INSAG-12

Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1

INSAG-12

A REPORT BY THE
INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

INSAG

IAEA

BASIC SAFETY PRINCIPLES FOR NUCLEAR POWER PLANTS 75-INSAG-3 Rev. 1

INSAG-12

A report by the International Nuclear Safety Advisory Group

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

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

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

Printed by the IAEA in Austria
October 1999
STI/PUB/1082

INSAG-12

BASIC SAFETY PRINCIPLES FOR NUCLEAR POWER PLANTS 75-INSAG-3 Rev. 1

INSAG-12

A report by the
International Nuclear Safety Advisory Group

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 1999

The International Nuclear Safety Advisory Group (INSAG) is an advisory group to the Director General of the International Atomic Energy Agency, whose main functions are:

(1) To provide a forum for the exchange of information on generic nuclear safety issues of international significance;
(2) To identify important current nuclear safety issues and to draw conclusions on the basis of the results of nuclear safety activities within the IAEA and of other information;
(3) To give advice on nuclear safety issues in which an exchange of information and/or additional efforts may be required;
(4) To formulate, where possible, commonly shared safety concepts.

VIC Library Cataloguing in Publication Data

Basic safety principles for nuclear power plants : 75-INSAG-3 rev. 1 / a report by the International Nuclear Safety Advisory Group. — Vienna : International Atomic Energy Agency, 1999.
p. ; 24 cm. — (INSAG series, ISSN 1025–2169 ; INSAG-12)
STI/PUB/1082
ISBN 92–0–102699–4
Includes bibliographical references.

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

VICL 99–00231

FOREWORD

by Mohamed ElBaradei
Director General

The International Atomic Energy Agency's activities relating to nuclear safety are based upon a number of premises. First and foremost, each Member State bears full responsibility for the safety of its nuclear facilities. States can be advised, but they cannot be relieved of this responsibility. Secondly, much can be gained by exchanging experience; lessons learned can prevent accidents. Finally, the image of nuclear safety is international; a serious accident anywhere affects the public's view of nuclear power everywhere.

With the intention of strengthening the IAEA's contribution to ensuring the safety of nuclear power plants, the Agency established the International Nuclear Safety Advisory Group (INSAG), whose duties include serving as a forum for the exchange of information on nuclear safety issues of international significance and formulating, where possible, commonly shared safety principles.

The present report is a revision of the original 75-INSAG-3 which was issued in 1988 to provide a statement of the objectives and principles of safe design and operation for electricity generating nuclear power plants. This revision was prepared in order to bring the text up to date with improvements in the safety of operating nuclear power plants as well as to identify principles to be applied for future plants. It presents INSAG's understanding of the principles underlying the best current safety policies and practices of the nuclear power industry.

The report is intended for use by governmental authorities and by the nuclear industry and its supporting organizations. Its aim is to promote excellent safety practices at all levels at nuclear power plants through a better understanding of their basis. Although INSAG consulted many experts from various countries in preparing this report, the IAEA did not seek comments on the draft from Member States. The report has not been adopted by the Board of Governors and is not an IAEA safety standard establishing internationally agreed requirements or recommendations.

I am pleased to have received this report and am happy to release it to a wider audience.

CONTENTS

PREAMBLE

PREAMBLE

INSAG here provides a self-standing report on safety principles for electricity generating nuclear power plants[1]. This report has been developed because:

— the means for ensuring the safety of nuclear power plants have improved over the years, and it is believed that commonly shared principles for ensuring a very high level of safety can now be stated for all nuclear power plants; and
— the international consequences of the Chernobyl accident in 1986 have underlined the need for common safety principles for all countries and all types of nuclear power plants.

INSAG has prepared this report in accordance with its terms of reference "to formulate, where possible, commonly shared safety concepts". The understanding and application of these safety principles should improve safety and benefit everyone, especially those in countries that use or intend to use nuclear power as an energy source.

Safety is never absolute in any endeavour. All of life is hazardous in some way. These safety principles do not guarantee that nuclear power plants will be absolutely free of risk, but, when the principles are adequately applied, the plants should be very safe and still effective in meeting society's needs for abundant useful energy.

Notwithstanding the few major accidents that have occurred, nuclear power has a safety record that is good compared with those of the viable competing options for producing electricity. Even so, there is great public concern about the safety of nuclear power. The essential contribution of nuclear power to the world's supply of energy over the coming years requires that this public apprehension be faced directly. The nuclear industry rightly addresses this special concern by seeking to reduce even further the probability and potential consequences of nuclear power plant accidents in the future.

The technology of nuclear power is unfamiliar to most people and is more complex than that of other currently viable means of generating electricity. Although it is a factor in public apprehension, this complexity of nuclear plants is partly due to extensive safety measures that are not taken in more familiar energy technologies.

INSAG considers it possible to make use of the fact that nuclear power is a high technology industry to attain the even higher level of safety that is the object of these safety principles. High technology does not jeopardize safety, as is often believed to

[1] Although this report concerns the safety of nuclear plants used to generate electricity, most of the points made are also valid for nuclear power plants used for other purposes.

be the case; it is the means by which safety is achieved. The objectives and principles set out in this report are directed towards the universal and effective achievement of this purpose in the future. To the extent that they can be implemented for existing plants, application of the principles will also improve safety where such improvement may be advisable.

A disciplined approach is needed when deciding whether to adopt proposed incremental safety improvements for any nuclear plant. The proposer justifies each significant improvement in terms of its urgency, safety merit and implementation cost. It is important to avoid concentrating resources on improvements that have only marginal effects, and to recognize that a safety improvement may also affect economic or other societal factors. Special care is needed to ensure that an intended safety improvement does not have detrimental effects that outweigh its benefits.

There is a close connection between the safety and the reliable operation of a nuclear power plant. Equipment failures or human errors that could cause accidents and consequent harm to the public are similar to shortcomings that lead to low capacity factors or necessitate expensive repairs. Conversely, the measures that contribute to plant safety will frequently help in achieving a good record of operation. It is expected that the principles expounded in this report will not only contribute to achieving the necessary high degree of safety, but also contribute to more efficient and more economical generation of electricity.

In the past there have been several instances of core damage to nuclear power plants. The causes were particular to specific features of design and especially to the operation of these plants. As a result of measures taken subsequently, the likelihood of an accident causing severe core damage has been reduced and plant safety thereby improved. This judgement is based upon the results of many safety assessments, which have confirmed the benefit of the changes made following these accidents.

The objective of achieving safety must permeate each activity performed in generating electricity at a nuclear power plant. There must be pervasive safety thinking on the part of those concerned in each phase, from siting and design to construction, commissioning, operation, maintenance, upgrades or modifications, training, decommissioning, and all related activities. This pervasive safety thinking is a key element in the ‘safety culture’ that is emphasized strongly in this report.

This revision of 75-INSAG-3 was prepared in order to take account of the recent development of and refinements in nuclear safety principles for nuclear power plants. When 75-INSAG-3 was issued in 1988, the total amount of experience that had been accumulated worldwide was about 4600 operating reactor-years. Today, the figure is about 8700 operating reactor-years. This greater experience in both the design and operation of nuclear plants, coupled with knowledge deriving from extensive research and development programmes, has led to significant gains in the safety and performance of most operating plants and in the safety of future plants now under construction. During this same period, significant structural changes have

occurred in national nuclear operating organizations to improve their effectiveness. These changes have placed greater emphasis upon the quality of management and its leadership and upon the need to manage change efficiently while ensuring that responsibilities and accountabilities are clear.

While the basic approach taken in 75-INSAG-3 has not changed, improvements have been made in this revision, resulting primarily from:

— A more comprehensive treatment of safety culture and defence in depth, two important fundamental principles that are discussed in 75-INSAG-3 and enlarged upon in the subsequent 75-INSAG-4 and INSAG-10 reports (see the list of INSAG publications at the end of this report).
— Increased application of nuclear plant operating experience, findings of safety analyses, and results of research and development.
— Use of self-assessment, including peer reviews or coupled with independent peer reviews, at all levels of the operating organization.
— Use of probabilistic safety assessment (PSA), as discussed in 75-INSAG-6, to evaluate design changes, to make operational decisions with regard to maintenance planning and scheduling and to develop risk informed nuclear safety regulations. PSA increasingly includes analyses of shutdown, startup and risks of operation at low power.
— Implementation of additional severe accident management to enhance accident prevention and to identify actions to be taken in the very unlikely event of an accident progressing beyond core damage to cause reactor pressure vessel damage or even containment damage.
— Incorporation of additional principles deemed important enough to include in this revision of 75-INSAG-3 concerning: classification of systems, structures, and components, storage of new and spent fuel, plant physical protection, and decommissioning.

INSAG, in this revision, recognizes the benefits of excellence in operational and human performance by promoting throughout the entire operating organization behaviour that supports the safety and reliability of nuclear power plants. The emphasis is placed upon reinforcing the right behaviour in all aspects of management, operation, maintenance and design modification rather than exclusively upon the results and outcomes of the work.

Another element given increased recognition is the fact that plants are ageing and that ageing can lead to the degradation of plant structures, systems and components as well as to time (e.g. cycle) dependent analyses no longer being applicable. The effects of ageing must be managed adequately so as to preserve plant safety. However, the availability of sufficient competent and experienced personnel must be ensured throughout the lifetime of nuclear installations.

Some nuclear power plants do not yet satisfy the safety principles of 75-INSAG-3. INSAG has devoted a specific report to develop a 'common basis for judging the safety of nuclear power plants built to earlier standards' (INSAG-8). That report proposes a process for assessing the safety of such plants and for establishing a safety improvement programme, when needed, recognizing that, if critical deficiencies are found and cannot be eliminated or compensated for, the plant would be shut down. For those plants allowed to continue operation, some elements of the operational excellence programme proposed in this revision could lead to improved performance. In particular, improvements in safety culture, human performance, self-assessment, peer reviews and risk based assessments could yield immediate safety benefits for reasonable additional costs.

Even though nuclear power technology is quite mature for some reactor systems, it is necessary to encourage the evolution and development of concepts that might be important in meeting long term global energy needs. Several future reactors (which could be built in significant numbers over the next 20 years) are being considered or are under development, and this has led to the identification of a number of additional desirable features and objectives that are set out in this revision of 75-INSAG-3. They include a simplification of design, operations and maintenance, and the increased use of information technology and digital technology. However, additional measures to prevent accidents and a further reduction in the probability and consequences of an off-site radioactive release remain the highest priorities among the future safety provisions.

INSAG hopes that this revised version of 75-INSAG-3 will be used as extensively throughout the world as the original edition and that it will continue to serve as a basic reference for the safety of nuclear power plants and for achieving a broad international consensus on basic safety principles for present reactors and future reactor concepts.

1. INTRODUCTION

1. Nuclear power plant safety requires a continuing quest for excellence. All individuals concerned need constantly to be alert to opportunities to reduce risks to the lowest practicable level. The quest, however, is most likely to be fruitful if it is based on an understanding of the underlying objectives and principles of nuclear safety, and the way in which its aspects are interrelated. This report is an attempt to provide a logical framework for such an understanding. The proposed objectives and principles of nuclear safety are interconnected and must be taken as a whole; they do not constitute a menu from which selection may be made.

2. The report takes account of current issues and developments. It includes the concept of safety objectives and the use of probabilistic safety assessment (PSA). Reliability targets for safety systems are discussed. The concept of a 'safety culture' is crucial. Attention has been paid to the need for planning for accident management.

3. In general, the concepts presented in this revision are not new. Rather, the best current philosophy is put forward. Most of the ideas have been applied in different combinations in many nuclear power programmes throughout the world. They are now consolidated and presented in a structured form with explanatory material.

4. The report contains objectives and principles. The objectives state what is to be achieved; the principles state how to achieve it. In each case, the basic principle is stated as briefly as possible. The accompanying discussion comments on the reasons for the principle and its importance, as well as exceptions, the extent of coverage and any necessary clarification. The discussion is as important as the principle it augments.

5. The principles do not differentiate between new and existing plants. However, there will be necessary differences in implementation. The global complement of reactors at any time will include plants of different origins, ages and designs. It must be for designers, manufacturers, constructors, regulators and operating organizations to decide how to apply the principles set out in this report to each individual case.

6. These principles do not constitute a set of regulatory requirements. INSAG believes, nevertheless, that future national and international practices will come to reflect the objectives and principles presented in this report.

7. However, some future types of nuclear power plants may achieve the intent of some of the principles presented in this report by special inherent features making the principles as presently formulated not entirely applicable. For such cases, it would be necessary to scrutinize closely the extent of the basis in proven technology.

1.1. STRUCTURE OF THE REPORT[2]

8. This report is structured around three overriding safety objectives, a set of six fundamental safety principles (three related to safety management, three related to defence in depth), and nine technical principles, which provide a general framework for a number of specific safety principles. Figure 1 illustrates this structured presentation of safety objectives and principles.

9. The safety objectives and principles indicated in Fig. 1 are set out in the remainder of this report. The safety objectives are stated and explained in Section 2. They are followed by the fundamental safety principles in Section 3. The specific safety principles are listed and discussed in Section 4.

10. The topics of the ultimate disposal of nuclear waste and the physical protection of nuclear materials are not included among the principles because, although they are important safety issues, they are on the periphery of the subject area of this report.

11. *Note finally and importantly* **that throughout the original 75-INSAG-3 report the principles and their accompanying discussion are stated not in the form of requirements, but on the assumption that the practices are in current use.** *The sense of the usage is that the principles and their discussion describe the situation that exists in well managed circumstances of the kind this report seeks to promote. That structure is modified in some parts of this report which state how the principles can or could be applied in future improvements.*

---

[2] A special effort was made to preserve the original structure and text in this revised version. The material in 75-INSAG-3 is reproduced in this version with minor clarifications or changes. The information updates are provided mostly in self-contained paragraphs. This approach has the advantage of not affecting the original format and contents of 75-INSAG-3. Furthermore, the Agency will make the original 75-INSAG-3 available upon request.

Objectives	General nuclear safety objective	Radiation protection objective	Technical safety objective				
Fundamental safety management principles	Safety culture	Responsibility of operating organization	Regulatory control and verification				
Fundamental defence in depth principles	Defence in depth	Accident prevention	Accident mitigation				
General technical principles	Proven engineering practices (3.3.1)	Quality assurance (3.3.2) Self-assessment (3.3.3) Peer reviews (3.3.4)	Human factors (3.3.5)	Safety assessment and verification (3.3.6)	Radiation protection (3.3.7)	Operating experience and safety research (3.3.8)	Operational excellence (3.3.9)
Specific principles	Siting	Design	Manufacturing and construction	Commissioning	Operation	Accident management	Decommis-sioning	Emergency preparedness

FIG. 1. INSAG safety objectives and principles for nuclear plants. The numbers refer to the relevant subsections in Section 3.3.

2. 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.

2.1. GENERAL NUCLEAR SAFETY OBJECTIVE

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 hazard 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, the risk associated with an accident or an event is defined as the arithmetic product of the probability of that accident or event and the adverse effect it would produce. The overall risk would then be obtained by considering the entire set of potential events and summing the products of their respective probabilities and consequences. In practice, owing to the large uncertainties that can be associated with the different probabilities and consequences, it is generally more convenient and useful to disaggregate the probabilities and the consequences of potential events, as discussed in INSAG-9. 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, 'safety goals', be formulated.

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. However, the main focus of this report is the safety of people. What follows is therefore expressed in these terms solely, but this is not to imply that INSAG has no regard for other factors.

2.2. RADIATION PROTECTION OBJECTIVE

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 as low as reasonably achievable, economic and social factors being taken into account, and below prescribed limits, and to ensure mitigation of the extent of radiation exposure 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[3] based on recommendations by the International Commission on Radiological Protection (ICRP) ensures appropriate radiation protection.

18. The aforementioned radiation protection standards have been developed to prevent harmful effects of ionizing radiation by keeping doses sufficiently low that deterministic effects are precluded and the probability of stochastic effects is limited to levels deemed tolerable. This applies to controlled circumstances. In the event of any accident that could cause the source of exposure to be not entirely under control,

[3] For example, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANISATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).

safety provisions in the plant are planned and countermeasures outside the plant are prepared to mitigate harm to individuals, populations and the environment.

2.3. TECHNICAL SAFETY OBJECTIVE

19. *Objective: To prevent with high confidence accidents in nuclear plants; to ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor; and to ensure that the likelihood of severe accidents with serious radiological consequences is extremely small.*

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 (see Sections 3.2.1 and 3.2.2, and subsequent sections).

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 during design and, when necessary, to mitigate its 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 existing plants, design basis accidents are generally associated with single initiating events; they are evaluated with conservative assumptions including aggravating failures and do not usually imply severe core damage.

22. Attention is also directed to accidents of very low likelihood which might be caused by multiple failures or which might lead to conditions more severe in existing plants than those considered explicitly in the design (accidents ‘beyond the design basis’). Some of these severe accidents could cause such deterioration in plant conditions that proper core cooling cannot be maintained, or that fuel damage occurs for other reasons. These accidents would have a potential for major radiological consequences if radioactive materials released from the fuel were not adequately confined. As a result of the accident prevention policy, they are of low probability of occurrence.

23. Since these accidents could nonetheless occur, other procedural measures (accident management) are provided for managing their course and mitigating their consequences. These additional measures are defined on the basis of operating experience, safety analysis and the results of safety research. Attention is given in design, siting, procedures and training to controlling the progression and consequences of accidents. Limitation of accident consequences requires measures to ensure safe shutdown, continued core cooling, adequate confinement integrity and off-site emergency preparedness. High consequence severe accidents are therefore extremely unlikely because they are effectively prevented or mitigated by defence in depth.

24. Notwithstanding the high level of safety so achieved, increased understanding of severe accidents beyond design basis events has led to complementary design features being implemented in some operating nuclear power plants as well as expanded guidelines and/or procedures to cope with severe accidents of very low likelihood beyond design basis.

25. For future nuclear power plants, consideration of multiple failures and severe accidents will be achieved in a more systematic and complete way from the design stage. This will include improving accident prevention (for example, reduced common mode failures, reduced complexity, increased inspectability and maintainability, extended use of passive features, optimized human–machine interface, extended use of information technology) and further reducing the possibilities and consequences of off-site radioactive releases.

26. In the safety technology of nuclear power, overall risk is obtained (as discussed in Section 2.1) by considering the entire set of potential events and their respective probabilities and consequences. 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.

27. The target for existing nuclear power plants consistent with the technical safety objective is a frequency of occurrence of severe core damage that is below about 10^{-4} events per plant operating year. Severe accident management and mitigation measures could reduce by a factor of at least ten the probability of large off-site releases requiring short term off-site response. Application of all safety principles and the objectives of para. 25 to future plants could lead to the achievement of an improved goal of not more than 10^{-5} severe core damage events per plant operating year. Another objective for these future plants is the practical elimination of accident sequences that could

lead to large early radioactive releases, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analyses so that their consequences would necessitate only protective measures limited in area and in time.

3. FUNDAMENTAL PRINCIPLES

28. A number of concepts are general in application, bearing in many important ways on the nature and application of the specific safety principles enunciated later. These important concepts are here called fundamental safety principles and they are identified in Section 3. They are of three kinds, relating to management, defence in depth and technical issues.

3.1. MANAGEMENT RESPONSIBILITIES

29. Three fundamental management principles are identified. They are connected with the establishment of a safety culture, the responsibilities of the operating organization, and the provision of regulatory control and verification of safety related activities.

3.1.1. Safety culture

30. *Principle: An established safety culture governs the actions and interactions of all individuals and organizations engaged in activities related to nuclear power.*

31. The phrase 'safety culture' refers to a very general matter, the personal dedication and accountability of all individuals engaged in any activity which has a bearing on the safety of nuclear power plants. The starting point for the necessary full attention to safety matters is with the senior management of all organizations concerned. Policies are established and implemented which ensure correct practices, with the recognition that their importance lies not just in the practices themselves but also in the environment of safety consciousness which they create. Clear lines of responsibility, communication, and authority backed up with adequate resources are established; sound procedures are developed; strict adherence to these procedures is demanded; internal reviews are performed of safety related activities; above all, staff training and education emphasize the reasons behind the safety practices established, together with the consequences for safety of shortfalls in personal performance. The

arrangements for the management of safety are documented as described in INSAG-13, 'Management of Operational Safety in Nuclear Power Plants'.

32. These matters are especially important for operating organizations and the staff directly engaged in plant operation. For the latter, at all levels, training emphasizes the significance of their individual tasks from the standpoint of basic understanding and knowledge of the plant and the equipment at their command, with special emphasis on the reasons underlying safety limits and the safety consequences of violations. Open attitudes are required in such staff to ensure that information relevant to plant safety is freely communicated; when errors of practice are committed, their admission is particularly encouraged. By these means, an all pervading safety thinking is achieved, allowing an inherently questioning attitude, the learning from experience, the prevention of complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters.

33. The concept of safety culture is refined in 75-INSAG-4, which proposes requirements on three levels:

Requirements at policy level

In any important activity, the manner in which people act is conditioned by requirements set at a high level. The highest level affecting nuclear plant safety is the legislative level, at which the national basis for safety culture is set. Similarly, an organization pursuing activities with a bearing on nuclear plant safety makes its responsibilities well known and understood in a safety policy statement. This statement is provided as a requirement to managers and staff, and to declare the organization's objectives and the public commitment of corporate management to nuclear plant safety.

Requirements on managers

The attitudes of individuals are greatly influenced by their working environment. The key to an effective safety culture in individuals is found in the practices moulding the environment and fostering attitudes conducive to safety. It is the responsibility of managers to institute such practices in accordance with their organization's safety policy and objectives.

Response of individuals

The response of all those who strive for excellence in matters affecting nuclear safety is characterized by a *questioning attitude*, plus a *rigorous and prudent*

approach, plus *communication*. The desired results are achieved only if the attitudes of individuals at all levels are responsive to the safety culture framework established by management.

34. A good nuclear safety culture has the following characteristics:

— When any possible conflict in priority arises, safety and quality take precedence over schedule and cost.
— Errors and near misses when committed are seen not only as a matter of concern but also as a source of experience from which benefit can be derived. Individuals are encouraged to identify, report and correct imperfections in their own work in order to help others as well as themselves to avert future problems.
— Plant changes or activities are conducted in accordance with procedures. If any doubt arises about the procedures, the evolution is terminated by returning the plant to a safe and stable condition. The procedures are evaluated and changed if necessary before proceeding further.
— When problems are identified, the emphasis is placed upon understanding the root cause of the problems and finding the best solutions without being diverted by who identified or contributed to the problem; the objective is to find 'what is right' and not 'who is right'.
— The goal of supervisory and management personnel is that every task be done right the first time. They are expected to accept and insist upon full accountability for the success of each work activity and to be involved in the work to the extent necessary to achieve success.
— Practices and policies convey an attitude of trust and an approach that supports teamwork at all levels and reinforces positive attitudes towards safety.
— Feedback is solicited from station personnel and contractors to help identify concerns, impediments and opportunities to improve. Management reinforces an attitude of individual behaviour that leads staff to identify problems promptly and fully.
— The organization has a commitment to continuous safety improvement and to manage change effectively.
— Senior managers prevent isolationism and encourage the establishment of a learning organization.
— Every individual, every supervisor and every manager demonstrates personal integrity at every opportunity that arises during the lifetime of the nuclear power plant.
— Every plant change, every meeting and every safety assessment is taken as an opportunity to teach, learn and reinforce the preceding characteristics and principles.

These characteristics and principles are not compromised or relaxed.

3.1.2. Responsibility of the operating organization

35. *Principle: The ultimate responsibility for the safety of a nuclear power plant rests with the operating organization. This is in no way diluted by the separate activities and responsibilities of designers, suppliers, contractors, constructors and regulators.*

36. Once the operating organization accepts possession, it is in complete charge of the plant, with full responsibility and commensurate authority for approved activities in the production of electric power. Since these activities also affect the safety of the plant, the operating organization establishes policy for adherence to safety requirements, establishes procedures for safe control of the plant under all conditions, including maintenance and surveillance, and retains a competent, fit and fully trained staff. The operating organization ensures that responsibilities are well defined and documented and that the resources and facilities for the tasks of its staff are in place.

37. The operating organization also has responsibilities in certain areas where its control is less direct, such as with contractors. By using its own staff and resources, or through agencies acting on its behalf, the operating organization institutes rigorous reviews, audits and, as necessary, approval processes to ensure that the factors which determine the safety of the plant are given the necessary attention. This applies, for example, to site investigation, design, manufacturing, construction, testing and commissioning.

38. This principle of the operating organization's overriding safety responsibility is a prime one. The responsibilities of other parties are also significant for safety as well as for financial and legal matters. Variations in national practices make it difficult to define the formal responsibilities of the other parties, but clearly designers, manufacturers and constructors are required as a minimum to provide a sound design and equipment that meets its specifications in terms of both engineering detail and performance of the intended function, meeting or exceeding quality standards commensurate with the safety significance of components or systems. The technical societies and the scientific community generally carry responsibilities for high standards of performance of individuals in the professional sense, and for maintaining and strengthening the basis on which the safety of nuclear power plants stands. The responsibilities of the regulators are discussed in Section 3.1.3.

3.1.3 Regulatory control and independent verification

39. *Principle: The government establishes the legal framework for a nuclear industry and an independent regulatory organization which is responsible for licensing and regulatory control of nuclear power plants and for enforcing the relevant regulations. The separation between the responsibilities of the regulatory organization and those of other parties is clear, so that the regulators retain their independence as a safety authority and are protected from undue pressure.*

40. A legally constituted regulatory organization provides governmental licensing, regulation and surveillance of the operation of nuclear power plants in respect of their safety. Activities of the regulatory organizations cover the following functional areas:

— specification and development of standards and regulations for safety;
— issue of licences to operating organizations, following appropriate assessments of nuclear safety, the financial viability of the applicant and its organizational and managerial capabilities;
— inspection, monitoring and review of the safety performance of nuclear plants and operating organizations;
— requiring corrective actions of an operating organization where necessary and taking any necessary enforcement actions, including withdrawal of licence, if acceptable safety levels are not achieved;
— advocacy of safety research, as discussed in Section 3.3.8; and
— dissemination of safety information (also discussed in Section 3.3.8).

41. The regulatory organization acts independently of designers, constructors and operators to the extent necessary to ensure that safety is the only mission of the regulatory personnel. The resources of the regulatory organization are sufficient for it to accomplish its functions without adversely affecting construction schedules or energy production, except where warranted for the assurance of safety. Expertise in a sufficiently wide range of nuclear technologies is available to the regulatory organization.

42. The regulatory organization does not attempt to take the primary responsibility for safe operation away from the operating organization, recognizing that such action has the potential to reduce safety levels.

43. To fulfil its functions effectively, the regulatory organization has the necessary legal authority, and it is provided with free access to facilities and to relevant information in the possession of the operating organization.

3.2. STRATEGY OF DEFENCE IN DEPTH

44. ‘Defence in depth’ 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 were to 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 specific safety principles that follow.

45. 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.

3.2.1. Defence in depth

46. *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.*

47. 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 equipment failure would lead to harm to the public, and even combinations of failures that are only remotely possible would lead to little or no harm. 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.

48. The principle of defence in depth is implemented primarily by means of a series of barriers which would 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 multibarrier system is not jeopardized and is capable of functioning as designed.

49. The strategy for defence in depth is twofold: first, to prevent accidents and second, if prevention fails, to limit the potential consequences of accidents and to prevent their evolution to more serious conditions. Defence in depth is generally structured in five levels. The objectives of each level of protection and the essential means of achieving them in existing plants are shown in Table I, which is reproduced from INSAG-10. If one level were to fail, the subsequent level comes into play, and so on. Special attention is paid to hazards that could potentially impair several levels of defence, such as fire, flooding or earthquakes. Precautions are taken to prevent such hazards wherever possible and the plant and its safety systems are designed to cope with them.

50. 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

TABLE I. LEVELS OF DEFENCE IN DEPTH IN EXISTING PLANTS

Levels	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

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.

51. All the levels 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 levels of defence in depth is never justification for continued operation in the absence of one level. 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.

52. 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.

53. 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.

54. The multibarrier system protects humans and the environment in a wide range of abnormal conditions. Preplanned countermeasures are provided, as a further component of defence in depth, against the possibility that radioactive material might still be released from the plant.

55. The Appendix presents a discussion of the means by which the separate components of defence in depth protect and complement each other. The importance of prevention and mitigation of accidents in defence in depth is treated in the following two corollaries.

3.2.2. Accident prevention

56. *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.*

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

58. The first 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 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 second means of preventing accidents is to foster a questioning attitude from the staff and to promote discussion of what could go wrong prior to initiating activities. 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.

59. Thus the prevention of accidents 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.

60. A number of PSAs have been made for a range of nuclear power plant designs in different countries. They show that sufficiently low probabilities of severe core damage are attainable in some designs. When effective preparation for accident management and for mitigation of the effects of severe accidents is taken into account, the results of these PSAs are consistent with the general nuclear safety objective stated in Section 2.1.

61. PSA also guides design and operation by identifying potential accident sequences that contribute to risk. Measures can then be taken to reduce this contribution.

62. The scope of PSA has been expanded into several new areas to prevent and reduce the occurrence of accidents:

— As a number of significant events occurred at shutdown or at low power[4], they were analysed by PSA which showed, as reported in INSAG-10, that in some cases the associated risk (contribution to frequency of core damage) is comparable with that associated with full power operation. PSA is now increasingly used to minimize risks associated with shutdown and low power by maintaining adequate defence in depth and the proper system availability to support the key safety functions of control of reactivity, shutdown cooling, maintenance of coolant inventory, maintenance of electrical power, spent fuel cooling, containment and maintenance of critical support systems.
— PSA is being employed to analyse the various plant systems, structures and components that are important for safety and to assess remedial actions when their performance is not satisfactory. PSA is used to evaluate diversity in systems and to prioritize resources to ensure that the most important components receive their proportionate share of available resources.
— PSA is beginning to be employed to develop risk informed safety programme strategies (e.g. in-service inspection).

In all such novel applications, PSA is used as another important technique to complement engineering judgement, experience, defence in depth concepts and design basis considerations. Also, as the uses of PSA increase, it is important that the models, the database and the calculations of PSA be kept accurate over the lifetime of the plants.

[4] Some characteristics of nuclear power plants — especially during shutdown — are unique, such as: there are configuration changes (i.e. equipment is removed for maintenance); additional personnel are at work and more activities are performed; conditions and configurations are less familiar to operators; events generally involve actions in the plant rather than in the control room; fire risk is generally increased (i.e. poor housekeeping, short circuits, overheating); operational limits and conditions, plant procedures, training programmes and/or regulatory requirements are not as well detailed; there is an increased potential for degradation of safety culture.

3.2.3. Accident mitigation

63. *Principle: In-plant and off-site mitigation measures are available and are prepared for that would substantially reduce the effects of an accidental release of radioactive material.*

64. Provisions for accident mitigation extend the defence in depth concept beyond accident prevention. The accident mitigation provisions are of three kinds, namely, accident management, engineered safety features and off-site countermeasures.

65. 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 ensured, radioactive material confined and the confinement function protected. In such circumstances, engineered safety features would act to confine any radioactive material released from the core so that discharges to the environment would be minimal. These engineered safety features include physical barriers, some of which have the single purpose of confining radioactive material. 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 humans by food-chains and other pathways.

66. Accident management in operating plants is being extended into the realm of increasingly severe accidents. This requires additional guidelines or procedures, further understanding of the prevailing phenomena, appropriate assignment of responsibilities, and training for managing accidents of increased severity. Designers and owners of future plants are seeking even more improvements in reducing off-site radiological releases, as discussed in paras 25 and 27.

3.3. GENERAL TECHNICAL PRINCIPLES

67. There are several underlying technical principles which are essential to the successful application of safety technology for nuclear power plants.

3.3.1. Proven engineering practices

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

69. 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 and subjected to necessary testing.

70. Numerous codes and standards have been adopted for application in nuclear power plants, after formulation by the professional engineering community and approval by the appropriate agencies. Some existing codes and standards have been modified from their 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]

71. 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 lifetime. When repairs and modifications are made, an analysis is conducted and a 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, a new analysis is conducted.

72. The construction techniques used for nuclear plants are applied in recognition of the critical safety issues in the plant design and accommodate them prior to

[5] The IAEA's Nuclear Safety Standards (NUSS) series of documents was developed in accordance with this principle.

commencement of physical construction. The construction aspects and techniques are also taken into consideration in the plant design in order to eliminate the need for changes in the design during construction. These considerations are an integral part of the approval process by operating organizations and regulatory authorities.

73. 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.

74. Standardization can offer economic advantages in 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. The advantages include more standardized siting requirements and engineering documentation for a set of plants. Also, standardization, if properly implemented, can promote more efficient operation, and thus safety, by direct sharing of operating experience and common training; and it can lead to more effective construction and quality assurance programmes. However, there is also a risk that standardization may lead to generic problems. This risk is reduced by adopting the concept of evolutionary improvements in the design of standardized plants.

3.3.2. Quality assurance

75. *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.*

76. 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 with 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.

77. 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 lifetime

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.

78. 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 that classification (see paras 161 and 182–185).

79. Quality assurance practices are a component of good management and are essential to the achievement and demonstration of high quality in products and operation. Organizational arrangements for sound quality assurance practices are requisite for all parties concerned, to provide a clear definition of the responsibilities and authorities of component groups and channels of communication and co-ordination between them. These arrangements are founded on the principle that the responsibility for achieving quality in a task rests with those performing it, others verify that the task has been properly performed, and yet others audit the entire process. The authority of the quality assurance staff is established firmly enough within the organization to allow them to identify problems of inadequate quality and to solve them. The selection and training of staff for quality assurance duties, adapted appropriately to national cultural and technical norms, receives special attention.

80. 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.

81. Quality assurance practices thus cover: validation of designs; procurement; 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.

82. An essential component of quality assurance is the documentary verification that tasks have been performed as required, that deviations have been identified and corrected, and that 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.

3.3.3. Self-assessment

83. *Principle: Self-assessment for all important activities at a nuclear plant ensures the involvement of personnel performing line functions in detecting problems concerning safety and performance and solving them.*

84. Self-assessment is a structured, objective and visible process whereby individuals, groups and management within an operating organization evaluate the effectiveness of their own operational safety measures against pre-established expectations and identify areas needing improvement. Those individuals involved in the activities being reviewed can improve the objectivity of the self-assessment through the participation of persons independent of the activities. The results are used to complement quality assurance audits and safety reviews conducted by independent personnel (i.e. those who are not directly involved in the tasks being performed). Self-assessments are used for single reviews in depth to find the basic causes of poor safety and performance; for periodic reviews of specific activities or programmes by teams of experienced in-house personnel and outside technical experts; for comparison of plant performance with existing management expectations and with best industry practices; and for frequent or continuous monitoring of activities at all levels of the entire organization. Strong support from management is essential to obtaining good results and to encouraging individuals at all levels of the organization to employ self-evaluation to improve performance rather than just solve problems.

85. Self-assessment reports are clear and deal with the problems found, their root causes and their generic implications. Corrective actions are tracked to completion and their effectiveness is verified in subsequent self-assessments. The involvement of individuals engaged in or responsible for the activity being reviewed is valuable in that it brings their knowledge and insights to the review process. Those individuals also gain understanding and valuable perspectives that can help them to assess and improve their own performance in their areas of responsibility.

3.3.4. Peer reviews

86. *Principle: Independent peer reviews provide access to practices and programmes employed at plants performing well and permit their adoption at other plants.*

87. ‘Peer reviews’ are conducted by a team of independent experts with technical competence and experience in the areas of evaluation. Judgements are based on the combined expertise of the team members. The composition of the team is tailored to the organization to be reviewed. Depending on specific needs, the review process can address general topics or concentrate on specific areas of special interest. The scope of this process is not limited to examination of documents or to interviews; it emphasizes plant performance. These reviews are neither inspections nor audits against specified standards. Instead, they comprise a comprehensive comparison of the practices applied by organizations with existing and internationally accepted good practices, and an exchange of expert judgements. They are aimed at increasing the effectiveness of practices and procedures of the organization being reviewed.

88. Peer reviews are themselves a ‘good practice’, complementing other types of assessment. Peer reviews are carried out at the national, bilateral and/or multilateral or international level, and they cover operating organizations as well as regulatory authorities. International organizations typically performing operational peer reviews are the World Association of Nuclear Operators (WANO) and the IAEA through its Operational Safety Review Teams.

3.3.5. Human factors

89. *Principle: Personnel engaged in activities bearing on nuclear plant safety are trained and qualified to perform their duties. The possibility of human error in nuclear power plant operation is taken into account by facilitating correct decisions by operators and inhibiting wrong decisions, and by providing means for detecting and correcting or compensating for error.*

90. One of the most important lessons of abnormal events, ranging from minor incidents to serious accidents, is that they have so often been the result of incorrect human actions. Frequently such events have occurred when plant personnel did not recognize the safety significance of their actions, when they violated procedures, when they were unaware of conditions in the plant, were misled by incomplete data or an incorrect mindset, or did not fully understand the plant in their charge. The operating organization must recognize the high technology aspect of nuclear power plants and must ensure that its staff is able to manage it satisfactorily.

91. The human error component of events and accidents has been too great in the past. The remedy is a twofold approach, through design, including automation, and through improved human performance, including the need to identify expected behaviours, to conduct pre-task reviews, to identify error-likely conditions and to

discuss outcomes and responses. In unusual circumstances, optimal use of human ingenuity is required.

92. Engineered features and administrative controls protect against violations of safety provisions. Moreover, attention to human factors at the design stage ensures that plants are tolerant 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. 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 generally 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 properly cleared with the control room staff. The layout and identification of remotely located controls is such as to reduce the chance of error in their selection.

93. 'Human factor improvements' are being made in plant hardware (e.g. in ergonomic layout), plant procedures, training and other areas to help prevent or mitigate human error. The objective is to simplify the information reaching the operating personnel and to enable control room personnel to have a clear understanding and control of the status of the plant. In operating plants, task analysis is employed as a technique to review operator and maintenance activities and to determine whether they can be improved by changing the work, the instructions or the procedures. Also, the input of experienced plant operators is sought to simplify the information flow, the control room functions and the process of operation. When replacement control and instrumentation equipment can no longer be purchased, it is replaced when possible by programmable controllers or 'minicomputer' systems which augment plant diagnostics. If the software of such controllers and minicomputers is important to safety, the computer software will be designed, implemented and tested according to structured software engineering principles and will include appropriate verification and validation. Additional quality assurance measures are necessary when it is changed by maintenance, including a clear definition of access rights and the assurance of adequate knowledge on the part of maintenance staff. For future nuclear power plants, the opportunities for human factor improvements will be much greater in that the layout and structure of the plants are not yet fixed. Also, digital computer systems are being introduced for safety functions and to substitute self-testing for

operator testing. Such computer systems need to be designed and installed to ensure that residual faults and design errors do not prevent any required safety action.

94. To keep the plant within the boundaries of a domain of safe operation, approved procedures for operation are followed. To ensure this, staff training and retraining receive strong emphasis, with classroom, simulator and plant based studies. Operation, maintenance and inspection aids are developed that take account of the strengths and weaknesses of human performance.

95. The foregoing discussion emphasizes the human factor in operation. This is especially important, but attention to this aspect must not lead to neglect of the human factor in maintenance and inspection. Errors in these activities have been important causes of component and system failures in the past. For this reason the procedures ensuring excellence in the performance of operating staff are also followed for maintenance staff.

3.3.6. Safety assessment and verification

96. *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.*

97. 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 provides the technical rationale for selection of, and describes the limiting set of design basis accidents and presents the results.

98. 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.

99. Methods have been developed to assess whether safety objectives are met. These methods are applied at the design stage, later in the lifetime 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.

100. In the deterministic method, design basis events are chosen to encompass a range of related possible initiating events that 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.

101. Probabilistic analysis is used to evaluate the likelihood of any particular sequence and its consequences. This evaluation may take into account the effects of mitigation measures inside and outside the plant. Probabilistic analysis is used to estimate risk and especially to identify the importance of any possible weakness in design or operation or during potential accident sequences that contribute to risk. The probabilistic method can be used to aid in the selection of events requiring deterministic analysis and the other way around.

102. Generic or plant specific PSAs are used increasingly to evaluate multiple failure situations and severe accidents. The process employs realistic assumptions and best estimate analyses. The analyses quantify available safety margins and they lead to nuclear plant design changes to reduce the likelihood of radioactive releases and their consequences. A summary of the extensive actions taken in various operating water cooled plants is shown in Table II. For future plants, deterministic and probabilistic safety assessments will be applied to attain the objectives of paras 25 and 27.

103. The safety assessment process is repeated in whole or in part as needed later in the plant's lifetime if ongoing safety research and operating experience make this possible and advisable. For example, a large number of requirements are specified for the surveillance test interval and allowed outage time for plant components and systems. PSA is being used to identify the components important to risk and to adjust the requirements for important components to be consistent with their risk contribution.

3.3.7. Radiation protection

104. Principle: A system of radiation protection practices, consistent with recommendations of the ICRP and the IAEA, is followed in the design, commissioning, operational and decommissioning phases of nuclear power plants.

TABLE II. IMPORTANT DESIGN MODIFICATIONS FOR SEVERE ACCIDENT SCENARIOS

Severe accident scenarios	Most frequent modifications
Reactivity accidents	• Enhanced makeup system • Enhanced or fast acting boron system • Automated dilution control
Release of combustible gases	• Nitrogen inerting • Igniters • Catalytic devices
High pressure core melt: DCH	• Enhanced RCS depressurization
High pressure core melt: SGTR	• Enhanced RCS depressurization
Impact on vessel support structure	• Physical barrier • Cavity flooding
Vessel penetration	• External vessel cooling
Direct contact with containment boundary	• Physical barrier; flooding
Slow containment overpressurization	• Filtered venting • Alternate cooling sources
Basemat melt through	• Cavity flooding • External vessel cooling
Containment bypass	• Eliminate high/low pressure interface • Additional isolation valves
Containment isolation	• Reduce risk of impaired containment
CANDU severe accident	• Increase availability of moderator/ shield tank heat sinks

Note: CANDU: Canadian deuterium uranium reactor; RCS: reactor coolant system; DCH: direct containment heating; SGTR: steam generator tube rupture.

105. Measures are taken to protect workers and the public against the harmful effects of radiation in normal operation, anticipated operational occurrences and accidents. These measures are directed towards control of the sources of radiation, including radioactive releases and waste; to the provision and continued effectiveness of protective barriers and personal protective equipment; and to the provision of administrative means for controlling exposures.

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

107. For the control, guidance and protection of personnel, procedures are written which define safe practices, the physical means of protection and the necessary administrative procedures for each task which might lead to the exposure of personnel to radiation. Special attention is given to dose intensive work.

108. These are the principal features that make it possible to meet the radiation protection objective. To ensure that it is met calls for continued vigilance, monitoring of plant conditions and the maintenance of a clean orderly plant.

3.3.8. Operating experience and safety research

109. *Principle: Organizations concerned ensure that operating experience and the results of research relevant to safety are exchanged, reviewed and analysed, and that lessons are learned and acted on.*

110. The organization operating a nuclear power plant maintains an effective system for collection and interpretation of operating experience, and it disseminates safety significant information promptly among its own staff and to other relevant organizations. The root causes of accidents are analysed. Events that may be regarded as precursors of accidents are identified and actions are taken to prevent any recurrence. Each operating organization seeks to learn from the experience of other organizations. The sharing of operating data is co-ordinated nationally and internationally.

111. The primary objective is that safety shortfalls are recognized and that corrections are made to prevent the recurrence, either at the same location or elsewhere, of safety related abnormal events, no matter where they first occurred. Most importantly, this principle reflects the point that an accident of any severity would most probably be marked by precursor events, and to this extent would be predictable and therefore avoidable. Feedback of experience also increases knowledge of the operating characteristics of equipment and performance trends, and provides data for numerical safety analysis.

112. Many operating organizations have a programme of gathering information specific to their plants and using it to trend and improve the plant performance. The accumulated information is on reported plant events, errors, near misses, problems, observations, and even suggestions for improvement. The information is reviewed by representatives from different plant functions and it is assigned a safety significance level. The important safety issues are investigated promptly and are subjected to root cause analysis before corrective actions are taken. Operational errors are considered important and are evaluated separately. A process is established to track the various assessments and corresponding corrective actions and to determine unfavourable trends, which can be reversed. Management involvement in this internal programme of information gathering and satisfactory resolution of issues is essential to success. The key to a good and substantive programme is whether employees are willing to report problems and suggest improvements.

113. Research to understand nuclear power plant performance, the response to abnormal occurrences and the possible sequences of events in severe accidents leads to improved interpretation of experience and better definition of corrective measures that might be necessary. Further advantages are gained by the use of research results to improve plant performance while still keeping acceptable safety margins. Results of research may be incorporated into nuclear power plant design, helping to make these plants still safer. More generally, research and development activities are needed to maintain knowledge and competence within organizations that support or regulate nuclear power plant activities.

114. Research efforts clearly enhance the safety of nuclear power plants and reduce the prevailing uncertainties in predicting their performance or the consequences of accidents. The scope of research and development programmes is broad so as to cover all areas of interest, including potential modifications to existing designs. The work ranges from investigating degradation mechanisms to the development of structural materials more resistant to corrosion; the qualification of fuel for extended burnup or with mixed oxide (MOX) fissionable material; the introduction of improved coolant chemistry to improve plant reliability and to reduce the impact of ageing; the development of system computer codes to predict plant performance during transients and in accidents and severe accidents and to reduce the uncertainties in previous safety analyses; the introduction of improved and computerized control systems and instrumentation to simplify the human–machine interface; and the development of a more realistic set of possible radioactive releases for predicting the consequences of severe accidents. Nuclear research and development is an essential element of nuclear plant safety and its continued support is very important. However, there is a need to prioritize research and development work with respect to its safety significance. Also, co-operative research on an international scale to reach a common understanding on

major safety issues is an important way to avoid duplication of efforts and to reduce costs.

3.3.9. Operational excellence

115. A principle on operational excellence is introduced in this revision of 75-INSAG-3 to emphasize and to bring together several operational aspects of safety not sufficiently covered previously.

116. *Principle: Operational excellence is achieved in present and future nuclear power plant operations by: augmenting safety culture and defence in depth; improving human performance; maintaining excellent material condition and equipment performance; using self-assessments and peer reviews; exchanging operating experience and other information around the world; increasing application of PSAs; and extending the implementation of severe accident management.*

117. Several of the proposed improvements in the operational excellence principle have been covered elsewhere: safety culture (paras 33 and 34); defence in depth (para. 49); self-assessment (paras 83–85); peer reviews (paras 86–88); human performance (para 93); PSA (paras 62 and 102); operating experience (para. 112); research (para. 114); severe accident mitigation (paras 66 and 102). These improvements are applicable to existing as well as future nuclear power plants.

118. Most of the preceding enhancements are aimed at improving human performance since a large fraction of plant events are caused by human error. Errors may be the result of the behaviour of a single individual, the collective behaviour of individuals, or the influences of the work environment, the organization or the management. Excellence in human performance is attained when all the individuals involved exhibit desirable behaviour and when the emphasis is put upon fostering or displaying a questioning attitude; reinforcing such desirable behaviour; encouraging leadership and promoting teamwork.

119. Several lessons have been learned from power plants striving for operational excellence. For instance, in seeking to obtain safety improvements to existing installations, account is taken of the balance between benefits and drawbacks (including costs). When the drawbacks of modifications far outweigh the likely gain in safety, generally they would not be undertaken. Also, account needs to be taken of the implications of changes for the usefulness of the experience gained and training developed in operating the plant in its existing configuration. Another example is that of organizational changes which can have the potential either to improve or to impair safety

performance. It is important to ensure, prior to implementation, that the effect of the proposed changes will not reduce safety, either when the change has been completed or during the transitional period while it is being implemented. Under all such circumstances, leadership and quality of management are essential as well as the ability to involve staff throughout the entire organization.

120. Another important characteristic of operational excellence is the adoption of a strong preventive and predictive maintenance strategy which, for example, detects ageing and performance related problems in their early stages and corrects them before they have a significant impact on safety. It is important to show that the life-time of the nuclear power plant is being managed to maintain safety so that the plant operating organization can make a valid up to date safety case. This process identifies systems, structures and components important to safety as well as non-safety-related systems, structures and components that directly support the safety related functions or are important to the performance of the balance of plant. The programme will show whether the measured or analysed degradation due to prevailing ageing mechanisms is acceptable in terms of safety. Furthermore, it would include an evaluation of time limited ageing analyses (e.g. allowable thermal cycles) and a demonstration that they are still applicable. Many of the considerations relating to ageing can be dealt with by non-destructive and other testing and examinations of nuclear power plants that are currently required. A proactive attitude, however, ensures that there is an all inclusive ageing programme which focuses upon operating experience problems associated with ageing and all the detectable and potentially significant adverse effects of ageing upon safety.

121. Another consideration is the reduced demand for power and the development of alternative means of generation in some countries. This means that there is a decrease in the demand for engineering skills required to design, construct, commission and operate nuclear power plants. This can lead to a loss of expertise and particularly a loss of corporate memory. Operational excellence recognizes the need for processes to manage the changes arising from such loss of expertise. They include the identification of core skills to ensure safety and arrangements to preserve those core skills by training of less experienced engineers, by the use of mentors and by exchanging resources with other organizations.

122. Measurable indicators of safety performance are used in attaining operational excellence. The indicators are employed by management to trend plant safety and performance and to compare them with other plants performing at a very high level.

123. To be effective and permanent, the drive to operational excellence must come from within the operating organization, the management and its staff. The attainment

of operational excellence has often been associated with increasing plant availability and reducing operating costs by streamlining and simplifying processes. However, it is essential that such gains be achieved with no reduction in overall plant safety.

3.3.10. Features for future nuclear power plants

124. Even though there has been a continuous effort to increase the scope of the severe accidents taken into consideration and to reduce their off-site consequences, a further reduction in potential radiological consequences is an important goal for future nuclear power plants. Consistent with the objectives of paras 25 and 27, other features are a significant reduction in system complexity with corresponding improvements in operability and maintainability. All future plants also need to continue to improve defence in depth. Prevention of accidents remains the highest priority but controlling the course of accidents and mitigating their consequences, if they happen, are also very important. This addition to 75-INSAG-3 provides a summary description of potential features for future nuclear power plants with primary emphasis being placed on water cooled nuclear reactors.

125. An important advantage of future plants is their ability to incorporate corrections to deficiencies identified in the past. The use of a checklist for such problem areas and their proposed resolution will ensure that no significant past difficulty is overlooked. Future plants have another advantage, because they can implement the results of research and development programmes, including those relating to new materials, improved coolant chemistry, methods of making best estimate predictions of operating margins and their uncertainties, and the findings from a large number of other safety analyses and research work. But, it is important that features incorporated into future plants be fully proven through adequate tests and, preferably, demonstration in operating plants.

126. Accident prevention is enhanced by reducing the frequency of equipment failures and the number of human errors. For equipment failure, this is achieved by simplifying the design and, in particular, reducing the number of active components, such as valves, which can fail or be mispositioned. Another approach is to increase the tolerance to equipment failure by selecting diversified equipment and to reduce the severity of transients by, for example, increasing the thermal inertia and response time of the primary system. The best opportunity for improving accident prevention lies in improved human–machine interfaces, additional use of information and digital technology, and self-testing protection systems. When computer systems are utilized for safety functions, there must be sufficient precautions taken against common cause failures of the computer systems. The quality and reliability of the

systems and additional measures such as an appropriate degree of diversity must be considered. Also, the production process must include integral testing of software and hardware systems, and good practices for software verification and validation. Another opportunity to improve accident prevention is to assess the measures taken at different levels of defence in depth and, where practical, to eliminate dependence between systems. Finally, adequate provisions in terms of space and installation are necessary to improve the performance and quality of non-destructive inspections and maintenance work.

127. Plant designers and owners/operators may provide additional margins in as many areas as appropriate for investment protection, operational flexibility and performance and increased assurance of future plant licensability.

128. Accident mitigation is enhanced to reduce the probability and consequences of radioactive releases. Features of the type listed in Table II and other novel concepts are being considered to practically eliminate large early radioactive releases and to reduce the protective measures necessary in terms of time and area for late containment failures.

129. For future nuclear power plants, the design features related to the prevention and mitigation of accidents, including severe accidents, will be determined on the basis of deterministic analysis, best estimate probabilistic considerations, the application of numerical safety targets and engineering judgment. Notably, the practical elimination of accident sequences which could lead to large early radioactive releases will be based, as far as necessary, on detailed deterministic and/or probabilistic studies. PSAs will be used from the design stage as a useful tool for in-depth analysis of the contribution of the different accident sequences to the risk. Reaching a final decision about features to be incorporated in future nuclear power plants will be an iterative process, with initial judgements made by the designers, based on experience and research results and with the help of PSAs. This is followed by review by plant owners/operators and regulators to confirm that an appropriate decision has been made. This process of careful evaluation and decision making will lead to a consistent and stable set of design features.

130. The risks associated with future nuclear power plants will become very low, owing to the reduction in both the likelihood and the radiological consequences of accidents. However, this statement supposes that careful attention is paid to the possibilities of common mode failures and to the uncertainties still prevalent in the understanding of phenomena associated with severe core damage. For these reasons, engineering judgment will be important in evaluating new design features with respect to the objectives set in paras 25 and 27.

131. With respect to siting issues, it is important to consider the technical safety objective as applicable to all future plants, even those that might be located so remotely that it can be demonstrated that solely as a result of low population density no serious radiological consequences would occur. Also, if a future plant is sited near a national boundary, transboundary considerations must be taken into account.

132. Future reactor concepts undoubtedly will influence the specific principles presented in Section 4. However, such changes cannot be identified until the future concepts are developed in more detail. For this reason, the material in Section 4 is particularly relevant to existing plants. If differences are anticipated for future plants, they are mentioned in brief and in general terms in Section 4.

4. SPECIFIC PRINCIPLES

133. The safety objectives and the fundamental principles, given earlier in Sections 2 and 3, provide a conceptual framework for the specific safety principles set out in Section 4. Figure 1 summarizes the structure and the categorization of safety objectives and principles. Figure 2 is a schematic representation of the specific safety principles. It shows their interrelationship to the fundamental concepts of defence in depth and safety culture. The concept of safety culture is shown to pervade all activities. From top to bottom on the left hand side of Fig. 2, all the principles are related to the levels of defence in order of increasing threat to safety, from normal operation to off-site and emergency response, indicating the provisions in design and operation that need to be made to address the challenges a plant could face. The horizontal order of the specific safety principles indicates their application during the main stages of a nuclear project, from its beginning to the end of plant lifetime. Colours have been chosen to represent groupings of principles: green for siting, orange for design, blue for manufacturing, construction and commissioning, red for operation and black for end of operating lifetime, which includes spent fuel storage and decommissioning. With respect to coherence and interrelation, a solid orange line connects some of the basic principles used to ensure a safe plant design, which incorporates physical protection of the plant in this revision. Similarly, a solid blue line indicates the importance of achieving and verifying the safety and the quality of the plant before permitting its operation. A solid red line connects the various attributes that contribute to excellence in operational safety and emphasizes the importance of feedback of operating experience. Thin green lines show connections between applicable principles, e.g. during accident management and under emergency conditions.

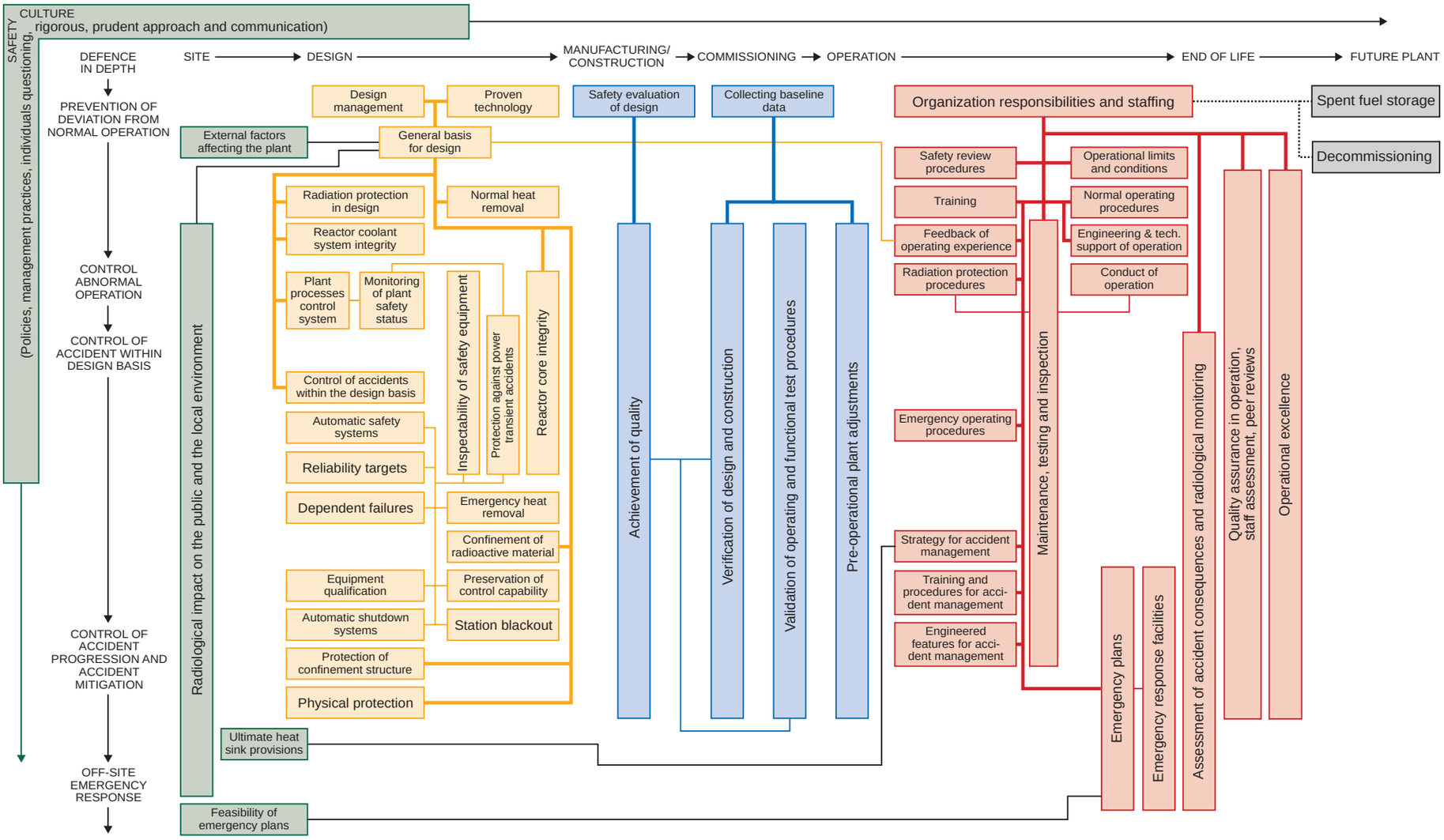

FIG. 2. Schematic presentation of the INSAG specific safety principles showing their coherence and their interrelations.

4.1. SITING

134. The site is the area within which a nuclear power plant is located and which is under the effective control of the operating organization. The selection of an appropriate site is an important process since local circumstances can affect safety. In certain cases, siting limitations are approached in a completely prescriptive manner, although more generally the choice of site is a balance between competing factors including economic interests, public relations and safety. Consequently, although the application of one of the following safety principles could conceivably lead to the rejection of a proposed site for purely safety reasons, the principles serve more to offer common guidance on the safety aspects of site selection. Changes foreseen over the lifetime of the plant are taken into consideration.

135. For future nuclear power plants, especially those of standardized designs, it is advantageous to ensure that such a standardized design could be safely sited at as many of the available sites as possible in countries where plants of that design are expected to be made available for order and/or construction.

4.1.1. External factors affecting the plant

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

137. Local factors include natural factors and human made hazards. Natural factors to be considered include geological and seismological characteristics and the potential for hydrological and meteorological disturbances. Human 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. This is developed in the form of quantified probabilities when possible. The corresponding risk evaluation takes into account the safety features provided by the design 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.

4.1.2. Radiological impact on the public and the local environment

138. *Principle: Sites are investigated from the standpoint of the radiological impact of the plant in normal operation and in accident conditions.*

139. Air, food-chains and water supplies provide pathways for the possible transport of radioactive material to humans. Site characteristics to be investigated are those

which can influence the pathways: physical characteristics such as topography, meteorology and hydrology; environmental characteristics such as type of vegetation and animal life; the use of land and water resources; and the population distribution around the site. The results of these investigations are used to demonstrate that the safety objectives are fulfilled, in normal operation with appropriate limits on effluent discharges, and for accidental radioactive releases with provisions for off-site countermeasures taken into account.

4.1.3. Feasibility of emergency plans

140. *Principle: The site selected for a nuclear power plant is compatible with the off-site countermeasures that may be necessary to limit the effects of accidental releases of radioactive substances, and is expected to remain compatible with such measures.*

141. In a later section on emergency planning (Section 4.8.1), there are discussions of measures for which preparation is made to cope with very improbable accidents that could affect public health and the environment. The feasibility of such emergency plans may be affected by features of the site and its surroundings, and this is taken into account in the initial site review. For future nuclear power plants, the protective emergency measures could be reduced in terms of both area of coverage and time of application in recognition of the objectives set in paras 25 and 27.

4.1.4. Ultimate heat sink provisions

142. *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.*

143. 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.

4.2. DESIGN

144. The primary objective of nuclear power plant designers is to provide a good 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. The plant specifications are consistent with the specified duty in terms of electrical output, projected lifetime, the manoeuvring necessary to meet system demands, and, importantly, the requirement to meet the safety objectives identified in Section 2 of this report and the safety principles in Sections 3 and 4. Designers also provide a system for recording the safety design basis of the plant and for maintaining conformity to the design basis in the design changes that occur throughout 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 provide information and recommend 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 that could lead to a major release of radioactive materials from the plant.

145. 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.

146. Safety designers analyse the behaviour of the plant under a wide range of conditions. These include normal operation and variable conditions encountered in manoeuvring. 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 the 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 mitigated effectively by means of accident management and measures available through emergency preparedness.

147. Future designs will evaluate additional multiple failures and severe core damage in consistency with the objectives of paras 25 and 27.

148. 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.

4.2.1. Design process

149. 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.

4.2.1.1. Design management

150. *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.*

151. 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 for each activity are essential. 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.

152. The design force is engaged in the preparation of safety analysis reports and other important safety documents. It also includes a co-ordinating group that 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. It has direct access to the design manager but does not necessarily report to that manager.

153. In accordance with the fundamental principle of Section 3.3.2, 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.

4.2.1.2. Proven technology

154. *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.

155. This principle is a specific application of the fundamental principle of Section 3.3.1 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 developed 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.

156. An example of this balance between proven technology and technological innovation is the recent interest in and broad application of 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 potential for increased reliability. Disadvantages include lower driving heads in fluid systems and reduced flexibility in abnormal conditions. Furthermore, special attention has to be paid to limitations in the existing data on the performance of new passive systems and adequate experimental and analytical verification of their performance is necessary. Finally, active components may still be necessary for startup and shutdown.

157. 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 modelling and data are used to predict plant performance, safety margins and the evolution of accident conditions. Where realistic modelling is not feasible, conservative models are used.

4.2.1.3. General basis for design

158. *Principle: A nuclear power plant is designed to cope with a set of 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.

159. 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 inherent plant features and normal plant systems.

160. Engineered safety systems are included in plant design, as discussed in Section 3.3, 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. Design assessments of engineered safety systems will provide assurance that there are no cross-linked interactions with other independent systems which could detrimentally impact their performance. 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 dominates 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.

161. All components, structures and systems can be classified on the basis of their function and significance for safety to provide a basis for determining the appropriate codes, standards and other requirements to be applied in their design, construction, installation, operation, maintenance, environmental qualification and inspection.

162. For future nuclear power plants, realistic assumptions and best estimate analyses are used to assess the additional multiple failures and severe core damage sequences considered in the design process.

4.2.2. General features

163. The second group of specific safety principles affecting the design of a nuclear power plant pertains to general features included for safety reasons.

4.2.2.1. Plant process control systems

164. *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.*

165. Important plant neutronic and thermal–hydraulic variables have assigned operating ranges, trip set points 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 set points 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 (see the principle in Section 4.2.2.2 on automatic safety systems). Trip set points 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 set points. Automatic controls are kept operational to keep parameters within prescribed ranges. Deficiencies that affect automatic controls are resolved expeditiously.

166. 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 it could also compromise safety by the effects of sudden and precipitous changes, and it could induce excessive wear which might impair the reliability of safety systems.

167. Therefore, the more important neutronic and thermal–hydraulic 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 set points in normal operation.

4.2.2.2. Automatic safety systems

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

169. 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 even in the most severe of these 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.

170. Stringent requirements preclude bypassing automatic safety systems. In current and future plants, consideration is given to improving safety systems in terms of reliability and response time.

171. 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.

172. 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. In the event of the modernization and/or refurbishment of instrumentation and control (I&C) systems important to safety in operating nuclear power plants, it is necessary to consider the interfaces to existing devices and environmental conditions such as those relating to the power supply, auxiliary equipment and electromagnetic interference (EMI).

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

4.2.2.3. Reliability targets

174. *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.*

175. 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 modelling 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.

176. For some systems, reliability targets may exceed values that 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.

4.2.2.4. Dependent failures

177. *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.*

178. 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.

179. 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, flooding, 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 human 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.

180. 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.

181. 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 the physical barriers and the safety systems contributing to the defence in depth of the plant 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.

4.2.2.5. Equipment qualification

182. *Principle: Safety components and systems are chosen that 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.

183. 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 ageing 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, including their interactions, as well as severe accidents for future nuclear power plants, consistent with the objectives set out in para. 25. The effects of external events such as earthquakes are also considered.

184. The required reliability is to be maintained throughout the plant's lifetime. 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 specification of environmental conditions, process conditions, duty cycles, maintenance schedules, service lifetime, type testing schedules, replacement parts and replacement intervals.

185. It is preferable that qualification be achieved by the testing of prototypical equipment. This is not always fully practicable for the vibration testing of large components or the ageing of equipment. In such cases, analysis or tests plus analyses are relied upon.

4.2.2.6. Inspectability of safety equipment

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

187. In-service inspection is relied upon to demonstrate that safety provisions are maintained throughout the lifetime of the plant. Provision is made at the design stage for inspection access, and for the ease and frequency of inspection. 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 the in-service inspection 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.

4.2.2.7. Radiation protection in design

188. *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.*

189. Designers provide for protection of the operating and maintenance staff from direct exposure to 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 the 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.

190. Attention is also paid at the design stage to radiological protection in the decommissioning phase. After the end of the operating lifetime 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 activity on the time-scale important for decommissioning, and to the need for convenient access for dismantling.

4.2.3. Specific features

191. Some required design features serve specific safety functions.

4.2.3.1. Protection against power transient accidents

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

193. 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 features 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 features are influenced by design choices. Negative reactivity feedback coefficients alone cannot prevent all conceivable 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. 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. 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. Furthermore, reliable means are provided to prevent fast (slug type) boron dilution (for pressurized water reactors).

194. 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 and automatic control and protection systems; to ensure that the removal or addition of a single control 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.

4.2.3.2. Reactor core integrity

195. *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.*

196. Fuel rods 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 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 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.

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

198. 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.

199. High quality of fuel rods 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 activity in the coolant during operation.

4.2.3.3. Automatic shutdown systems

200. *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.

201. Safety shutdown systems are independent in function from the reactivity control systems used for normal operation of the reactor. Common sensors or devices may only 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 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 buses 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.

202. One unlikely event which must be analysed 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, consistent with the technical safety objective of Section 2.3. 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 with account taken of this failure of plant protection.

4.2.3.4. Normal heat removal

203. *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.*

204. 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. For example, control rod drive pumps were used to maintain the reactor coolant inventory during the Browns Ferry fire in 1975.

4.2.3.5. Startup, shutdown, and low power operation

205. *Principle: Components, structures, and systems used during startup, low power and shutdown operations are designed to maintain or 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.*

206. During low power and shutdown operation, plant conditions can be different to those required for full power operation (see para. 62). 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 capacity 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.

4.2.3.6. Emergency heat removal

207. *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.*

208. 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 removal of shutdown heat has led in some cases to consideration of the use of special cooling system designs, such as dedicated and protected systems for decay heat removal and systems based on natural circulation or conduction. The atmosphere is sometimes considered as a possible ultimate heat sink.

4.2.3.7. Reactor coolant system integrity

209. *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 lifetime of the plant.*

210. 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.

211. 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.

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

213. Analyses of the 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 small 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 or depth that would be 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

that 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 of hydrogen.

214. 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.

215. During the lifetime 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 that prove necessary and are feasible. Access for, ease of and frequency of inspection are taken into account in the design.

216. Ferritic steel reactor pressure vessels for some existing plants are subject to inspection and operating restrictions that would not be necessary if technological issues that are 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 consumables will have a very low content of elements that accelerate radiation induced deterioration, especially copper and phosphorus. Sensitive steels will not 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.

4.2.3.8. Confinement of radioactive material

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

218. A special system is required to retain radioactive material that might be released as a result of an accident, unless it has been shown that adequate protection against such a release has been secured by other means. No actual system could retain all the

radioactive material arising from a major accident, especially in view of the large inventory of radioactive noble gases. The special systems still have the function of preventing leakage of almost all the more significant radioactive materials. Such special 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 subsystem that completes the sealing process on demand, and other subsystems protecting the structure (see the principle in Section 4.2.3.9). Together these constitute a containment system.
— Confinement may be effected 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, e.g. on filters.
— The structure maintains its integrity in both the short term and the long term under the pressure and temperature conditions that could prevail in design basis accidents.
— 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.

219. 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.

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

4.2.3.9. Protection of confinement structure

221. *Principle: If specific and inherent features of a nuclear power plant would not prevent detrimental effects on the confinement 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.

222. This principle particularly affects existing plants in which a confinement structure is used as a containment structure. 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. 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. These higher values are in most cases less than those corresponding to the ultimate strength of the containment.

223. If severe accident sequences could lead to pressures causing stresses exceeding the estimated ultimate strength of the containment, that structure might fail. If it were to fail 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.

224. If this contribution to risk is so large as to conflict with the safety objectives, special measures to protect the containment structure are taken. Some measures that have been used or discussed in specific cases are hydrogen igniters, autocatalytic recombiners, filtered vent systems, area spray systems and fuel debris retainers (see Table II).

225. As noted in paras 25 and 27, a more systematic approach can be employed to improve the containment and/or confinement function for severe accidents in future nuclear power plants.

226. Similar considerations apply for confinement structures not designed for high internal pressures.

4.2.3.10. Monitoring of plant safety status

227. 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.

228. 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 a 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 part monitoring systems, monitoring of excessive and unusual vibration or noise, and systems to detect coolant leaks or unusual levels of radiation, temperatures or moisture.

229. 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 factor experts assist designers by identifying the most appropriate organization and presentation of these data.

4.2.3.11. Preservation of control capability

230. *Principle: The 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.*

231. The environment in the 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 is degraded for any reason, operators receive a clear warning. Suitable equipment for personal protection is provided.

232. 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.

4.2.3.12. Station blackout

233. Principle: Nuclear plants are so designed that the simultaneous[6] loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.

234. Electrical power is essential for nuclear power plant safety systems. Safety assessments show that the consequences of station blackout can be a dominant component of the total risk. 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.

235. In particular, nuclear power plants are designed to withstand, without loss of safety function, a simultaneous loss of on-site and off-site AC electrical power (a station blackout) for a specified 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.

236. Additional electrical power generating sources (e.g. connection to a hydroelectric power station or installation of gas turbine generators) are used in some nuclear power plants to improve the response to station blackout.

4.2.3.13. Control of accidents within the design basis

237. Principle: Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and

[6] The use of 'simultaneous' is not intended to imply that the loss of on-site and off-site power necessarily occurs at the same time.

instrumentation needed by the plant staff for following and intervening in the course of accidents.

238. 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, 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 range from 10 to 30 minutes or longer depending on the situation.

239. 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.

4.2.3.14. New and spent fuel storage

240. *Principle: Plant designs provide for the handling and storage of new and spent fuel in such a way as to ensure protection of workers and to prevent the release of radioactive material.*

241. Facilities are required to handle and store new and spent fuel assemblies. The quantity of new and spent fuel to be stored varies with the design of the plant and the individual refuelling requirements. The storage facilities keep the new and spent fuel in a safe and subcritical array under all anticipated storage conditions. The facilities and fuel racks take into account external loads and forces (e.g. in an earthquake). Since the spent fuel contains a significant inventory of fission products, shielding from radiation and a safe means of loading the assemblies into shipping casks are provided. The integrity of spent fuel cladding is preserved by redundant and reliable means of removing decay heat. Provision is also made for inspecting new and spent

fuel, for testing, handling and storing defective fuel, and for retrieving fuel for remedial action, e.g. for shipping it off-site for post-irradiation examination. Monitoring for radioactive releases, ensuring subcriticality, providing physical protection and continued cooling of the spent fuel are important elements in operating such facilities.

4.2.3.15. Plant physical protection

242. *Principle: The design and operation of a nuclear power plant provide adequate measures to protect the plant from damage and to prevent the unauthorized release of radioactive material arising from unauthorized acts by individuals or groups, including trespass, unauthorized diversion or removal of nuclear materials, and sabotage of the plant.*

243. Protection of the plant and equipment from unauthorized acts is already ensured by design features provided for other reasons, such as locating redundant safety equipment in different areas of the plant and providing for an emergency control room. Additional physical protection is provided through a designed combination of security hardware and devices, security guards, and appropriate layout and design of the facility for access control. Physical protection issues are considered early in the planning stages of a nuclear power plant. In addition, a physical protection audit is carried out at the design stage on the basis of potential threats. An active protection programme is in effect from receipt of the first batch of fuel to the final stages of decommissioning. Emergency physical protection procedures are available to handle effectively any possible threats.

244. Physical protection measures are co-ordinated with nuclear safety programmes to ensure that physical protection is not jeopardizing nuclear safety. For example, physical protection measures will not jeopardize nuclear safety under emergency conditions.

4.3. MANUFACTURING AND CONSTRUCTION

245. A primary safety requirement is that a nuclear power plant be manufactured and constructed according to the design intent. This is accomplished by maintaining attention to a range of issues, from the broad aspect of accountability of the organizations involved to the diligence, competence and care of the individual workers.

4.3.1. Safety evaluation of design

246. *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.

247. 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 co-ordinate safety evaluation with manufacturing and construction to ensure that important safety options are not foreclosed and that licensing decisions are timely.

248. 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 check points are established as required during construction so that satisfactory final design, installation and verification of the adequacy of safety related equipment can be reviewed.

4.3.2. Achievement of quality

249. *Principle: The plant manufacturers and constructors discharge their responsibilities for the provision of equipment and construction of high quality by using well proven and established techniques and procedures supported by quality assurance practices.*

250. The supply of equipment manufactured and constructed satisfactorily according to specification is an immediate responsibility of the plant manufacturer, whose success in this regard depends on the effectiveness of its practices and procedures and the way it adheres to them. Manufacturing and construction are guided by detailed specifications for processes and products, and for methods of testing and inspection. Equipment manufacturers are chosen who have demonstrated their capabilities in meeting the special and exacting requirements for nuclear power plants, which are often specific to the nuclear industry and which are based on codes and standards containing acceptance criteria for the final work products. Suppliers of important safety related equipment often have their competence checked and certified by third parties.

251. The manufacturer establishes procedures for the control of processes and documents; identification and control of materials and components; setting of inspection and test schedules; maintenance of records, hold points and corrective procedures for deviations; the whole being subject to a hierarchy of quality assurance practices.

The manufacturer is responsible for the development and validation of its manufacturing practices and quality control methods, for staff training and for providing satisfactory working conditions.

252. Although the manufacturer has immediate responsibility for the quality of the equipment and plant supplied, the operating organization discharges its general responsibility for the safety of the plant by setting up arrangements within its own company, or by using organizations acting on its behalf, to review and audit the practices and documentation of the manufacturers and contractors, including quality assurance practices and organization. For important safety related items, these arrangements are available for review by regulatory authorities.

4.4. COMMISSIONING

253. It is necessary to demonstrate that the completed plant is satisfactory for service before it is made operational. For this purpose a well planned and properly documented commissioning programme is prepared and carried out. The operating organization, including future operating staff, participates in this phase. Plant systems are progressively handed over to the operating staff as the installation and testing of each item are completed.

254. By the time the commissioning programme reaches the stage of fuel loading, all items important to safety at that stage have been handed over to the operating organization. In some places the process has an intermediate stage in which another organization conducts the commissioning operations effectively as an agent for the future plant operator.

4.4.1. Verification of design and construction

255. *Principle: The commissioning programme is established and followed to demonstrate that the entire plant, especially items important to safety and radiation protection, has been constructed and functions according to the design intent, and to ensure that weaknesses are detected and corrected.*

256. To ensure that the design intent has been met, the commissioning programme includes checks of safety equipment and its functional characteristics, and of provisions for radiation protection. Testing is progressive; less onerous conditions are achieved first and hold points are used to ensure that adequate test results are obtained before proceeding to the next stage. The commissioning programme and its results are subject to surveillance and review by the regulatory authorities. Some phases of commissioning take place during construction. Elements of systems are tested; as

complete systems are finished, they are also tested. Variations from the design intent that are found in these checks are assessed, corrected and referred to the operating organization so that any effect on plant operation can be taken into account. Where complete tests of components and systems under realistic conditions cannot be made, tests are performed in combination under conditions as close as possible to realistic.

257. Commissioning continues through fuel loading, criticality and power ascension. Commissioning results are subject to close review by the regulatory authorities. They are also used by designers to improve future plant designs.

4.4.2. Validation of operating and functional test procedures

258. *Principle: Procedures for normal plant and systems operation and for functional tests to be performed during the operating phase are validated as part of the commissioning programme.*

259. Procedures to be followed during the operating phase are written before and during commissioning on the basis of information supplied by the designer and the manufacturers. Advantage is taken of the commissioning phase to test and update these operating procedures for the plant and its systems, to check out the methods that will later be used in functional testing of equipment related to safety, and in general to exercise the plant. The plant simulator is used to validate operating functional testing procedures. This activity also gives the operating staff essential preparation and training, familiarizing them with locations of systems, system responses, system peculiarities and system interactions. It is one of the principal reasons for involving the plant operating staff in commissioning activities at an early stage.

4.4.3. Collecting baseline data

260. *Principle: During commissioning tests, detailed diagnostic data are collected on components having special safety significance and the initial operating parameters of the systems are recorded.*

261. Baseline data are collected during commissioning and early operation as reference points to assist in later surveillance for the detection of incipient degradation of the plant components. Included in this process are the fundamentally important inspections and tests of the reactor pressure vessels and other primary component boundaries. In general, baseline data are collected during commissioning for all safety related parameters that are to be routinely measured and monitored during operation.

4.4.4. Pre-operational plant adjustments

262. *Principle: During the commissioning programme, the as-built operating characteristics of safety and process systems are determined and documented. Operating points are adjusted to conform to design values and to safety analyses. Training procedures and limiting conditions for operation are modified to reflect accurately the operating characteristics of the systems as built.*

263. Process and safety systems are tested and calibrated during the pre-operational period. The information obtained indicates where adjustments are needed to ensure that the plant, the plant simulator, the safety analysis, operating staff training and operating procedures conform to a unified basis. In this way, the plant is made to work in the intended fashion when it is brought to the normal operating state.

4.5. OPERATION

264. The operating organization is responsible for providing all equipment, staff, procedures and management practices necessary for safe operation, including the fostering of an environment in which safety is seen as a vital factor and a matter of personal accountability for all staff. It may seem on occasion that emphasis on safety might be in conflict with the requirement to achieve a high capacity factor and to meet all demands of electricity generation. This conflict is more apparent than real, and it can at most be transitory, in that the factors of design, construction and operational management that promote safety generally coincide with those that contribute to reliability in operation. Reliability is not served by compromising safety in the short term.

4.5.1. Organization, responsibilities and staffing

265. *Principle: The operating organization exerts full responsibility for the safe operation of a nuclear power plant through a strong organizational structure under the line authority of the plant manager. The plant manager ensures that all elements for safe plant operation are in place, including an adequate number of qualified and experienced personnel.*

266. Day to day responsibility for plant safety resides with the plant manager, who ensures that the necessary elements for achieving safety are present and that the need for safety governs operations at the plant. The plant manager is supported by the executive management of the operating organization, which assigns adequate financial and technical support, material, chemistry, radiological protection and other staff

resources to the operation. Safety responsibilities for all levels and functions of the operating organization are clearly stated in job descriptions.

267. Enough qualified staff are employed to carry out all normal activities without undue stress or delay, including the supervision of work done by external contractors during periods of exceptional workload such as maintenance outages. Staffing specifications also ensure backup for key positions and take account of attrition and the time required for retraining.

268. Staffing requirements for abnormal operational occurrences are analysed to ensure the capability of carrying out any specialized tasks, such as accident management, damage assessment and control, fire-fighting, search and rescue, first aid treatment, off-site monitoring and off-site communications. These staffing requirements take into account the availability of emergency services in the locality.

4.5.2. Safety review procedures

269. *Principle: Safety review procedures are maintained by the operating organization to provide a continuing surveillance and audit of plant operational safety and to support the plant manager in the overall safety responsibilities.*

270. Among the regular activities at the plant there is a line process of safety management which covers all aspects of day to day operations and reports to the plant management. Beyond this, the operating organization provides means for independent safety review, from within the organization itself or with assistance from specialist institutions or other bodies. The principal objective is to ensure that, in those matters that are important for safety, the plant manager will be supported in his accountability by arrangements that are independent of the pressures of plant operation. However this independent review is performed, it is an activity that is separate from plant operation, and that provides safety review on a continuing basis to verify that plant management establishes sound practices and adheres to requirements. The reports from this activity are formal and are provided directly to senior management in the operating organization. Particular attention is paid in these processes to the feedback of experience; the examination of abnormal events and reported plant deficiencies both locally and at similar plants; reviews of validity and modification of operating procedures; safety related plant modifications; training and qualification of staff; response to regulatory requirements; and the general attitudes of management and staff towards the safety of the plant.

271. Most particularly, in individual matters of special safety importance, such as intended abnormal plant manoeuvres, unusual tests or experiments, major plant engineering, or changes in safety limits or conditions, special procedures are first formulated by the line operating and safety staff, and these are subject to the independent review process as part of the mechanism of obtaining formal approval.

4.5.3. Conduct of operations

272. *Principle: Operation of the plant is conducted by authorized personnel, according to strict administrative controls and observing procedural discipline.*

273. The plant is operated only by suitably trained and qualified staff, who consistently demonstrate in their activities the promotion of safe and reliable operation. They are aware of the significance for safety of their activities and of the consequences for safety of errors. Plant operations are carried out in an environment conducive to safety with staff discipline, the avoidance of inappropriate work patterns and attention to good housekeeping. Managers and supervisors reinforce desired behaviour and practices. The operators on duty monitor the status of the plant on a continuous basis to confirm that components and systems are performing satisfactorily or are in an appropriate state of readiness. They ensure that plant deficiencies and departures from required conditions or plant configurations are detected, and that prompt remedial action is taken. Warning alarms are investigated and required action taken. Unusual phenomena are investigated (such as noise or apparent changes in process or core performance) and appropriate action is taken if there is a danger to vital components or an unexplained response to controls of process or safety systems. Control room and plant routines include observing checklists, recording pertinent plant data, keeping up to date operating logs, passing on data and instructions in shift turnover, and regular walk-down of the plant during shift operations. Particular attention is paid to monitoring when the plant status is changed.

274. The plant is operated on the basis of a hierarchy of approved procedures subject to strict document control. Deviation from these procedures requires approval at a level appropriate to the significance of the changes for safety. Written procedures are kept current. Maintenance and surveillance of plant components and systems are subject to strong control, and maintenance activities are approved by authorized personnel. Plant modifications important for safety are pursued only under approved procedures. Plant configuration is maintained within the intent of the design and safety analysis by adherence to procedures that include strict reporting arrangements

for changes in configuration and reviews at appropriate intervals. Plant drawings and descriptions are kept up to date.

275. A formal communication system exists for the transmission of orders and for the transfer of information related to the reliable and safe operation of the plant. This system includes reliable and retrievable recording of instructions and information of possible importance, and of the fact that instructions and orders were received and understood.

276. Measures are enforced that ensure that operating and maintenance staff on duty are alert and mentally unimpaired. If any such personnel are found to be under the influence of alcohol or of consciousness altering drugs, disciplinary action is taken. Further alcohol or drug abuse is grounds for dismissal from positions of responsibility.

277. Special attention is given to physical features and administrative procedures to prevent unauthorized actions, whether intentional or unintentional, by plant personnel or others, that could jeopardize safety.

4.5.4. Training

278. *Principle: Programmes are established for training and retraining operations and maintenance, technical support, chemistry and radiation protection personnel to enable them to perform their duties safely and efficiently. Training is particularly intensive for control room staff, and includes the use of plant simulators.*

279. The training programme includes the identification of training requirements, the development of training specifications and materials, programme implementation and evaluation. Formal training of operators, maintenance, technical support, chemistry and radiation protection personnel, covers such key areas of technology as neutronics, thermal hydraulics and radiation protection, to the level necessary for the task to be performed. Operator training develops knowledge of the plant and its operation, both theoretically and practically. It includes thorough knowledge of the plant's layout, the locations of important components and systems, the locations and functions and effects of their controls, and the normal line-up of plant systems. Emphasis is placed on systems having safety significance. Trainees learn routines for normal operation of the plant, and the plant's response to the onset of faults that could cause damaging accidents if not counteracted. This aspect of training is aimed at improving diagnostic skills. Training covers lessons learned from operating

experience both locally and elsewhere. Operators learn both normal and emergency operating procedures. The operator training programme includes desk studies, use of simulators, on the job training and plant familiarization, leading to formal approval of operators (e.g. by licensing).

280. Through the training programmes, operators, maintenance, technical support, chemistry and radiation protection personnel are apprised of the principal results of any PSAs of the plant, showing the importance of plant systems in preventing plant damage or severe accidents. They are aware of the locations of all significant amounts of radioactive material in the plant, and understand the measures to prevent its dispersal. Most importantly, the training of operating staff emphasizes the importance of maintaining the plant within its operational limits and conditions. The consequences of violating limits are emphasized. The importance is stressed of maintaining subcriticality when the plant is not operating, of continued core cooling at all times, and of the controlled retention of all radioactive materials. Continuous training is provided at intervals to ensure that knowledge and understanding essential to safe and efficient plant operation are retained and refreshed, in particular for handling abnormal and accident conditions. Structured initial training and refresher training are given on a representative simulator. Team work is emphasized in operator training, particularly in simulator exercises on dealing with incidents and accidents.

281. Complementary training is provided to prepare staff for specialized duties required in the event of an accident. In judging the need for and extent of such training, standby arrangements and the availability of off-site services are taken into account. Specific training is provided for all staff members who have assignments under the emergency plans.

282. Training of maintenance staff goes beyond the teaching of basic task skills to emphasize the potential safety consequences of technical or procedural error. Training and qualification of maintenance staff reflects the realization that where there has been a record of plant operational unreliability and faulty, spurious and accidental activation of safety systems in the past, it has often been caused by errors in maintenance procedures and practices. Training of maintenance staff covers such incidents. Testing of maintenance staff examines their familiarity with these lessons. Training of technical support, chemistry, radiation protection and other staff recognizes the safety importance of their duties.

283. The training of senior operations and management staff emphasizes the special problems of managing a nuclear power plant, with the exceptional demand for safety and the need for familiarity with emergency procedures. The training also includes

discussion of operating experience and of the management/supervisor role in enforcing operational standards and practices.

4.5.5. Operational limits and conditions

284. *Principle: A set of operational limits and conditions is defined to identify safe boundaries for plant operation. Minimum requirements are also set for the availability of staff and equipment.*

285. As discussed in Section 4.2.2.1, a set of inviolable safety limits defines the extremes of the region of operating variables and conditions within which conservative analysis shows that the plant will not suffer undesirable effects or unacceptable damage. Operational limits for normal operation and trip points as necessary are set on key plant variables which are controlled by automatic systems. To ensure that anticipated transients do not lead to infringement of the safety limits, the operational limits and trip points are set conservatively on the basis of reliable analysis. Operational limits and conditions are defined for all the stages of commissioning, power operation, shutdown, shutting down, starting up, maintenance, testing and refuelling. Scheduled tests and inspections are performed to recalibrate instruments measuring and displaying the values of variables which have safety limits, and to check the correctness of trip points.

286. Additional conditions ensure that safety systems are either in operation or ready for use. These conditions are defined according to the reliability and the response expected of the systems. Minimum staffing requirements are also laid down, including, importantly, staffing requirements for the control room. These conditions may be temporarily suspended only for well justified testing or other special purposes, with compensating provisions and with prior safety analysis and approval at a level appropriate to the safety significance of the issue.

287. The original set of operational limits or conditions as well as any subsequent changes are subject to safety review and approval by the operating organization and the regulatory organization according to their safety significance. As a vital part of safety culture, it is essential that plant personnel understand the reasons for the safe limits of operation and the consequences of violation. Operational limits may not be infringed deliberately except in accordance with formal procedures that ensure both full recognition of the safety implications and provision of any necessary compensating factors.

4.5.6. Normal operating procedures

288. *Principle: Normal plant operation is controlled by detailed, validated and formally approved procedures.*

289. Plant operating procedures are based on plant design and safety analysis and validated by computer simulation, plant commissioning and the feedback of operating experience. They are presented in sufficient detail to permit the operators to perform plant operations without their further elaboration. From the safety standpoint, the procedures, if properly followed, ensure that the plant's operational limits or conditions are not exceeded and that the necessary safety related components, systems and structures are available. Specifications included in the procedures cover periodic testing, periodic calibration and periodic inspection of safety systems. Particular attention is given in these procedures to changes of operational states, low power operation, test conditions and occasions when parts of safety systems may be unavailable by intent. In the procedures for core loading and unloading, attention is given to avoiding unplanned criticality or other accidents that could occur. Operating procedures are revised only after approval in accordance with established procedures, and the documents that define the operating procedures are subject to managerial control in accordance with quality assurance procedures. Operators are trained on major revisions to operating procedures prior to their implementation. Special controls and procedures are implemented for special tests.

4.5.7. Emergency operating procedures

290. *Principle: Emergency operating procedures are established, documented and approved to provide a basis for suitable operator response to abnormal events.*

291. The engineered systems installed to take care of abnormal events within the design basis of the plant would be actuated automatically upon initiation of any such event. The operating staff are trained to take advantage of the period identified in the design as 'requiring no immediate operator action' to detect and identify the causes of the automatic response. Additional information conveyed to the operators by instruments and display systems would help them in deciding on action to prevent or mitigate plant damage. Also, emergency operating procedures are available for accidents taken into account in the design and for any accidents beyond the design basis that are considered to contribute significantly to risk. These procedures generally embody responses based on a diagnosis of the event occurring. If the event cannot be diagnosed in time, or if further evaluation of the event causes the initial diagnosis to be discarded, the emergency operating procedures define responses to the symptoms observed, from knowledge less of the nature of the event itself than of the plant conditions arising as deduced from these symptoms. Actions based on symptom oriented procedures are designed to restore critical safety functions. The emergency operating procedures also facilitate long term recovery from an accident and limitation of its radiological consequences for the plant personnel and the public. These procedures are part of the training programme of operating and radiation protection

staff. They include ultimate emergency procedures to facilitate management of severe accidents.

4.5.8. Radiation protection procedures

292. *Principle: The radiation protection staff of the operating organization establish written procedures for the control, guidance and protection of personnel, carry out routine monitoring of in-plant radiological conditions, monitor the exposure of plant personnel to radiation, and also monitor releases of radioactive effluents.*

293. Specialist staff under the control of the plant management provide a comprehensive radiation protection service. This covers personnel monitoring and dose records, measurement of radiation levels in key areas, measurement of radiological effluents from the plant, monitoring the cleanup of contamination and the preparation of radioactive waste for storage or disposal, and supervision and monitoring of the entry of personnel into radiation areas. The radiation monitoring staff also have assigned responsibilities in the event of emergencies. Following appropriate training members of the operating staff may assume some of these radiation protection duties. Written procedures are issued as necessary to cover radiation protection functions.

294. The radiation protection staff have direct access to senior plant management as necessary to advise on and secure the observance of radiation protection procedures. Individual workers are motivated by the management and by the radiation protection staff to control their own dose and exposure and to keep their own routine radiation exposures as low as practicable.

295. Special equipment is provided to assist in radiation protection for some in-plant maintenance and surveillance activities. This is especially important for safety related systems: the possibility of personnel exposures must not be allowed to reduce the care taken of the safety systems. Workers who must perform tasks under conditions of high dose rates are trained in the use of special equipment and with mockups of the systems to be serviced.

4.5.9. Engineering and technical support of operations

296. *Principle: Engineering and technical support, competent in all disciplines important for safety, is available throughout the lifetime of the plant.*

297. The continuing safe operation of a nuclear power plant requires the support of an engineering organization, which can be called on as required to assist with plant

modifications, repairs and special tests, and to provide analytical support as necessary for the safety of the plant. This resource may be provided within the operating organization itself, or it may be available from the plant suppliers or specialist groups. It is the responsibility of the operating organization to ensure that the resources required are available.

298. Issues relating to the continued availability of knowledgeable and competent engineers in the nuclear power industry are addressed. These include the potential loss of staff owing to competition for engineering expertise from other industrial sectors and the need to consider the effects of staff reductions and loss of expertise as a result of retirement and the closure of nuclear power plants. These factors all lead to the loss of key and experienced personnel and their knowledge about the nuclear industry. As noted under para. 121, it is important to define the necessary complement of core skills to ensure safety and to preserve it over the years.

4.5.10. Feedback of operating experience

299. *Principle: Plant management institutes measures to ensure that events significant for safety are detected and evaluated in depth, and that any necessary corrective measures are taken promptly and information on them is disseminated. The plant management has access to operational experience relevant to plant safety from other nuclear power plants around the world.*

300. The importance for safety of an effective programme for the feedback of operational experience has been stressed in the fundamental principle in Section 3.3.8 related to operating experience and safety research. The plant manager reports promptly to the top management of the operating organization and to the regulatory organization any abnormal occurrence of significance for safety so that its implications can be properly analysed, the root cause identified and the information communicated to other nuclear power plants. Good operating practices, when judged to have potentially significant benefits for safety, are also reported in an appropriate way.

301. Independently of the generic analyses which may follow an abnormal and potentially damaging occurrence, the plant manager takes the necessary measures to prevent the recurrence of similar events at the plant, or at least takes measures to ensure that its repetition would not lead to an accident. Any corresponding modification, of either hardware or procedures, is made only after a safety assessment shows that the change will not jeopardize plant safety and after measures are taken to ensure quality appropriate to the safety significance.

302. Plant management personnel use the safety information gained from the operating experience of other nuclear power plants as a source of lessons applicable at their own plants to improve plant safety.

303. Regular maintenance and surveillance by the plant staff or by personnel at other similar plants is a source of information on safety related systems and components. Pooling of information through owners' groups is helpful in this way. The information is compiled and processed, and submitted to trend analysis either at the plant or in co-operation with other similar plants to identify incipient faults or degradation, such as those due to ageing. Measures are taken to prevent failures or to reverse adverse trends revealed by the processing of such information.

304. Plant management is aware of the safety significance of risk assessment for the plant, and co-operates in the performance of risk assessments by contributing the data needed.

4.5.11. Maintenance, testing and inspection

305. *Principle: Safety related structures, components and systems are the subject of regular preventive and predictive maintenance, inspection, testing and servicing when needed, to ensure that they remain capable of meeting their design requirements throughout the lifetime of the plant. Such activities are carried out in accordance with written procedures supported by quality assurance measures.*

306. When a nuclear plant goes into operation, regular and scheduled preventive maintenance and surveillance are begun to ensure that structures, components and systems continue to operate as desired, with their capability to meet the design objectives undiminished by ageing, wear or other deterioration. Trend analysis (e.g. of wear and vibration) is used to improve the effectiveness of the programme. These activities play an essential role in preventing failures in subsequent operation. Deficiencies thus detected are corrected in a timely fashion. Conformity to written and approved procedures is required where important safety related systems are concerned. The procedures ensure that the control room staff remain informed of the status of any such work under way.

307. An approved schedule of inspection is followed, based on assessment at the design stage and testing during commissioning, and it is modified according to experience. Special attention is devoted to the surveillance of the multibarrier system, in particular the primary coolant boundary, which is subject to neutron irradiation,

thermal and pressure cycling and ageing as a normal consequence of use. Where necessary, use is made of tests performed on removable samples that have been exposed to service conditions. Maintenance activities are planned and executed in recognition of the importance of safety related systems and bearing in mind the possibility that imprudent maintenance practices can reduce the potential benefit of defence in depth.

308. A major component of reassurance that essential safety functions are available when called upon is the periodic functional testing of safety systems. The frequency, extent and nature of such testing is determined by the reliability required, and by the practical capability to simulate the function. In circumstances where full demonstration is not possible in periodic testing, testing of individual components and partial systems is performed to demonstrate the reliability of the safety function.

309. Since incorrectly performed maintenance and testing can cause problems, consideration is given to the optimization of such maintenance features as the frequency and extent of preventive maintenance, and to instructions from equipment manufacturers, operating experience and trend analysis, training and procedures.

310. Radiation exposure of personnel during maintenance is controlled and limited by means of work plans, rehearsals and monitoring for radiation control.

311. Achieving high safety standards in maintenance requires that key maintenance personnel be aware of the safety aspects of the tasks they are performing. Maintenance workers are therefore carefully prepared for their duties to reduce the possibility of human error in these cases. Maintenance sometimes requires disabling particular safety systems. This is only permitted if carefully written, tested and approved procedures are followed and compensatory measures taken, in accordance with Section 4.5.5. The associated risk is assessed and found acceptable. Maintenance staff are trained on the particular equipment that they service. When work is performed on equipment by individuals who are not members of the trained and qualified plant staff, it is supervised and checked by on-site personnel who have been fully trained in the performance and significance for safety of the work and who are themselves qualified to perform it.

4.5.12. Quality assurance in operation

312. *Principle: An operational quality assurance programme is established by the operating organization to assist in ensuring satisfactory performance in all plant activities important to plant safety.*

313. This specific principle fulfils the fundamental principle on quality assurance (Section 3.3.2) for the area of operations. The operational quality assurance programme supports the line managers who are responsible for the quality of work performed, including the plant manager who has responsibility for the safety of the entire plant.

4.6. ACCIDENT MANAGEMENT

314. 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, after conditions have come to exceed the design of the plant but 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.

315. 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.

316. 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.

317. 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.

4.6.1. Strategy for accident management

318. *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.*

319. Analysis is made of accidents beyond the design basis that have potential for severe core degradation and failure of barriers preventing 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.

320. Continued analysis of severe accidents and additional research and development tests to simulate them are increasing the available knowledge of severe accident behaviour. A typical example is the large international effort to carry out experimental and analytical studies of the presence of water on the outside surface of the pressure vessel (of a pressurized water reactor), in order to establish the cooling effectiveness as a function of vessel size. Such activities lead to new physical measures and/or extend the guidance provided for severe accident management.

321. As the severity of an accident increases and its likelihood of occurrence decreases, the measures to be taken become less certain and more difficult to specify because they depend upon plant specific characteristics. Plant design layout, capability, location and redundancy of plant emergency systems, availability of auxiliary heat sinks and other features of the balance of plant determine the success or failure of a prescribed strategy for severe accident management. Similarly, the ability of the containment to withstand a potential overpressure, the elevation of the reactor pressure vessel, the geometry and size of the reactor cavity, and the geometry of sumps have a role in strategic decisions to preserve containment integrity. These factors are taken into account in extending the guidance for severe accident management.

322. In future plants, the objectives of paras 25 and 27 will be applied to the prevention and mitigation of severe accidents and they will influence the degree and scope of accident management for such plants.

4.6.2. Training and procedures for accident management

323. *Principle: Nuclear plant staff are trained and retrained in the procedures to follow if an accident occurs that exceeds the design basis of the plant.*

324. The members of the operating staff are made familiar with the features of the analysis described in the principle in Section 4.6.1 as part of their training programme. The procedures used for accident management are the plant emergency operating procedures, including those parts dealing with ultimate emergencies. Ultimate emergency procedures are general in nature and serve to remind the operators of the capabilities of the plant for mitigating the course and consequences of severe accidents. The ultimate procedures are also flexible so that they can be adjusted to the uncertainties of more extreme accidents. Training and testing of plant operators ensure their familiarity with the symptoms of accidents beyond the design basis and the procedures for accident management. Simulators are indispensable training tools. However, they must be able to represent correctly the way in which an accident would evolve, at least up to the occurrence of extensive fuel damage. Personnel assignments are defined for a specialist team to advise operators in the event of an accident that exceeds the design basis. This team includes personnel who are familiar with the severe accident analysis for the plant.

325. Since existing training simulators do not tend to simulate severe core damage, the training for severe accidents concentrates on plant walk throughs, classes on the associated phenomena and the strategies and/or guidance proposed for dealing with their hazards and risks.

4.6.3. Engineered features for accident management

326. *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 an accident beyond the design basis.*

327. 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 activity in primary coolant.

328. 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, concentrated on restoring and maintaining the core cooling and the confinement functions. These changes include the installation of filtered vents, hydrogen igniters and passive autocatalytic recombiners in some cases (see Table II).

4.7. DECOMMISSIONING

329. *Principle: Consideration is given in design and plant operations to facilitating eventual decommissioning and waste management. After the end of operations and the removal of spent fuel from the plant, radiation hazards are managed so as to protect the health of workers and the public during plant decommissioning.*

330. A plant that is shut down remains an operating plant until its decommissioning and is subject to the normal control processes and procedures to ensure safety. In particular, the principles that govern a plant in a shutdown state apply (see Section 4.2.3.14). After the end of operations and the removal of spent fuel from the plant, a significant radiation hazard remains which must be managed to protect the health of workers and the public. The removal of plant equipment and its decontamination can be facilitated if appropriate consideration is given at the design stage to decommissioning and disposal of the wastes arising from decommissioning. Examples include using materials to minimize residual activity (on time-scales relevant for decommissioning) and to minimize the transport of radioactive material, thus minimizing the activation of long lived radionuclides, particularly those that are easily mobilized such as ^{36}Cl and ^{14}C, and designing for ease of removal. Such factors are now being taken into account during design for other reasons, such as ease of maintenance, replacement of components and minimization of worker doses. However, the implications of design choices and design changes for eventual decommissioning and

waste disposal will also be considered in design audits during the design process. Similarly, during operations and maintenance, due attention is paid to the fact that the plant will ultimately be decommissioned. Thus, for example, good records are kept of contamination control and contamination incidents. Such records will facilitate the characterization and segregation of waste streams arising from decommissioning for disposal and facilitate planning for radiation protection during decommissioning. Finally, minimizing waste production as far as is reasonably practical during decommissioning is another means of limiting the volume of waste for disposal.

4.8. EMERGENCY PREPAREDNESS

331. 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.

332. In 1986, the Convention on Early Notification of a Nuclear Accident entered into force. A State which is party to this Convention, and which suffers a nuclear accident entailing an actual or potential release of radioactive materials that could result in transboundary effects significant for radiological safety in another State, is required to notify, either directly or through the IAEA, those States that may be so affected. The ability to respond in conformity with this Convention is an essential aspect of emergency preparedness.

4.8.1. Emergency plans

333. *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, significant 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.*

334. 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 and they are updated based upon experience. The tests are reviewed and witnessed, as appropriate by the regulator. 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.

335. 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 the 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 geographical 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.

4.8.2. Emergency response facilities

336. *Principle: A permanently equipped emergency centre is available off the site for emergency response. On the site, a similar centre is provided for directing emergency activities within the plant and communicating with the off-site emergency organization.*

337. 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.

338. 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 emergency centre. Protective equipment is provided for emergency personnel.

4.8.3. Assessment of accident consequences and radiological monitoring

339. *Principle: Means are available to the responsible site staff to be used in early prediction of the extent and significance of any release of radioactive materials if an accident were to occur, for rapid and continuous assessment of the radiological situation, and for determining the need for protective measures.*

340. Assessment methods are available to plant management that allow the prediction of the doses or potential doses that could result from an actual or a possible release of radioactive materials. On-site monitoring is used to characterize the source term and release rates. For off-site data, facilities are provided in the form of mobile radiological monitoring teams and in many cases a network of fixed monitoring stations. Facilities are also available for rapid analysis and interpretation of the levels and nature of activity in large numbers of samples.

341. Decisions on the need for protective measures are made on the basis of recommendations from the operating organization and intervention levels or guidelines set by competent national and international bodies. These authorities must receive relevant information speedily and be competent to make the judgements that may be necessary.

Appendix

ILLUSTRATION OF DEFENCE IN DEPTH

A.1. The use of defence in depth in nuclear power plant design and operation is the subject of three fundamental principles (Sections 3.2.1 to 3.2.3). Defence in depth provides the basic framework for most of nuclear power plant safety. The concept has been refined and strengthened through years of application. All safety analysis for nuclear power plants, both deterministic and probabilistic, revolves around evaluation of the performance of the plant subject to different modes of defence in depth, and the reliability of these modes.

A.2. There are many such modes of protection of people and the environment against the possibility and the effects of accidents at nuclear power plants, varying according to the challenges to the plant arising from different abnormal events. The modes can be classified according to the severity of the challenge, measured in terms of extraordinary demands on equipment and staff performance or in terms of any resultant plant damage.

A.3. The concept of defence in depth as applied to existing nuclear power plants is illustrated in Fig. 3. The first line covers the strategy for defence in depth, which is twofold: first, accident prevention and second, accident mitigation. The next row in Fig. 3 describes the five operational states of a nuclear power plant:

—State 1: Normal operation including shutdown state,
—State 2: Anticipated operational occurrences,
—State 3: Complex operational occurrences and design basis accidents,
—State 4: Severe accidents,
—State 5: Post-severe accident situations.

A.4. The operational states are ordered with severity increasing from left to right. The classes start with states of normal operation that pose no challenge to the safety of the plant. The challenges arising from anticipated operational occurrences would be countered in a straightforward manner by the appropriate response of normal plant systems. More severe challenges would accompany the third category of operating events, bounded by design basis accidents. For these, engineered safety features would be required to supplement the protection afforded by normal plant systems. At the extreme of the scale of severity are accidents beyond the design basis, for which management measures are required to limit the consequences of damage.

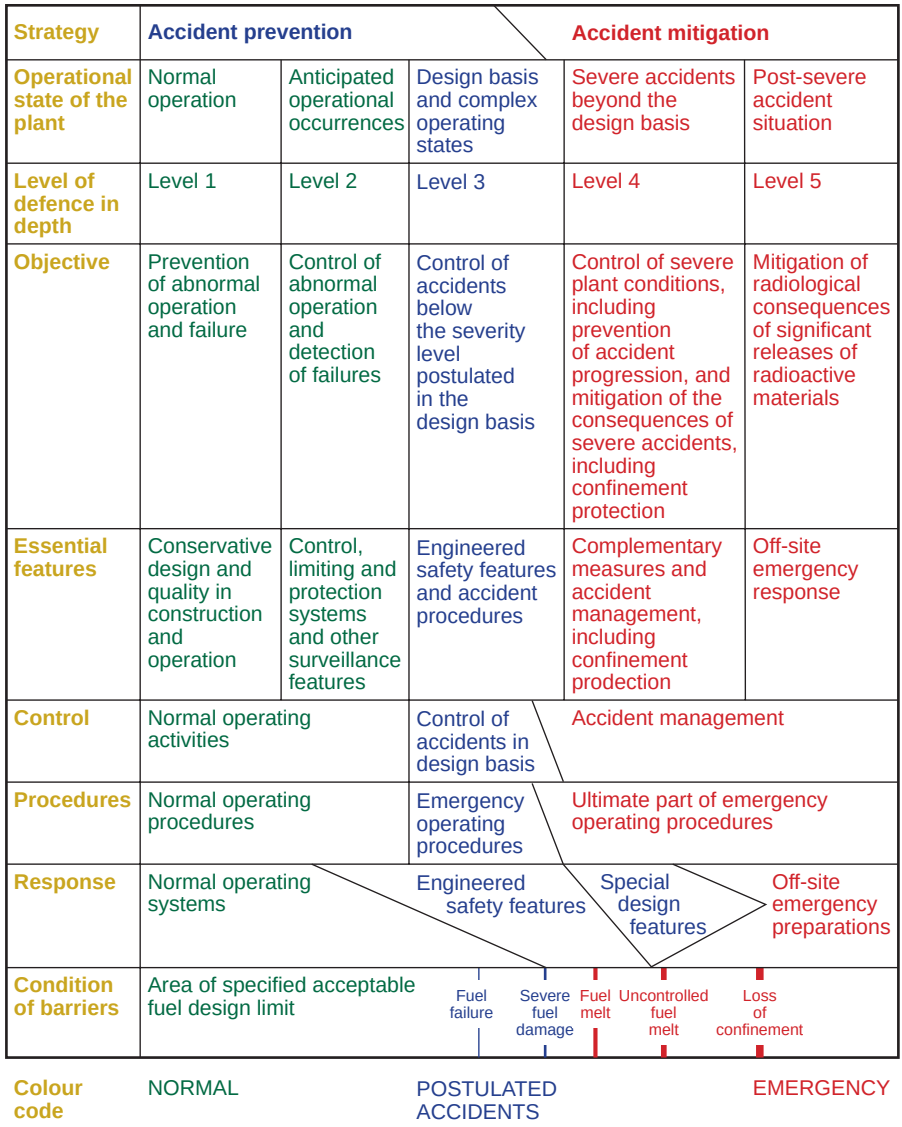

FIG. 3. Overview of defence in depth.

A.5. The lengths of the boxes in the row labelled ‘states’ are not intended to indicate any scale of probability for the states listed in them. If a representative probability scale were shown, only normal operational events would have a probability high enough to be visible on the diagram. Nevertheless, this graphic display provides a simple co-ordinate for the defence in depth required for each state.

A.6. The third row in Fig. 3 designates the level of defence in depth associated with a particular operational state. The major objectives fulfilled through the application of defence in depth principles, for each level, are brought out in the fourth row. One of the important tenets of the defence in depth approach is the minimization of the potential for excursions to more severe operational states from the current operational state. Measures adopted to effect this include provision of adequate design margins, utilization of self-limiting characteristics, operation in a fault tolerant stable domain, reliance on passive safety features and adequate protection from external events. The essential features provided to meet those objectives are indicated in the fifth row in Fig. 3.

A.7. The sixth row of the diagram is labelled ‘control’. This shows that normal plant actions satisfy requirements for events encountered in normal operation or those in anticipated operational occurrences. A separate set of measures would be required for complex operating events that have much lower probabilities of occurrence. These begin to include accident management at the upper end of the range, including measures to ensure the retention of fission products and other radioactive materials in cases in which some damage to fuel might have occurred. For severe accidents beyond the design basis, accident and severe accident management would come into full play, using normal plant systems, engineered safety features, special design features and off-site emergency measures in mitigation of the extent and effects of the accident.

A.8. The other rows show, respectively, how, procedures, response and the integrity of barriers would depend on the class of events and their severity. The entire picture in each case is provided by the vertical axis through the event at its indicated severity.

A.9. For instance, an accident beyond the design basis with a severity at the lower end of the range might generate damage to the reactor core that precludes reuse of the fuel elements, perhaps with extensive distortion and failure of cladding, but with no melting of the fuel itself. Such an accident would release some radioactive materials into the primary coolant circuit, with consequences beyond those for which detailed provisions are made in emergency operating procedures. The less prescriptive and more indicative ultimate operating procedures would then be used by the operating staff to limit the extent of the release of radioactive materials from the primary coolant circuit and to restore the plant to a controlled and cooled state. These procedures would make use of normal plant systems, engineered safety features and special design features of the plant. Mitigation at this level of severity would be so successful that there would be no appreciable release of radioactive material beyond the confinement, so no off-site emergency measures would be called on.

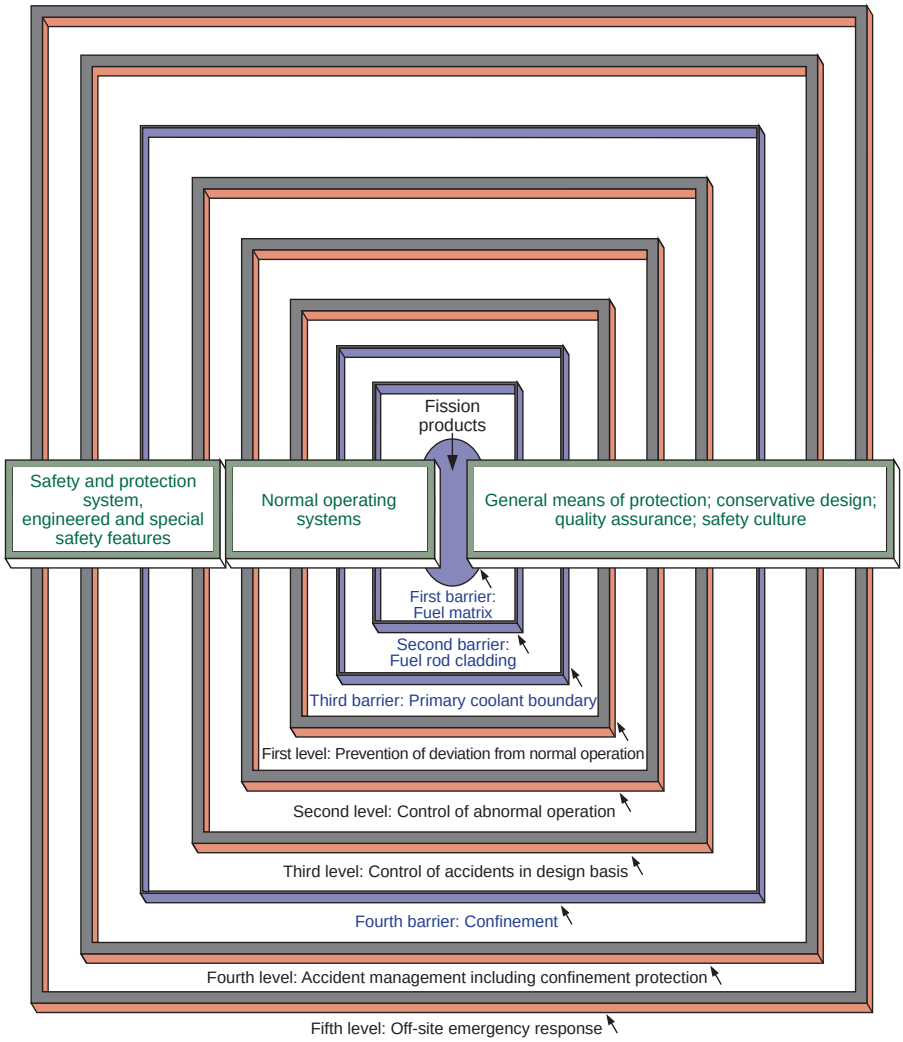

FIG. 4. The relation between physical barriers and levels of protection in defence in depth.

A.10. A second, complementary view of defence in depth is given in Fig. 4, which shows the relation between the physical barriers and the levels of protection that together constitute defence in depth. This shows the interaction among these components as a series of obstacles between the radioactive material in its normal state and any harm to the public or the environment as a result of its dispersal due to an accident.

A.11. The figure shows radioactive material at the centre. A first level of protection in defence in depth is a combination of conservative design, quality assurance, surveillance activities and a general safety culture that strengthens each of the successive obstacles to the release of radioactive materials.

A.12. The first three physical barriers are the fuel matrix, the fuel cladding and the boundary of the primary coolant system. All nuclear power plants now operating or under consideration have all these barriers; some gas cooled reactors also have another barrier in the form of a graphite moderator in which fuel particles with a graphite or ceramic coating are embedded.

A.13. The second level of defence in depth is control of operation, including response to abnormal operation or to any indication of system failure. This level of protection is provided to ensure the continued integrity of the first three barriers. Together, these constitute the normal operating systems and barriers.

A.14. A third level of protection is afforded by those engineered safety features and protective systems that are provided to prevent the evolution of failures of equipment and personnel into design basis accidents, and design basis accidents into severe accidents, and also to retain radioactive materials within the confinement.

A.15. The confinement is a fourth barrier which is provided unless it has been shown that the function is provided by other means.

A.16. A fourth level of protection comprises measures that include accident and severe accident management, directed to preserving the integrity of the confinement.

A.17. The fifth level is that of off-site emergency response, aimed at mitigating the effects of the release of radioactive materials to the external environment.

A.18. Figures 3 and 4 are primarily applicable to existing plants. They will change for future plants because the likelihood and consequences of barrier failures will be reduced. At this time, the design details of future plants are not defined and equivalent figures cannot be generated.

INDEX OF KEYWORDS
(by paragraph number)

MEMBERS OF THE INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

Abagian, A.A.

Allan, C.J.

Baer, A.

Birkhofer, A. *(Chairperson)*

Chang, S.H.

Gonzalez-Gomez, E.

Kakodkar, A.

Levy, S.

Ma, Y.

Matsuura, S.

Quéniart, D.

Sajaroff, P.

Taylor, R.H.

Víta, J.

Winkler, B.C.

INSAG WORKING GROUP

Allan, C.J.

Birkhofer, A.

Kakodkar, A.

Levy, S. *(Chairperson)*

Quéniart, D.

Sajaroff, P.

Taylor, R.H.

INVITED EXPERTS

Frescura, G.

Madden, V.

IAEA STAFF

Höhn, J.

Zhong, W. *(Scientific Secretary)*

W. Zhong of the IAEA Secretariat is responsible for matters relating to INSAG in the Department of Nuclear Safety.

LIST OF PARTICIPANTS FOR THE ORIGINAL VERSION OF 75-INSAG-3

MEMBERS OF THE INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

Birkhofer, A.

Chung, K.T.

Dai, C.

Edmondson, B.

Kouts, H.J.C.

Lepecki, W.

Meneley, D.

Nozawa, M.

Rabold, H.

Sidorenko, V.A.

Tanguy, P.

Veeraraghavan, N.

Vuorinen, A.P. *(Chairperson)*

INSAG WORKING GROUP

Edmondson, B.

Kouts, H.J.C. (*Chairperson*)

Meneley, D.

Vuorinen, A.P.

WORKING GROUP EXPERTS

Domaratzki, Z.

Guimbail, H.

Harrison, J.R.

Herttrich, P.M.

Högberg, L. (*Co-chairperson*)

Isaev, A.

Krüger, F.W.

Mattson, R.J. (*Chairperson*)

Prêtre, S.

Soda, K.

INVITED EXPERTS

Bukrinski, A.M.

Mattson, R.J.

IAEA STAFF

Almeida, C.

Bliselius, P.

Collins, H.

Fischer, J.

Franzen, L.F.

Giuliani, P.

Haydin, M.

Iansiti, E. (*Scientific Secretary for INSAG)*

Jankowski, M.

Karbassioun, A.

Kenneke, A.

Konstantinov, L.V.

Laaksonen, J.T.

Lederman, L.

Niehaus, F.

Novak, S.

Palabrica, R.

Rosen, M.

Salo, A.

Thomas, B.

Tolstykh, V.D.

Yaremy, E.

PUBLICATIONS OF THE INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

75-INSAG-1	Summary report on the post-accident review meeting on the Chernobyl accident	1986
75-INSAG-2	Radionuclide source terms from severe accidents to nuclear power plants with light water reactors	1987
75-INSAG-3	Basic safety principles for nuclear power plants	1988
75-INSAG-4	Safety culture	1991
75-INSAG-5	The safety of nuclear power	1992
75-INSAG-6	Probabilistic safety assessment	1992
75-INSAG-7	The Chernobyl accident: Updating of INSAG-1	1993
INSAG-8	A common basis for judging the safety of nuclear power plants built to earlier standards	1995
INSAG-9	Potential exposure in nuclear safety	1995
INSAG-10	Defence in depth in nuclear safety	1996
INSAG-11	The safe management of sources of radiation: Principles and strategies	1999