regulations.

21.c In deciding on the design features to be provided in future plants for coping with severe accidents, both the prevention of core damage and mitigation of its consequences are pursued to the maximum practicable extent, consistent with the application of deterministic analyses, numerical safety targets, and a certain amount of engineering judgement. In selecting the means for addressing severe accidents, practical issues such as constructability, maintainability, and cost targets are taken into account. Finally, and very importantly, design features that are provided to address severe accidents are not expected to meet the stringent design criteria and requirements applied to the engineered safety features to cope with design basis accidents, such as redundancy, diversity, and conservative analysis and acceptance criteria. However design features for addressing severe accidents are still engineered in a way which would give reasonable confidence that they are capable of achieving their design intent.

21.d With respect to siting issues, it is important to consider the Technical Safety Objective as applicable to all plants, even those that might be so remotely located that it can be demonstrated that no serious radiological consequences would occur as a sole result of low population density. Also, if a future plant is sited near a national boundary, due consideration is given to the national safety policies of the neighbouring country.

24. In the safety technology of nuclear power, risk is defined (as in Section 2.1) as the product of the likelihood of occurrence of an accident and its potential radiological consequences. **In practice, this mathematical relationship begins to lose its usefulness when the uncertainties in the calculation dominate the absolute numbers. For example, calculations of core damage frequency are more useful to the designer and decision maker than calculations of off-site release frequencies, because the latter calculations involve extremely low probabilities, making the uncertainties very large.** The Technical Safety Objective for accidents is to apply accident prevention, management and mitigation measures in such a way that overall risk is very low and no accident sequence, whether it is of low probability or high probability, contributes to risk in a way that is excessive in comparison with other sequences.

24.a Although the same low probability sequences are addressed in the Complementary Design Objective as are addressed in the Technical Safety Objective, the above cautions and limitations regarding extremely low probability numbers are even more pronounced. Therefore even greater use of engineering judgement is required in evaluating designs with regard to the Complementary Design Objective.

24.b Internal and external events are considered in a balanced fashion to ensure that the analysis will be sufficiently complete and that the combined risk from both types of events will be acceptably low.

24.c Probabilistic methods can be used as a complementary means of determining the accidents and accident sequences to be considered in the design. Probabilistic targets are established for parameters such as core damage frequency, large off-site release probability, or others as appropriate. For use of probabilistic methods and probabilistic targets, guidelines on appropriate use are established so that the scope and methodologies of analysis are known, and uncertainties are considered properly and factored into their use as decision aids. For example, best estimate methods and assumptions are used in probabilistic assessments. Specifically, guidance from INSAG-6 is followed. Further, caution is used in applying probabilistic targets in the regulatory process. Rather, insights from PSA can be used effectively to establish risk-significant deterministic criteria for regulations. With these cautions, probabilistic safety targets can be important tools in the decision process outlined in paragraph 21.a for deciding which severe accident sequences are to be addressed in the design.

25. **As an example, INSAG has suggested a numerical** target for **future** nuclear power plants consistent with the technical safety objective **of INSAG-3, as** a likelihood of occurrence of severe core damage that is below about 10^{-5} events per plant operating year. **In addition, INSAG has suggested that** severe accident management and mitigation measures should **permit achieving a** probability of large off-site releases requiring short term off-site response **that is below about 10^{-6} events per reactor operating year.**

II.3. FUNDAMENTAL PRINCIPLES

II.3.2. STRATEGY OF DEFENCE IN DEPTH

39. 'Defence in depth' (for more details see Appendix of INSAG-3) is singled out amongst the fundamental principles since it underlies the safety technology of nuclear power. All safety activities, whether organizational, behavioural or equipment related, are subject

to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defence in depth, and it is repeatedly used in the safety principles that follow.

39.a For future plants, the defence in depth approach will remain the basis for sound design. Compared to many existing plants, the expected safety enhancement will include, from the design stage, the explicit consideration of severe accidents in such a way that the likelihood of serious radiological consequences is extremely small. Also, numerical safety targets such as those given by example in paragraph 25 indicate that significant improvements are expected for future plants. Furthermore, designers of future plants seek to meet the more restrictive Complementary Design Objective of "no significant radiological release," in order to satisfy other objectives, such as simplification of the off-site emergency response. These two factors correspond to a reinforcement of the defence in depth in future plants, and consequently to a significant safety enhancement.

40. Two corollary principles of defence in depth are defined, namely, accident prevention and accident mitigation. These corollary principles follow the general statement of defence in depth.

Defence in depth

41. *Principle: To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective.*

42. The defence in depth concept provides an overall strategy for safety measures and features of nuclear power plants. When properly applied, it ensures that no single human or mechanical failure would lead to injury to the public, and even combinations of failures that are only remotely possible would lead to little or no injury. Defence in depth helps to establish that the three basic safety functions (controlling the power, cooling the fuel and confining the radioactive material) are preserved, and that radioactive materials do not reach people or the environment.

43. The principle of defence in depth is implemented primarily by means of a series of barriers which should in principle never be jeopardized, and which must be violated in turn before harm can occur to people or the environment. These barriers are physical, providing for the confinement of radioactive material at successive locations. The barriers may serve operational and safety purposes, or may serve safety purposes only. Power operation is only allowed if this multi-barrier system is not jeopardized and is capable of functioning as designed.

44. The reliability of the physical barriers is enhanced by applying the concept of defence in depth to them in turn, protecting each of them by a series of measures. Each physical barrier is designed conservatively, its quality is checked to ensure that the margins against failure are retained, its status is monitored, and all plant processes capable of affecting it are controlled and monitored in operation. Human aspects of defence in depth are brought into play to protect the integrity of the barriers, such as quality assurance, administrative controls,

safety reviews, independent regulation, operating limits, personnel qualification and training, and safety culture. Design provisions including both those for normal plant systems and those for engineered safety systems help to prevent undue challenges to the integrity of the physical barriers, to prevent the failure of a barrier if it is jeopardized, and to prevent consequential damage of multiple barriers in series. Safety system designers ensure to the extent practicable that the different safety systems protecting the physical barriers are functionally independent under accident conditions.

45. All of the components of defence are available at all times that a plant is at normal power. Appropriate levels are available at other times. The existence of several **layers** of defence in depth is never justification for continued operation in the absence of one **layer**. Severe accidents in the past have been the result of multiple failures, both human and equipment failures, due to deficiencies in several components of defence in depth that should not have been permitted.

46. System design according to defence in depth includes process controls that use feedback to provide a tolerance of any failures which might otherwise allow faults or abnormal conditions to develop into accidents. These controls protect the physical barriers by keeping the plant in a well defined region of operating parameters where barriers will not be jeopardized. Care in system design prevents cliff edge effects which might permit small deviations to precipitate grossly abnormal plant behaviour and cause damage.

47. Competent engineering of the barriers and the measures for their protection coupled with feedback to maintain operation in optimal ranges leads to a record of smooth, steady performance in producing electricity on demand. This indicates the proper implementation of the most important indicator of the success of defence in depth, which is operation with little or no need to call on safety systems.

48. The multi-barrier system protects humans and the environment in a wide range of abnormal conditions. Pre-planned countermeasures are provided, as a further component of defence in depth, against the possibility that radioactive material might still be released from the plant.

Accident prevention

50. *Principle: Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents, particularly any which could cause severe core damage.*

51. The design, construction, operation and maintenance of nuclear power plants has as its primary objective the generation of electricity reliably and economically. The safety implications of decisions in all these areas must be borne in mind. The following is concentrated on these safety aspects.

52. The **primary** means of preventing accidents is to strive for such high quality in design, construction and operation of the plant that deviations from normal operational states are infrequent. Safety systems, **provided for design basis accidents,** are used as a backup to feedback in process control to prevent such deviations from developing into accidents. Safety systems make use of redundancy and diversity of design and the physical separation of parallel components, where appropriate, to reduce the likelihood of the loss of a vital safety function. Systems and components are inspected and tested regularly to reveal any

degradation which might lead to abnormal operating conditions or inadequate safety system performance. Abnormal conditions possibly affecting nuclear safety are promptly detected by monitoring systems that give alarms and in many cases initiate corrective actions automatically. The operators are trained to recognize readily the onset of an accident and to respond properly and in a timely manner to such abnormal conditions. They have also been well trained in appropriate operating procedures, with which they have become familiarized.

53. Thus the prevention of accidents **within the design basis** depends on conservatively designed equipment and good operational practices to prevent failure, quality assurance to verify the achievement of the design intent, surveillance to detect degradation or incipient failure during operation, and steps to ensure that a small perturbation or incipient failure would not develop into a more serious situation.

53.a For addressed severe accidents, the above measures are supplemented by design features and by procedures and appropriate training of staff to respond to events outside the design basis.

55. Probabilistic safety assessment also guides design and operation by identifying potential accident sequences that could contribute excessively to risk. Measures can then be taken to reduce this contribution. **In addition PSA can be used as a check on deterministic design features by identifying, for example, single failure components, or potential common cause failures.**

Accident mitigation

56. *Principle: [...] Mitigation measures are available and are prepared for that would substantially reduce the effects of any accidental release of radioactive material.*

57. Provisions for accident mitigation extend the defence in depth concept beyond accident prevention. The accident mitigation provisions are of three kinds, namely, **design features,** accident management **features,** and off-site counter-measures. **Strengthening the first two kinds of on-site features may be used to reduce or even eliminate the need for most of the off-site mitigation features.**

57.a Even though accident prevention always has priority, it is important to include adequate measures in the design to mitigate design basis accidents and addressed severe accidents. Inclusion of such mitigation features contributes to defence in depth by providing more margin directed towards limiting the consequences of accidental release of radioactive material from the plant.

58. Accident management includes preplanned and ad-hoc operational practices which, in circumstances in which the design specifications of the plant are exceeded, would make optimum use of existing plant equipment in normal and unusual ways to restore control. This phase of accident management would have the objective of restoring the plant to a safe state with the reactor shut down, continued fuel cooling assured, radioactive material confined and the confinement function protected. In such circumstances, **design** features would act to confine any radioactive material released from the core so that discharge to the environment would **comply with the Technical Safety Objective No. 19.** These **design** features include physical barriers, some of which have the single purpose of confining radioactive material.

58.a Off-site countermeasures are available, going beyond the level of protection provided in most human endeavours, to compensate for the remote possibility that safety measures at the plant might fail. In such a case, the effects on the surrounding population or the environment would be mitigated by protective actions, such as sheltering or evacuation of the population, and by prevention of the transfer of radioactive material to man by food-chains and other pathways. **For reactor designs meeting the Complementary Design Objective, simplification of these off-site mitigation measures may be allowed.**

II.3.3. GENERAL TECHNICAL PRINCIPLES

Proven engineering practices

60. *Principle: Nuclear power technology is based on engineering practices which are proven by testing and experience, and which are reflected in approved codes and standards and other appropriately documented statements.*

61. Systems and components are conservatively designed, constructed and tested to quality standards commensurate with the safety objectives. Approved codes and standards are used whose adequacy and applicability have been assessed and which have been supplemented or modified if necessary. If opportunities for advancement or improvement over existing practices are available and seem appropriate, such changes are applied cautiously.

62. Numerous codes and standards have been adopted for nuclear use, after formulation by the professional engineering community and approval by the appropriate agencies. Some existing codes and standards have been modified from an original form to take into account unique features of their use for nuclear plants and the elevated importance assigned to the safety of nuclear plants. Approved codes have the simultaneous objectives of reliability and safety. They are based on principles proven by research, past application, testing and dependable analysis.[5]

63. Well established methods of manufacturing and construction are used. Dependence on experienced and approved suppliers contributes to confidence in the performance of important components. Deviations from previously successful manufacturing and construction practices are approved only after demonstration that the alternatives meet the requirements. Manufacturing and construction quality is ensured through the use of appropriate standards and by the proper selection, training and qualification of workers. The use of proven engineering continues throughout the plant's life. When repairs and modifications are made, analysis is conducted and review is made to ensure that the system is returned to a configuration covered in the safety analysis and technical specifications. Where new and unreviewed safety questions are posed, new analysis is conducted.

63.a The construction techniques used for nuclear plants incorporate procedures in which the design and assessment of safety issues are addressed at an early stage. These aspects form an integral part of the approval process by authorities and operating organizations. Careful attention during design to construction aspects and techniques will help minimize the need for changes to the design during construction.

---

[5]The IAEA's NUSS series of documents has been developed in accordance with this principle.

64. The design and construction of new types of power plants are based as far as possible on experience from earlier operating plants or on the results of research programmes and the operation of prototypes of an adequate size.

64.a A natural development of principle 60 is the use of standardization, which has large economic advantages to both design and operation, and may provide some potential indirect safety advantages, by concentrating the resources of designers, regulators and manufacturers on specific design and fabrication methods. These advantages may also include a basis for a more standardized set of siting interface requirements, and standardized engineering documentation for a set of plants. There is of course a risk that standardization may lead to generic problems. Nevertheless properly implemented standardization can also foster more efficient operation, and thus safety, by direct sharing of operating experience and common training; and can also foster more effective construction and quality assurance programs.

Quality assurance

65. *Principle: Quality assurance is applied throughout activities at a nuclear power plant as part of a comprehensive system to ensure with high confidence that all items delivered and services and tasks performed meet specified requirements.*

66. The comprehensive system referred to in the principle begins with analysis and design in accordance with the preceding principle on proven engineering, and it continues into the use of quality assurance methods. Other fundamental technical safety principles are also important in this respect, particularly those on safety assessment and verification and on operating experience and safety research.

67. High quality in equipment and in human performance is at the heart of nuclear plant safety. The goal is to ensure that equipment will function and individuals will perform in a satisfactory way. The processes in which high quality is sought are subject to control and verification by quality assurance practices. Throughout the life of the plant, these practices apply to the entire range of activities in design, supply and installation, and to the control of procedures in plant testing, commissioning, operation and maintenance.

70. Quality assurance programmes provide a framework for the analysis of tasks, development of methods, establishment of standards and identification of necessary skills and equipment. Within this framework is the definition of the items and activities to which quality assurance applies and the standards or other requirements to be implemented through instructions, calculations, specifications, drawings and other statements.

71. Quality assurance practices thus cover validation of designs; supply and use of materials; manufacturing, inspection and testing methods; and operational and other procedures to ensure that specifications are met. The associated documents are subject to strict procedures for verification, issue, amendment and withdrawal. Formal arrangements for handling of variations and deviations are an important aspect of quality assurance programmes.

72. An essential component of quality assurance is the documentary verification that tasks have been performed as required, deviations have been identified and corrected, and action has been taken to prevent the recurrence of errors. The necessary facilities are provided for this, including a hierarchy of documentation, quality control procedures which provide

sampling of work products, opportunity for observation of actual practices and witnessing of tests and inspections, and sufficient staff and other resources.

Human factors

73. *Principle: [...] The possibility of human error in nuclear power plant operation is taken into account in both the design and operational controls and procedures by facilitating correct decisions by operators and inhibiting wrong decisions, and by providing means for detecting and correcting or compensating for error.*

76. Engineered features and administrative controls protect against violations of safety provisions. Moreover, **proper** attention to human factors at the design stage **can help to reduce the likelihood and consequences of** human error. This is achieved, for example, through the actuation of automatic control or protection systems if operator action causes a plant parameter to exceed normal operational limits or safety system trip points. Designs of protection systems ensure that operator intervention to correct faults is required only in cases where there is sufficient time for diagnosis and corrective action. **Typically, operator action is not required for 30 minutes following the first automatic response, (Ref. INSAG-5, para. 6.4), although future designs may be capable of extending this period considerably.** The control room layout provides for localization and concentration of data and controls used in safety related operations and in accident management. Diagnostic aids are provided to assist in the speedy resolution of safety questions. The data available in the control room are sufficient for the diagnosis of any faults that may develop and for assessing the effects of any actions taken. Reliable communication exists between the control room and operating personnel at remote locations who may be required to take action affecting the state of the plant. Administrative measures ensure that such actions by operators at remote locations are first cleared with the control room. The layout and identification of remotely located controls is such as to reduce the chance of error in their selection.

76.a Plants are designed to be "user friendly". This is a term more commonly encountered in connection with computers, but it is also appropriate in describing properties of the plant sought for purposes of good human factors. The designs are user friendly in that the layout and structure of the plant are readily understandable and integrated to most effectively provide the required functions with the minimum number of systems, structures, and components. Experience has shown that design simplicity also leads to improved human performance. Components are located and identified unambiguously so they cannot easily be mistaken one for another. The control room and its information systems are designed with information flow and processing that enables control room personnel to have a clear and complete current understanding of the status of the plant. Computer systems for diagnosis and supervision are designed such that operating personnel can easily and correctly understand the status of the plant and have access to key and unambiguous information which is needed to confirm safe plant operation and to permit operator actions in case of abnormal conditions.

76.b Design engineers seek simple layouts and endeavour to eliminate unnecessary components and systems. Choices are sought that will help to simplify normal operating procedures, emergency operating procedures, inspection, testing and maintenance. Above all, simplicity helps the operating and maintenance personnel to understand the plant and its operation, both normal and abnormal. Improved understanding will build confidence in the validity of decisions by the staff under all conditions. It will reduce the likelihood that common cause failure modes could exist without having been recognized.

76.c Errors by operating staff at a nuclear plant are infrequent, but do sometimes occur. They are judged to be more likely if decisions must be made under time pressure. Therefore, required immediate response by means of automatic action is provided for abnormal situations, especially within the design basis. The information systems inform control room personnel of an automatic action and why it is being taken. In general, advanced plant designs incorporate more capable instrumentation and control, and therefore provide for better diagnosis and control functions as compared to actions previously expected of the operator. Automated response continues for at least a reasonable predetermined time (grace period) to allow for operator assessment of correct plant operation. The opportunity remains for the operators under pre-established operating procedures to override automatic actions if diagnosis shows that they need supplementing or correcting.

Safety assessment and verification

79. *Principle: Safety assessment is made before construction and operation of a plant begin. The assessment is well documented and independently reviewed. It is subsequently updated in the light of significant new safety information.*

80. Safety assessment includes systematic critical review of the ways in which structures, systems and components might fail, and identifies the consequences of such failures. The assessment is undertaken expressly to reveal any underlying design weaknesses. The results are documented in detail to allow independent audit of the scope, depth and conclusions of the critical review. The safety analysis report prepared for licensing contains a description of the plant sufficient for independent assessment of its safety features. It includes information on the features of the site that the design must accommodate. It provides detailed information on the major features of systems, especially of those systems used in reactor control and shutdown, cooling, the containment of radioactive material and particularly the engineered safety features. It describes the analysis of the limiting set of design basis accidents and presents the results.

81. The safety analysis report and its review by the regulatory authorities constitute a principal basis for the approval of construction and operation, demonstrating that all safety questions have been adequately resolved or are amenable to resolution.

82. Methods have been developed to assess whether safety objectives are met. These methods are applied at the design stage, later in the life of the plant if changes to plant configuration are planned, and in the evaluation of operating experience to verify the continued safety of the plant. Two complementary methods, deterministic and probabilistic, are currently in use. These methods are used jointly in evaluating and improving the safety of design and operation.

83. In the deterministic method, design basis events are chosen to encompass a range of related possible initiating events which could challenge the safety of the plant. Analysis is used to show that the response of the plant and its safety systems to design basis events satisfies predetermined specifications both for the performance of the plant itself and for meeting safety targets. The deterministic method uses accepted engineering analysis to predict the course of events and their consequences.

83.a. For addressed severe accidents, designers prepare detailed deterministic and probabilistic assessments of their designs, demonstrating margins against addressed

severe accident scenarios and conformance to overall objectives and safety targets. The insights from these assessments are used to justify certain features which become part of the design. Deterministic and probabilistic analysis of severe accidents is performed on a best estimate basis.

84. **Probabilistic safety analysis is used to comprehensively review in a realistic way, the design of the plant under a wide variety of failure conditions, to estimate the level of safety achieved by design, and to eliminate design weaknesses. Elimination of these weaknesses reduces both the probability of severe accidents and the uncertainty in this probability. It is important that this tool is effective. Its effectiveness is linked to the accuracy of the data base, the realism of the calculations, and the proper treatment of uncertainties in the models. For future plants, special care is taken to ensure that the models and data used for new systems and features are applicable and reliable.**

Radiation protection

86. *Principle: A system of radiation protection practices, consistent with recommendations of the ICRP and the IAEA[6], is followed in the design, commissioning and operational phases of nuclear power plants.*

87. Measures are taken to protect workers and the public against the harmful effects of radiation in normal operation, anticipated operational occurrences, **design basis accidents and addressed severe accidents.** These measures are directed towards control of the sources of radiation; to the provision and continued effectiveness of protective barriers and personal protective equipment; and to the provision of administrative means for controlling exposures.

88. Radiation protection is considered in the design process by paying attention to both specific details and broad aspects of plant layout.

II.4. SPECIFIC PRINCIPLES

External factors affecting the plant

97. *Principle: The choice of site takes into account the results of investigations of local factors which could adversely affect the safety of the plant.*

98. Local factors include natural factors and man made hazards. Natural factors to be considered include geological and seismological characteristics and the potential for hydrological and meteorological disturbances. Man made hazards include those arising from chemical installations, the release of toxic and flammable gases, and aircraft impact. The investigations required give information on the likelihood of significant external events and their possible effects on nuclear power plant safety **which are to be considered in the design**. This is developed in the form of quantified probabilities when possible. The corresponding **safety** evaluation takes into account the safety features provided by the design

---

[6]INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, Recommendations of the International Commission on Radiological Protection, ICRP Publication No. 60, Pergamon Press, Oxford and New York (1992); INTERNATIONAL ATOMIC ENERGY AGENCY, **International** Basic Safety Standards for **Protection Against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1994).**

to cope with these events. Special attention is given to the potential for extreme external events and to the feasibility of installing compensating safety features.

103. *Principle: The site selected for a nuclear power plant has a reliable long term heat sink that can remove energy generated in the plant after shutdown, both immediately after shutdown and over the longer term.*

104. In some cases, extreme conditions in such events as earthquakes, floods and tornadoes could threaten the availability of the ultimate heat sink unless adequate design precautions are taken. The choice of the atmosphere as an ultimate heat sink is acceptable, provided that the design ensures that the heat removal system would withstand any extreme event that must be taken into account.

II.4.2. DESIGN

II.4.2.1. Design process

109. The specific design principles are divided into three groups: those related to the general process of designing a nuclear plant to be safe; those stating general features to be incorporated into a plant so as to make it safe; and those stating more specific features.

Design management

110. *Principle: The assignment and subdivision of responsibility for safety are kept well defined throughout the design phase of a nuclear power plant project, and during any subsequent modifications.*

111. The design of a safe plant is under the authority of a highly qualified engineering manager whose attitudes and actions reflect a safety culture and who ensures that all safety and regulatory requirements are met. Separate aspects of design may be served by different sections of a central design group and by other groups subcontracted to specific parts of the project. An adequate number of qualified personnel is essential in each activity. The engineering manager establishes a clear set of interfaces between the groups engaged in different parts of the design, and between designers, suppliers and constructors.

112. The design force is engaged in the preparation of safety analysis reports and other important safety documents. It also includes a coordinating group which has the responsibility of ensuring that all safety requirements are fulfilled. This group remains familiar with the features and limitations of components included in the design. It communicates with the future operating staff to ensure that requirements from that source are recognized in the design and that there is appropriate input from the designer to the operating procedures as they are prepared and to the planning and conduct of training.

113. In accordance with the fundamental principle **65**, quality assurance is carried out for all design activities important to safety. An essential component of this activity is configuration control, to ensure that the safety design basis is effectively recorded at the start and then kept up to date when design changes occur.

Proven technology

114. *Principle: Technologies incorporated into design have been proven by experience and testing. Significant new design features or new reactor types are introduced only after thorough research and prototype testing at the component, system or plant level, as appropriate.*

115. This principle is a specific application of the fundamental principle **60** to nuclear power plant design. Disciplined engineering practice requires a balance between technological innovation and established engineering practices. Design is in accordance with applicable national or international standards, particularly those specifically for nuclear use, which are accepted by the professional engineering community and recognized by the appropriate national or international institutions. These standards reflect engineering practices proven in past use. It is nevertheless always necessary to allow for consideration of the need for, and the value of, improvements beyond established practice. These are first brought to the level of 'proven engineering' through appropriate testing and scaling up if needed.

115.a An example of this balance between proven technology and technological innovation is the recent emergence of broad interest in passive safety features. The advantages and disadvantages of these passive features are carefully considered in the design process. The essential advantages of passive features are their independence from external support systems such as electric power; their generally greater simplicity, and their higher reliability. Disadvantages include lower driving heads in fluid systems and lower flexibility in abnormal conditions. Furthermore, active components can still be necessary for startup and shutdown. Special attention has to be paid to limitations in the existing data on the performance of new passive systems.

116. Most application of engineering technology requires the use of analytical methods. The physical and mathematical models used in design are validated by means of experimental or operational testing and analysis of data. Results of more complex analysis are verified by pertinent experimentally based benchmark calculations, type testing and peer review. Where possible, realistic modeling and data are used to predict plant performance, safety margins and the evolution of accident conditions. Where realistic modeling is not feasible, conservative models are used.

General basis for design

117. *Principle: A nuclear power plant is designed to cope with a set of design basis events including normal conditions, anticipated operational occurrences, extreme external events and accident conditions. For this purpose, conservative rules and criteria incorporating safety margins are used to establish design requirements. Comprehensive analyses are carried out to evaluate the safety performance or capability of the various components and systems in the plant.* ***In addition, prevention and mitigation of addressed severe accidents are explicitly taken into account in the design, consistent with overall design and safety objectives. However, best-estimate, as opposed to conservative rules and criteria, are used in the evaluation process.***

118. The various events that the plant has to accommodate are classified according to their probabilities of occurrence. Attention in design ensures that there is no damage to the plant as a result of events classed as normal operating events, or for which there is a reasonable expectation of occurrence during the lifetime of the plant. At a much lower level of

probability are combinations of human and mechanical failure that could jeopardize the protection provided by plant features and normal plant systems.

119. Engineered safety systems are included in plant design, as discussed in **General technical principles**, to protect against the possibility of occurrence of classes of accidents that would otherwise contribute significantly to risk, or to mitigate the consequences of such accidents. Any engineered safety system is designed to prevent or to mitigate a specific spectrum of accidents. The accidents in this spectrum that tax the features of the safety system most are termed the design basis accidents for that system. The plant and the engineered safeguards are so designed that none of these accidents or accident sequences dominate the total risk. In design, attention is given to requirements for such future activities as maintenance and periodic testing, to ensure continued conformity to the principle. In addition, design features are provided to address severe accidents. These features are not required to meet conservative, safety-grade requirements, but rather are designed using best-estimate analyses, assumptions, and performance standards. **This same general approach applies to passive safety features being considered for future plants. Passive features intended to cope with design basis events should also meet safety-grade requirements where applicable. Passive features intended to address severe accidents need not meet such stringent requirements.**

119.a Systems, structures and components required to prevent or mitigate design basis accidents or to address severe accidents, and which are shared among two or more units, are designed so that in the event of an accident at one unit, such sharing will not impair the ability to perform safety or accident management functions of the remaining units, or to impede an orderly shutdown and cooldown of any of the units as needed.

Classification of components, structures, and systems

119.b ***Principle: All safety related components, structures and systems are classified on the basis of their functions and significance with regard to safety, and they are so designed, manufactured and installed that their quality is commensurate with this classification.***

119.c This classification provides a basis for determining the appropriate design codes and standards to be applied to components, structures and systems. All items important to safety are designed, constructed, operated and inspected to requirements that are commensurate with their safety function.

Safety evaluation of design

193. *Principle: Construction of a nuclear power plant is begun only after the operating organization and the regulatory organization have satisfied themselves by appropriate assessments that the main safety issues have been satisfactorily resolved and that the remainder are amenable to solution before operations are scheduled to begin.*

194. The options available to the designers for modifying plant safety features become restricted as fabrication and construction proceed. For this reason it is necessary to coordinate safety evaluation with manufacturing and construction to ensure that important safety options are not foreclosed and that licensing decisions are timely.

195. At approximately the stage when preliminary design has been completed a safety analysis is performed. This overall analysis is reviewed with the regulatory authorities to ensure that regulatory requirements have been met or will be met, and the plant will be safe for operation. This determination may be subject to outstanding issues expected to be resolved during construction and before operation starts. Additional checkpoints are established as required during construction so that satisfactory final design, installation and verification of the adequacy of safety related equipment can be reviewed.

II.4.2.2. General features

Plant process control systems

121. *Principle: Normal operation and anticipated operational occurrences are controlled so that plant and system variables remain within their operating ranges. This reduces the frequency of demands on the safety systems.*

122. Important plant neutronic and thermal-hydraulic variables have assigned operating ranges, trip setpoints and safety limits. The safety limits are extreme values of the variables at which conservative analysis indicates that undesirable or unacceptable damage to the plant may be initiated. The trip setpoints are at less extreme values of the variables which, if attained as a result of an anticipated operational occurrence or an equipment malfunction or failure, would actuate an automatic plant protective action such as a programmed power reduction, plant shutdown or an even more marked response. Trip setpoints are chosen such that plant variables would not reach safety limits. The operating range, which is the domain of normal operation, is bounded by values of the variables less extreme than the trip setpoints.

123. It is important that trip actions are not induced too frequently, especially when they are not required for protection of the plant or the public. Not only would this interfere with the normal, productive use of the plant, but also it could compromise safety by the effects of sudden and precipitous changes, and it could induce excessive wear which might impair the reliability of safety systems.

124. Therefore, the more important neutronic and thermalhydraulic variables are automatically maintained in the operating range. This is done by feedback systems acting on electrical and mechanical controls when variables begin to depart from the operating range. The normal operating state is then restored. The limits to the normal operating range are chosen so that the feedback action prevents variables from reaching trip setpoints in normal operation.

Automatic safety systems

125. *Principle: Automatic safety systems are provided that would safely shut down the reactor, maintain it in a cooled state, and limit any release of fission products that might possibly ensue, if operating conditions were to exceed predetermined setpoints.*

126. Despite the high quality of the design and construction and any self-controlling features of the plant, it is anticipated that sequences of events originating either inside or outside the plant will occasionally occur that exceed the protective capabilities of normal plant control systems. These hypothetical failures constitute a broad range of initiators of accidents against which the design is evaluated. Engineered safety features are incorporated

as necessary to ensure that plant damage, especially damage to the reactor core, would be limited **in the case of** design basis accidents. In such circumstances, reactor power would be controlled, core cooling would be maintained and any radioactive material released from the fuel would remain confined by suitable physical barriers.

127. Initiation and operation of the engineered safety features are highly reliable. This reliability is achieved by the appropriate use of fail-safe design; by protection against common cause failures; and by independence between safety systems and plant process systems. The design of these systems ensures that failure of a single component would not cause loss of the function served by a safety system (the single failure criterion). Where a system is relied upon to perform both safety and process functions, special consideration is given to ensuring that the safety function is not affected by expected or inadvertent process control demands.

128. Proven engineering practice, operating experience and safety analysis call for high reliability of electrical and instrumentation systems supporting safety systems. Many of the mechanical and fluid systems that shut down the reactor, cool the fuel or confine the radioactive materials depend upon electricity to power their active components, indicate their status and control their operation. Thus, the reliability of safety systems is determined by the reliability of the electrical, fluid and instrumentation systems that support them.

128.a Computer systems which are used for safety functions are designed and installed to ensure that residual faults do not prevent any required safety actions. This can be achieved by diversity of software and hardware, or by separate continuous monitoring systems. The production process for safety critical software and hardware incorporates the highest standards of system specification and best practices, which are applied throughout its life cycle, including commissioning, operation, maintenance, and modification. This process also provides assurance that faults are eliminated by a comprehensive method of verification and validation by the manufacturer, together with integrated software and hardware system testing, and on-site testing which confirms the reliability of the software.

129. Plant design includes the capability to test automatic safety systems throughout the plant's life, with automatic self- tests where possible. Test conditions seek to reproduce operating conditions.

129.a Severe accident conditions may not be fully controlled by the provisions described above, and may need the development and provision of additional measures. Therefore, the need for systems to respond to severe accidents is also considered in the design. The design of such measures is based on different practices to those applied to engineered safety features. Less conservative approaches are used throughout, such as best estimate analysis, manual actions, non-safety grade equipment, etc.

Reliability targets

130. *Principle: Reliability targets are assigned to safety systems or functions. The targets are established on the basis of the safety objectives and are consistent with the roles of the systems or functions in different accident sequences. Provision is made for testing and inspection of components and systems for which reliability targets have been set.*

131. Generally applicable design requirements for high reliability of safety systems and functions are translated into specific reliability targets. The reliability of support services required for the operation of safety systems or functions, such as electrical power or cooling water, is considered in the formulation of reliability targets. Appropriate reliability targets are set to ensure performance on demand and operation throughout the required duration of performance. These targets are based on engineering analysis. Detailed probabilistic methods are useful in determining the reliability required of safety systems and functions. Regardless of how the reliability targets are established, a reliability analysis is conducted during the design process to ensure that safety systems and functions can meet them. Functional testing and system modeling are used to demonstrate that the reliability targets will continue to be met during plant service. The need for continued assurance of reliability during operation places a requirement on the designer to provide systems which are testable in service, under realistic demand and performance conditions if possible.

132. For some systems, reliability targets may exceed values which can be demonstrated. If it is necessary to ensure this greater functional reliability, additional independent systems are used, each of which is capable of performing the assigned safety function. Diversity and physical separation of these systems reduce the possibility of common mode failures.

Dependent failures

133. *Principle: Design provisions seek to prevent the loss of safety functions due to damage to several components, systems or structures resulting from a common cause.*

134. The appropriate design method to prevent damage to two or more systems simultaneously is determined by specific circumstances. Among the methods used are physical separation by barriers or distance, protective barriers, redundancy linked with diversity and qualification to withstand the damage.

135. Some common cause events that must be considered would have their origins in occurrences internal to the plant. These include the loss of common electrical power sources, depletion of fuel for diesel generators, loss of common service functions, fire, explosion, projectiles ejected in the failure of rotating or pressurized components, system interaction, or error in design, operation, maintenance or testing. Failures due to undetected flaws in manufacturing and construction are also considered. Common cause events external to the plant include natural events such as earthquakes, high winds and floods, as well as such man made hazards as aircraft crashes, drifting explosive clouds, fires and explosions, which could originate from other activities not related to the nuclear power plant. For a site with more than one reactor unit, events that could originate in the units on the site are considered as additional external initiating events for the other units.

136. Because of the importance of fire as a source of possible simultaneous damage to several components, design provisions to prevent and combat fires in the plant are given special attention. Fire resistant materials are used to the extent possible. Fire-fighting capability is included in the design specifications. Lubrication systems use non-flammable lubricants or are protected against the initiation and the effects of fires. The design takes advantage of the methods identified for preventing common cause failures.

137. Of the extreme external hazards, seismic events receive special attention owing to the extent to which they can jeopardize safety. A nuclear power plant is protected against earthquakes in two ways: by siting it away from areas of active faulting and related potential

problems such as susceptibility to soil liquefaction or landslides; and by designing it to bear the vibratory loads associated with the most severe earthquake that could be expected to occur in its vicinity, on the basis of historical input and tectonic evidence. This is termed the design basis earthquake. Seismic design of plant structures, components and systems is carried out using response function methods, making use of a frequency spectrum for the design basis earthquake that is appropriate to the site. Seismic design takes account of soil-structure interaction, the potential amplification and modification of seismic motion by the plant structures, and interaction between components, systems and structures. The design ensures that the failure of non-safety-related equipment in an earthquake would not affect the performance of safety equipment.

Equipment qualification

138. *Principle: Safety components and systems are chosen which are qualified for the environmental conditions that would prevail if they were required to function. The effects of ageing on normal and abnormal functioning are considered in design and qualification.*

139. The conditions under which equipment is required to perform a safety function may differ from those to which it is normally exposed, and its performance may be affected by aging or by service conditions as plant operation goes on. The environmental conditions under which equipment is required to function are identified as part of the design process. Among these are the conditions expected in a wide range of accidents, including extremes of temperature, pressure, radiation, vibration, humidity and jet impingement. The effects of external events such as earthquakes are also considered.

140. The required reliability is to be maintained throughout the plant's life. Attention is given during design to the common cause failure effects of ageing and to the effects of ageing on the plant's capacity to withstand the environmental effects of accidents considered in the design. Ageing is taken account of in the design by the appropriate definition of environmental conditions, process conditions, duty cycles, maintenance schedules, service life, type testing schedules, replacement parts and replacement intervals.

141. It is preferable that qualification be achieved by the testing of prototypical equipment. This is not always fully practicable (e.g. for vibration of components or of equipment etc.) In such cases, analysis or tests plus analyses are relied upon.

Inspectability **and maintainability** of safety equipment

142. *Principle: Safety related components, systems and structures are designed and constructed so that they can be inspected,* ***and maintained*** *throughout their operating lives to* ***assure*** *their continued acceptability for service with an adequate safety margin.*

143. In-service inspection is relied upon to demonstrate that safety provisions are maintained throughout the life of the plant. Provision is made at the design stage for inspection **and maintenance** access, and for the ease and frequency of inspection **and maintenance**. In-service inspection of the primary coolant system boundary receives special attention because of the great reliance placed upon coolant retention and the environmental conditions to which the primary system boundary is exposed for a long period of time. The radiological protection of workers is also carefully considered in designing for in-service

inspection **and maintenance** of safety equipment. Other safety systems that receive attention in design to ensure their inspectability include electrical cable runs, junction boxes, penetrations of the confinement system boundary, coolant and lubrication systems, and components including organic materials and other materials that may degrade with age or as a result of radiation exposure.

Radiation protection in design

144. *Principle: At the design stage, radiation protection features are incorporated to protect plant personnel from radiation exposure and to keep emissions of radioactive effluents within prescribed limits.*

145. Designers provide for protection of the operating and maintenance staff from direct radiation and from contamination by radioactive material. Care is taken in the design of radioactive waste systems to provide for conservative adherence to authorized limits. The design ensures that all plant components containing radioactive material are adequately shielded and that the radioactive material is suitably contained. This protection is effective in routine operations, and is also helpful in non-routine circumstances such as during maintenance and engineering modification, when activities are more varied. Design of the plant layout takes into account radiation protection requirements, by attention to the appropriate location of plant components and systems, shielding requirements, confinement of radioactive materials, accessibility, access control, the need for monitoring and control of the working environment, and decontamination. Consideration is given to use of materials which do not become exceptionally radioactive with long half-lives under neutron irradiation; to the avoidance of design features which promote the retention of activated material in locations from which it can be removed only with difficulty; and to the use of surface finishes which facilitate decontamination. Facilities for personnel and area monitoring and personnel decontamination are included in the plant design.

II.4.2.3. Specific features

Protection against power transient accidents

148. *Principle: The reactor is designed so that reactivity induced accidents are protected against, with a conservative margin of safety.*

149. A reactivity induced accident would be one in which an increase in reactivity occurred, either globally or locally, causing the reactor power to exceed the heat removal rate and thus to damage the fuel. Two kinds of properties of a nuclear plant are important in counteracting such an increase in reactivity. One is negative reactivity feedback, and the other is the system which introduces a neutron absorber or reduces the reactivity by some other means, to compensate for the reactivity increase or to curtail power generation. Both kinds of features are affected by **reactor and fuel** design choices. Negative reactivity feedback coefficients alone cannot prevent all imaginable reactivity induced accidents or damage due to such accidents, but they can be effective in doing this in many cases, through their stabilizing effects. Therefore, the design of a reactor core usually relies in part on such inherent features to assist in preventing reactivity induced accidents. Where inherent characteristics alone cannot prevent reactivity induced accidents, control systems are designed to ensure reliable reactivity control under all operating conditions, **including low power operations**. The safety shutdown system is designed to have the reliability and effectiveness necessary for the timely suppression of reactivity induced power transients and the prevention

of damage to the reactor core from such a cause, **again under all operating conditions, including low power operations**. The great importance of achieving this is reflected in the commensurate assurance that the combination of inherent feedback features, reactivity control systems and shutdown systems achieves its purpose with a satisfactory margin. This assurance includes an experimental and analytical demonstration that the reliability of the shutdown system is adequate, and analysis to verify also that the effects of possible transients would be tolerable.

150. Attention is given to ensuring that external events, failures of equipment or human errors would not lead to reactivity induced accidents. In addition, attention is given to the prevention of reactivity induced accidents that might result from actions originating otherwise than in the normal operation of the plant. The most important design measures to be taken are those that combine limits on withdrawal rates of shim, control and safety rods with strategies of rod management, automatic control and protection systems, **and appropriate fuel design**; to ensure that the removal or addition of a single fuel rod would not introduce transients that would cause significant damage to an on-line reloaded reactor core; and that a reactor being batch loaded would not become critical during the loading process. The withdrawal of any single control rod in the completely shut down reactor does not make the reactor core critical.

Reactor core integrity

151. *Principle: The core is designed to have mechanical stability. It is designed to tolerate an appropriate range of anticipated variations in operational parameters. The core design is such that the expected core distortion or movement during an accident within the design basis would not impair the effectiveness of the reactivity control or the safety shutdown systems or prevent cooling of the fuel.*

152. Fuel **elements** tend to be distorted and displaced if there is a steep radial gradient of heating rate across the core of a reactor. If this is not countered, core distortion may result, possibly inducing reactivity changes or inhibiting the **timely** insertion of safety and control rods or elements. In some cases, distortion could affect the hydraulic diameters of specific channels, and hence the cooling of the fuel. Similar effects could **also** result from radiation damage in graphite moderated reactor cores unless allowance is made to take account of the radiation induced dimensional changes in the graphite. Some precautions, such as restraints, may be necessary to prevent undesirable effects of thermal, mechanical and radiation induced distortion of the core.

153. Fuel **element** vibration induced by thermal-hydraulic effects is prevented by mechanical constraint. This prevents associated neutronic fluctuations and excessive fretting and wear of cladding. Fuel **elements** and other core components are restrained so that abrupt shifts in position cannot cause sudden or large reactivity changes. Care is exercised to ensure that restraints do not themselves introduce safety problems.

154. Analysis supported by suitable experiments verifies that the core is geometrically stable against potential earthquakes, system transients and other dynamic forces to which it might be subjected.

155. High quality of fuel **elements** is an important safety requirement. Damaged or distorted fuel can potentially inhibit cooling and the reactivity reduction process. Furthermore, cladding failure represents a basic loss of defence in depth. Less severe damage

may reduce the ability of the fuel to withstand accident conditions. For these reasons, special quality assurance measures are taken in the design and manufacture of fuel. Continued fuel integrity is verified by monitoring the level of radioactivity in the coolant during operation.

Automatic shutdown systems

156. *Principle: Rapidly responding and highly reliable reactivity reduction for safety purposes is designed to be independent of the equipment and processes used to control the reactor power. Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are being intentionally taken or whenever a chain reaction might be initiated accidentally.*

157. Safety shutdown systems are independent in function from the reactivity control systems used for normal operation of the reactor. Common sensors or devices may be used if reliability analysis indicates that this is acceptable. Under all conditions taken into account in the design, when the core is critical or may become critical, safety shutdown mechanisms with sufficient negative reactivity are poised to **rapidly** initiate safe shutdown if required. The rate of reactivity addition is an important parameter in some accident sequences, and design steps are required to retain this parameter within appropriate limits defined by the design basis. Electrical busses and logic circuits of the shutdown system are separate from instruments used for normal control so that no interference is possible between the demands of normal control and the demands of safe shutdown. Only when the reactor is in a predefined 'guaranteed shutdown state' with sufficient subcriticality can the safety shutdown systems be safely disabled.

158. One unlikely event which must be analyzed is the failure of an automatic shutdown system to act when it is called upon. The scenario is highly plant dependent, and it varies with the circumstances leading to the signal for automatic shutdown. The consequences might be an excessive increase in reactivity, an excessive primary circuit pressure, excessive fuel temperatures or some other potential cause of damage to the plant. The plant is so designed that these anticipated transients without scram (ATWS) do not contribute appreciably to risk. This is achieved by making the accidents sufficiently unlikely or by ensuring that they will not lead to severe core damage. Attention to prevention of these accidents or to limitation of their effects ensures that the safety objective is met even taking into account this failure of plant protection.

Normal heat removal

159. *Principle: Heat transport systems are designed for highly reliable heat removal in normal operation. They would also provide means for the removal of heat from the reactor core during anticipated operational occurrences and during most types of accidents that might occur.*

160. The primary heat removal system is a reliable means of cooling the core in normal operation. It is also the preferred means of shutdown heat removal and for decay heat removal after an abnormal occurrence or in most accidents. There may be other systems, not necessarily safety related, but used in normal reactor operations, that can alternatively perform this important safety function of removal of residual heat. Their availability for use adds to defence in depth.

Emergency heat removal

161. *Principle: Provision is made for alternative means to restore and maintain fuel cooling under accident conditions, even if normal heat removal fails or the integrity of the primary cooling system boundary is lost.*

162. Certain abnormal conditions could impair the capability to remove heat of all normal active in-plant systems. In some reactors, natural circulation would be adequate for decay heat removal in these circumstances, provided that the primary coolant boundary remains intact and some capability for heat removal is maintained on the secondary side. In other cases, for which severe core damage could possibly occur if no alternative heat removal path is provided, a capability for emergency heat removal is needed. This includes residual heat removal systems and emergency core cooling systems, and emergency feedwater systems to ensure the capability of heat removal on the secondary side. In the past, the unreliability of the shutdown heat removal function has been found to be a significant contributor to total risk for some nuclear plants. The need for highly reliable shutdown heat removal has led in some cases to consideration of the use of special cooling system designs, such as dedicated and protected decay heat removal systems and systems based on natural circulation or conduction. The atmosphere is sometimes **used** as a possible ultimate heat sink.

Reactor coolant system integrity

163. *Principle: Codes and standards for nuclear vessels and piping are supplemented by additional measures to prevent conditions arising that could lead to a rupture of the primary coolant system boundary at any time during the operational life of the plant.*

164. The reactor coolant boundary is a critical system because its failure could lead to impairment of the ability to cool the fuel, and in extreme cases to loss of confinement of the radioactive fuel. This is particularly important for a pressurized reactor vessel, since catastrophic failure of this component would not be tolerable.

165. For all components forming part of the main coolant boundary, and especially for the reactor vessel, careful attention must be paid to design, materials, fabrication, installation, inspection and testing, with particular emphasis on use of established codes of practice and experienced suppliers, and detailed attention to the achievement of high quality. Analysis is carried out to demonstrate that the structures can withstand the stresses likely to be imposed under the more extreme expected loading conditions.

166. Multiple inspections are conducted during and after fabrication and installation of the primary system boundary. They use ultrasonic, radiographic and surface methods. Hydraulic overpressure testing to pressures well above those expected in operation confirms the strength of the system before it is made radioactive.

167. Analyses of strength of metallic parts of the primary system boundary are based on the assumption that small defects may have been introduced during manufacture and remained undetected in the inspection process owing to their size. Such analyses show that design, operating restrictions and periodic inspections provide assurance with an ample margin over the lifetime of the plant that undetected cracks would not grow to a length which is critical under the maximum stresses to be encountered. Undue challenges to the integrity of the envelope of a pressurized reactor are prevented by ensuring adequate overpressure protection. For ferritic steel vessels, any combination of pressure and low temperature which might

cause brittle failure (including combinations that might be encountered in design basis accidents) is prevented. Mechanisms of deterioration of the primary system boundary are taken into account in the design of the plant, including fatigue, corrosion, stress corrosion and embrittling effects of irradiation and hydrogen.

168. The use of prestressed concrete pressure vessels is current practice for gas cooled reactor plants. Most statements made earlier generally apply to these as well, with differences only in detail, even though the structures are very different. An important additional requirement for such vessels is attention to the condition and loading of the prestressing tendons, and to the condition of the insulation, the liner, the liner cooling system, penetrations and similar features, as installed and subsequently in service.

169. During the life of the plant, the continued fitness of the coolant boundary for service is verified by inspection, analysis, and testing of exposed samples of archival vessel material, by monitoring for leaks using systems designed for this purpose, and by making any repairs or replacements which prove necessary and are feasible. Access for, ease of and frequency of inspection are taken into account in the design.

170. Ferritic steel reactor pressure vessels for some existing plants are subject to inspection and operating restrictions that would not be necessary if technological issues now understood had been well researched at the time of fabrication of the vessels. In future, welds are not to be made in regions of higher neutron flux levels, especially longitudinal welds at the vessel belt line. Steels for the vessels and welding consumable will have a very low content of elements that accelerate radiation induced deterioration, especially copper and phosphorus. Sensitive steels are not to be used. Steels used will be readily weldable, and, together with their weldments, will have high fracture toughness at all temperatures in the operating region. The vessels will have diameters large enough to ensure sufficient attenuation of the fast neutron flux between the core boundary and the vessels' inner surfaces.

Confinement of radioactive material

171. *Principle: The plant is designed to be capable of retaining* ***most or all of*** *the radioactive material that might be released from fuel, for the entire range of accidents considered in the design.*

172. Systems are required to retain radioactive material that might be released as a result of **design basis accidents and addressed severe accidents,** unless it has been shown that adequate protection against such releases has been secured by other means **in order to satisfy principles 19 and 19a**. These systems have the function of preventing leakage of almost all the more significant radioactive materials. Such systems providing a confinement function have common features:

A structure encloses the region into which radioactive material from fuel, consisting principally of fission products, could be released in the event of the loss of fuel integrity.

Confinement may be effected by making the structure so strong that when it is sealed it can withstand a high internal pressure. It is then called a containment structure. The containment structure usually has **a safety system or subsystem** that completes the sealing process on demand **in response to design basis accidents**, and other

subsystems protecting the structure (see the principle **175**). Together these constitute a containment system.

Confinement may be **augmented** by equipping the structure with devices that permit pressure due to an accident to be relieved to the exterior while ensuring that the bulk of any radioactive material released from fuel is retained.

The structure maintains its **integrity** both in the short term and the long term under the pressure and temperature conditions which could prevail during design basis accidents. **An appropriate confinement function is also provided for addressed severe accidents to meet the Technical Safety Objective and as necessary, the Complementary Design Objective.**

Openings and penetrations, when they have been secured, and other singular points in the structure are designed to meet requirements similar to those for the structure itself so that they do not render it vulnerable as potential pathways for the release of radioactive material.

If analysis shows that residual reactor heat could lead to an increase of atmospheric temperature inside the containment and thereby generate a pressure threatening the integrity of the structure, provision is made for the removal of this heat.

173. It must be demonstrated that the confinement capability is such that the design basis targets for limiting the leakage of any radioactive material are met. Provision is therefore made for functional testing to ensure that design objectives are met.

174. Design measures are taken to prevent circumstances arising in which, in the event of an accident, radioactive materials could bypass the **containment** and be released directly to the environment.

174.a It is expected that most reactor designs will have a pressure retaining containment structure unless it can be demonstrated that the retention of radioactive materials can be assured without a structure with pressure retaining capability. It is also expected that these containment structures or other plant features will protect against those external events addressed in the design.

Protection of confinement **function and containment** structure

175. *Principle: If specific and inherent features of a nuclear power plant would not prevent detrimental effects on the* ***containment*** *structure in a severe accident, special protection against the effects of such accidents is provided, to the extent needed to meet the general safety objective.*

176. This principle particularly affects a **containment** structure used **to provide the confinement function,** as discussed in the previous principle. A containment structure is designed to withstand the internal pressure that can be expected to result from the design basis accident for this structure, calculated using substantial safety factors. **The containment structure and associated systems are also designed to protect against those external challenges addressed in the design.** Calculations indicate that in extreme cases some severe accidents beyond the design basis could generate pressures higher than the design pressure for the containment structure. **For current plants, various solutions are adopted, and** these

higher values are in most cases less than those corresponding to the ultimate strength of the containment.

177. **For many current plants**, if severe accident sequences could lead to pressures causing stresses exceeding the estimated ultimate strength of the containment, that structure might fail. If it failed catastrophically early in the accident sequence, a significant release of radioactive material might occur, necessitating protective measures outside the plant. Such circumstances could produce an appreciable contribution to the calculated risk. **For most current plants, various actions are taken to address these issues, including backfitting of new systems, modifications to existing systems and structures, development of new accident management capabilities, etc.**

177.a For future plants, the containment structure is analyzed for the pressures and temperatures resulting from addressed severe accident phenomena (e.g., hydrogen generation and burning, low pressure melt ejection, core–concrete reactions). Analysis may show that the design pressure and temperature for the structure is exceeded, depending on the design; but these pressures and temperatures are expected to remain less than those corresponding to the ultimate strength of the structure, for those severe accidents addressed in the design. These severe accidents are selected and evaluated using best-estimate analysis. If they lead to pressures and temperatures causing stresses exceeding the estimated ultimate strength of the structure, and if other preventive or mitigative actions to delay or diminish these stresses are not achievable, then strengthening of the structure or introduction of additional features is considered. Other challenges to the confinement function may also be addressed that could lead to similar actions. For some other potential challenges to the containment (e.g., external challenges) that are not accompanied by failures in other safety functions or other defence-in-depth barriers, the Technical Safety Objective can be met through demonstrating reasonable assurance of maintaining those other functions or barriers.

Monitoring of plant safety status

180. *Principle: Parameters to be monitored in the control room are selected, and their displays are arranged, to ensure that operators have clear and unambiguous indications of the status of plant conditions important for safety, especially for the purpose of identifying and diagnosing the automatic actuation and operation of a safety system or the degradation of defence in depth.*

181. Continued knowledge and understanding of the status of the plant on the part of operating staff is a vital component of defence in depth. The control room is therefore provided with display of the information on plant variables needed to ascertain the status in normal operation, to detect and diagnose off-normal conditions, and to observe the effect of corrective responses by control and safety systems. Information from both internally and externally initiated events is considered for control room display. Early warning of developing problems is provided, including loose parts monitoring systems, monitoring of excessive and unusual vibration or noise, and systems to detect coolant leaks or unusual levels of radiation, temperatures or moisture.

182. The means of transmitting and displaying information include meters and status lights, parameter trend displays, prioritized alarms and various diagnostic aids as well as reliable personal communication between control room personnel and distant operating or maintenance staff. Care is taken by designers to ensure that the operators have the means of

monitoring the most useful and important information, and to prevent distraction by more peripheral information. Experienced operating staff as well as human factors experts assist designers by identifying the most appropriate organization and presentation of these data.

Preservation of **plant** control capability

183. *Principle: The **main** control room is designed to remain habitable under normal operating conditions, anticipated abnormal occurrences and accidents considered in the design. Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control room for circumstances in which the main control room may be uninhabitable or damaged.*

184. The environment in the **main** control room is protected against abnormal conditions that might compromise the operators' effectiveness or jeopardize their health. These might be conditions arising in the plant, or the result of some occurrence external to the plant. In the event that the environment of the control room were degraded for any reason, operators would receive a clear warning. Suitable equipment for personal protection is provided.

185. Although unlikely, situations are conceivable in which the main control room could become uninhabitable or damaged to the extent that it is no longer usable. Alternative means are provided to ensure that safe plant conditions would be maintained if this happened. One or more supplementary locations are instrumented and equipped with the necessary controls so that the operators could take actions at these locations to ensure that the basic safety functions of reactor shutdown, residual heat removal and confinement of radioactive materials are achieved and maintained in the long term. Actions bringing about a change in system performance may sometimes need to be taken at remote locations, e.g. the local change of a valve setting. Where such control actions and monitoring are expected to occur at different points, communication between the points is reliable.

Station blackout

186. *Principle: Nuclear plants are so designed that the simultaneous loss of normal on-site and off-site AC electrical power (a station blackout) will not lead to fuel damage **for a certain period of time**.*

187. Electrical power is essential for nuclear power plant safety systems. The reliability of the electrical power supply is commensurate with the reliability demanded of the safety systems which it serves. Both normal and backup power supplies are designed to ensure high reliability. The reliability of backup electrical power supplies for safety systems is sometimes augmented by means of diverse power supplies, such as direct drive diesels, direct drive steam turbines and batteries for instruments and other DC components.

188. In particular, nuclear power plants are designed to withstand, without loss of safety function, a simultaneous loss of **normal** on-site and off-site AC electrical power (a station blackout) for a **certain** period of time. The period of time is a function of the plant design, the reliability of core cooling systems driven by other motive means, the ability to dissipate decay heat by other means, such as natural circulation and thermal conduction, and special provisions for restoring cooling or electrical power before damage occurs.

189. *Principle: Provisions are made at the design stage for the control of accidents, [...] including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents.*

190. The plant operating staff are provided with appropriate safety equipment, instrumentation and operating procedures for response to and control of accidents within the design basis. Design is such that abnormal developments are first met automatically by the restoration of normal conditions by means of the feedback characteristics of neutronic and process controls. These are backed up by the normal capability for shutdown, continued cooling and protection against the release of radioactive materials. Further protection is available through automatic actuation of engineered safety systems. By means of such measures, any onset of abnormal behaviour would be dealt with automatically by appropriately designed systems for at least a predetermined period of time **["decision interval"]**, during which the operating staff could assess systems, review possibilities and decide on a subsequent course of action for conditions not adequately responded to by the automatic functioning of plant systems. The design makes provision for diagnostic aids and symptom based emergency procedures for use in these circumstances. Typical decision intervals for operator action **for future plants are** 30 minutes or longer, depending on the **system or** situation.

190.a The ability of plant systems and operators to control or halt the progression of addressed severe accidents is considered explicitly in the plant design process for future plants. Controls for such sequences need not be automatic, and equipment used for response need not be safety grade.

191. The role of the operator in these circumstances is to ensure that all systems have responded correctly to the abnormal situation, to diagnose the abnormal event in a timely manner, to intervene if required and to restore critical safety functions. Instrumentation and information display systems support these roles, including safety parameter display systems and other sophisticated computer aids to help the operating staff trend and diagnose the evolution of accidents within the design basis.

Startup, shutdown, and low power operation

191.a ***Principle: Components, structures and systems used during startup, low power and shutdown operations are designed to maintain or quickly restore the reactivity control, decay heat removal and the integrity of the fission product barriers, so as to prevent the release of radioactive material resulting from accidents initiated during those operations.***

191.b During low power and shutdown operation, plant conditions can be different to those required for full power operation. During low power operation reactivity coefficients may be different, and the plant may be operating far from the setpoints of certain automatic protective features. During shutdown, fuel handling may take place, the reactor coolant system and containment buildings may be open, and various systems and components may be out of service for maintenance or replacement. It is important for the reactor designer and the operating organization to consider these conditions so that sufficient redundancy, reliability and capability in equipment, including instrumentation, is provided in the design to assure adequate detection of, and

protection against conditions which could lead to exceeding specified limits. This includes considering loss of coolant inventory, decay heat removal and reactivity control.

Spent fuel storage

191.c ***Principle: The plant design includes provisions to adequately protect against the release of radioactive material from spent fuel storage and handling.***

191.d A substantial inventory of fission products is contained in spent fuel. Facilities to store spent fuel ensure reactivity and coolant inventory control, decay heat removal, and provide features to maintain cladding integrity. Events which could cause loss of these functions are considered in the design. Sufficient confinement capability is provided for radioactive material which could be released from the spent fuel. In addition, the amount of spent fuel to be stored over the life of the reactor is considered.

Plant security

191.e ***Principle: The plant layout, building design and equipment arrangement facilitates guarding against unauthorized entry of persons or goods and facilitates the procedures for protection of plant equipment and personnel.***

191.f Protection of the plant from any unauthorized acts can be facilitated by locating redundant safety equipment in different locations, locating vital safety equipment in inner areas and designing buildings for access control and monitoring.

Decommissioning

191.g ***Principle: The design of a nuclear plant and the decommissioning programme take into account the need to limit the exposures during the decommissioning to as low as is reasonably achievable.***

146. Attention is paid at the design stage to radiological protection in the decommissioning phase. **Some of the tasks associated with decommissioning have in practice already been performed (for example steam generator replacement).** After the end of the operating life of the plant, and after the removal of all nuclear fuel, substantial amounts of radioactive material will remain on the site. Consideration is given to the choice of materials which will have low residual radioactivity on the time-scale important for decommissioning, and to the need for convenient access for dismantling. **These features serve to enable decommissioning to be accomplished with as low as reasonably achievable exposures to staff.**

II.4.6. ACCIDENT MANAGEMENT

260. Among the very low probability accidents beyond the design basis are some that could lead to circumstances in which adequate core cooling might not be maintained, or in which substantial fuel degradation may occur or may be imminent. Provisions are made to deal with such circumstances even though they are of low probability. Accident management as a component of accident prevention includes the actions to be taken by operators during the evolution of an accident sequence, **even** before a severe accident actually develops. Such operator actions could alter or reverse the course of an accident. Accident management as a component of accident mitigation includes constructive action by the operating staff in the

event of a severe accident, directed to preventing the further progress of such an accident and alleviating its effects. Accident management includes actions that could be taken to protect the confinement function or otherwise to limit any potential releases of radioactive material to the environment.

261. Previous safety principles dealing with analysis of operating experience, monitoring of plant status and control of accidents within the design basis would also contribute to the accident management capability. In addition, arrangements specific to accident management are made.

262. The goal in managing an accident that exceeds the design basis would be to return the plant to a controlled state in which the nuclear chain reaction is essentially terminated, continued fuel cooling is ensured and radioactive materials are confined. Accident management would include taking full opportunity to use existing plant capabilities, if necessary going beyond the originally intended functions of some systems and using some temporary or ad hoc systems to achieve this goal. Accident management would be responsive to the specific circumstances of the event, even though they might not have been anticipated. Advantage would be taken of whatever time might be available between correct diagnosis of the symptoms and the impending release of fission products to the environment. For the diagnosis of events beyond the design basis and the execution of accident management activities, somewhat longer periods than those for design basis accidents could be available to the operating staff.

263. The ability to benefit from accident management requires the training of operating staff and the provision of information to the control room and a capability for control of events from this location. This greatly increases the likelihood that operators would have sufficient indication of adverse conditions and the knowledge and availability of equipment necessary to take corrective actions.

Strategy for accident management

264. *Principle: The results of an analysis of the response of the plant to potential accidents beyond the design basis are used in preparing guidance on an accident management strategy.*

265. Analysis is made of accidents that have **the** potential for severe core degradation, and **causing the** failure of barriers **which** prevent the release of radioactive material. The symptoms of specific accidents are identified for use in diagnosis. Measures to be taken to reduce significantly the extent of plant damage or the effects of radiation are also identified. These might use normal plant systems in normal or unusual ways or special plant features provided especially for accident management. **It is recognized that accident management may start before accident conditions exceed plant design conditions or before the occurrence of core damage.**

Design features for accident management

268. *Principle: Equipment, instrumentation and diagnostic aids are available to operators, who may at some time be faced with the need to control the course and consequences of accidents beyond the design basis.*

269. The development of abnormal plant behaviour following equipment malfunction or operator error could be rapid in some circumstances; the operating staff would then have to diagnose the cause quickly and plan appropriate corrective action. Equipment is provided especially to assist in this. It comprises instrumentation reading out in the control room, environmentally qualified and capable of providing the information needed to recognize abnormal conditions, to correct faults and to determine the effects of corrective action. Examples of instrumentation provided specifically for accident management are coolant inventory trending systems for pressurized water reactors, monitors for very high containment pressure, hydrogen monitors and monitors of radioactivity in primary coolant.

270. The capability for accident mitigation has always been important in nuclear plant design. The use of confinement structures and containment systems is evidence of this objective. Some of this equipment is useful in more extreme circumstances than envisaged in the original specifications because of the safety margin provided in design. Certain design changes to mitigate the effects of **severe accidents** have been made in recent years, concentrating on restoring and maintaining the core cooling and the confinement functions.

II.4.7. EMERGENCY PREPAREDNESS

271. Emergency planning and preparedness comprise activities necessary to ensure that, in the event of an accident, all actions necessary for the protection of the public and the plant staff could be carried out, and that decision making in the use of these services would be disciplined.

Emergency plans

273. *Principle: Emergency plans are prepared before the startup of the plant, and are exercised periodically to ensure that protection measures can be implemented in the event of an accident which results in, or has the potential for,* ***serious*** *releases of radioactive materials within and beyond the site boundary. Emergency planning zones defined around the plant allow for the use of a graded response.* ***Plants that meet the more restrictive standard of the Complementary Design Objective (e.g., "no significant radiological consequences") may be able to achieve commensurate reduction in emergency planning requirements.***

274. Emergency plans are prepared for measures to be taken on and off the site to protect the public from any serious releases of radioactive materials from the plant. The plans are tested appropriately by exercising their communications and logistics. The emergency plans define organizational arrangements and the division of responsibilities for emergency action, and they are flexible enough to be adapted to particular circumstances as they arise.

275. The emergency plans define the actions that would be taken in the event of a severe accident to re-establish control of the plant to protect staff and public, and to provide the necessary information speedily to the regulatory organization and other authorities. Emergency planning zones defined around the plant provide a basic geographic framework for decision making on implementing protective measures as part of a graded response. These measures include as required early notification, sheltering and evacuation, radioprotective prophylaxis and supply of protective equipment, radiation monitoring, control of ingress and egress, decontamination, medical care, provision of food and water, control of agricultural products, and dissemination of information. **For plants that meet the Complementary**

Design Objective of "no significant radiological consequences" the extent of and degree to which these measures apply may be reduced.

Emergency response facilities

276. *Principle: A permanently equipped emergency centre is available off the site for emergency response.* ***However, for plants that meet the Complementary Design Objective of "no significant off-site radiological consequences", the need for the off-site facility may not be justified.*** *On the site, a similar centre is provided for directing emergency activities within the plant* ***if necessary*** *and communicating with the off- site emergency organization.*

277. The off-site emergency centre is where all emergency action is determined and initiated, apart from on-site measures to bring the plant under control and protect staff. It has a reliable capability to communicate with the similar centre at the plant, with all important units of the emergency response organization, such as police and fire services, and governmental and public information sources. Since commercial telephone services may not be reliable in an emergency, other modes of communication are also available, such as dedicated telephone lines and radio transmission. Information on meteorology at the site and on radiation levels, if any, is provided to the emergency centres. Maps of the local area are available indicating the emergency planning zones and their characteristics. A means is available of permanently recording important information received and sent.

278. The on-site emergency centre is a location at which all on- site measures can be determined and initiated, apart from detailed control of the plant. It is equipped with instrumentation relaying important plant conditions. The centre is the location where data on plant conditions would be compiled for transmission to the off-site **organizations**. Protective equipment is provided for emergency personnel.

REFERENCES

[1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants. Report by the International Nuclear Safety Advisory Group, Safety Series No. 75-INSAG-3, IAEA, Vienna (1988).

[2] The Safety of Nuclear Power: Strategy for the Future (Proc. Conf. Vienna, 1991) IAEA, Vienna (1992).

[3] INTERNATIONAL SAFETY ADVISORY GROUP, The Safety of Nuclear Power, Safety Series No. 75-INSAG-5, IAEA, Vienna (1992).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Fundamentals: The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).

[5] INTERNATIONAL SAFETY ADVISORY GROUP, Probabilistic Safety Assessment, Safety Series No. 75-INSAG-6, IAEA, Vienna (1992).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Plants Design, Safety Series No. 50-C-D (Rev.1), IAEA, Vienna (1988).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, Vienna (1991).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Objectives for the Development of Advanced Nuclear Plants, IAEA-TECDOC-682, Vienna (1993).

CONTRIBUTORS TO DRAFTING AND REVIEW

Allen, P.	Atomic Energy Control Board, Canada
Azeez, S.	Atomic Energy Control Board, Canada
Baranaev, Y.D.	Institute of Physics and Power Engineering, Obninsk, Russian Federation
Besi, A.	Joint Research Centre/CEC, Ispra
Cho, Kun-Woo	Permanent Mission of the Republic of Korea
Cowley, J.S.	Nuclear Installations Inspectorate, United Kingdom
Dennielou, Y.	Electricité de France/Septen, France
De Valkeneer, M.	Tractabel, Belgium
Eendebak, B.T.	N.V. Kema, Netherlands
Ewing, D.J.F.	Health & Safety Executive, United Kingdom
Ferreli, A.	ENEA-Directorate for Nuclear Safety and Health Protection, Italy
Foskolos, K.	Paul Scherrer Institut, Switzerland
Frisch, W.L.	Gesellschaft fuer Reaktorsicherheit mbH, Germany
Gasparini, M.	International Atomic Energy Agency
Goetzmann, C.A.	International Atomic Energy Agency
Kabanov, L.	International Atomic Energy Agency
Kaufer, B.	Organisation for Economic Co-operation and Development/Nuclear Energy Agency
King, T.	United States Nuclear Regulatory Commission, USA
Kleinpeter, M.	Organisation des Producteurs d'Energie Nucléaire, Paris
Kroeger, W.	Paul Scherrer Institut, Switzerland
Kupitz, J.	International Atomic Energy Agency
Lienard, M.	Belgatom SA, Belgium
Madonna, A.	ENEA-Directorate for Nuclear Safety and Health Protection, Italy
Maqbul, N.	Pakistan Atomic Energy Commission, Pakistan
Meyer, P.J.	Siemens AG/KWU, Germany
Pedersen, T.	ABB Atom AB, Sweden
Petrangeli, G.	ENEA-Directorate for Nuclear Safety and Health Protection, Italy
Power, J.C.	Atomic Energy Control Board, Canada
Rabotnov, N.S.	Institute of Physics and Power Engineering, Obninsk, Russian Federation
Royen, J.	Organisation for Economic Co-operation and Development/Nuclear Energy Agency

Soda, K.	Japan Atomic Energy Research Institute, Japan
Spinks, N.J.	Atomic Energy Control Board, Canada
Tripputi, I.	Ente Nazionale per l'Energia Elettrica, Italy
Valtonen, K.	Finnish Centre for Radiation and Nuclear Safety, Finland
Verlaeken, M.	AIB-Vincotte Nuclear, Belgium
Vine, G.L.	Electric Power Research Institute, USA
Yvon, M.	Nuclear Power International, France
Zaffiro, C.	ENEA-Directorate for Nuclear Safety and Health Protection, Italy

Technical Committee Meeting

Vienna, Austria, 11–15 November 1991

Advisory Group Meeting

Vienna, Austria: 29 June – 3 July 1992

Technical Committee Meeting

Vienna, Austria: 19–23 April 1993

Advisory Group Meeting

Vienna, Austria: 4–7 October 1993

Advisory Group Meeting

Vienna, Austria: 25–28 April 1994

Consultants Meetings

Vienna, Austria: 1–5 June 1992, 7–11 December 1992,
25–28 April 1994, 3–7 October 1994, 21–25 November 1994

95-01627

QUESTIONNAIRE ON IAEA-TECDOCs

It would greatly assist the International Atomic Energy Agency in its analysis of the effectiveness of its Technical Document programme if you could kindly answer the following questions and return the form to the address shown below. Your co-operation is greatly appreciated.

Title: **Development of safety principles for the design of future nuclear power plants**
Number: **IAEA-TECDOC-801**

1. How did you obtain this TECDOC?

[ ] From the IAEA:
  [ ] At own request
  [ ] Without request
  [ ] As participant at an IAEA meeting
[ ] From a professional colleague
[ ] From library

2. How do you rate the content of the TECDOC?

[ ] Useful, includes information not found elsewhere
[ ] Useful as a survey of the subject area
[ ] Useful for reference
[ ] Useful because of its international character
[ ] Useful for training or study purposes
[ ] Not very useful. If not, why not?

3. How do you become aware of the TECDOCs available from the IAEA?

[ ] From references in:
  [ ] IAEA publications
  [ ] Other publications
[ ] From IAEA meetings
[ ] From IAEA newsletters
[ ] By other means (please specify)
[ ] If you find it difficult to obtain information on TECDOCs please tick this box

4. Do you make use of IAEA-TECDOCs?

[ ] Frequently
[ ] Occasionally
[ ] Rarely

5. Please state the institute (or country) in which you are working:

Please return to:
R.F. Kelleher
Head, Publishing Section
International Atomic Energy Agency
P.O. Box 100
Wagramerstrasse 5
A-1400 Vienna, Austria