

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

AFGHANISTAN	GUATEMALA	PARAGUAY
ALBANIA	HAITI	PERU
ALGERIA	HOLY SEE	PHILIPPINES
ARGENTINA	HUNGARY	POLAND
AUSTRALIA	ICELAND	PORTUGAL
AUSTRIA	INDIA	QATAR
BANGLADESH	INDONESIA	ROMANIA
BELGIUM	IRAN, ISLAMIC REPUBLIC OF	SAUDI ARABIA
BOLIVIA	IRAQ	SENEGAL
BRAZIL	IRELAND	SIERRA LEONE
BULGARIA	ISRAEL	SINGAPORE
BURMA	ITALY	SOUTH AFRICA
BYELORUSSIAN SOVIET SOCIALIST REPUBLIC	JAMAICA	SPAIN
CAMEROON	JAPAN	SRI LANKA
CANADA	JORDAN	SUDAN
CHILE	KENYA	SWEDEN
CHINA	KOREA, REPUBLIC OF	SWITZERLAND
COLOMBIA	KUWAIT	SYRIAN ARAB REPUBLIC
COSTA RICA	LEBANON	THAILAND
COTE D'IVOIRE	LIBERIA	TUNISIA
CUBA	LIBYAN ARAB JAMAHIRIYA	TURKEY
CYPRUS	LIECHTENSTEIN	UGANDA
CZECHOSLOVAKIA	LUXEMBOURG	UKRAINIAN SOVIET SOCIALIST REPUBLIC
DEMOCRATIC KAMPUCHEA	MADAGASCAR	UNION OF SOVIET SOCIALIST REPUBLICS
DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA	MALAYSIA	UNITED ARAB EMIRATES
DENMARK	MALI	UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
DOMINICAN REPUBLIC	MAURITIUS	UNITED REPUBLIC OF TANZANIA
ECUADOR	MEXICO	UNITED STATES OF AMERICA
EGYPT	MONACO	URUGUAY
EL SALVADOR	MONGOLIA	VENEZUELA
ETHIOPIA	MOROCCO	VIET NAM
FINLAND	NAMIBIA	YUGOSLAVIA
FRANCE	NETHERLANDS	ZAMBIA
GABON	NEW ZEALAND	ZIMBABWE
GERMAN DEMOCRATIC REPUBLIC	NICARAGUA	
GERMANY, FEDERAL REPUBLIC OF	NIGER	
GHANA	NIGERIA	
GREECE	NORWAY	
	PAKISTAN	
	PANAMA	

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

© IAEA, 1988

Permission to reproduce or translate the information contained in this publication may be obtained by writing to the International Atomic Energy Agency, Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria.

Printed by the IAEA in Austria  
March 1988

SAFETY SERIES No.75-INSAG-3

# BASIC SAFETY PRINCIPLES FOR NUCLEAR POWER PLANTS

A report by the  
International Nuclear Safety Advisory Group

U. S. NUCLEAR REGULATORY COMMISSION  
~~LIBRARY NICHOLSON LANE BRANCH~~  
WASHINGTON, D.C. 20555

INTERNATIONAL ATOMIC ENERGY AGENCY  
VIENNA, 1988

U. S. NUCLEAR REGULATORY COMM

## CONTENTS

PREAMBLE .....	1
1. INTRODUCTION .....	3
1.1. STRUCTURE OF THE REPORT .....	5
2. OBJECTIVES .....	6
2.1. GENERAL NUCLEAR SAFETY OBJECTIVE .....	6
2.2. RADIATION PROTECTION OBJECTIVE .....	7
2.3. TECHNICAL SAFETY OBJECTIVE .....	8
3. FUNDAMENTAL PRINCIPLES .....	10
3.1. MANAGEMENT RESPONSIBILITIES .....	10
3.1.1. Safety culture .....	10
3.1.2. Responsibility of the operating organization .....	11
3.1.3. Regulatory control and independent verification .....	12
3.2. STRATEGY OF DEFENCE IN DEPTH .....	13
3.2.1. Defence in depth .....	13
3.2.2. Accident prevention .....	15
3.2.3. Accident mitigation .....	16
3.3. GENERAL TECHNICAL PRINCIPLES .....	16
3.3.1. Proven engineering practices .....	16
3.3.2. Quality assurance .....	17
3.3.3. Human factors .....	19
3.3.4. Safety assessment and verification .....	20
3.3.5. Radiation protection .....	21
3.3.6. Operating experience and safety research .....	22
4. SPECIFIC PRINCIPLES .....	23
4.1. SITING .....	23
4.1.1. External factors affecting the plant .....	23
4.1.2. Radiological impact on the public and the local environment ...	26
4.1.3. Feasibility of emergency plans .....	26
4.1.4. Ultimate heat sink provisions .....	26

4.2. DESIGN .....	27
4.2.1. Design process .....	28
4.2.1.1. Design management .....	28
4.2.1.2. Proven technology .....	29
4.2.1.3. General basis for design .....	29
4.2.2.. General features .....	30
4.2.2.1. Plant process control systems .....	30
4.2.2.2. Automatic safety systems .....	31
4.2.2.3. Reliability targets .....	32
4.2.2.4. Dependent failures .....	32
4.2.2.5. Equipment qualification .....	34
4.2.2.6. Inspectability of safety equipment .....	34
4.2.2.7. Radiation protection in design .....	35
4.2.3. Specific features .....	35
4.2.3.1. Protection against power transient accidents .....	36
4.2.3.2. Reactor core integrity .....	37
4.2.3.3. Automatic shutdown systems .....	38
4.2.3.4. Normal heat removal .....	38
4.2.3.5. Emergency heat removal .....	39
4.2.3.6. Reactor coolant system integrity .....	39
4.2.3.7. Confinement of radioactive material .....	41
4.2.3.8. Protection of confinement structure .....	42
4.2.3.9. Monitoring of plant safety status .....	43
4.2.3.10. Preservation of control capability .....	43
4.2.3.11. Station blackout .....	44
4.2.3.12. Control of accidents within the design basis .....	45
4.3. MANUFACTURING AND CONSTRUCTION .....	45
4.3.1. Safety evaluation of design .....	45
4.3.2. Achievement of quality .....	46
4.4. COMMISSIONING .....	47
4.4.1. Verification of design and construction .....	47
4.4.2. Validation of operating and functional test procedures .....	48
4.4.3. Collecting baseline data .....	48
4.4.4. Pre-operational plant adjustments .....	48
4.5. OPERATION .....	49
4.5.1. Organization, responsibilities and staffing .....	49
4.5.2. Safety review procedures .....	50
4.5.3. Conduct of operations .....	50
4.5.4. Training .....	52
4.5.5. Operational limits and conditions .....	53
4.5.6. Normal operating procedures .....	54

4.5.7. Emergency operating procedures .....	55
4.5.8. Radiation protection procedures .....	55
4.5.9. Engineering and technical support of operations .....	56
4.5.10. Feedback of operating experience .....	56
4.5.11. Maintenance, testing and inspection .....	57
4.5.12. Quality assurance in operation .....	59
4.6. ACCIDENT MANAGEMENT .....	59
4.6.1. Strategy for accident management .....	60
4.6.2. Training and procedures for accident management .....	60
4.6.3. Engineered features for accident management .....	61
4.7. EMERGENCY PREPAREDNESS .....	61
4.7.1. Emergency plans .....	62
4.7.2. Emergency response facilities .....	62
4.7.3. Assessment of accident consequences and radiological monitoring .....	63
Appendix: ILLUSTRATION OF DEFENCE IN DEPTH .....	64
INDEX OF KEYWORDS .....	69
LIST OF PARTICIPANTS .....	73

## PREAMBLE

INSAG here provides a self-standing document on safety principles for electricity generating nuclear power plants<sup>1</sup>. This document has been developed because:

- the means for assuring 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 have emphasized the need for common safety principles for all countries and all types of nuclear power plants.

INSAG has prepared this document 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 implemented, 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.

---

<sup>1</sup> Although this document 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.



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 is unfamiliar to the public. It does not jeopardize safety, as is often believed to be the case; it is the means by which safety is achieved. The objectives and principles set out in this document 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 other 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 document will not only contribute to achieving the necessary high degree of safety, but will also contribute to more efficient and more economic generation of electricity.

In the past there have been some instances of severe core damage to nuclear power plants. The causes were very particular to specific features of design and 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, operator training, and all related activities. This pervasive safety thinking is a key element in the 'safety culture' that is emphasized strongly in this document.

## 1. INTRODUCTION

1. Nuclear power plant safety requires a continuing quest for excellence. All individuals concerned should constantly 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 can 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. 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 in this review 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 document.

Objectives	General nuclear safety objective	Radiation protection objective	Technical safety objective		
Fundamental management principles	Safety culture	Responsibility of operating organization	Regulatory control and verification		
Defence in depth principles	Defence in depth	Accident prevention	Accident mitigation		
General technical principles	Proven engineering practices	Quality assurance	Human factors	Safety assessment and verification	Radiation protection
					Operating experience and safety research
Specific principles	Siting	Design	Manufacturing and construction	Commissioning	Operation
					Accident management
					Emergency preparedness

FIG. 1. INSAG safety objectives and principles for nuclear power plants.

7. However, some future types of nuclear power plants may achieve the intent of some of the principles presented in this document by special inherent features making the principle 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

8. This report is structured around three overriding safety objectives and a set of twelve fundamental safety principles (three related to safety management, three related to defence in depth, and six 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 document. 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 security 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 document.

11. *Note finally and importantly that throughout the document 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 document seeks to promote.*

## 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 hazards that attend any industrial endeavour. The protection system is effective as stated in the objective if it prevents significant addition either to the risk to health or to the risk of other damage to which individuals, society and the environment are exposed as a consequence of industrial activity already accepted. In this application, risk is defined as the arithmetic product of the probability of an accident or an event and the adverse effect it would produce. These health risks are to be estimated without taking into account the countervailing and substantial benefits which the nuclear and industrial activities bestow, both in better health and in other ways important to modern civilization. When the objective is fulfilled, the level of risk due to nuclear power plants does not exceed that due to competing energy sources, and is generally lower. If another means of electricity generation is replaced by a nuclear plant, the total risk will generally be reduced. The comparison of risks due to nuclear plants with other industrial risks to which people and the environment are exposed makes it necessary to use calculational models in risk analysis. To make full use of these techniques and to support implementation of this general nuclear safety objective, it is important that quantitative targets, 'safety goals', are formulated.

15. It is recognized that although the interests of society require protection against the harmful effects of radiation, they are not solely concerned with the radiological

safety of people and the avoidance of contamination of the environment. The protection of the resources invested in the plant is of high societal importance and demands attention to all the safety issues with which this report is concerned. However, the main focus of this document 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 kept as low as reasonably achievable and below prescribed limits, and to ensure mitigation of the extent of radiation exposures due to accidents.*

17. Radiation protection is provided in nuclear power plants under normal conditions and separate measures would be available under accident circumstances. For planned plant operating conditions and anticipated operational occurrences, compliance with radiation protection standards based on ICRP recommendations<sup>2</sup> ensures appropriate radiation protection. That is, the ICRP's system of dose limitation provides appropriate protection for planned situations anticipated to occur once or more in the lifetime of a plant.

18. The aforementioned radiation protection standards have been developed to prevent harmful effects of ionizing radiation by keeping exposures sufficiently low that non-stochastic effects are precluded and the probability of stochastic effects is limited to levels deemed 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, safety provisions in the plant are planned and countermeasures outside the plant are prepared to mitigate harm to individuals, populations and the environment.

<sup>2</sup> For example INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Standards for Radiation Protection (1982 edn), Safety Series No. 9, IAEA, Vienna (1982).

### 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.

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.

22. Attention is also directed to accidents of very low likelihood but more severe 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 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. In the safety technology of nuclear power, risk is defined (as in Section 2.1) as the product of the likelihood of occurrence of an accident and its potential radiological consequences. 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.

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

### 3. FUNDAMENTAL PRINCIPLES

26. 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

27. 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

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

29. 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 and communication 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.

30. 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 prevention of complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters.

##### 3.1.2. Responsibility of the operating organization

31. *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, constructors and regulators.*

32. 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.

33. The operating organization also has responsibilities in certain areas where its control is less direct. 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.

34. 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

35. *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.*

36. 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 safety assessments;
- 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 3.3.6; and
- dissemination of safety information (also discussed in Section 3.3.6).

37. 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.

38. 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

39. '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 should occur it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defence in depth, and it is repeatedly used in the specific safety principles that follow.

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

#### 3.2.1. Defence in depth

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

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

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



44. The reliability of the physical barriers is enhanced by applying the concept of defence in depth. In turn, protecting each of them by a series of measures. Each physical barrier is designed conservatively, its quality is checked to ensure that the margins against failure are retained, its status is monitored, and all plant processes capable of affecting it are controlled and monitored in operation. Human aspects of defence in depth are brought into play to protect the integrity of the barriers, such as quality assurance, administrative controls, safety reviews, independent regulation, operating limits, personnel qualification and training, and safety culture. Design provisions including both those for normal plant systems and those for engineered safety systems help to prevent undue challenges to the integrity of the physical barriers, to prevent the failure of a barrier if it is jeopardized, and to prevent consequential damage of multiple barriers in series. Safety system designers ensure to the extent practicable that the different safety systems protecting the physical barriers are functionally independent under accident conditions.

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

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

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

48. The 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.

49. 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

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

51. The design, construction, operation and maintenance of nuclear power plants has as its primary objective the generation of electricity reliably and economically. 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.

52. 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 operators are trained to recognize readily the onset of an accident and to respond properly and in a timely manner to such abnormal conditions. They have also been well trained in appropriate operating procedures, with which they have become familiarized.

53. Thus the prevention of accidents 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.

54. A number of probabilistic safety assessments 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. When effective preparation for accident management and for mitigation of the effects of severe accidents is taken into account, the results of these probabilistic safety assessments are consistent with the general nuclear safety objective in Section 2.1.

55. Probabilistic safety assessment also guides design and operation by identifying potential accident sequences that could contribute excessively to risk. Measures can then be taken to reduce this contribution.

### 3.2.3. Accident mitigation

56. *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.*
57. 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.
58. Accident management includes preplanned and ad hoc operational practices which, in circumstances in which the design specifications of the plant are exceeded, would make optimum use of existing plant equipment in normal and unusual ways to restore control. This phase of accident management would have the objective of restoring the plant to a safe state with the reactor shut down, continued fuel cooling assured, radioactive material confined and the confinement function protected. In such circumstances, engineered safety features would act to confine any radioactive material released from the core so that discharge 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 man by food-chains and other pathways.

### 3.3. GENERAL TECHNICAL PRINCIPLES

59. 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

60. *Principle: Nuclear power technology is based on engineering practices which are proven by testing and experience, and which are reflected in approved codes and standards and other appropriately documented statements.*
61. Systems and components are conservatively designed, constructed and tested to quality standards commensurate with the safety objectives. Approved codes and standards are used whose adequacy and applicability have been assessed and which

have been supplemented or modified if necessary. If opportunities for advancement or improvement over existing practices are available and seem appropriate, such changes are applied cautiously.

62. Numerous codes and standards have been adopted for nuclear use, after formulation by the professional engineering community and approval by the appropriate agencies. Some existing codes and standards have been modified from an original form to take into account unique features of their use for nuclear plants and the elevated importance assigned to the safety of nuclear plants. Approved codes have the simultaneous objectives of reliability and safety. They are based on principles proven by research, past application, testing and dependable analysis<sup>3</sup>.

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

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

#### 3.3.2. Quality assurance

65. *Principle: Quality assurance is applied throughout activities at a nuclear power plant as part of a comprehensive system to ensure with high confidence that all items delivered and services and tasks performed meet specified requirements.*
66. The comprehensive system referred to in the principle begins with analysis and design in accordance with the preceding principle on proven engineering, and it continues into the use of quality assurance methods. Other fundamental technical safety principles are also important in this respect, particularly those on safety assessment and verification and on operating experience and safety research.

<sup>3</sup> The IAEA's NUSS series of documents has been developed in accordance with this principle.



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

68. 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.

69. 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 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.

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

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

72. An essential component of quality assurance is the documentary verification that tasks have been performed as required, deviations have been identified and corrected, and action has been taken to prevent the recurrence of errors. The neces-

sary 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. Human factors

73. *Principle: Personnel engaged in activities bearing on nuclear power 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.*

74. 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 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.

75. The human error component of events and accidents has been too great in the past. The remedy is a twofold attack, through design, including automation, and through optimal use of human ingenuity in unusual circumstances.

76. 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 sufficient for the diagnosis of any faults that may develop and for assessing the effects of any actions taken. Reliable communication exists between the control room and operating personnel at remote locations who may be required to take action affecting the state of the plant. Administrative measures ensure that such actions by operators at remote locations are first cleared with the control room. The layout and identification of remotely located controls is such as to reduce the chance of error in their selection.

77. 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.

78. 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.

#### 3.3.4. Safety assessment and verification

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

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

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

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

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

84. 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 any possible weaknesses in design or operation that might cause excessive contribution to risk. The probabilistic method can be used to aid in the selection of events requiring deterministic analysis.

85. The process is repeated in whole or in part as needed later in the plant's life if ongoing safety research and operating experience make this possible and advisable.

#### 3.3.5. Radiation protection

86. *Principle: A system of radiation protection practices, consistent with recommendations of the ICRP and the IAEA<sup>4</sup>, is followed in the design, commissioning and operational phases of nuclear power plants.*

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

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

<sup>4</sup> INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, Recommendations of the International Commission on Radiological Protection, ICRP Publication No. 26, Pergamon Press, Oxford and New York (1977); INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Standards for Radiation Protection (1982 edn), Safety Series No. 9, IAEA, Vienna (1982).

89. For the continuing 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.

90. 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.

### 3.3.6. Operating experience and safety research

91. *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.*

92. 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.

93. The primary objective is that no safety related event goes undetected 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.

94. Research to understand nuclear power plant performance, response to abnormal occurrences, and possible sequences of events in severe accidents leads to improved interpretation of experience feedback 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.

## 4. SPECIFIC PRINCIPLES

95. The structure of safety principles is completed by the specific safety principles set out in this section. There are seven categories of specific safety principles. Five are arranged in the order of progression of a nuclear project from its inception through its operating stage: siting, design, manufacture and construction, commissioning and operation. Two further categories of principles are added to address the management and mitigation of the effects of severe accidents, even though these are unlikely. The safety objectives and the fundamental principles given earlier provide a conceptual framework for the specific safety principles and find wide application throughout the seven categories. Figure 1 summarizes the structure and the categorization of safety objectives and principles. Figure 2 is a schematic representation of the specific safety principles.

### 4.1. SITING

96. 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 implementation 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.

#### 4.1.1. External factors affecting the plant

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

98. Local factors include natural factors and man made hazards. Natural factors to be considered include geological and seismological characteristics and the potential for hydrological and meteorological disturbances. Man made hazards include those arising from chemical installations, the release of toxic and flammable gases, and aircraft impact. The investigations required give information on the likelihood of significant external events and their possible effects on nuclear power plant safety. 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.

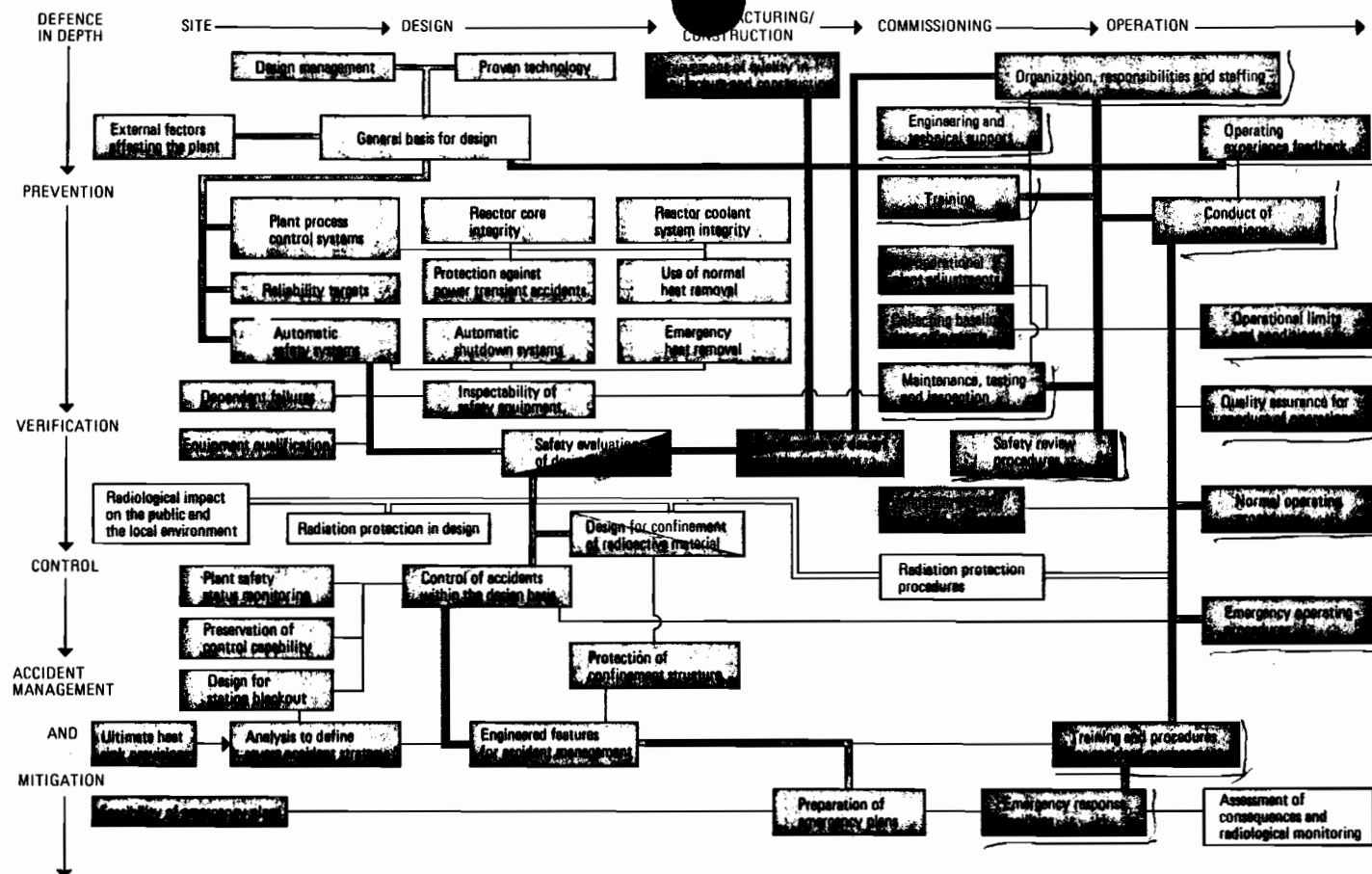


FIG. 2. Schematic presentation of the INSAG specific safety principles showing their coherence and their interrelations. All 50 principles are represented according to two criteria: from left to right, in order of progression of a nuclear plant project from its beginning to plant operation; and from top to bottom, in order of increasing threat to safety, from normal operation of the plant to the occurrence of a nuclear accident. The colours have been chosen correspondingly: blue for siting and design, green for manufacturing, construction and commissioning, and red for operation. Yellow indicates principles related to radiation protection. The vertical criterion is similar to the progression from accident prevention to accident mitigation as defined in the defence in depth concept. Principles dealing with safety evaluation or verification have been classified intermediately. A solid blue line connects some of the basic principles used to ensure a consistent safe plant design. Similarly, a solid green 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 aspects which contribute to excellence in operational safety, and emphasizes the importance of feedback of operating experience. Thin lines indicate significant connections between principles.

#### 4.1.2. Radiological impact on the public and the local environment

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

100. 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 in accidental radioactive releases with provisions for off-site countermeasures taken into account.

#### 4.1.3. Feasibility of emergency plans

101. *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.*

102. In the later section on emergency planning (Section 4.7.1), 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.

#### 4.1.4. Ultimate heat sink provisions

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

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

#### 4.2. DESIGN

105. 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 document 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 throughout the design changes that occur in construction and commissioning. At the design stage, consideration is given to the needs and performance capabilities of the personnel who will eventually operate the plant, and to the requirement that the designer will supply information and recommended practices for incorporation into operating procedures. Design choices are made which facilitate the achievement of the first safety priority, accident prevention. Special attention is also given to the prevention and mitigation of the consequences of accidents which could lead to a major release of radioactive materials from the plant.

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

107. Safety designers 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 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.

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

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



#### 4.2.1. Design process

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

##### 4.2.1.1. Design management

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

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

112. The design force is engaged in the preparation of safety analysis reports and other important safety documents. It also includes a co-ordinating group which has the responsibility of ensuring that all safety requirements are fulfilled. This group remains familiar with the features and limitations of components included in the design. It communicates with the future operating staff to ensure that requirements from that source are recognized in the design and that there is appropriate input from the designer to the operating procedures as they are prepared and to the planning and conduct of training. It has direct access to the design manager but does not necessarily report to that manager.

113. 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

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

115. This principle is a specific application of the fundamental principle 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 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.

116. Most application of engineering technology requires the use of analytical methods. The physical and mathematical models used in design are validated by means of experimental or operational testing and analysis of data. Results of more complex analysis are verified by pertinent experimentally based benchmark calculations, type testing and peer review. Where possible, realistic 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

117. *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.*

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

At a much lower level of probability are combinations of human and mechanical failure that could jeopardize the protection provided by inherent plant features and normal plant systems.

119. 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. Any engineered safety system is designed to prevent or to mitigate a specific spectrum of accidents. The accidents in this spectrum that tax the features of the safety system most are termed the design basis accidents for that system. The plant and the engineered safeguards are so designed that none of these accidents or accident sequences dominate the total risk. In design, attention is given to requirements for such future activities as maintenance and periodic testing, to ensure continued conformity to the principle.

#### 4.2.2. General features

120. 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

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

122. Important plant neutronic and thermal-hydraulic variables have assigned operating ranges, trip setpoints and safety limits. The safety limits are extreme values of the variables at which conservative analysis indicates that undesirable or unacceptable damage to the plant may be initiated. The trip setpoints are at less extreme values of the variables which, if attained as a result of an anticipated operational occurrence or an equipment malfunction or failure, would actuate an automatic plant protective action such as a programmed power reduction, plant shutdown or an even more marked response (see the principle in Section 4.2.2.2 on automatic safety systems). Trip setpoints are chosen such that plant variables would not reach safety limits. The operating range, which is the domain of normal operation, is bounded by values of the variables less extreme than the trip setpoints.

123. It is important that trip actions be not induced too frequently, especially when they are not required for protection of the plant or the public. Not only would this interfere with the normal, productive use of the plant, but also it could compromise

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

124. Therefore, the more important neutronic and 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 setpoints in normal operation.

##### 4.2.2.2. Automatic safety systems

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

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

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

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

safety systems is determined by the reliability of the electrical, fluid and instrumentation systems that support them.

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

#### 4.2.2.3. Reliability targets

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

131. Generally applicable design requirements for high reliability of safety systems and functions are translated into specific reliability targets. The reliability of support services required for the operation of safety systems or functions, such as electrical power or cooling water, is considered in the formulation of reliability targets. Appropriate reliability targets are set to ensure performance on demand and operation throughout the required duration of performance. These targets are based on engineering analysis. Detailed probabilistic methods are useful in determining the reliability required of safety systems and functions. Regardless of how the reliability targets are established, a reliability analysis is conducted during the design process to ensure that safety systems and functions can meet them. Functional testing and system 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.

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

#### 4.2.2.4. Dependent failures

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

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

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

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

137. Of the extreme external hazards, seismic events receive special attention owing to the extent to which they can jeopardize safety. A nuclear power plant is protected against earthquakes in two ways: by siting it away from areas of active faulting and related potential problems such as susceptibility to soil liquefaction or landslides; and by designing it to bear the vibratory loads associated with the most severe earthquake that could be expected to occur in its vicinity, on the basis of historical input and tectonic evidence. This is termed the design basis earthquake. Seismic design of plant structures, components and systems is carried out using response function methods, making use of a frequency spectrum for the design basis earthquake that is appropriate to the site. Seismic design takes account of soil-structure interaction, the potential amplification and modification of seismic motion by the plant structures, and interaction between components, systems and structures. The design ensures that the failure of non-safety-related equipment in an earthquake would not affect the performance of safety equipment.



#### 4.2.2.5. Equipment qualification

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

139. The conditions under which equipment is required to perform a safety function may differ from those to which it is normally exposed, and its performance may be affected by 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. The effects of external events such as earthquakes are also considered.

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

141. It is preferable that qualification be achieved by the testing of prototypical equipment. This is not always fully practicable for the vibration 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

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

143. In-service inspection is relied upon to demonstrate that safety provisions are maintained throughout the life of the plant. Provision is made at the design stage for inspection 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

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

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

146. Attention is also paid at the design stage to radiological protection in the decommissioning phase. After the end of the operating life of the plant, and after the removal of all nuclear fuel, substantial amounts of radioactive material will remain on the site. Consideration is given to the choice of materials which will have low residual radioactivity on the time-scale important for decommissioning, and to the need for convenient access for dismantling.

#### 4.2.3. Specific features

147. Some required design features serve specific safety functions.

#### 4.2.3.1. Protection against power transient accidents

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

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

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

#### 4.2.3.2. Reactor core integrity

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

152. Fuel 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.

153. 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 exercised to ensure that restraints do not themselves introduce safety problems.

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

155. High quality of fuel 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 level of radioactivity in the coolant during operation.

#### 4.2.3.3. Automatic shutdown systems

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

157. Safety shutdown systems are independent in function from the reactivity control systems used for normal operation of the reactor. Common sensors or devices may 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 busses and logic circuits of the shutdown system are separate from instruments used for normal control so that no interference is possible between the demands of normal control and the demands of safe shutdown. Only when the reactor is in a predefined 'guaranteed shutdown state' with sufficient subcriticality can the safety shutdown systems be safely disabled.

158. One unlikely event which must be 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. This is achieved by making the accidents sufficiently unlikely or by ensuring that they will not lead to severe core damage. Attention to prevention of these accidents or to limitation of their effects ensures that the safety objective is met even taking into account this failure of plant protection.

#### 4.2.3.4. Normal heat removal

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

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

#### 4.2.3.5. Emergency heat removal

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

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

#### 4.2.3.6. Reactor coolant system integrity

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

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

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

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

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

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

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

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

#### 4.2.3.7. Confinement of radioactive material

171. *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.*

172. 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 an 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 4.2.3.8). 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.

The structure maintains its integrity both in the short term and the long term under the pressure and temperature conditions which could prevail during design basis accidents.

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

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

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

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

#### 4.2.3.8. Protection of confinement structure

175. *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.*

176. This principle particularly affects a confinement structure used as a containment structure, as discussed in the previous principle. A containment structure is designed to withstand the internal pressure that can be expected to result from the design basis accident for this structure, calculated using substantial safety factors. 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.

177. If severe accident sequences could lead to pressures causing stresses exceeding the estimated ultimate strength of the containment, that structure might fail. If it failed catastrophically early in the accident sequence, a significant release of radioactive material might occur, necessitating protective measures outside the plant. Such circumstances could produce an appreciable contribution to the calculated risk.

178. 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, filtered vent systems, area spray systems and fuel debris retainers.

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

#### 4.2.3.9. Monitoring of plant safety status

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

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

182. The means of transmitting and displaying information include meters and status lights, parameter trend displays, prioritized alarms and various diagnostic aids as well as reliable personal communication between control room personnel and distant operating or maintenance staff. Care is taken by designers to ensure that the operators have the means of monitoring the most useful and important information, and to prevent distraction by more peripheral information. Experienced operating staff as well as human factors experts assist designers by identifying the most appropriate organization and presentation of these data.

#### 4.2.3.10. Preservation of control capability

183. *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.*



184. 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 were degraded for any reason, operators would receive a clear warning. Suitable equipment for personal protection is provided.

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

#### 4.2.3.11. Station blackout

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

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

188. In particular, nuclear power plants are designed to withstand, without loss of safety function, a simultaneous loss of 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.

#### 4.2.3.12. Control of accidents within the design basis

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

190. The plant operating staff are provided with appropriate safety equipment, instrumentation and operating procedures for response to and control of accidents within the design basis. Design is such that abnormal developments are first met automatically by the restoration of normal conditions by means of the feedback characteristics of neutronic and process controls. These are backed up by the normal capability for shutdown, continued cooling and protection against the release of radioactive materials. Further protection is available through automatic actuation of engineered safety systems. By means of such measures, any onset of abnormal behaviour would be dealt with automatically by appropriately designed systems for at least a predetermined period of time, 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.

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

### 4.3. MANUFACTURING AND CONSTRUCTION

192. A primary safety requirement is that a nuclear power plant is 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

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

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

195. At approximately the stage when preliminary design has been completed a safety analysis is performed. This overall analysis is reviewed with the regulatory authorities to ensure that regulatory requirements have been met or will be met, and the plant will be safe for operation. This determination may be subject to outstanding issues expected to be resolved during construction and before operation starts. Additional 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

196. *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.*

197. 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 his practices and procedures and the way he adheres to them. Manufacture 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.

198. The manufacturer establishes procedures for process and document control, materials and component identification and control, inspection and test schedules, maintenance of records, hold points and corrective procedures for deviations, the whole subject to a hierarchy of quality assurance practices. The manufacturer is responsible for the development and validation of his manufacturing practices and quality control methods, for staff training and for providing satisfactory working conditions.

199. 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

200. 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.

201. 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

202. *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.*

203. 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. 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.

204. 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

205. *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.*

206. 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. 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

207. *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.*

208. 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

209. *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.*

210. 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 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

211. 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 in the long term is not served by compromising safety in the short term.

#### 4.5.1. Organization, responsibilities and staffing

212. *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.*

213. 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. He is supported by the executive management of the operating organization, which assigns adequate financial, technical, material and manpower resources to the operation. Safety responsibilities for all levels and functions of the operating organization are clearly stated in job descriptions.

214. 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.



215. 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

216. *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 his overall safety responsibilities.*

217. 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 which is separate from plant operation, and which 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.

218. 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

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

220. 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. 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 check-lists, 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.

221. 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.

222. 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.

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

224. 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

225. *Principle: Programmes are established for training and retraining operations and maintenance 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.*

226. The training programme includes the identification of training requirements, the development of training specifications and materials, programme implementation, and evaluation. Formal training of operators 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).

227. Through the training programmes, operators are apprised of the principal results of any probabilistic safety assessments 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. Retraining 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.

228. 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, stand-by 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.

229. 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.

230. 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.

#### 4.5.5. Operational limits and conditions

231. *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.*

232. 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.

233. 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.

234. 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

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

236. 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.

#### 4.5.7. Emergency operating procedures

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

238. 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 extreme accidents that could lead to large releases of radioactive materials.

#### 4.5.8. Radiation protection procedures

239. *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.*

240. 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. Members of the operating staff

may assume some of these radiation protection duties. Written procedures are issued as necessary to cover radiation protection functions.

241. 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 keep their own routine radiation exposures as low as practicable.

242. 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 mock-ups of the systems to be serviced.

#### 4.5.9. Engineering and technical support of operations

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

244. 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.

#### 4.5.10. Feedback of operating experience

245. *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 worldwide.*

246. The importance for safety of an effective programme for the feedback of operational experience has been stressed in the fundamental principle in Section 3.3.6 related to operating experience and safety research. The plant manager reports promptly to the top management of his operating organization and to the regulatory organization any abnormal occurrence of significance for safety so that its implica-

tions 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.

247. 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.

248. 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.

249. 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.

250. 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 to the data needed.

#### 4.5.11. Maintenance, testing and inspection

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

252. 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. Defi-

ciencies 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.

253. 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.

254. 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.

255. 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.

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

257. 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. 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

258. *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.*

259. 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

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

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

262. The goal in managing an accident that exceeds the design basis would be to return the plant to a controlled state in which the nuclear chain reaction is essentially terminated, continued fuel cooling is ensured and radioactive materials are confined. Accident management would include taking full opportunity to use existing plant capabilities, if necessary going beyond the originally intended functions of some systems and using some temporary or ad hoc systems to achieve this goal. Accident



management would be responsive to the specific circumstances of the event, even though they might not have been anticipated. Advantage would be taken of whatever time might be available between correct diagnosis of the symptoms and the impending release of fission products to the environment. For the diagnosis of events beyond the design basis and the execution of accident management activities, somewhat longer periods than those for design basis accidents could be available to the operating staff.

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

#### 4.6.1. Strategy for accident management

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

265. Analysis is made of accidents 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.

#### 4.6.2. Training and procedures for accident management

266. *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.*

267. 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.

#### 4.6.3. Engineered features for accident management

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

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

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

#### 4.7. EMERGENCY PREPAREDNESS

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

272. In 1986 a Convention on Early Notification 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.

#### 4.7.1. Emergency plans

273. *Principle: Emergency plans are prepared before the startup of the plant, and are exercised periodically to ensure that protection measures can be implemented in the event of an accident which results in, or has the potential for, 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.*

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

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

#### 4.7.2. Emergency response facilities

276. *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.*

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

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

#### 4.7.3. Assessment of accident consequences and radiological monitoring

279. *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.*

280. Assessment methods are available to plant management which allow prediction of potential exposure due to 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 levels and nature of radioactivity in large numbers of samples.

281. 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 which may be necessary.

## Appendix

### ILLUSTRATION OF DEFENCE IN DEPTH

282. 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.

283. 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. This latter classification is illustrated in the second line of Fig. 3.

284. The figure shows events (second line) 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 abnormal 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 complex 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.

285. The lengths of the boxes on the line labelled 'events' are not intended to indicate any scale of probability for the events 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 event.

286. The third line 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 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.

287. The other lines show respectively how strategy, systems, procedures 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.

288. 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.

289. 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.

290. 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.

291. 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.



## INDEX OF KEYWORDS

*Accident management:* 3, 9, 15, 16, 19, 27, 50, **59–61**, 65, 68  
*Accident mitigation:* 13, **16**, 25, 59, 61  
*Accident prevention:* 8, 9, 13, **15**, 16, 25, 27, 59  
*Accidents beyond the design basis:* 8, 27, 42, 55, **59–61**, 64, 65  
*Accidents within the design basis:* 8, 20–21, **45**, 55, 59, 64, 68  
*Ageing:* **34**, 57, 58  
*Anticipated transients without scram (ATWS):* 38  
*As low as reasonably achievable:* 7  
*Automatic safety systems:* **30–32**  
*Automatic shutdown systems:* 30, 31, 36, **38**  
*Availability of staff and equipment:* 53  
  
*Chernobyl accident:* 1  
*Cliff edge effects:* 14  
*Commissioning:* 2, 11, 18, 21, 23, 25, 27, **47–48**, 53, 54, 58  
*Common cause failures:* 31, **32**, 33, 34  
*Commonly shared safety concepts:* 1  
*Competing energy sources:* 6  
*Confinement:* 9, 13, 16, 35, 39, **41–44**, 59, 61, 65, 68  
*Containment:* 20, 41, **42**, 61  
*Convention on Early Notification:* 62  
*Coolant system integrity:* 39  
*Core integrity:* 37  
*Criticality:* 36, **38**, 48, 52, 54  
  
*Decision intervals for operators:* 19, **45**, 60  
*Decommissioning:* 35  
*Dedicated and protected decay heat removal systems:* 39  
*Defence in depth:* 5, 9, 10, **13**, 14, 16, 25, 37, 39, 43, 58, **64–68**  
*Dependent failures:* 32  
*Design tolerant of human error:* 19  
*Deterministic method and analysis:* 8, 20, **21**, 64  
*Diagnosis of accidents:* 19, 45, 55, 60  
*Diversity:* 15, **32–33**  
*Dose intensive work:* 22

*Emergency heat removal:* 39  
*Emergency operating procedures:* 45, 52, 53, 55, 60, 65  
*Emergency preparedness:* 9, 27, 61, 62  
*Engineered safety features:* 8, 16, 20, 27, 31, 61, 64, 65, 68  
*Engineered safety features for accident management:* 61, 65  
*Equipment qualification:* 34  
  
*Feasibility of emergency plans:* 26  
*Feedback of operating experience:* 22, 25, 50, 54, 56  
*Filtered vent systems:* 43  
*Fracture toughness:* 41  
*Fuel debris retainers:* 43  
  
*Graded response in emergencies:* 62  
  
*Heat removal by natural circulation:* 39, 44  
*High technology:* 2, 19  
*Human factors:* 19, 20, 43  
*Hydrogen igniters:* 43, 61  
  
*Independent verification:* 12, 20  
*Inherent feedback:* 36  
*Inspectability of safety components:* 34  
  
*Manufacturing and construction:* 17, 23, 33, 45, 46  
*Monitoring of plant safety status:* 43, 45  
  
*Normal heat removal systems:* 38, 39  
  
*Off-site emergency preparedness:* 9, 16, 26, 62, 65, 68  
*Operating procedures:* 15, 27, 28, 45, 48-50, 52, 54, 55, 60, 65  
*Operational limits and conditions:* 52, 53  
  
*Physical separation for safety related components:* 15, 32-33  
*Plant manager:* 49, 50, 56, 57, 59  
*Plants with more than one reactor unit:* 33  
*Preservation of control capability:* 43  
*Probabilistic method and analysis:* 21, 32, 64  
*Probabilistic safety assessment:* 3, 15, 52

*Process control systems:* 30  
*Protection of confinement:* 42  
  
*Quality assurance:* 14, 15, 17-18, 28, 37, 46, 47, 54, 57, 59, 65  
*Quest for excellence:* 3  
  
*Radiation protection:* 6, 7, 21, 22, 25, 35, 47, 52, 55, 56  
*Radiological monitoring:* 63  
*Reactivity feedback:* 36  
*Reactivity induced accidents:* 36  
*Reactor coolant system integrity:* 39  
*Realistic modelling in safety assessment:* 29  
*Regulatory requirements:* 3, 28, 46, 50  
*Reliability targets:* 3, 32  
*Reliable long term heat sink:* 26  
*Responsibility of the operating organization:* 11, 56  
*Risk analysis:* 6  
*Root causes:* 22, 57  
  
*Safety analysis report:* 20  
*Safety assessment:* 3, 15, 17, 20, 57  
*Safety culture:* 2, 3, 8, 10, 14, 15, 28, 54, 65  
*Safety functions:* 13, 15, 31-32, 34-35, 39, 44-45, 55, 58  
*Safety principles and regulatory requirements:* 3  
*Safety research:* 8, 12, 17, 21, 22, 56  
*Safety shutdown systems:* 36, 37, 38  
*Safety targets:* 21  
*Selection and training:* 18  
*Severe accidents:* 8-9, 14-15, 22-23, 42, 52, 59, 60-62, 65, 68  
*Severe core damage:* 2, 9, 15, 38, 39  
*Significant addition to risk:* 6  
*Simulators:* 20, 52-53, 61  
*Single failure:* 31  
*Siting:* 2, 8, 23, 25, 33  
*Station blackout:* 44  
*Stochastic effects:* 7  
*Symptom based accident response:* 45, 55, 60

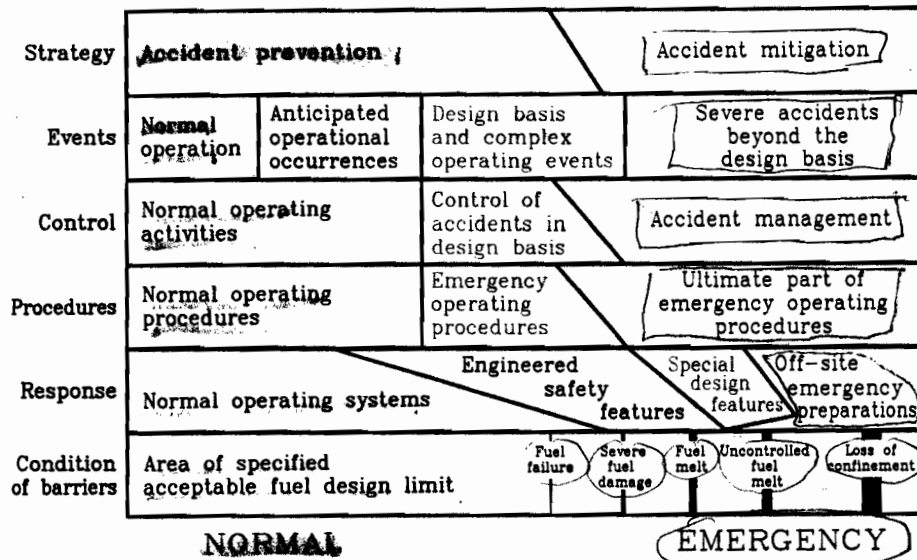


FIG. 3. Overview of defence in depth.

292. 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.

293. 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.

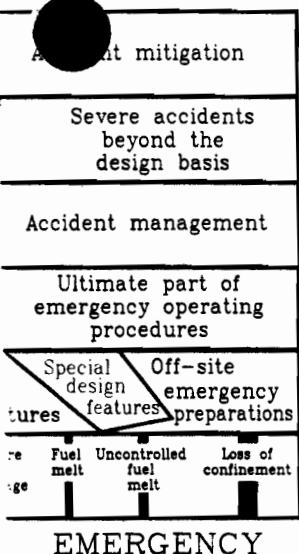
294. The confinement is a fourth barrier which is provided unless it has been shown that the function is provided by other means.

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

296. 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.



FIG. 4. The relation between the levels of defence in depth.



pth.

era...cluding response  
re. The level of protection  
three barriers. Together,  
ers.

ineered safety features and  
on of failures of equipment  
accidents into severe acci-  
confinement.

d unless it has been shown

t include accident manage-  
ment.

e, aimed at mitigating the  
rnal environment.

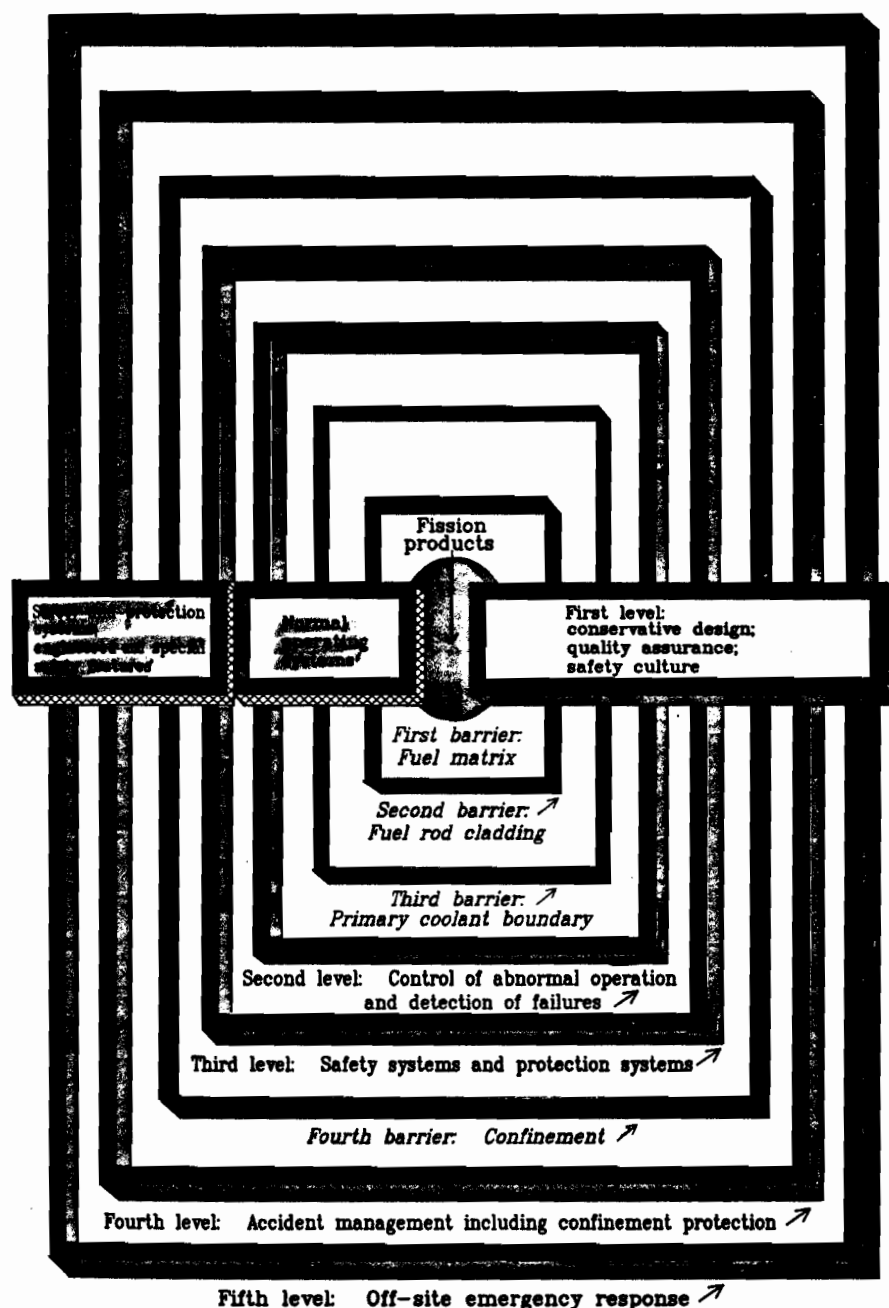


FIG. 4. The relation between physical barriers and levels of protection in defence in depth.

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

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

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

© IAEA, 1992

Permission to reproduce or translate the information contained in this publication may be obtained by writing to the International Atomic Energy Agency, Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria.

Printed by the IAEA in Austria  
January 1992

SAFETY SERIES No. 75-INSAG-5

# THE SAFETY OF NUCLEAR POWER INSAG-5

A report by the  
International Nuclear Safety Advisory Group

U. S. NUCLEAR REGULATORY COMMISSION  
LIBRARY  
WASHINGTON, D.C. 20555  
APR 7 1992

INTERNATIONAL ATOMIC ENERGY AGENCY  
VIENNA, 1992

11-  
969  
.A1  
I63  
no.91  
c.2

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.

THIS SAFETY SERIES IS ALSO PUBLISHED IN  
FRENCH, RUSSIAN AND SPANISH

#### VIC Library Cataloguing in Publication Data

The safety of nuclear power : INSAG-5 : a report by the  
International Nuclear Safety Advisory Group. Vienna :  
International Atomic Energy Agency, 1992.

83 p. ; 24 cm. — (Safety Series No. 75-INSAG-5)

ISSN 0074-1892

STI/PUB/910

ISBN 92-0-100192-4

1. Nuclear reactors — Safety measures. I. International  
Atomic Energy Agency. II. International Nuclear Safety  
Advisory Group. III. Series.

VICL

92-0002

## FOREWORD

by the Director General

The International Atomic Energy Agency's activities related to nuclear safety are based upon a number of premises. First and foremost, each Member State carries full responsibility for the safety of its nuclear facilities. States can only be advised, not relieved of this responsibility. Secondly, much can be gained by exchanging experience worldwide; lessons learned can prevent serious accidents. Finally, the image of nuclear safety is international; an 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, leading experts in nuclear safety were invited by the Agency to form the International Nuclear Safety Advisory Group (INSAG). This group serves as a forum for the exchange of information and for the provision of advice to the IAEA on nuclear safety issues of international significance. INSAG seeks not only to identify such issues, but also to draw conclusions on the basis of worldwide nuclear safety research and operational experience. It advises on areas where additional efforts are required. Where possible, it seeks to formulate common safety concepts.

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



## CONTENTS

SUMMARY .....	1
PROLOGUE .....	8
1. IMPORTANT ELEMENTS OF THE HISTORY OF NUCLEAR PLANT SAFETY .....	14
1.1. Safety in the earliest days .....	14
1.2. Evolutionary development .....	15
1.3. Preventing nuclear excursions .....	15
1.4. Requirement for an ultimate barrier .....	16
1.5. Protection from accidents .....	16
1.6. Introduction of probabilistic safety analysis .....	17
1.7. The accident at Three Mile Island .....	18
1.8. The Chernobyl accident .....	19
1.9. Management for safety .....	20
1.10. Engineering for safety .....	21
1.11. The message of INSAG-3 .....	21
1.12. Lessons from other events .....	21
1.13. Use of experience feedback .....	21
1.14. The role of research .....	22
1.15. Some comments on the history .....	22
2. CURRENT REACTOR SAFETY PRINCIPLES .....	24
2.1. Modern safety concepts .....	24
2.2. Safety objectives .....	25
2.3. Fundamental principles .....	25
2.4. Specific Safety Principles .....	27
3. SAFETY OF NUCLEAR PLANTS .....	29
3.1. Future nuclear plants .....	30
3.2. How the record is measured .....	30
3.3. The historical record of water cooled reactors .....	30
3.4. Use of probabilistic safety assessment .....	31
3.5. Probabilistic assessment of operational experience .....	32
3.6. Exceptional cases .....	33
3.7. Conclusion .....	33

4.	NUCLEAR FUEL CYCLE .....	34
4.1.	Nuclear fuel cycle .....	35
4.2.	Front end of the fuel cycle .....	36
4.3.	Back end of the fuel cycle .....	37
4.4.	The effects on humans .....	40
5.	FEATURES DESIRED IN FUTURE PLANTS .....	41
5.1.	Further improvement of safety .....	42
5.2.	Future features .....	43
6.	CONTINUED IMPROVEMENT OF NUCLEAR POWER PLANT SAFETY .....	47
6.1.	Directions of change .....	47
6.2.	Benefits from design evolution .....	48
6.3.	Evolutionary design improvements for the near future .....	49
6.4.	Natural limits on evolutionary improvability .....	50
6.5.	Water reactors with passive safety features .....	51
6.6.	Absolute safety? .....	53
6.7.	Prospects for change: a judgement .....	54
7.	CONCLUSIONS .....	55
Appendix I:	IAEA SAFEGUARDS AGAINST PROLIFERATION OF NUCLEAR WEAPONS .....	57
Appendix II:	NUCLEAR RADIATION AND ITS EFFECTS .....	59
Appendix III:	RELATIVE HEALTH RISKS IN ELECTRICITY GENERATION .....	66
	REFERENCES .....	81
	MEMBERS OF THE INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP AND WORKING GROUP EXPERTS .....	83

## SUMMARY

Electricity has come close to joining food, shelter and clothing as one of the basic necessities. Yet most electricity is generated in plants that burn fossil fuels (coal, and to a lesser extent, oil and natural gas) with such adverse effects on the environment as atmospheric pollution, acid rain and probable 'greenhouse' warming of the Earth.

Nuclear power has already demonstrated that it can supply large amounts of electricity efficiently and economically. Nuclear plants do not produce the undesired waste products that are released from fossil fuelled plants. However, all technologies have some undesirable impacts, and those that are commonly attributed to nuclear plants concern safety, nuclear waste disposal and possible misuse of material in the proliferation of nuclear weapons.

Safeguards against nuclear proliferation are among the IAEA's responsibilities. Since this topic does not fall within INSAG's area of expertise, its discussion here is confined to Appendix I, which describes the IAEA's principal responsibilities in preventing the growth of nuclear weapons capability. The members of INSAG are experts on nuclear safety and radioactive waste disposal, and their views on these topics are presented in the body of this report.

It is necessary to understand the spirit in which INSAG has prepared this report. INSAG is an advocacy group for safety in the use of nuclear energy. Its members have worked in their separate countries for many years in the furtherance of nuclear safety, and continue to do so. This report is an assessment of how well the efforts to reach an acceptable level of safety have succeeded up till now, and how well they may be expected to succeed in the future.

## IMPORTANT ELEMENTS OF THE HISTORY OF NUCLEAR PLANT SAFETY

The possibility of unusual hazards from peaceful, beneficial applications of nuclear energy was recognized at an early time. Therefore, even before action was taken to build the first of these peaceful nuclear energy systems, the future developers had resolved to seek an exceptionally high level of safety. This objective, which was unprecedented in industrial development, has been maintained and improved upon throughout the evolutionary process that followed. The objective has not always been achieved, but the safety record has been remarkably good when compared to that of other new technologies when they were introduced. Only two large accidents causing public anxiety have occurred, and only one of these has led to radiation induced health effects on workers or the public.

An early step that contributed to this record, and that later had singular importance, was the widespread adoption of an ultimate means of protection at water

cooled and moderated reactors, in the form of strong, tight enclosing structures designed to prevent the release of any radioactive material from an accident. This came to be refined into a strategy for safety of nuclear plants called 'defence in depth', based on several successive protective barriers and additional protective means of ensuring continued integrity of these barriers. Even if one line of protection were to fail if called upon, others would continue to provide the protection. The structured protective process includes both safety systems and safety practices.

At different stages of the historical development of nuclear energy, the focus of attention fell on different safety concerns that had arisen, leading to solution of a succession of safety questions. The completeness and effectiveness of the protective practices adopted in answer to these questions are now based on lessons learned (including those from the two severe accidents to nuclear power plants), and on a well developed field of engineering, covering both engineering systems and human factors.

## CURRENT REACTOR SAFETY PRINCIPLES

The safety of nuclear plants has been developed and refined over a period of more than 35 years. The design features and practices developed to ensure safety have been consolidated in a logical structure in IAEA Safety Series No. 75-INSAG-3, Basic Safety Principles for Nuclear Power Plants<sup>1</sup> (referred to in the following as INSAG-3). These Safety Principles show how the safety of modern nuclear power plants rests on the foundation of defence in depth, with its protective design features and operating practices that augment and support each other both sequentially and in parallel. The Safety Principles stress the importance of a 'safety culture' permeating all activities related to generating electricity at a nuclear power plant and ensuring that performance is at a level of competence and dedication above and beyond simple conformance with good practice. They incorporate safety targets at a very high level, so that with existing nuclear plants the probability of an accident causing severe core damage but no effects off the site should not be greater than once in ten thousand years and the probability of an accident requiring protective measures off the site should not be greater than once every one hundred thousand years. Future nuclear plants should better this by a factor of at least ten.

INSAG-3 contains fifty specific Safety Principles. These begin with the selection of a site for a nuclear plant and proceed through its design, construction, commissioning, operation and final decommissioning. Additional Safety Principles establish the need to develop and put into place accident management features and measures and to establish a plan incorporating emergency measures, even though such capability is expected never to be called on.

<sup>1</sup> INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, Safety Series No. 75-INSAG-3, IAEA, Vienna (1988).

## SAFETY OF NUCLEAR PLANTS

This publication considers the safety of nuclear plants of types that will continue to be built and operated for some time to come. These will use light water or heavy water as the coolant and the neutron moderating agent. The safety of such plants can be estimated from the safety records and the probabilistic safety assessments of plants of similar types that have been built in the past. Both methods of estimating their safety face some difficulties; the former demands accumulation of an extensive operating history that is available only after a substantial period of time, and the latter suffers from its well known wide band of uncertainty. Yet useful estimates can be made.

The historical record is reviewed first. With one severe accident, that to the Three Mile Island nuclear power plant in the United States of America, in about 5000 reactor-years of operation, the historical record of severe accidents to light and heavy water nuclear plants seems to be not quite as good as the INSAG target for existing nuclear plants. This target is a likelihood of occurrence of severe core damage below once in 10 000 reactor-years of operation. But the record is acceptably close to this target. INSAG's companion target for existing plants is that the probability of an accident requiring short term off-site response in the form of protective measures against radioactive material should be less than about once in 100 000 reactor-years of operation. No such off-site protective measures have ever been needed up to now for either light water or heavy water nuclear plants, though the operating record is too short to warrant a conclusion that the quantitative target has been met.

When attempts are made by means of probabilistic safety assessment (PSA) to determine the safety of individual plants, the wide uncertainty bands prevent any definitive estimate. Yet a number of assessments give broad support to a conclusion that with certain exceptions existing nuclear plants with water reactors meet the safety targets that INSAG has set for them. The exceptions are being addressed in regulatory programmes in the countries affected, and INSAG believes that where in specific cases the safety of a plant is estimated to fall short of the INSAG targets for existing plants, corrective measures should be applied.

The assessments of the safety of existing plants form the basis for INSAG's judgement that current nuclear plants with water reactors are acceptably close to meeting the near term safety targets, and that future nuclear plants of similar types, meeting the Safety Principles in INSAG-3, will also meet the INSAG long term targets for future plants, and will be safer than existing plants by a factor of at least ten.

## NUCLEAR FUEL CYCLE

INSAG recognizes, however, that the safety of the nuclear option must be evaluated in terms of its complete fuel cycle, not simply of electricity generating

plants. The other parts of the cycle include the front end activities of mining and the chemical and physical preparation of uranium into fuel elements, and the back end activities of spent fuel storage and disposal. In some countries, the last activity includes chemical reprocessing, which makes part of the contents of the spent fuel reusable and is capable of greatly reducing the volume of waste to be disposed of. The amount of actual waste from a nuclear plant is very small, a factor of about 300 000 smaller than that from a coal burning power plant. The amount of spent fuel removed from a nuclear plant is smaller by a factor of about 10 000 than the amount of ash from a coal fired power plant.

Among the hazards attached to the fuel cycle, those associated with uranium mining stand out. The conventional hazards to uranium miners are the same as those faced by other hard rock miners, and are smaller than hazards faced by coal miners. Uranium miners also experience risks from inhalation of radon, but with proper ventilation these are held below recommended limits set by international organizations to protect the workers. The only other source of hazard from the front end of the fuel cycle is that associated with tailings piles, which are the residue from the extraction of uranium from ore. These are sources of radon. These man-made deposits emit only a very small part of the radon released everywhere on Earth by rocks, soil and sea water, but they must be segregated because they are more concentrated sources. Action must therefore be taken to ensure that tailings piles are kept isolated and confined.

The initial step in the back end of the fuel cycle is storage of spent fuel at the nuclear plants after its removal from the reactors. This is a straightforward and time tested process, spent nuclear fuel having been stored under water in deep pools without incident for decades, ever since the first nuclear reactors went into operation.

Following temporary storage at the nuclear plant, final disposal of the waste is required. Though it is sometimes said that the problem of disposal of highly radioactive waste from nuclear plants has not been solved, this is not the case. There is not a great deal of such waste to be stored, because nuclear plants do not use very much fuel, and there is widespread agreement in the nuclear community on the mode of disposal to be used. The waste is to be encased in containers which are highly resistant to corrosion and stored in dry man-made caverns deep within the Earth. The material to be stored may consist of the fuel elements themselves, in which case the fission products remain locked in the fuel in which they were produced. However, some countries follow the path of reprocessing the spent fuel to recover some of the valuable content and to reduce the volume of actual waste. The fission products are then converted into a long lived glass, which is stored in caverns in corrosion resistant containers. Research is being conducted in several countries on other, more speculative, methods of disposal of the waste from reprocessed nuclear fuel, an example being a proposal for use of transmutation of some of the radioactive ingredients.

Repositories are to be sited and designed such that no one should ever be, exposed to radiation from waste stored within them, over all future time. If unusual and unexpected developments at some future time were to expose this material to the world of human existence, maximum radiation doses to any individuals are still to be well below those from natural radiation exposure.

The adverse effects on human beings from the front end and the back end of the nuclear fuel cycle are a minor part of the total radiological impact of nuclear power, which is itself very small compared to the normal exposure of people to cosmic rays, radon and direct radiation from the Earth.

## FEATURES DESIRED IN FUTURE PLANTS

The current slowdown in the growth of the nuclear power industry offers an opportunity to further consolidate nuclear plant safety by means of design improvements for future reactors. This could start by incorporating more naturally the safety features that have been added on to earlier designs. Plants built according to such restructured designs may be less expensive in the long run, may be less complex and may be more readily accepted by the public.

Beyond this process of consolidation of past gains is an opportunity for further substantial improvement of the level of safety of nuclear plants through future design choices. INSAG lists in this report directions that it believes should be followed in the designs of future plants, building on and even exceeding in certain respects the safety capability offered by the Safety Principles of INSAG-3. It is believed that the level of safety that could be achieved from these advances would be substantially higher even than that attached to the previously stated INSAG targets. The safety would exceed that of competing means of generating electricity by at least a factor of ten, and would reach a level unprecedented in this modern technological world. As a cautionary note, however, INSAG also believes that implementation should take into account the need to devote the resources of society to the most fruitful means of reducing risk of all kinds, not only that from nuclear power.

The features identified as desirable are as follows:

The Basic Safety Principles of INSAG-3 should become mandatory, with the following predominant features:

- Defence in depth continues to be the fundamental means of ensuring the safety of nuclear plants.
- The three fundamental safety tenets continue to be: maintain cooling, control the power level; and confine the radioactive material.

More specific aspects of design should be addressed as follows:

- The concept of plant design should be extended to include the operating and maintenance procedures required for it.

- Design should avoid complexity.
- Plants should be designed to be 'user friendly'.
- Design should further reduce dependence on early operator action.
- The design of the system provided to ensure confinement of fission products after a postulated accident should take into account the values of pressure and temperature encountered in severe accident analysis.
- Accidents that would be large contributors to risk should be designed out or should be reduced in probability and/or consequences.
- The plant should be adequately protected by design against sabotage and conventional armed attack.
- Design features should reduce the uncertainty in the results of probabilistic safety analysis.
- Consideration should be given to passive safety features.

#### CONTINUED IMPROVEMENT OF NUCLEAR POWER PLANT SAFETY

Work is proceeding in several countries on designs of advanced nuclear plants based on reactors cooled and moderated with light or heavy water. Some designs are well advanced, for nuclear plants now being built or available to be built soon. These are close evolutionary descendants of plants that now exist. They embody numerous improvements in safety over present plants, generally on the lines advocated in this report. Though they are limited in some respects in the ability to improve on good current practice, the most recent series of light and heavy water nuclear plants can fully comply with the Safety Principles in INSAG-3 and can meet the safety objectives that INSAG has proposed for future nuclear plants.

Designs with safety features that would be largely passive in function are also being developed in a number of countries. A substantial amount of work remains to be done on these concepts, including detailed design, some research and development, and safety review for licensing. Yet some designs are far enough developed that they could be available for construction late in the 1990s. These largely passive designs could incorporate many or all of the additional safety features INSAG has proposed in this report. However, passive safety is not necessarily improved safety in all cases, and the benefit must be carefully weighed before the choice is made. Plants in this category will provide an unparalleled degree of safety if they live up to their promise.

A third class of designs includes concepts proposed by several groups seeking complete freedom from the possibility of severe accidents. These designs are all at the conceptual stage, and a great deal of work is needed to establish feasibility and to evaluate the extent to which the safety gains can be realized.

INSAG believes that the level of safety desirable for nuclear power plants can be achieved with light and heavy water reactors that are now being realized and that even greater safety can be projected for plants that are being proposed as their successors. However, society may demand an even larger improvement in safety as the cost of approving continuation of the nuclear option. If this is to be the case, imaginative and revolutionary concepts such as some briefly discussed in this report might offer an acceptable solution, and that could justify their accelerated development.

#### GENERAL CONCLUSION

INSAG concludes that there is no technically valid reason to reject a role for nuclear power in meeting society's needs for an expanding source of electricity, and further, that the fullest exploitation of the nuclear option to alleviate environmental concerns should be pursued.

## PROLOGUE

A number of international conferences have recently been held to consider the adverse effects of the growing use of energy throughout the world. The effects most commonly discussed are those of increased burning of fossil fuels, especially coal but also oil and to some extent natural gas. The major effects are atmospheric pollution, acid rain and probable 'greenhouse' warming of the Earth. To these must be added the large quantities of carcinogens and heavy metals, such as mercury, lead and uranium, emitted in smoke from burning of coal. These have serious health effects. Furthermore, the extensive burning of fossil fuel depletes carbon reserves that have been formed over hundreds of millions of years. From a practical standpoint, these reserves can never be replaced.

Some of the international conferences have also considered the technologies that may be used to reduce the impacts of greater use of energy. In the conclusions of the conferences, the nuclear option has sometimes been dismissed for reasons associated with the acceptability of nuclear energy. In the Hamburg manifesto, which was a summary of conclusions of the World Conference on Climate and Development, held in Hamburg, Federal Republic of Germany, in November 1988, it was said that "The nuclear option as a means of reducing CO<sub>2</sub> emission was raised but the lack of means to deal with the triple problems of safety, waste disposal and weapons potential inhibited serious consideration." In reports from some other conferences, such as the workshops held at Villach, Austria, and Bellagio, Italy, in September–November 1987, nuclear energy is simply listed among the alternate energy sources available to replace the combustion of fossil fuel. The report of the conference in Toronto, Canada, in June 1988 on *The Changing Atmosphere: Implications for Global Security* said that "There is a need to revisit the nuclear power option. If the problems of safety, waste and nuclear arms proliferation can be solved, nuclear power could have a role to play in reducing CO<sub>2</sub> emissions."

Reviews such as those at the conferences cited reflect pressure throughout the world to increase certain forms of energy production and consumption, especially within nations with lower per capita incomes. The pressure stems from population growth, changes in industrial practices and the rising aspirations of the people in these poorer parts of the world.

### THE NEED FOR ELECTRICITY

The conferences devoted particular attention to electricity as a component of the energy mix whose share continues to increase. The essential, beneficial role of electricity in the present stage of civilization has not been questioned. The overriding requirement for generation of adequate supplies of electricity was implicit in the discussion. Electricity has come close to joining food, shelter and clothing as one of

the basic necessities. Without electricity, which is heavily used almost everywhere, the average span of life would be shorter and the quality of life would be greatly decreased. The conferences implicitly recognized this essential role of electricity.

Yet most electricity is generated in plants that burn fossil fuel, especially coal and to a lesser extent oil and natural gas. Burning fossil fuel to produce electricity generates much more carbon dioxide than is commonly realized, because it requires about three times as much heat energy as the amount of electrical energy produced. The amount of carbon dioxide released is proportional to the amount of heat produced by combustion. The generation of electricity in fossil fuelled electrical plants is therefore one of the major sources of man-made atmospheric generation of CO<sub>2</sub>. For the same reason, the burning of fossil fuel to produce electricity has in addition greater consequences of other kinds than is realized by most people, such as the emission of hydrocarbons (which are linked to the initiation of cancer) and of heavy metals (which damage health in a number of ways). If the adverse effects of fossil fuels on human life and the environment are real, it will be necessary to use every available means to reduce them.

In discussions on the possibility of the increased use of nuclear power in supplying electricity, it is recognized that nuclear power plants do not generate the undesirable products that are released from fossil fuelled plants. Nuclear plants do not emit CO<sub>2</sub> or other greenhouse gases, do not release chemical compounds that cause acid rain, and generate no smoke containing carcinogens or heavy metals. As is well known, nuclear plants and their associated nuclear fuel cycle can and do release some radioactive material, but this action is easily manageable, and in normal operation the amount of such material released is held to very low and harmless levels.

### CONSERVATION AND RENEWABLE ENERGY

There are some who believe that there is no need for additional capacity for the generation of electrical energy. They believe that the solution to problems of increased pollution lies in concerted efforts to reduce the demand, i.e. conservation, along with the greatly increased use of renewable energy, especially solar and wind.

INSAG agrees that use of renewable energy technologies can and should be extended to the degree practicable. Yet these methods have not flourished up to the present time. Some, such as geothermal, hydropower and biomass (wood burning), are found to degrade the environment in their own ways. Others, such as solar and wind power, have been unable so far to overcome the problem of the high cost of generating large amounts of electricity from energy sources that are diffuse, low density and available only some of the time.



INSAG does not dispute the view that there is opportunity for further conservation in the industrialized nations of the world, but points out that much of the reduction that was possible twenty years ago has now taken place, and the demand for electricity continues to grow inexorably in these industrialized countries. In some places, the urge to conserve has reduced the use of other forms of energy, but greater use of electricity was needed to accomplish this.

Clearly, energy conservation will not solve the growth in demand for electricity in the poorer countries that are struggling to improve the lifestyles of their people. There the pressures for energy of all forms far outstrip any capability of conservation and renewable energy technologies. Either all acceptable modes of producing electricity and other forms of useful energy will have to be called on, or the world will be helplessly locked into the present division between the energy rich and the energy impoverished.

Considerations such as these have induced INSAG to take up the question of the role of nuclear energy in helping to meet the world's future demands for electricity.

## PERCEIVED PROBLEMS

The problems that aforementioned conferences associated with nuclear power concern safety, nuclear waste disposal and the possible misuse of material in the proliferation of nuclear weapons. It is important that these questions affecting the acceptability of nuclear energy be addressed. In this publication, INSAG addresses them for its mandated areas. The members of INSAG are expert on nuclear plant safety and radioactive waste disposal. These are topics on which a fresh review by INSAG can have value, and that review is presented here. However, safeguards against nuclear proliferation are outside INSAG's mandate. These safeguards are included in the IAEA's activities in accordance with its Statute, and have been extensively reviewed in numerous public forums. That area is not examined here, though Appendix I is devoted to a summary of the measures pursued by the IAEA.

The concerns that inhibit greater use of nuclear energy are related to safety in one way or another. Most people now realize that normal operation of a nuclear power station poses no threats. Yet the fear of accidents remains widespread. This fear arises partly from the unfamiliarity of people with nuclear energy and to some extent from a subliminal association with weapons of mass destruction. It also arises from the tendency of most individuals, in greater or smaller measure, to base judgments and actions on perceived rather than actual risk. They are concerned about the possibility of large scale release of radioactive material. The nuclear power industry has been unable so far to dispel a view held by many that accidents with devastating consequences cannot be ruled out at any nuclear plant, and that nuclear power is therefore undesirable no matter how unlikely such an accident may be.

For the layman, the concept was turned to reality by the Chernobyl accident, which had consequences that were devastating in nearby areas in the Union of Soviet Socialist Republics and that aroused deep anxieties over a much wider region. There is a growing perception that the after-effects of the accident, including the psychological, were worse in the USSR than had been thought at first, though it is doubtful whether some of the biological and medical effects believed to have been seen afterwards were caused by radioactive material released in the accident. Analysis has also shown that these effects of radiation outside the USSR were greatly exaggerated in the publicity given to the accident at the time and afterwards.

The worst consequences of this accident were found not so much in the direct effects of radiation, but in the climate of fear that it aroused, and the social upheaval and disruption of life as so many people were uprooted from their homes.

There was also deep public anxiety during and after the earlier accident to the Three Mile Island nuclear plant in the United States of America. It has since been well established, however, that this accident did not injure anyone, because the containment building retained all but a very small part of the harmful fission products released from the damaged reactor core. In fact, no one had to be evacuated from the region around Three Mile Island, though at the time this was not clear and some thought then that such a course might be necessary.

## CONTENTS OF THE REPORT

Though concern regarding nuclear plants is widespread, nuclear plants have become numerous in many countries. Approximately 425 nuclear power plants are now in existence, supplying about 17% of the world's electricity. More nuclear plants come on line every year, and construction of others is still being initiated, although the rate of building is nowhere near that of a decade ago. The total number of operating plants continues to grow, even though some of the older plants have been shut down as not being economical or because their designs did not meet modern safety standards.

The question being explored in this report is, if events so move as to cause large scale construction of nuclear plants to start again, will the new plants be adequately safe?

INSAG therefore considers in the following the safety of the nuclear industry in the future, addressing on the way the question as to whether disposal of waste from nuclear power plants is so difficult a problem that it rules out increased use of the technology. If the answers arising from such a review are encouraging, it may be concluded that nuclear plants could be of substantial help in solving future environmental problems, more even than today. If they are discouraging and barriers to use of the nuclear option are almost insuperable, it would be wise to know that now.

INSAG first addresses the question of nuclear plant safety from three stand-points: the technical basis for safety, the historical record, and recent estimates of the level of safety that analysis indicates has been reached. The safety aspects of the rest of the nuclear fuel cycle are then discussed, including the storage and disposal of nuclear waste, in order to round out the view of the potential radiological impact of future electricity generation.

At this point INSAG introduces a list of features that should even further enhance the safety of nuclear plants to be designed in the future. These features build upon the Safety Principles enunciated in IAEA publication No. 75-INSAG-3, Basic Safety Principles for Nuclear Power Plants [1]. When incorporated in future nuclear plants, they should substantially improve safety even beyond the targets of INSAG-3.

The last part of this report contains a review of nuclear plants proposed for future construction, including evolutionary developments from present designs, derivatives of such designs incorporating numerous passive safety features, and proposed concepts that might embody exceptional safety features. These are discussed in the context of the features desirable in future plants. If it is concluded by society that plants which are evolutionary developments from current designs embody adequate safety, there would be little reason to look deeply today into the more radically new designs, which will have high development costs. But if society is reluctant to continue along present lines, or seeks a step function improvement in safety over that promised by current conditions and trends, the more imaginative designs will be valuable.

#### ADDITIONAL COMMENTS

Two further appendices are included which are not part of the main discussion of the report, but which have the role of placing the main discussion in context and lending it perspective. Appendix II is a condensed discussion of nuclear radiation and its effects. This is provided because much of the information gleaned from the popular press on nuclear radiation and its effects on human beings is misleading or wrong. As a result, the topic is not well understood by most people, and is often misunderstood. Yet assessment of the safety of nuclear plants depends critically on this important subject. The brief discussion of nuclear radiation and its effects on human beings is based entirely on publications of the United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR).

In any analysis of risk from whatever source, the balancing of risks of diverse kinds and origins must also be borne in mind. No action in life is free of risk, and everyone faces numerous risks every day. An optimum situation with regard to risk will occur when life's choices are made in such a way as to minimize the total risk. In reducing the total risk, it is important to devote society's limited resources to the areas where the risk is greater. INSAG has therefore extracted, in Appendix III,

results from a recent, peer reviewed, study of the relative risk of comparative ways of producing electricity. No attempt is made to estimate the countervailing benefit of electricity whatever its origin, though this must outweigh most if not all harmful effects that can be imagined.

#### FINAL NOTE

It is necessary to understand the spirit in which INSAG has prepared this report. INSAG is an advocacy group for safety in the use of nuclear energy. Its members have worked in their separate countries for many years in the furtherance of nuclear safety, and continue to do so. This report is an assessment of how well the efforts to reach an acceptable level of safety have succeeded and how well they may be expected to succeed in the future.

# 1. IMPORTANT ELEMENTS OF THE HISTORY OF NUCLEAR PLANT SAFETY

## SUMMARY

The possibility of unusual hazards from peaceful, beneficial applications of nuclear energy was recognized at an early time. Therefore, even before action was taken to build the first of these peaceful nuclear energy systems, the future developers had resolved to seek an exceptionally high level of safety. This objective, which was unprecedented in industrial development, has been maintained and improved upon throughout the evolutionary process that followed. The objective has not always been achieved, but the safety record has been remarkably good when compared to that of other new technologies when they were introduced. Only two large accidents causing public anxiety have occurred, and only one of these has led to radiation induced health effects on workers or the public.

An early step that contributed to this record, and that later had singular importance, was the widespread adoption of an ultimate means of protection at water cooled and moderated reactors, in the form of strong, tight enclosing structures designed to prevent the release of any radioactive material from an accident. This came to be refined into a strategy for safety of nuclear plants called 'defence in depth', based on several successive protective barriers and additional protective means of ensuring continued integrity of these barriers. Even if one line of protection were to fail if called upon, others would continue to provide the protection. The structured protective process includes both safety systems and safety practices.

At different stages of the historical development of nuclear energy, the focus of attention fell on different safety concerns that had arisen, leading to solution of a succession of safety questions. The completeness and effectiveness of the protective practices adopted in answer to these questions are now based on lessons learned (including those from the two severe accidents to nuclear power plants), and on a well developed field of engineering, covering both engineering systems and human factors.

### 1.1. SAFETY IN THE EARLIEST DAYS

Shortly after the Second World War, the United States Atomic Energy Commission formed an Advisory Committee on Reactor Safeguards, to consider the safety of the nuclear reactors that then existed. This Committee, consisting of safety experts outside the main line of nuclear plant development, has been in existence ever since, and it has reviewed the safety of all commercial nuclear plants in the USA. Similar practices were adopted in most other countries where nuclear energy

was being developed. The intent in all cases was to bring the best minds to bear on reactor safety.

At the first International Conference on the Peaceful Uses of Nuclear Energy, in Geneva, Switzerland, in 1955, there were many scientific papers on concepts and plans for nuclear reactors both for research purposes and for the production of electricity. In these papers, safety considerations were prominent.

### 1.2. EVOLUTIONARY DEVELOPMENT

Development of the methods to make nuclear plants safe has surpassed the classic pattern for other engineering disciplines. It has not only sought understanding of how systems fail, so as to prevent that failure, but also included development of methods to avert the consequences of failure. It has grown from earlier and simpler concepts and methods into a methodology that rests on a broad foundation of experience. This process had to keep pace with increasing demands made on it, because the nuclear plants themselves have also evolved in size and complexity. Moreover, it had to respond to a steadily mounting desire by people everywhere for improved safety in every sphere of life.

Vitally important in the improvement has been enhancement of understanding of the technical basis for safety. That understanding has been developed in a long, intensive programme of research into the engineering aspects of safety, supplemented by feedback of experience from many thousands of reactor-years of operating experience, supported by lessons learned from the severe accidents to the nuclear power plants at Three Mile Island and Chernobyl and from lesser incidents at other plants.

### 1.3. PREVENTING NUCLEAR EXCURSIONS

Improved understanding has included deepened insight into design basis accidents, which are the types of accidents that the plant must be able to withstand without harm to people or the environment. From the first, it had been known that a nuclear reactor could not explode like an atomic bomb, but it was recognized that events with sharp, energetic power increases could not be ruled out altogether. Therefore, in the early days, concerns were focused on design to ensure continued control of the nuclear chain reaction. The early emphasis on these nuclear events, which would be far smaller than those produced by a nuclear weapon but still potentially harmful, arose because of accidents to two small experimental reactors, the NRX in Canada in 1952 and the SL-1 in the USA in 1961. Though the former accident injured no one, the latter killed three workers. Research in the 1950s and early 1960s led to understanding of reliable means by which good reactor core design could help to avoid nuclear accidents.

Unfortunately, these methods were not well implemented at the Chernobyl reactor, when it later had its accident as a result of loss of control of the nuclear chain reaction.

#### 1.4. REQUIREMENT FOR AN ULTIMATE BARRIER

It was realized in the USA as early as 1952 that accidents to nuclear plants could not be ruled out absolutely, and so special protection from the consequences of severe accidents was added at plants. The Advisory Committee on Reactor Safeguards introduced a requirement that certain nuclear plants must be housed in sturdy, leaktight buildings that were to serve as an ultimate form of protection, to prevent radioactive material escaping from the plant if an accident did take place in spite of all precautions. This requirement was soon adopted for light water and heavy water nuclear power plants throughout most of the world. However, the early light water reactors in the USSR and in eastern Europe were provided only with partial containment buildings. It was only in the mid-1970s that full containment of newer light water reactors was also introduced in eastern Europe. Lack of a tight, sturdy containment building around large gas cooled reactors in some countries has been compensated for by other design features. The metallic confinement vaults that enclosed the reactor cores of the water cooled, graphite moderated RBMK reactor plants in the USSR could withstand rupture of a single fuel channel, and perhaps even a few of them, but could not contain an accident of the type and magnitude of that which occurred at Chernobyl.

On looking back, it can be seen that this early decision, to require a containment system having as its sole purpose the protection of the public from all eventualities, became a keystone of safety strategy for light and heavy water nuclear power plants. It provided the final barrier to fission product release in the system of defence in depth that had already begun to be developed at this earliest stage. Even now an important part of safety design of these plants is devoted to ensuring that the containment system would be reliable and effective if it were ever needed.

#### 1.5. PROTECTION FROM ACCIDENTS

Defence in depth includes mechanisms and measures to maintain a nuclear plant in a safe and acceptable condition. It includes supplementary features to make sure that departure from such a condition would not develop into an accident, especially one that might cause harm to people. It also includes other measures to make sure that even if prevention of accidents did not succeed, harm would still be averted. Both kinds of protection, prevention of accidents and mitigation of any consequences, are needed.

Prevention of accidents to a nuclear plant is equivalent to making sure that the cooling capability is always sufficient to prevent overheating of the nuclear fuel. The rate of generation of nuclear heat must not become too great, and the effectiveness of cooling must not be excessively degraded through loss of the coolant or reduction of its flow rate, for instance through failure of pumps or reduced pumping power.

Early safety authorities often assumed that protection against the most extreme accident of any kind would automatically protect against smaller accidents of the same kind. Mechanical systems called 'engineered safety features' were added to plants to protect against the extreme accidents. The extreme accidents came to be termed 'design basis accidents' because they defined the limiting design features of plant systems, including engineered safety features.

The use of engineered safety features in defence in depth became widespread and is now the principal means of protection of nuclear plants from all kinds of accidents. Examples are emergency core cooling systems that would come into play if the normal means of cooling failed. Engineered safety features are now designed to be effective against a wide range of hypothetical accidents, not simply the most extreme ones. The design analysis is based on extensive safety research programmes, thorough testing during commissioning of plants and in-service inspection over the operating life of the plant.

Additional engineered systems have also been added to ensure that the engineered safety features do not fail and numerous operating practices have been adopted with the same objective. This use of defence in depth has been expanded and become highly sophisticated as the nuclear plants have evolved. It has been supplemented by accident management procedures that would be used if an accident began to develop and that would avert the accident or mitigate its consequences.

#### 1.6. INTRODUCTION OF PROBABILISTIC SAFETY ANALYSIS

A major step forward took place when a group under Rasmussen in the USA introduced simultaneous estimation of the probabilities and consequences of accidents beyond those considered in the design basis. The method used has come to be called probabilistic safety analysis (PSA). It traces sequences of failures, including failures of the engineered safety features themselves, estimating the probability of failure at each step, and combining the individual failure probabilities into an overall probability that the full sequence can occur. The consequences of an accident are usually estimated in a separate calculation.

The methods of PSA analyse the behaviour of the reactor and its safety features as a complete system. Interdependences of systems are highlighted, such as simultaneous reliance of several systems on common power supplies and cooling circuits. Even though the results obtained with PSA are not precise, they have led to many

insights on safety and have been of great value in guiding safety designs and practices. Some of the results are given later in this report, where they are used in viewing the overall safety of current nuclear plants.

The methods of PSA were pioneered by Farmer and his co-workers in the United Kingdom, and were developed further by a group under Rasmussen in an analysis of the safety of two nuclear plants in the USA [2]. The work in the USA revealed that the preventive measures in nuclear plant design would not make accidents as unlikely as had been thought, but harm from an accident would be much less than had been previously believed.

### 1.7. THE ACCIDENT AT THREE MILE ISLAND

Both of these general conclusions as to probabilities and consequences of accidents were validated a few years later when a severe accident occurred at Unit 2 of the Three Mile Island nuclear power plant in the USA, destroying the reactor but causing no injuries. The accident also confirmed a number of other points. Up to that time, severe accidents to nuclear plants had only been assumed to be possible. Now it was found that they could indeed take place, and it was seen that they could be very costly. The wisdom of having a tight containment building about a water reactor was confirmed. While very large amounts of fission products were freed from the damaged reactor core, the bulk of them reaching the inside of the containment building, the release of radioactive material from the containment building to the environment was trivial measured in terms of radiation exposure of people nearby. Thorough studies made later by several impartial groups, including several commissioned by the State of Pennsylvania, showed that the accident could hardly have caused any injury from radiation, even at an immeasurable level. However, people in a wide area about the plant had been frightened, and their fear had been partly the result of the total lack of preparation for a possible accident.

The accident at Three Mile Island led to an important improvement in the safety of nuclear plants throughout the world. Some of the knowledge and insight gained could be used immediately in improving safety at other nuclear plants. An important example was the realization that the human element had not been adequately included in previous safety considerations, and this observation prompted numerous advances in design and operating practices at nuclear plants. Other important changes in both hardware and practices followed research stimulated by the accident.

The value of probabilistic analysis in revealing safety weaknesses was highlighted, for the type of accident that occurred had been estimated by the Rasmussen group to be among those that were the more probable. However, the amount of fission products released at Three Mile Island was far smaller than had been predicted

by the Rasmussen analysis. Later research has shown that this was a beneficial result of the large amounts of water released into the containment building during the accident, water which retained most of the fission products released from damaged fuel.

### 1.8. THE CHERNOBYL ACCIDENT

The destruction of the Chernobyl Unit 4 RBMK (Soviet light water cooled, graphite moderated) reactor in 1986 had consequences far more extensive than those of Three Mile Island. Not only were people killed in combating the accident, but the results were severe outside the boundary of the site, and were felt over a large part of the USSR and even beyond. Many people living in areas out to a considerable distance were affected by the fallout of fission products and had to be evacuated, and the disruption of the lives of many still continues. The damage was consistent with the general conclusions of a 1957 study in the USA of the hypothetical outcome of a severe accident to a nuclear plant with no effective containment building. It had been predicted that the impact would be widespread, involving many people in surrounding areas, with large tracts of land downwind becoming unusable for a long time afterwards.

The full toll of the Chernobyl accident on life and health in the USSR is still being assessed. Thirty persons among the operating crew of the plant and the fire brigades that responded to the call for help were killed. Many others had to be treated for severe burns and radiation induced illness. The effects in future years through cancer induced among inhabitants of areas with heavy deposition of fission products are still being estimated. It is now clear, however, that the number of additional cancer cases will be far too small to be seen against the naturally occurring cancer rate (it is not commonly realized that cancer normally causes about 20% of all deaths). Estimating the long term effects of the Chernobyl accident continues to be difficult, because it is necessary to distinguish real physical harm from psychological trauma. Effects of trauma are seen not only among those who received high radiation doses but also among many who received radiation doses comparable to the amount received from natural radiation, or even much less.

At Chernobyl, it was again seen that protection against accidents with loss of control of the nuclear chain reaction is essential. The Chernobyl plant had been designed with an operational mode that could cause the nuclear chain reaction to grow suddenly by a very large factor if it were not stopped immediately. There was no rapid means to stop it under the conditions of the accident.

The accident also reinforced three lessons that had been taught by the Three Mile Island accident. First, safety is much higher when nuclear reactors are housed in sturdy, reliable, leaktight structures capable of retaining the fission products from the worst possible accident. If the Chernobyl reactor had been located in a full sized, reliable containment building, the accident might have been as benign in terms of



harm to the workers and the public as was that at Three Mile Island. However, it is debatable whether a full containment building could have been designed for a plant of the Chernobyl type. In any event, it is unlikely that any more plants of the Chernobyl design will ever be built.

Second, though design defects set the stage for both of these severe accidents, to differing degrees, the immediate causes in both cases were mistakes by operating personnel. The mistakes occurred because operators did not fully understand their plants. Training and operating practices that prevent such mistakes, and features that would protect the plant and the public even if mistakes were made, are of the highest importance in the safety of nuclear plants. They are discussed in Basic Safety Principles for Nuclear Power Plants [1].

Third, if people can cause accidents, they can also be expected to mitigate the effects of an accident once it has begun. Accident management was practised both at Three Mile Island and at Chernobyl, with important consequences in both cases. At Three Mile Island, the operating staff restored cooling to the badly damaged reactor soon enough to prevent release of large amounts of radioactive material to the environment. At Chernobyl, evacuation of nearby people greatly reduced their exposure to radiation and the cleanup operations performed later have reduced the long term effects, especially in nearby areas. Accident management may lead to stopping an accident, with public health protected as at Three Mile Island, or it may extend to massive measures to reduce effects on the public, as at Chernobyl. The importance of accident management is also discussed in INSAG-3.

## 1.9. MANAGEMENT FOR SAFETY

Realization has grown that management for safety must develop a strong safety culture in operating organizations, a topic covered in detail in the INSAG publication Safety Culture [3] and discussed further in Section 2.3 of the present report.

One important underlying cause of the accidents at Three Mile Island and Chernobyl was the failure of the management processes which should have provided this safety culture, as an essential ingredient in a high level of safety. In both cases, there were weaknesses in design, operating practices, training and feedback of operating information, and there was no organized mechanism to ensure that weaknesses were recognized and corrected.

This realization has led to the formation of new national and international bodies which have as their objective the development of good working practices in nuclear plant operation, and the assurance that these practices are followed. These organizations have been very effective in improving understanding of the importance of safety by the nuclear power industry and helping to achieve the high standards necessary to ensure it. They are responsible for much of the improvement in safety in recent years.

## 1.10. ENGINEERING FOR SAFETY

The accidents also led to careful review of the engineered features of some nuclear plants that analysis and experience have shown to possess inherent safety problems. This process is continuing. It has led to modification of some plants (including those of the RBMK design used at Chernobyl), temporary shutdown of some plants for further study and permanent shutdown of a few where analysis indicated that improvement would be too costly or too difficult.

## 1.11. THE MESSAGE OF INSAG-3

The Chernobyl accident also led INSAG to accelerate preparation of INSAG-3 [1]. This publication presents the commonly shared principles underlying the safety of nuclear plants, principles that had solidified over a number of years through international interchange of information and experience. It lists three safety objectives and twelve general principles supporting fifty specific Safety Principles.

Since it was issued, INSAG-3 has been reviewed and discussed in many national and international forums. The reviews have confirmed that the Safety Principles are in fact commonly shared throughout the field of nuclear plant safety.

INSAG-3 is discussed further in Section 2.

## 1.12. LESSONS FROM OTHER EVENTS

Important safety lessons were also learned from events that were not so severe. An extensive electrical fire at the Browns Ferry nuclear plant in the USA was followed by improvements in fire prevention at nuclear plants in many countries. Several incidents at other plants showed the importance of a reliable supply of cooling water. Other incidents revealed previously unrecognized ways by which a single failure could incapacitate several apparently unrelated systems.

These incidents, which were not termed severe accidents because they did not damage the reactor core, helped to improve the safety of water reactors throughout the world.

## 1.13. USE OF EXPERIENCE FEEDBACK

The sharing of operational experience, either by direct information exchange or through national or international organizations, has become one of the most effective ways to improve nuclear safety worldwide. This has come to be recognized by most organizations operating nuclear power plants, which now maintain a system to



collect and interpret operating experience and to disseminate safety information promptly. The practice is on the way to becoming universal. The primary objective is that no abnormal event goes undetected and that problems are corrected so as to prevent recurrence, in order to avoid all accidents which could result more or less directly from such events, either at the same location or elsewhere. This reflects the expectation that an accident of any severity would most probably be marked by a precursor such as an equipment failure or a mistake that could have been the cause of an accident if it had been combined with a series of other failures or adverse conditions and had not been compensated for or corrected by defence in depth. The results of analysis based on precursors are presented in Section 3.5 of this report.

#### 1.14. THE ROLE OF RESEARCH

The historical advances that have just been discussed were in the nature of discrete events occurring against a background of continuous improvement of engineering methods and insights, based on extensive research. In this respect, the development of reactor safety followed a path familiar in all fields of engineering. Much of the engineering on which the safety of nuclear plants rests is conventional and is taken from other engineering disciplines. But in application to nuclear safety the methods have been extended to develop deeper understanding of failure and its causes than is commonly found in engineering. Some of the engineered safety features of nuclear plants are meant to provide protection against the effects of extensive system failure causing severe damage to the plant, even though such failures are not expected to occur throughout the life of the plant. Therefore these features should never be needed. Yet they must be able to work as planned if they should ever be called upon. Assurance of reliability requires analysis of conditions where the normal engineering database is poor, especially because of high temperatures that would be expected.

The safety research programmes that provided the necessary engineering base have spanned the past 35 years. The research around the world, funded by both governmental and private sources, has cost the equivalent of more than US \$5000 million. The engineering methods for ensuring safety of modern nuclear plants have now achieved the status of a mature science.

#### 1.15. SOME COMMENTS ON THE HISTORY

No other technological development except possibly that of aviation has been accompanied by as intense a focus on safety as has nuclear energy. Some will say that such a concentration has been appropriate, because of the extraordinary hazard. That may well be true; INSAG would not wish to see a world with nuclear plants

lacking the inherent safety features and the defence in depth that have been developed over the past three decades.

Society has invested heavily in learning how to structure safety into nuclear plants; the process has been expensive and time consuming and it has been accompanied by the two well publicized failures that have just been discussed. These failures occurred because previous lessons were ignored and complacency caused the guard to be lowered.

This recognition is also a lesson learned from the history of the safety of nuclear plants and the lesson has been applied to preventing similar failures in the future. Defence in depth has been deepened, in terms of both hardware and practices.

The analysis now turns to the questions, what is the system at present, and how well is it working?

## 2. CURRENT REACTOR SAFETY PRINCIPLES

### SUMMARY

The safety of nuclear plants has been developed and refined over a period of more than 35 years. The design features and practices developed to ensure safety have been consolidated in a logical structure in INSAG-3 [1]. These Safety Principles show how the safety of modern nuclear power plants rests on the foundation of defence in depth, with its protective design features and operating practices that augment and support each other both sequentially and in parallel. The Safety Principles stress the importance of a 'safety culture' permeating all activities related to generating electricity at a nuclear power plant and ensuring that performance is at a level of competence and dedication above and beyond simple conformance with good practice. They incorporate safety targets at a very high level, so that with existing nuclear plants the probability of an accident causing severe core damage but no effects off the site should not be greater than once in ten thousand years and the probability of an accident requiring protective measures off the site should not be greater than once every one hundred thousand years. Future nuclear plants should better this by a factor of at least ten.

INSAG-3 contains fifty specific Safety Principles. These begin with the selection of a site for a nuclear plant and proceed through its design, construction, commissioning, operation and final decommissioning. Additional Safety Principles establish the need to develop and put into place accident management features and measures and to establish a plan incorporating emergency measures, even though such capability is expected never to be called on.

### 2.1. MODERN SAFETY CONCEPTS

Until the Chernobyl accident, no commercial nuclear power plant had ever had an accident causing radiation injury to members of the public or to the workers at the plant. There has been no such occurrence since. No commercial power plant with a reactor of the light or heavy water type has ever had such an accident.

The Chernobyl plant was one of several plants of similar design that had physical characteristics causing safety to be heavily dependent on correct operating practices. Other plants of this type are now under review to determine how their design can be improved, and some backfitting to correct weaknesses in design has already been done.

It is now clear that, for some time to come, future nuclear power plants will be evolutionary improvements on the light and heavy water plants that now exist.

These are the focus of attention in this report. It is also expected that the future plants will conform closely to the Safety Principles of design and operation in INSAG-3 [1]. The remainder of Section 2 discusses important aspects of INSAG-3 which are relevant to the present analysis and expands on the brief earlier reference.

### 2.2. SAFETY OBJECTIVES

Several safety objectives were identified in INSAG-3. From the standpoint of the present report, the most significant is the dual objective of preventing severe accidents and fully protecting against the consequences of any accident if one should nonetheless occur. The level of safety appropriate to nuclear plants has been widely discussed, and safety goals have been adopted in several countries. In some countries, goals are expressed in qualitative terms, requiring nuclear risk to be far below other risks that people customarily face in life. Some goals also require that nuclear plants be safer than competing ways of producing electricity. In some European countries, safety goals require that plants be designed and operated so that at most a very small fraction of the fission products in the core could be released from a severely damaged reactor (in Sweden and Finland, for instance, the fraction is 0.1%). Other safety goals set limits on possible adverse health effects even if an accident were to occur and protective devices failed to function as designed.

In INSAG-3, a safety target was proposed for existing nuclear power plants of a likelihood of occurrence of severe core damage that is below about once in ten thousand operating years. Accident management and mitigation measures should reduce the probability of large off the site releases requiring short term off the site response to less than once in one hundred thousand years. Implementation of all the Safety Principles at future plants should lead to safety improvements by a further factor of ten.

It is important that this target for the future be understood in ordinary terms. In a world with 1000 nuclear plants of a future type, more than twice as many as plants now existing, 100 years on the average would elapse between accidents of the Three Mile Island type, which cause no damage off the site. A millennium (1000 years) on the average would pass between accidents requiring protection of people off the site.

### 2.3. FUNDAMENTAL PRINCIPLES

INSAG then stated certain Fundamental Principles which would lead to the desired level of safety. Throughout the Fundamental Principles run several important threads. One is the importance of a rational organizational structure with line responsibility and authority, a precept to be followed during design, construction, operation

and in fact at all stages. The need for review of safety by competent individuals and groups both within and without the operating organization is stressed. Radiation protection practices are discussed. Further attention is given to such important matters as feedback of information gained on safety, training and qualification of operating and maintenance personnel, formality of procedures, maintenance of good records and keeping up to date the drawings and descriptions of the plant and its systems. All the Fundamental Principles are important. In the next three sections special emphasis is given to three topics embedded in INSAG-3.

### Safety imperatives

There are three important operating requirements to prevent the release of radioactive material from the plant, and especially from the active core of the reactor. They are:

- controlling the reactor power;
- cooling the fuel;
- confining the radioactive material within the appropriate barriers.

Most of the protective features of the plant's design, and most of its safety measures, can be directly tied to these requirements.

### Defence in depth

The technical basis for safety of a nuclear plant is defence in depth, a concept introduced in the historical review in Section 1. Defence in depth includes the design features and operating practices that endow a nuclear plant with a 'forgiving' character. A first line of defence is provided by maintaining the plant within the prescribed, normal range of operation. A second line of defence includes features and measures that would respond to departure from the normal operating range, caused by either failure of equipment or human error. The response can be the return of operating conditions to their normal range, or it can even consist of stopping the neutron chain reaction. A third line of defence includes features and measures that would compensate for any failure of the previous lines of defence, preventing a disturbance from developing into an accident. Another line of defence would limit the extent of an accident if one occurred, preventing severe damage to the nuclear plant. Yet another line of defence is provided to ensure that an accident causing damage did not harm workers or people in surrounding areas. Defence in depth is structured into the plant to provide protection against all kinds of accidents, including mechanical or human failure within the plant, or events outside the plant, such as storms, floods or serious earthquakes. The defence provided would also be effective against sabotage if it were attempted.

There can be no absolute assurance that nuclear plants built and operated on the lines of defence in depth are completely free of the possibility of damaging accidents. Safety specialists know this. Rather, their strategy is to treat nuclear plant safety as a quantitative, relative concept, recognizing that it can never be total, and they seek instead to be sure of its achievement at an exceptionally high level. After all, there is no such thing as absolute safety in any endeavour, and nuclear power is no exception. But it is possible for safety to be so good that most people would regard it as absolute. This is the goal in the field of nuclear safety.

### Safety culture

In all types of activities, for organizations and for individuals at all levels, adequate attention to safety has many elements:

- Individual awareness of the importance of safety.
- Knowledge and competence, conferred by training and instruction of personnel and by their self-education.
- Commitment, requiring that senior managers demonstrate the high priority they attach to safety and that individuals adopt the common goal of safety.
- Motivation, through leadership, the setting of objectives and systems of rewards and sanctions, and through individuals' self-generated attitudes.
- Supervision, including audit and review practices, with readiness to respond to individuals' questioning attitudes.
- Responsibility, through formal assignment and description of duties and their understanding by individuals.

Safety culture has two general components. The first, which is the necessary framework of practice within an organization, is the responsibility of the management hierarchy. The second is the attitude of staff members at all levels in responding to and benefiting from the framework. A central feature is that safety culture requires performance above and beyond simple conformance with good practice.

The concept of safety culture has fundamental importance, expressing the means by which personal dedication is ensured and is made to contribute to safety. IAEA Safety Series publication No. 75-INSAG-4 [3] analyses in detail the meaning of safety culture and points out ways by which it can be recognized and achieved.

## 2.4. SPECIFIC SAFETY PRINCIPLES

The Fundamental Principles in INSAG-3 lay a general basis for the structure of activities and measures to achieve safety. Their interpretation and application is found in the fifty specific Safety Principles that follow. The Safety Principles are formulated to structure the defence in depth, through detailed statements of means by

which safety is to be secured at all stages in the existence of a nuclear power plant. There are Safety Principles covering siting, design (both the process of design and design features), construction and manufacture, initial commissioning, and operation. Other Safety Principles are devoted to accident management and emergency procedures.

These Safety Principles cannot be summarized in a way that relates their important content, for they are highly detailed. The reader is referred to INSAG-3 for the particulars. All fifty specific Safety Principles are essential, and optimal safety requires careful attention to each.

INSAG believes that nuclear plants fully conforming to the Safety Principles will achieve the high level of safety that INSAG has sought, as stated in Section 2.2.

### 3. SAFETY OF NUCLEAR PLANTS

#### SUMMARY

This publication considers the safety of nuclear plants of types that will continue to be built and operated for some time to come. These will use light water or heavy water as the coolant and the neutron moderating agent. The safety of such plants can be estimated from the safety records and the probabilistic safety assessments of plants of similar types that have been built in the past. Both methods of estimating their safety face some difficulties; the former demands accumulation of an extensive operating history that is available only after a substantial period of time, and the latter suffers from its well known wide band of uncertainty. Yet useful estimates can be made.

The historical record is reviewed first. With one severe accident, that to the Three Mile Island nuclear power plant, in about 5000 reactor-years of operation, the historical record of severe accidents to light and heavy water nuclear plants seems to be not quite as good as the INSAG target for existing nuclear plants. This target is a likelihood of occurrence of severe core damage below once in 10 000 reactor-years of operation. But the record is acceptably close to this target. INSAG's companion target for existing plants is that the probability of an accident requiring short term off-site response in the form of protective measures against radioactive material should be less than about once in 100 000 reactor-years of operation. No such off-site protective measures have ever been needed up to now for either light water or heavy water nuclear plants, though the operating record is too short to warrant a conclusion that the quantitative target has been met.

When attempts are made by means of PSA to determine the safety of individual plants, the wide uncertainty bands prevent any definitive estimate. Yet a number of assessments give broad support to a conclusion that with certain exceptions existing nuclear plants with water reactors meet the safety targets that INSAG has set for them. The exceptions are being addressed in regulatory programmes in the countries affected, and INSAG believes that where in specific cases the safety of a plant is estimated to fall short of the INSAG targets for existing plants, corrective measures should be applied.

The assessments of the safety of existing plants form the basis for INSAG's judgement that current nuclear plants with water reactors are acceptably close to meeting the near term safety targets, and that future nuclear plants of similar types, meeting the Safety Principles in INSAG-3, will also meet the INSAG long term targets for future plants, and will be safer than existing plants by a factor of at least ten.

### 3.1. FUTURE NUCLEAR PLANTS

The plan is to infer the safety expected from future nuclear plants, using as a starting point the safety of existing plants of similar types. Only two of the kinds of nuclear plants now in use are being proposed for extensive future construction. These are the ones that use reactors cooled and moderated by light or heavy water. The light water reactors (LWRs) proposed for future use are of either the pressurized (PWRs) or the boiling water (BWRs) types. The heavy water reactors (HWRs) are variants of the CANDU plants designed and built in Canada. Attention is therefore confined to plants of these general types.

### 3.2. HOW THE RECORD IS MEASURED

Section 2 introduced the concept of safety targets. It was stated that such targets have been adopted in a number of countries and some have been put forward by INSAG. How can it be ascertained whether they have been achieved?

Only two methods seem possible, and both face difficulties. The first is analysis of the historical record. The second is PSA. These are examined in turn.

### 3.3. THE HISTORICAL RECORD OF WATER COOLED REACTORS

Approximately 5000 reactor-years of operation have now been accumulated with commercial nuclear plants cooled and moderated with light or heavy water. By the end of this decade that number will have grown to nearly 10 000 reactor-years. Only one large accident has taken place at a water reactor, leading to severe damage of the reactor core; this was the accident at Three Mile Island.

An argument can be made that the Three Mile Island nuclear power plant was not operated in accordance with modern safety standards, and that would be true. But to ignore the accident at Three Mile Island in the statistical record for this reason would not be appropriate. Until the accident took place it had been generally assumed that the plant was being operated safely.

The record is then one severe core damage accident with no off-site effects in about 5000 reactor-years. At first sight that is not quite as good as INSAG's target for existing plants, which is that there should be no more than one severe accident to a reactor core in 10 000 reactor-years, but statistically it is not inconsistent with that target. Year by year, the record will approach it more closely if, as expected, no further severe accidents occur.

INSAG's companion target is phrased in terms of the need for off-site protective measures. None were necessary at Three Mile Island, although for a time poor understanding as to what had taken place caused measures to be considered. So there

have been no requirements for off-site protection from accidents over the 5000 reactor operating years, against a target of no more than one in 100 000 reactor-years. Clearly, the historical record is far too short to be helpful and many years must pass without a need for off-site protective action before the record can be said to match this INSAG target.

### 3.4. USE OF PROBABILISTIC SAFETY ASSESSMENT

The problem is very different when probabilistic safety assessment is used to estimate how well nuclear plants meet safety targets. PSA can be used where the chance of harm from an accident is very low. However, the precision is poor in these cases.

PSA is now used extensively in improving the safety of nuclear plants. Its greatest value is found in the identification of weaknesses in design or operation, since these define the accidents making the greatest contribution to the risk.

PSA provides estimates of such quantities as the probability that in a single year at a plant there might be a specific kind of accident that would severely damage the reactor core. It can also be used to estimate the types and amounts of fission products that might escape the containment building after a severe accident, and the effects on people residing nearby and the environment. The effects are calculated in terms of fatalities per year, the probability per year of fatal cancers and the probable financial damage averaged over time. These quantities can be summed for all possible kinds of severe accidents to give an estimate of the total risk.

This estimate can also be used as an assessment of the level of safety achieved with nuclear plants. The estimate must be used with care, especially because the precision diminishes when the calculation is extended from core damage probability to off-site consequences. For this reason, the estimates for individual plants are not definitive measures of the safety of these plants. When a set of results for several plants is assembled, however, those sources of inaccuracies that are random and that are different from one plant to another tend to cancel, so that the overall accuracy can be better than that of the individual cases.

The methods and results of PSA were given a searching review in the report NUREG-1150 by the United States Nuclear Regulatory Commission [4]. Results were presented from new PSAs on five nuclear plants in the USA, developed through the use of methods that produced improved estimates of the effects of uncertainty in input data. The depth of analysis in the project and the international peer review that the report received place the results of NUREG-1150 in a class separate from and above those of other PSAs. The conclusions relevant to the INSAG safety targets were as shown in Table I.

The presentation of results did not permit direct estimation of the probability of requiring off-site action. Therefore those values in Table I are estimates of the

TABLE I. CONCLUSIONS OF NUREG-1150 [4]

	Core damage probability per 10 000 years	Probability of requiring off-site action per 100 000 years
Surry	0.2	0.3
Peach Bottom	0.02	0.3
Zion (modified)	0.6	1.0
Sequoyah	0.6	2.0
Grand Gulf	0.4	0.1

probability that an accident will occur that causes one or more subsequent cancer fatalities. This is a conservative substitute for the INSAG safety target.

All of the plants analysed in NUREG-1150 appear to exceed the INSAG target for the expected frequency of core damage for nuclear plants of the present generation, i.e. core damage occurring less than once in ten thousand years. All but Sequoyah meet or do better than the second target (a need for off-site action less than once in 100 000 years). Sequoyah misses by a factor of two, which is well within the uncertainty in the estimates.

It must be noted that the original analysis for Zion identified one type of accident as the major contributor to the risk, causing the total probability of core damage to be greater than once per 10 000 years. For that reason, modifications are being made at Zion to prevent this exceptional sequence which will reduce the estimated probability of severe core damage to the value 0.6 per 10 000 years in Table I. This illustrates how improvement in the safety of a plant can result from its PSA, which is one of the most important benefits of this methodology.

There have also been many PSAs for nuclear plants in the USA and other parts of the world which, however, were not peer reviewed internationally as were those of NUREG-1150 [4].

### 3.5. PROBABILISTIC ASSESSMENT OF OPERATIONAL EXPERIENCE

While the absolute values of probabilities calculated with PSA are not as precise as one would like, the trends with time are more meaningful. A report has been published by a researcher at the Nuclear Regulatory Commission in the USA [5] that

compares the current rate of accident 'precursors'<sup>2</sup> with that in previous years. This has been used as a basis for estimating the probability of the severe accidents themselves. It was concluded that for the past few years the average probability of core damage has been much lower than it was before the lessons learned from the Three Mile Island accident were implemented in operating plants. It was estimated that the probability of core damage for a single plant has been reduced from a value of the order of 1 per 1000 years before 1979 to a value now of between 1 per 10 000 and 1 per 100 000 years.

Since in most of the world the same improvements in safety are being made, the conclusion can be extrapolated accordingly.

### 3.6. EXCEPTIONAL CASES

It is estimated that several nuclear plants with water reactors have probabilities of core damage an order of magnitude higher than the INSAG target because of inadequate safety systems or specific design weaknesses that have not yet been corrected or compensated for. National regulatory programmes are actively pursuing their improvement. It may be that within the accuracy of their PSAs, even these plants would really meet the INSAG targets, but in the interest of conservatism, INSAG believes that when any plant does not seem to meet the safety target, it should be improved accordingly.

### 3.7. CONCLUSION

INSAG concludes from the preceding review of the historical record and the PSAs that, with certain exceptions, light and heavy water nuclear plants of the current generation have levels of safety in reasonable agreement with the INSAG targets. INSAG further concludes that similar plants to be built in the future that fully meet the Safety Principles enunciated in INSAG-3 will be safer still, and should meet the long term target of a level of safety ten times higher than that of existing plants.

<sup>2</sup> An accident precursor is an equipment failure or a mistake that could have been the cause of a severe accident if it had not been compensated for or corrected by defence in depth.



## 4. NUCLEAR FUEL CYCLE

### SUMMARY

INSAG recognizes, however, that the safety of the nuclear option must be evaluated in terms of its complete fuel cycle, not simply of electricity generating plants. The other parts of the cycle include the front end activities of mining and the chemical and physical preparation of uranium into fuel elements, and the back end activities of spent fuel storage and disposal. In some countries, the last activity includes chemical reprocessing, which makes part of the contents of the spent fuel reusable and is capable of greatly reducing the volume of waste to be disposed of. The amount of actual waste from a nuclear plant is very small, a factor of about 300 000 smaller than that from a coal burning power plant. The amount of spent fuel removed from a nuclear plant is smaller by a factor of about 10 000 than the amount of ash from a coal fired power plant.

Among the hazards attached to the fuel cycle, those associated with uranium mining stand out. The conventional hazards to uranium miners are the same as those faced by other hard rock miners, and are smaller than hazards faced by coal miners. Uranium miners also experience risks from inhalation of radon, but with proper ventilation these are held below recommended limits set by international organizations to protect the workers. The only other source of hazard from the front end of the fuel cycle is that associated with tailings piles, which are the residue from the extraction of uranium from ore. These are sources of radon. These man-made deposits emit only a very small part of the radon released everywhere on Earth by rocks, soil and sea water, but they must be segregated because they are more concentrated sources. Action must therefore be taken to ensure that tailings piles are kept isolated and confined.

The initial step in the back end of the fuel cycle is storage of spent fuel at the nuclear plants after its removal from the reactors. This is a straightforward and time tested process, spent nuclear fuel having been stored under water in deep pools without incident for decades, ever since the first nuclear reactors went into operation.

Following temporary storage at the nuclear plant, final disposal of the waste is required. Though it is sometimes said that the problem of disposal of highly radioactive waste from nuclear plants has not been solved, this is not the case. There is not a great deal of such waste to be stored, because nuclear plants do not use very much fuel, and there is widespread agreement in the nuclear community on the mode of disposal to be used. The waste is to be encased in containers which are highly resistant to corrosion and stored in dry man-made caverns deep within the Earth. The material to be stored may consist of the fuel elements themselves, in which case the fission products remain locked in the fuel in which they were produced. However,

some countries follow the path of reprocessing the spent fuel to recover some of the valuable content and to reduce the volume of actual waste. The fission products are then converted into a long lived glass, which is stored in caverns in corrosion resistant containers. Research is being conducted in several countries on other, more speculative, methods of disposal of the waste from reprocessed nuclear fuel, an example being a proposal for use of transmutation of some of the radioactive ingredients.

Repositories are to be sited and designed such that no one should ever be exposed to radiation from waste stored within them, over all future time. If unusual and unexpected developments at some future time were to expose this material to the world of human existence, maximum radiation doses to any individuals are still to be well below those from natural radiation exposure.

The adverse effects on human beings from the front end and the back end of the nuclear fuel cycle are a minor part of the total radiological impact of nuclear power, which is itself very small compared to the normal exposure of people to cosmic rays, radon and direct radiation from the Earth.

### 4.1. NUCLEAR FUEL CYCLE

The safety of nuclear energy is not solely a question of the safety of the plants producing the electricity. An entire industrial complex is required to supply nuclear fuel to the reactors, and another complex still in a formative stage in many countries will be engaged in disposing of the used fuel after its removal from the nuclear plants. These complexes are the parts of what is called the nuclear fuel cycle.

The front end of the nuclear fuel cycle consists of mining and milling of ore, extraction and purification of the uranium, conversion to the feedstock for the manufacture of nuclear fuel (the most important step for light water reactors being enrichment in the fissile isotope  $^{235}\text{U}$ ) and fabrication of fuel elements. After irradiation in the reactor, where some of the uranium is converted to fission products, the fuel elements are removed from the reactor and temporarily stored deep in a pool of water at the site. Two options are available for subsequent treatment in the back end of the cycle: the spent fuel can be sent directly to final storage as waste, or it can be reprocessed chemically to recover the useful fraction of the contents and the waste from this step can be sent to final storage.

In a large nuclear plant, fission consumes only from 1 to 3 kg of uranium per day. Most of the uranium in the fuel is not fissioned at all; the daily average of fuel used in the reactor is typically about 100 kg, of which all but about 4 kg is unchanged by its use in the reactor and is in principle recoverable. This is to be compared to about 10 million kg of coal burned daily in a corresponding coal fired power plant. The amount of waste from a nuclear plant is correspondingly small compared to that from a coal burning plant.

As is true of all large scale industrial activities, nuclear fuel cycle operations have their specific health and environmental risks. The sources of this risk in the nuclear fuel cycle are the mild radioactivity of the raw material, uranium, and the intense radioactivity of spent fuel (from fission products formed in the reactor during operation). As stated earlier, the quantity of waste is relatively small, but care has to be taken to handle it and to dispose of it in such a way that the fission products and their radiation do not become an unacceptable hazard to man and the environment.

#### 4.2. FRONT END OF THE FUEL CYCLE

The raw material of nuclear energy is the element uranium. Uranium is found to some extent everywhere on Earth — in soil, rocks and even in all sea water. Uranium is radioactive, but since its rate of radioactive decay is so slow, the radioactivity is mild. Nevertheless, when the uranium in nature becomes concentrated, as in some ores and in the residue from mining, certain requirements for health protection become necessary.

Mining and milling of uranium pose certain occupational risks which are similar to those found in many other mining operations, because the methods are basically similar. A notable exception is coal mining, which is much more hazardous because of the possibility of fires and explosions, and the breathing of coal dust, which causes debilitating and often fatal black lung disease among coal miners.

Unless suitable precautions are taken, uranium miners are also exposed to specific hazards from breathing a higher than usual concentration of the radioactive gas radon and its radioactive daughters, which are products of the radioactive decay of uranium. Uranium decays into a sequential chain of radioactive elements that includes radium, with radon near the end of the chain. The chain ends with a non-radioactive isotope of lead. Radon is present everywhere in the air as a result of the radioactive decay of uranium throughout nature. Radon is more concentrated in uranium mines because more uranium exists there. Breathing radon can lead to a higher risk of lung cancer from the deposition of its radioactive decay products in the lungs. When proper ventilation is provided, the annual radiation dose received by uranium miners from radon and its decay products is reduced to an amount within recommended occupational exposures, at which effects are very small. In addition, the number of uranium miners needed to support an industry is relatively small. Even so, and even with precautions taken, radiation doses to miners tend to be higher than doses to workers in most other parts of the fuel cycle. When the conventional hazards of mining are also taken into account, this part of the fuel cycle is found to be the most hazardous to workers.

Residual tailings from milling of uranium ore still contain a small residue of uranium and most of the radium that accompanied the original uranium. Tailings are

discharged from mills to impoundments. The tailings piles accumulating in the impoundments act as sources of radioactive radon gas, augmenting the normal release of radon from soil everywhere. The total rate of release of radon from tailings piles is minute compared with the amount of radon that enters the Earth's atmosphere from the normal radioactive decay of uranium in soil, and is especially small compared with that released from the soil during ploughing for the planting of crops, but the contribution from the tailings piles is localized and can cause nearby concentrations of radon to be undesirably high. The specific safety requirement in this connection is to make sure that the tailings remain confined and isolated. The lifetimes of radon isotopes are short, and isolation is found to be adequate when a tailings pile is covered with a layer of material such as concrete or asphalt, or a thick layer of soil to retain the radon until it has decayed. This precaution also guards against the ingestion of dust carrying uranium and its other radioactive daughters. Such a solution is only temporary, because radon will continue to be evolved, effectively forever, and a more permanent solution will be needed, such as reburial in empty mines.

Some tailings piles have not been well managed and protected in the past, and at times the tailings and waste rock piles have even been mined for building material for houses. The hazards associated with this material are not severe, but they are to be avoided, and this point is now well recognized.

The occupational exposures and local and regional dose commitments from such other front end fuel cycle activities as manufacturing and handling nuclear fuel are negligible, being far below normal radiation doses from natural background radiation. They are included in the estimates of risk in Appendix III.

#### 4.3. BACK END OF THE FUEL CYCLE

It is frequently said that no solution to the problem of disposing of nuclear waste has been found. In fact, several satisfactory means of waste disposal have been considered at length, and there is widespread agreement in the scientific community on the broad outline of the preferred methods. Some alternative choices are still retained within the general strategy, but these generally reflect differences in details of the fuel cycle adopted by different countries.

The problem is made easier by the fact that the volume of fuel burned in a nuclear plant is so small, and it is therefore possible to store the amount of spent fuel or waste produced over a plant's entire lifetime in a relatively modest space. This is an outstanding ecological advantage of nuclear power; the waste it generates is not automatically spread over the environment as is the case with waste gases from coal fired power stations. On the contrary, the radioactive material in the nuclear waste is confined for long periods, perhaps forever, in the fuel elements in which it was first generated. Retention of these used elements for periods of many years during

operation of the plant is no problem at all; the technology for storage in water filled pools has been used for decades. Dry storage in shielded containers has also been demonstrated and is in use in a number of countries. Storage of fuel at a nuclear plant by either method causes no radiation exposure of either the public or the workers.

### Permanent disposal of spent fuel

It is in connection with methods to be used in the longer term that controversy has arisen. Some countries have chosen to dispose of their spent nuclear fuel without first reprocessing it to recover the useful uranium and plutonium that it contains. The fuel would first be encased in containers with the void space filled with some inert material. The entire package of the container with its contents would be designed to resist corrosion or other chemical attack. The encapsulated fuel elements would be buried in deep man-made caverns in geological formations carefully chosen for stability and the assurance that they would be free from the entry of groundwater over long periods of time. Absence of water would ensure freedom from corrosion and would prevent dispersal of radioactive material by water pathways. There have been numerous studies of this method of disposal of spent nuclear fuel, many by such impartial bodies as national academies and government commissions. All have concluded that these disposal methods would safely confine the material for very long periods of time, enough for it to become non-hazardous through the process of radioactive decay. The stored waste should remain intact for periods of the order of 10 000 years or more. This approaches twice the duration of civilization on Earth. It is also approximately the length of time since the end of the last ice age.

Although many members of the public remain sceptical, the majority of the scientific community is convinced that protection of people and the environment can be ensured over these long time periods and into the indefinite future. This confidence is based on understanding of the underlying scientific information: corrosion rates of storage containers, removal of heat from spent fuel, geology, and potential movement of water through waste repositories and the surrounding geological formations. The underlying scientific information is based on relevant research and the analytical techniques for extrapolating into the future can be checked in laboratory and field experiments.

Even so, public opposition has dramatically slowed the onset of storage of spent fuel in most countries that intend to make use of this method. The political and industrial will to implement the process has not been as strong as it might have been. This situation has only been tolerable because of the continued ability of nuclear plant operating organizations to retain spent fuel in storage pools at plants for very long periods of time, a possibility that exists because there is relatively little spent fuel. Of course, such an interim solution cannot be continued forever.

### Spent fuel reprocessing

Many countries with large nuclear programmes have decided in favour of reprocessing the spent fuel. Commercial reprocessing plants are in operation in several countries, such as at Sellafield in the United Kingdom and La Hague and Marcoule in France. The capacity of these plants represents only about 5% of the spent fuel from present nuclear power plants, but additional reprocessing plants are being built.

Reprocessing consists of dissolving the spent fuel in an appropriate acid and then chemically separating the constituents. The plutonium can be reused as a fuel in a fast reactor or in a light or heavy water reactor. The uranium can be stored, to be introduced at some future time into a fast breeder reactor to make more plutonium for use as a reactor fuel. The fission products and the inert components such as the metallic fuel cladding are segregated as waste and are directed to final disposal as described in the next subsection. Small amounts of certain radioactive nuclides are released to the atmosphere during reprocessing; these are principally tritium,  $^{14}\text{C}$ ,  $^{85}\text{Kr}$  and  $^{129}\text{I}$ . These nuclides would disperse quickly through the environment and so their concentrations would always be low. They add minutely to the global dose commitment from naturally occurring radioactivity. UNSCEAR [6] has estimated the dose commitments from these nuclides if all spent fuel presently produced were to be reprocessed (the total radiation dose over all time of all people involved). These dose commitments are found to be very small compared to those due to natural sources.

However, if the nuclear industry were greatly to expand, with reprocessing of spent fuel commonly pursued, some measures would have to be introduced to segregate and store some noble gases that are radioactive fission products (principally  $^{85}\text{Kr}$ ). The technology for doing this is known and has been developed.

### Storage of waste from reprocessing

After reprocessing, the fission products from the spent fuel will be concentrated in the high level waste, to be converted into a long lived glass and encased in corrosion resistant containers. These will be placed in the final repository. The repository will be an underground cavern similar to those for unreprocessed fuel. Selection of a geological environment that would have only a small likelihood of incursion of water would provide protection against corrosion and leaching of the containers of waste, and would prevent water transport of radioactive contents to where they might introduce a hazard.

## The Oklo phenomenon

A high degree of confidence that no dispersal of stored waste from reprocessing would ever take place followed the discovery of deposits of uranium ore at Oklo in Gabon. There, about a thousand million years ago, the concentration of uranium in a swampy region was so great that a natural nuclear chain reaction took place. It continued at a low level over a very long period of time, generating far more fission products than any man-made nuclear plant. Almost all of the fission products remain in place where they were produced, even the continued presence of the water in the swamp having failed to disperse them.

## Radiation exposures from storage

All countries having national waste management programmes proceed from a consensus that nuclear waste should be stored in such a way that no subsequent radiation exposure of human beings would be expected, and that if disruption of a waste repository did occur, radiation exposures should be a small fraction of that due to natural background sources. The current recommendations of the International Commission on Radiological Protection (ICRP) for repository planning call for a maximum annual effective dose to any individual from a repository accident to be well below the normal background radiation dose.

## Decommissioning of nuclear plants

At the end of their lifetimes, nuclear plants will be decommissioned and eventually dismantled. While the costs are thought by some to be of concern, the effects on human health and safety will be minor. In particular, the radioactive wastes from dismantling a nuclear power plant will pose no threat to public health. Their total radioactivity is far less than that of the spent nuclear fuel.

## 4.4. THE EFFECTS ON HUMANS

The adverse effects on human beings of the front end and the back end of the nuclear fuel cycle have been included in the analysis presented in Appendix III in estimates of the overall risk from generating electricity by nuclear plants. They are a minor part of the total radiological risk from nuclear power, which is itself very small compared to the risk from the normal exposure of people to cosmic rays, radon and direct radiation from the Earth.

## 5. FEATURES DESIRED IN FUTURE PLANTS

### SUMMARY

The current slowdown in the growth of the nuclear power industry offers an opportunity to further consolidate nuclear plant safety by means of design improvements for future reactors. This could start by incorporating more naturally the safety features that have been added on to earlier designs. Plants built according to such restructured designs may be less expensive in the long run, may be less complex and may be more readily accepted by the public.

Beyond this process of consolidation of past gains is an opportunity for further substantial improvement of the level of safety of nuclear plants through future design choices. INSAG lists in this report directions that it believes should be followed in the designs of future plants, building on and even exceeding in certain respects the safety capability offered by the Safety Principles of INSAG-3. It is believed that the level of safety that could be achieved from these advances would be substantially higher even than that attached to the previously stated INSAG targets. The safety would exceed that of competing means of generating electricity by at least a factor of ten, and would reach a level unprecedented in this modern technological world. As a cautionary note, however, INSAG also believes that implementation should take into account the need to devote the resources of society to the most fruitful means of reducing risk of all kinds, not only that from nuclear power.

The features identified as desirable are as follows:

The Basic Safety Principles of INSAG-3 should become mandatory, with the following predominant features:

- Defence in depth continues to be the fundamental means of ensuring the safety of nuclear plants.
- The three fundamental safety tenets continue to be: maintain cooling; control the power level; and confine the radioactive material.

More specific aspects of design should be addressed as follows:

- The concept of plant design should be extended to include the operating and maintenance procedures required for it.
- Design should avoid complexity.
- Plants should be designed to be 'user friendly'.
- Design should further reduce dependence on early operator action.
- The design of the system provided to ensure confinement of fission products after a postulated accident should take into account the values of pressure and temperature encountered in severe accident analysis.

- Accidents that would be large contributors to risk should be designed out or should be reduced in probability and/or consequences.
- The plant should be adequately protected by design against sabotage and conventional armed attack.
- Design features should reduce the uncertainty in the results of probabilistic safety analysis.
- Consideration should be given to passive safety features.

### 5.1. FURTHER IMPROVEMENT OF SAFETY

It is an important duty of the nuclear power industry to ensure that its operations are as safe as can reasonably be achieved. This means that opportunities for improvements should be taken, though always with regard to the balance of safety benefit against additional cost and the possible need for improvements in safety elsewhere in society. Attention to this duty is a proper response to the evident wish of the public that nuclear power should be exceptionally safe.

Worldwide, there is a slowdown in the development of the nuclear option, and it is right, therefore, to examine what may be possible in terms of consolidation and improvement of safety. Consolidation means that design improvements now recognized should take their place directly in the design rather than as superimposed requirements. This will allow simplification of designs, and features and layouts can be made more user friendly. If public acceptance became easier, there would be an added advantage of reduced generation costs.

If additional safety improvements are deemed necessary, to establish more clearly the future of the nuclear option, it is possible to take matters further. Other design options can be contemplated, such as those discussed in generic terms in the following. Such further improvements would ensure achievement of long term safety exceeding the assurance offered by the Safety Principles of INSAG-3. As that publication stated, the safety level sought from the measures it advocates would already far exceed what can be achieved for electricity generation by other means, and would be without precedent in any other area of technology.

As a restraining principle, and even if the force of public pressure is strong, such safety improvements should be pursued only if they can be implemented without disproportionate cost. Thus action towards the goal of extreme safety should be weighed against the possibility that it would be wiser to direct society's resources to other areas where the level of safety is much poorer.

### 5.2. FUTURE FEATURES

*The Basic Safety Principles of INSAG-3 [1] remain valid and should become mandatory.*

Designs may seek to realize some of the Safety Principles in ways that are more rational or more straightforward than in existing plants, but the Safety Principles are not thereby altered. The Safety Principles relating to design come first to mind when future plants are contemplated, but it must be remembered that safety is a discipline broader than design. Attention is needed in all phases to ensure that the other Safety Principles of INSAG-3 are also met.

From the concepts presented in INSAG-3, two are of such fundamental importance that they must continue to be emphasized in any general consideration of the safety of nuclear plants.

- Defence in depth must continue to be the fundamental means of ensuring the safety of nuclear plants. It may be supplemented by design features that offer exceptional protection against some kinds of accidents, or may be implemented by them, but it cannot be supplanted by these features. Defence in depth should still include sequential barriers to the release of fission products, and plant features that protect these barriers. Defence in depth should continue to be augmented after commissioning through a well planned and well formulated mode of operation, documented in detail and carefully taught to operating staff.
- The three fundamental safety tenets are still: maintain cooling, control the power level and confine the radioactive material. These tenets are the basis for avoiding accidents to nuclear power plants during operation and for controlling accidents if they begin. All relevant activities in design, construction and operation are directed in greater or lesser degree to ensuring adherence to the tenets, and the demonstration that they are met must be convincing.

Beyond the Safety Principles of INSAG-3, but in extension of them, are further opportunities for improvement of safety. INSAG believes that new plant designs, whether derived in an evolutionary manner or by stepwise development on radically different lines, should begin to draw on such opportunities.

- (1) *The concept of plant design should be extended to include the operating and maintenance procedures required for it.*

The design alone cannot confer safety on the plant, because operation and maintenance must also conform to the assumptions made in the safety analysis. The design can be considered complete only after the operating and maintenance regimes are specified in limiting conditions for operation and appropriate operating and maintenance procedures. Thus the supplier of a plant has not discharged all his responsi-



bility for safety solely by providing a plant with a safe design and equipment of high quality. The supplier must ensure that the operator is provided with the information needed to perform in accordance with the operating and maintenance assumptions inherent in the design.

(2) *Design should avoid complexity.*

The design engineers should seek simple layouts and should endeavour to eliminate unnecessary components and systems. This does not mean that the numbers of components and systems should be minimized, because excessive zeal in getting rid of them can run counter to safety. It does mean that there should be good reasons for the presence of each component and system. Choices should be sought that will help to simplify normal operating procedures, emergency operating procedures, inspection, testing and maintenance. Above all, simplicity should help the operating and maintenance personnel to understand the plant and its operation, both normal and abnormal. Improved understanding will build confidence in the validity of decisions by the staff under all conditions. It will reduce the likelihood that common cause failure modes could exist without having been recognized.

(3) *Plants should be designed to be 'user friendly'.*

'User friendly' is a term more commonly encountered in connection with computers, but it is also appropriate in describing properties of the plant sought for purposes of good human factors. The design should be user friendly in that the layout and structure of the plant are readily understandable so that human error is unlikely. Components should be located and identified unambiguously so they cannot easily be mistaken one for another. Operations should not be required simultaneously at points distant from each other. The control room and its artificial intelligence system should be designed after a failure modes and effects analysis of the plant, with information flow and processing that enable control room personnel to have a clear and complete running understanding of the status of the plant.

(4) *Design should further reduce dependence on early operator action.*

Errors by operating staff at a nuclear plant are not as frequent as sometimes thought, but they do sometimes occur. They are most likely if decisions must be made under time pressure. Therefore any required immediate response to an abnormal situation should be automatic. The artificial intelligence system should clearly inform control room personnel of any such automatic action and why it is being taken. Automated response should continue for at least a reasonable predetermined time dependent on prior assessment, but the opportunity should remain for the operators to override automatic actions if diagnosis shows that they need supplementing or correcting.

(5) *The design of the system provided to ensure confinement of fission products after a postulated accident should take into account the values of pressure and temperature encountered in severe accident analysis.*

The possible severe accidents should be analysed by realistic methods, which should demonstrate the capability of confinement with ample margin under conditions of temperature and pressure to which the confinement system might be subjected if an accident took place.

(6) *Accidents that would be large contributors to risk should be designed out or should be reduced in probability and/or consequences.*

Though this topic is broadly addressed in INSAG-3, the thrust of the present report calls for added emphasis on it. By 'reduction of probability' is meant that such accidents should not remain large contributors to risk. The types of severe accidents in this category are generally those that might lead to bypass or early failure of the confinement function. The intention is elimination of the higher risk 'outliers' among the possible event sequences for potential accidents. This implies optimization of protection by balanced design. INSAG does not look for steps to be taken to reduce the estimated probability of core melt from a single sequence to below once in ten million years for a specified nuclear plant, because estimates at these levels are unreliable.

(7) *The plant should be adequately protected by design against sabotage and conventional armed attack.*

Nuclear plants are naturally well protected against violent events, since they are surrounded by thick, strong shielding against the radiation generated within them, they commonly have strong confinement systems encasing them and they possess substantial defence in depth through their safety systems. These also protect against the possibility of sabotage by plant personnel and against malevolent intrusion. However, further protection against unwanted intrusion is ordinarily provided. If this natural defensive state is suitably enhanced, it should not remain necessary at future plants to depend on extensive security measures and large protective security forces. Review of vulnerability of the plant to violent attack should be part of the design process.

(8) *Design features should reduce the uncertainty in the results of probabilistic safety analysis.*

Probabilistic safety analysis is used to estimate the level of safety achieved by design and to eliminate design weaknesses. It is important that this tool be effective.



The effectiveness is reduced when the calculated results are not precise. All of the recommended improvements would reduce both the probability of severe accidents and the uncertainty in this probability.

(9) *Consideration should be given to passive safety features.*

Passive safety features are the engineered safety features that ensure plant shut-down, continued cooling and retention of fission products. A safety system is passive if it accomplishes its function automatically without drawing on an external, artificial power source such as electricity. The benefit of not requiring an external power source is that the safety function does not depend on the reliability of a different system. Such an advantage of passivity may become overwhelming. However, though it may seem evident that passive systems are always safer, that may not be so in all cases. There may be safety disadvantages that would outweigh the gain. The superiority of the choice should be shown by demonstration or analysis.

## 6. CONTINUED IMPROVEMENT OF NUCLEAR POWER PLANT SAFETY

### SUMMARY

Work is proceeding in several countries on designs of advanced nuclear plants based on reactors cooled and moderated with light or heavy water. Some designs are well advanced, for nuclear plants now being built or available to be built soon. These are close evolutionary descendants of plants that now exist. They embody numerous improvements in safety over present plants, generally on the lines advocated in this report. Though they are limited in some respects in the ability to improve on good current practice, the most recent series of light and heavy water nuclear plants can fully comply with the Safety Principles in INSAG-3 and can meet the safety objectives that INSAG has proposed for future nuclear plants.

Designs with safety features that would be largely passive in function are also being developed in a number of countries. A substantial amount of work remains to be done on these concepts, including detailed design, some research and development, and safety review for licensing. Yet some designs are far enough developed that they could be available for construction late in the 1990s. These largely passive designs could incorporate many or all of the additional safety features INSAG has proposed in this report. However, passive safety is not necessarily improved safety in all cases, and the benefit must be carefully weighed before the choice is made. Plants in this category will provide an unparalleled degree of safety if they live up to their promise.

A third class of designs includes concepts proposed by several groups seeking complete freedom from the possibility of severe accidents. These designs are all at the conceptual stage, and a great deal of work is needed to establish feasibility and to evaluate the extent to which the safety gains can be realized.

INSAG believes that the level of safety desirable for nuclear power plants can be achieved with light and heavy water reactors that are now being realized and that even greater safety can be projected for plants that are being proposed as their successors. However, society may demand an even larger improvement in safety as the cost of approving continuation of the nuclear option. If this is to be the case, imaginative and revolutionary concepts such as some briefly discussed in this report might offer an acceptable solution, and that could justify their accelerated development.

### 6.1. DIRECTIONS OF CHANGE

The previous sections have stated that future nuclear power plants should fully meet the Safety Principles of INSAG-3 and that they should go beyond to take advan-

tage of opportunities for further improvement identified in Section 5. The changes taking place in the design of plants, some under way and some as yet only contemplated, are now reviewed. This overview shows that all future plants, in both the near term and the far term, will exploit features that have been identified in this publication.

Work is proceeding in several countries on advanced designs of nuclear power plants with reactors cooled with light or heavy water. The units that will be built in the near future and those most likely to follow shortly after are evolutionary developments from currently operating plants. The changes are in the direction of simplification, improved operating features and, above all, higher levels of safety.

It is recognized everywhere that future nuclear plants should be designed so that accidents are very unlikely at the very least, and are as near to impossible as technology allows. This is the first and most important objective of defence in depth. Beyond this, plants must be able to accommodate severe accidents without harm to workers or the public. Ultimately, plants would be so safe that there would be no technical justification for an emergency plan involving evacuation of the nearby population.

All evolutionary designs aim at eliminating certain pervasive sources of erosion of defence in depth: poor quality, human ignorance and human error in operation. The means being employed would also be effective against sabotage if it were attempted, though it must be noted that no instance is known of a wilful attempt to cause a serious accident to an operating nuclear power plant. Evolutionary improvement is addressed not only to enhanced design of plants but also to the need for quality at all stages, including those of construction and operation. Those improvements are in keeping with the Safety Principles of INSAG-3.

The planned improvements in reactor designs for the near future are substantial, and they will be further augmented in successor plants.

In the following, there is first a discussion of designs based on proven technology, which incorporate evolutionary improvements and are being constructed or are planned for early construction. Then plants are discussed that will incorporate an increased use of passive safety features and which could be committed for construction later in this decade. Finally, there is a brief review of revolutionary new concepts that have been advocated on the grounds that they promise safety approaching the absolute. These still require extensive feasibility studies to be followed by detailed engineering and a commitment to construct such a plant does not seem possible until the following decade.

## 6.2. BENEFITS FROM DESIGN EVOLUTION

The evolutionary process, proceeding on the lines of proven technology, is the means by which problems are generally overcome in all engineering development.

It builds on the strengths of existing technology, correcting identified shortcomings and profiting from successful lines. Future nuclear plants, incorporating the results of evolutionary improvement, will be built and operated with even more quality than existing plants, should have fewer operational incidents and reportable operational events, and will be more accident resistant.

What level of safety can be expected from such evolutionary improvements in design? INSAG believes that these future plants, having profited from the experience of the past, can conform fully to the Safety Principles of INSAG-3 and can achieve the safety targets that INSAG established for future plants. This means that in a world with a thousand operating nuclear power plants of the advanced designs, more than twice the number of plants now existing, an accident severely damaging some nuclear plant somewhere should not be expected more often than once a century, and an accident somewhere threatening to harm people should not occur more often than once in a millennium.

## 6.3. EVOLUTIONARY DESIGN IMPROVEMENTS FOR THE NEAR FUTURE

Designs incorporating evolutionary improvements on several current types of light water nuclear power plants have progressed to the point where construction could begin soon. The design criteria and the key features have been set, the safety characteristics have been evaluated in safety analyses, the supporting development is well along, and the process of obtaining regulatory certification is under way or in some cases is complete.

Many proposed changes in design aim at a significant increase in particular safety margins, which will greatly improve resistance to accidents of all kinds. Concerns as to human error will be reduced, through plants that are more 'forgiving'. Such changes do not require sacrifice in performance; on the contrary, both safety and performance are expected to profit and it has only been necessary to achieve the proper balance between the two.

One improvement, already adopted for some light and heavy water pressurized water plants, is increase of capacity of the pressurizer and the secondary side of the steam generator, to slow the response of pressure and temperature of the plant to changes in power level. Two other changes already implemented in many light water reactors are the introduction of pressure vessels that have been made without longitudinal welds, and with a geometrical arrangement of their contents that reduces the incidence of fast neutrons on the wall of the vessel. These measures will increase the lifetime of plants and reduce the need for special measures of protection. The improvements in vessel design alone will yield substantial benefits in both safety and economics.

Contemplated design changes will also further reduce any routine release of radioactive material from the plant. Such releases are already well below regulatory

limits and are so low that any possible radiation resulting from them is at levels far below those due to natural background radiation. Yet even more reduction is possible, at an added cost. Public anxiety seems to demand such reductions, though the benefit is not large.

Numerous changes are being made in different ways in different designs to improve the performance of components and systems, with the objectives both of reliability and safety. The following list is not exhaustive but only illustrative. Greater use of burnable neutron absorbers in fuel reduces changes in reactivity as the operation of PWRs proceeds and thereby reduces the requirements on their soluble boron systems. The newer BWRs for Japan and the USA use the internal recirculation pumps pioneered by European designs to eliminate large pipes that have required special inspection and occasional replacement at considerable cost in time and money. The emergency core cooling systems of all types of plants are improved to introduce some passive features and to provide for the use of supplementary sources of water as extended backup. The advanced heavy water reactors incorporate reductions in the linear power generation of the fuel and improved protection against external events. All of these design changes enhance accident prevention and implement Safety Principles of INSAG-3.

#### 6.4. NATURAL LIMITS ON EVOLUTIONARY IMPROVABILITY

There seems to be a limit to the benefits to be gained from evolutionary improvement of current designs. Three main factors set the basis for this limitation. These are: human factors in operation, the complexity of plants and limits on the benefit from confinement systems. To go beyond in the search for greater safety would require more radical changes, of the kinds discussed later in this section.

##### Human factors in operation

All advanced designs include changes affecting human factors in fundamental ways, making the plants more user friendly in the sense discussed previously. The most pronounced changes are made in the use of advanced electronics, especially in control rooms, where microprocessors and video display units are employed extensively. To varying degrees, the different evolutionary designs introduce artificial intelligence to assist the operating staff in monitoring the status of the plant and to provide them with prompt notice of the onset of any abnormal operating conditions. Some of the new designs also include software endowing the instrumentation and control circuitry with a diagnostic capability, to guide the operating staff in responding to any abnormality.

Even where there is a greater degree of automatic response to abnormal conditions, with the operator informed immediately of the action taken (this is the practice

at some operating plants), evolutionary designs rely on operators to take any further action after some specified time, typically beyond 30 minutes following the first automatic response. The possibility remains that human error could occur in the course of these subsequent actions, even though the extended period provided for reflection would remove time pressure. Furthermore, a small possibility always exists that a computer software error could lead to inappropriate automatic action or could mislead the operating staff. Software errors can be reduced significantly in number and impact through sound software design practices and prior testing, including testing using plant simulators, but the elimination of errors can never be absolutely guaranteed. INSAG therefore concludes that there is an inherent limit to improvement through reduction of human error. This limit underscores the importance of designs that are 'forgiving' and that incorporate defence in depth so effective that harm would be averted even if failure were to occur.

##### Complexity of plant

Simplification of design is cited in many policy statements as one of the most important ways to improve safety. INSAG shares this view. One of the greatest benefits of simplicity is that the plant is more transparently understandable to the operating staff, a prerequisite for improving the human aspects of safety. Some simplification has occurred in plants now being built and about to be built. However, significant alteration will require radical design changes and it is not likely to be seen in plants to be committed for construction in the next few years. It is more to be expected of plants with follow-on designs, such as those discussed in Section 6.5.

##### Benefits of confinement

All evolutionary designs assign high importance to the ultimate safety provided by the containment structure. Filtered venting systems are included in some designs to protect the containment from possible overpressure while limiting the amount of radioactive material that could be released if a severe accident ever occurred. The use of core catchers to retain molten debris from a badly damaged reactor core is contemplated in some countries. Other designs include stronger containment structures. However, eliminating all possibility that the confinement function will be bypassed has been in the past an elusive goal, and this could set a limit to the benefits of strengthening the confinement structure or otherwise improving its reliability.

#### 6.5. WATER REACTORS WITH PASSIVE SAFETY FEATURES

The improvements just discussed are in the nature of modifications to designs of plants now operating. If further safety improvements are to be made, more fundamental changes will be needed. To develop these to the point where a plant with

an altogether new design can be built requires a substantial amount of further work. Additional research and development will be needed to show that safety concepts can be turned into engineering reality, and a detailed engineering design must be provided and analysed before a request for regulatory approval and a firm decision to construct can be made.

A report [7] by the Electric Power Research Institute in the USA lists the principal safety characteristics of water reactors with passive safety features:

- completely passive shutdown and cooling systems;
- no external electric power needed for safety functions;
- containment function so reliable and effective that early public action need not be required in the event of an accident.

They are compatible with the features proposed in Section 5 of this report.

Most of the concepts in this category are for plants with lower levels of power production than those of the latest generation of plants that have been built. The lower power levels permit simplification of the plants.

No thorough safety review of these plants that stress passive safety features can be made before a complete detailed design is available. However, several such concepts having power levels in the range 600 to 800 MW(e) are being actively worked on. Some are expected to be available for construction by as early as 1995.

These small passive designs seek to bypass some of the limitations of evolutionary improvements to current designs. Since there would always be a risk of human error during actions by operators following an accident, human action would not be required until after a long 'grace' period following an abnormal event (on the order of three days), and only simple actions would be needed after that. Loss of all AC power would not be a source of common mode failure of safety systems requiring power following an accident, since dependence of safety systems on AC power is being eliminated. The design limits the possible severity of even remotely possible accidents, so they could not cause the confinement to fail.

When a detailed design becomes available, several matters will have to be reviewed. These include the dependence of safety on the quality of design and construction, the possibility of maintenance errors, and the extent to which proven engineering supports the safety features of the design. The analysis of safety will demand a searching review of accident scenarios to establish that no new and previously unsuspected type of accident could undermine the advantages sought from the passive safety systems and the reliable containment structure.

The passive designs should be given the same careful safety review as is provided for current and evolutionary designs, and that will be given to the plants being built in the near future. The relative merits of the evolutionary concepts and the passive safety concepts may be too difficult to assess. They could both reduce risk to levels so low that comparison may well be meaningless. There is no need to express a preference at this time. The two types could coexist in the long term.

## 6.6. ABSOLUTE SAFETY?

The term 'absolute safety' generally means the achievement of safety through the elimination or avoidance of plant inherent hazards, such as the removal of any possibility of excess reactivity that might lead to a large increase in reactor power. Some design groups, motivated by a desire to achieve such absolute safety, have proposed unusual concepts for nuclear plants to be built in the future. It should be recognized that such proposals are still at the conceptual design stage, and some of the features claimed for them may be more difficult to realize in practice than seems apparent in advance. Some of the features that proponents seek to incorporate in their concepts are the following:

- Impossibility of a nuclear power excursion, because the available excess reactivity is too low;
- Removal of afterheat (following shutdown) by conduction, natural convection or radiation, without any need for electric power or active transfer of heat to a final heat sink;
- Passive methods of removal of heat following a loss of coolant;
- Prevention of a loss of coolant through design;
- Avoidance of all need for operator action following an abnormal occurrence.

The concepts have been developed or considered by several organizations which have demonstrated their capability in the nuclear field.

Among the designs at a more advanced stage are the following. Safe Integral Reactor (SIR), a 320 MW(e) design being developed jointly by Combustion Engineering, Rolls Royce, Stone and Webster, and the United Kingdom Atomic Energy Authority, has all the major components housed in a single large vessel. The Modular High Temperature Gas Cooled Reactor (MHTGR) proposed by General Atomic is a concept for a 350 MW(th) graphite moderated reactor in which the role of the confinement structure is replaced by an impervious coating on the particles of fuel. The Integral Fast Reactor (IFR) in the USA is to use metallic uranium or plutonium as fuel. The Process Inherent Ultimate Safety (PIUS) design of ASEA AB-Brown Boveri Combustion Engineering seeks to approach core safety solely by means of inherent features of thermal hydraulics and the reliable action of gravity in producing natural circulation.

Though the designs have been motivated by the desire to achieve absolute safety, INSAG continues to assume that there can be no absolute safety in the sense that accidents could not occur. This has historically been true of all large scale technology, the fundamental reason being that safety will always depend to some extent on the reliability of mechanisms and on correct human action. Furthermore, a great deal of engineering development must take place before it is found whether these imaginative concepts can achieve the desired objectives and whether they are economically practical. Searching examination will have to be conducted to ensure that

the novel designs do not introduce new safety questions of a kind not previously encountered.

#### 6.7. PROSPECTS FOR CHANGE: A JUDGEMENT

INSAG believes that, with particular exceptions, plants that presently exist meet the safety objectives it has set for them. Plants developed as evolutionary descendants of the latest existing plants are in good design conformity with the safety objectives INSAG has set for the future. Plants with passive safety features would begin to attain an exceptional level of safety, if analysis shows that the features are as effective in meeting objectives as early review has implied.

INSAG believes that the level of safety desirable for nuclear power can be achieved with light and heavy water reactors that have the planned improvements over plants now operating. However, society may demand an even larger improvement in safety as the price of approving a major expansion of the nuclear option. If this is to be the case, imaginative and revolutionary concepts such as those briefly discussed here might offer an acceptable solution, and that could justify their accelerated development.

## 7. CONCLUSIONS

At various points in this report, INSAG has provided conclusions regarding the world's need for energy, and electricity in particular, the safety of nuclear energy, the safety of the nuclear fuel cycle and the likely course of development of nuclear energy in the future.

- (1) INSAG notes and accepts the widespread view that the demand for energy worldwide will grow, particularly as developing countries seek to improve the lifestyles of their people. Electricity will continue to be a growing component of the energy mix, increasing more rapidly than the total energy production. The potential of renewable energy sources and conservation measures is insufficient to meet the likely demand and exploitation of all acceptable means of energy production, particularly of electricity, will be necessary.
- (2) It is noted, moreover, that there is growing acceptance that emissions from generating plants that produce electricity by burning fossil fuels cause extensive environmental harm. In contrast, nuclear energy causes no such emissions.
- (3) There is a widely held fear, however, of nuclear power generation and of related activities. Such concerns must be shown to be unfounded if the nuclear option is to be exploited fully to the benefit of humankind.
- (4) INSAG has defined safety objectives for both existing and future nuclear plants, such that the risk attached to their operation should be acceptably low, and has defined Safety Principles, the implementation of which would secure the objectives.
- (5) The need for expanded electricity production has led to continued construction of nuclear plants throughout the world, albeit at a rate lower than that of a few years ago as a result of public concerns. All relevant signs indicate that, at least for some time, new nuclear plants will continue to be evolutionary developments from the light and heavy water cooled and moderated plants that are the principal types in use today.
- (6) INSAG has reviewed the available information on the safety of these types of existing plants, seeking to determine how closely existing plants of these kinds meet INSAG safety objectives. It is found from the historical record that nuclear plants of the light and heavy water types that are likely to continue to be built are now in approximate conformance with the INSAG safety targets for plants in current use. Recent state of the art probabilistic safety analyses also support this conclusion, although there are apparently some outstanding exceptions where nuclear plants require improvement to attain this safety status.
- (7) The evolutionary descendants of current types of water reactor plants that have been designed in accordance with the Basic Safety Principles in INSAG-3 and

should be operated in accordance with these Principles should meet the even more stringent safety targets proposed by INSAG for future plants. This would mean that in a world with a thousand operating nuclear power plants of the advanced designs, more than twice the number of plants now existing, an accident severely damaging some nuclear plant somewhere should not occur more often than once in a century, and an accident somewhere threatening to harm people should not occur more often than once in a millennium.

- (8) On reviewing the other phases of the nuclear power generation cycle, INSAG finds no basis for concern, especially considering the care they now receive. In particular, this conclusion has been reached in connection with the disposal of nuclear waste, a topic that arouses concern in many quarters.
- (9) INSAG also notes that if society so wishes and is willing to devote the necessary resources, even more improvement of safety of nuclear plants is possible. Designs of plants that will have evolved further from the present types may be suited to such gains, as may other more radical designs that have yet to be proven in detail.
- (10) INSAG concludes that there is no technically valid reason to reject a role for nuclear power in meeting society's needs for an expanding supply of electricity and, further, that the fullest exploitation of the nuclear option should be pursued to allay environmental concerns.

## Appendix I

### IAEA SAFEGUARDS AGAINST PROLIFERATION OF NUCLEAR WEAPONS

All nuclear weapons are based on the rapid release of enormous amounts of energy from fission of the isotope of uranium with mass number 235 ( $^{235}\text{U}$ ) or certain isotopes of plutonium.

Uranium-235 is found in nature, as 0.7% of the uranium in uranium ores, and can be separated from the more abundant isotope  $^{238}\text{U}$  in large isotope separation facilities. These plants are customarily used to increase the percentage of  $^{235}\text{U}$  to about 4%, which makes the uranium suitable for use in an LWR. The same kind of plant can be structured to produce uranium with a much higher percentage of  $^{235}\text{U}$ , say above 90%, which is then suitable for use in a nuclear weapon. The change in structure of the plant would be substantial and would be very difficult to hide from an observer.

Plutonium is produced in nuclear reactors in a process that begins when neutrons are captured in the  $^{238}\text{U}$  which is present with the  $^{235}\text{U}$  in nuclear fuel. The plutonium can be separated from the spent fuel in a chemical reprocessing facility. It can later be reused in a nuclear plant as a fuel in place of  $^{235}\text{U}$ , or it can be left in the spent fuel for disposal. Plutonium extracted through chemical reprocessing of fuel from a nuclear power plant could also be used in a nuclear weapon. However, it is not a preferred material for this purpose because after extraction from the spent fuel it contains too much of other plutonium isotopes which would make handling difficult and which would be likely to reduce the energy yield of the weapon. For these reasons, countries that are known to have developed nuclear weapons using plutonium have chosen to make it in special nuclear reactors designed and operated to produce plutonium of a composition better suited to nuclear weapons.

In spite of these reasons which would make it inconvenient to use the commercial nuclear fuel cycle as a source of fissionable material for nuclear weapons, that possibility remains. As the number of nations with nuclear power plants has grown, there has been increased concern that the number having nuclear weapons would also increase, with the commercial fuel cycle providing the capability. A broad international consensus has arisen that this possibility should be avoided through some form of international inspection that can reassure the world that such misuse is not taking place, or that can provide advance warning if it seems to have begun.

The safeguards system implemented by the IAEA, especially in those States which have ratified the Nuclear Non-Proliferation Treaty (NPT), is intended to confirm compliance by such States with their voluntarily undertaken non-proliferation obligations. The NPT has been formally ratified by 143 countries.

On their adherence to the Treaty, countries (or States) not possessing nuclear weapons agree not to acquire them, either by their own efforts or by receipt from another country. Signatory countries having nuclear weapons agree not to transfer



them to countries not possessing them. Each country without nuclear weapons agrees to place its entire peaceful nuclear industry under safeguards to be administered by the IAEA. On a voluntary basis, comparable safeguards on peaceful nuclear industries are also applied in most nuclear weapons States, for the purpose of levelling the burden on those inspected.

In return for the commitment made by the 'non-nuclear-weapons' countries, the countries with nuclear weapons agree to assist other countries to develop a peaceful nuclear energy capability. They also promise to negotiate towards reduction of their nuclear arsenals.

The safeguards by the IAEA are administered in accordance with an internationally developed model agreement [8].

The safeguards by the Agency relative to a 'non-nuclear-weapons' country adhering to the Treaty are applied as verification of accounts maintained by the country on all source and special fissionable material (*all* source and special fissionable materials are subject to IAEA safeguards under INFCIRC/153 type agreements) in its possession. Special fissionable material is uranium enriched in the isotopes  $^{235}\text{U}$  and/or  $^{233}\text{U}$  and plutonium. The concept requires that the country maintain such accounts, listing the amounts of source and special fissionable materials at different locations, and that it report to the Agency all transfers of such materials between the locations. The Agency checks the accounts by inspections directed at inventory verification at specific points in the industrial process termed 'strategic points'. The number of such inspections the Agency can make in a given year is a function of the amount of nuclear material in the country.

The NPT is a unique incursion into the sovereign rights of the countries that have accepted it. There has never been another similar widespread acceptance by countries of an international right to invasion of their privacy. Yet the powers of the IAEA are limited. It has no enforcement authority. It is restricted to judgements it can make based on information it has received on the distribution of nuclear material subject to safeguards in the world, and its verification of the information.

The power of the NPT is of a different kind. If a country refuses to adhere to the NPT for whatever stated reason, this fact is of interest to the international community. And if circumstances arise in some country that prevent the IAEA from verifying the information on safeguarded nuclear material in its possession, that fact is also of importance. In this way the IAEA provides an early warning system that would not otherwise exist, as to problems developing on the international non-proliferation front.

Some people have been critical of the IAEA because it has taken no active role with respect to countries that are believed to harbour intentions to develop a nuclear weapons capability and that on occasion are suspected of moving towards doing so. In fact, the IAEA goes as far as the sovereign nations of the world permit, and it accomplishes what the nations intended it to do. Any action beyond this must be taken by separate or joint action of the nations themselves.

## Appendix II

### NUCLEAR RADIATION AND ITS EFFECTS

#### II.1. WHY DISCUSS NUCLEAR RADIATION?

There is a strong parallel between fire and nuclear radiation. Properly used, both have the potential for substantially improving the quality of human life. Both are encountered in daily life, although this is a feature of nuclear radiation not commonly recognized. Both are generated incidentally to certain industrial processes, which themselves have great benefit. If misused or allowed to escape suitable control, both can cause severe injury to human beings and other living things.

Nuclear radiation is produced incidentally to the operation of nuclear power plants to produce electricity, and it is generated in the decay of the fission products that are the residue from this operation. Appreciation of the factors affecting the safety of nuclear power plants requires a good understanding of the nature, sources and effects of nuclear radiation.

#### II.2. WHAT IS RADIATION?

The term radiation is applied to certain ways in which energy is transmitted through space from one place to another. A number of phenomena come under the term. The word includes sound transmission, beams of high speed elementary particles of matter and electromagnetic waves in many manifestations. The elementary particles of matter include electrons such as those which impinge on the screen of the picture tube of a television set to make the image, or other parts of atoms (sometimes called subatomic particles). Electromagnetic waves include gamma rays, X rays, light ranging from the ultraviolet through the visible spectrum to the infrared, and radio waves, which also span a broad range from ultra-high frequency to very low frequency. All these forms of electromagnetic radiation are vibratory oscillations of the electromagnetic field. They differ from one another only in the frequency of the vibrations, which is highest for some gamma rays and X rays and lowest for some radio waves, with visible light in between.

#### II.3. WHAT IS IONIZING RADIATION?

The term ionizing radiation is applied to the more energetic forms of radiation that ionize some of the atoms of matter that they strike. The process of ionization is that of freeing an electron from its bound state in an atom. The atom is left chemically active and chemical changes may therefore occur. Since even small amounts

of matter contain huge numbers of atoms, an individual act of ionization affecting a single atom causes only a very slight overall effect. The net effect of high intensity radiation causing a large number of ionizations can become important.

Ionizing radiation includes high speed electrons and subatomic particles and electromagnetic radiation ranging from ultraviolet light through X rays and gamma rays.

#### II.4. WHAT IS NUCLEAR RADIATION?

Nuclear radiation<sup>3</sup> is ionizing radiation emitted from the nuclei of atoms. It may be produced in the course of radioactive decay or it may be generated when the nucleus of an atom has been struck by other energetic radiation. Radioactivity is a property of a number of kinds of naturally occurring elements that change spontaneously, atom by atom, to other elements. As they do so they briefly emit what is called nuclear radiation, in the form of minute bursts of high energy electromagnetic radiation (gamma rays), and energetic particles (alpha rays and beta rays). As stated earlier, gamma rays are high energy, penetrating radiation in the same class as light and radio waves. Beta rays are high speed electrons, identical to those that give all matter its electrical properties. Alpha rays are the heavier centres of helium atoms.

#### II.5. NATURAL OCCURRENCE OF NUCLEAR RADIATION

All matter is composed solely of atoms of naturally occurring chemical elements. Some of those naturally occurring elements have forms that are radioactive. The naturally occurring radioactive elements are found everywhere in nature, and so is the nuclear radiation they emit. Nuclear radiation is essential to the processes that cause the Sun and stars to shine. The nuclear radiation produced naturally on the Earth is a result of an atomic process that started at the beginning of the Universe and has never ceased. It is emitted from the naturally occurring radioactive elements in the rocks and soil, in the air, and even incorporated in all living matter, including the human body. In addition, but to an extent far less than its natural rate of generation, nuclear radiation has been produced by some human activities in the course of this century. The nuclear radiation produced through human action is identical to that produced by nature.

---

<sup>3</sup> In the following, the term 'radiation' is often used to mean nuclear radiation, which is the focus here. When the more general concept of ionizing radiation is meant, that will be made clear.

#### II.6. ABUNDANCE OF NATURAL RADIATION

The Earth has always been bathed in nuclear radiation, some that has escaped from the Sun and stars and some from natural processes on Earth. All observations indicate that when life began on Earth, it was exposed to an intensity of nuclear radiation even higher than that now about us, but not higher by a large factor. All the development and change in life forms and patterns took place under radiation conditions not very different from those we now experience.

However, the intensity of natural nuclear radiation on the Earth can be very different from one locality to another. At higher elevations, such as on mountains and at heights at which aircraft fly, there is less air above to shield from the incoming cosmic radiation from the Sun and stars, and so the natural radiation which is due to cosmic rays is much greater at these elevations. More importantly, the amount of radiation from the rocks and the soil is much greater in some places than in others because of differences in the kinds of rock and soil. At many places on the Earth, radiation levels from the soil and the rocks are ten to a hundred times the average values. Many of these places with high levels of natural radiation are densely populated.

#### II.7. THE USES OF IONIZING RADIATION

Although the harmful effects of ionizing radiation and more particularly nuclear radiation are here discussed at length, it must be pointed out that radiation also has important beneficial uses. X rays are extensively used in medicine and industry because of their ability to penetrate matter. The widespread application of radiation treatment to certain forms of cancer makes use of X rays, nuclear radiation from several kinds of radioactive elements (some artificially made and some found naturally), and radiation from some particle accelerators more commonly used in physics research. Many of the medicines used throughout the world are sterilized by exposing them to massive doses of ionizing radiation after they have been packaged. Exposure to ionizing radiation is used to destroy insects in stored grain. Increasing use is being made of preservation of foods by submitting them to ionizing radiation, as early fears of this practice have been seen to be groundless. In these applications, nuclear radiation is often the form of ionizing radiation used.

A large part of modern physical, biological, medical and chemical research depends critically on the use of ionizing radiation. Few if any of the advances made in these vital sciences during the past forty years could have been made without the help of ionizing radiation in general and nuclear radiation in particular.

## II.8. THE NEED TO PROTECT AGAINST RADIATION

It is well known that very high levels of nuclear radiation are harmful to human beings and to other forms of life. Also, for reasons shortly to be discussed, there is reason to believe that lower levels can sometimes be harmful. Therefore, although the additional amount of nuclear radiation humans have added to the natural rate of production is almost everywhere smaller than the background level, it is customary to provide special protection against it. The added protection is meant to ensure that radiation levels can only be excessive where human access is strictly limited or is prevented, such as near X ray machines or inside the shielding of a nuclear reactor.

## II.9. THE EFFECTS OF HIGH DOSES OF RADIATION

An individual who suddenly received a large enough exposure to nuclear radiation would soon die; if the dose were below a given threshold, the individual would not die. There is a region between the two values where exposure would cause some to die and not others, depending mostly on the state of health at the time and on the medical treatment afterwards. These are all very large amounts of radiation, far above any levels found naturally.

Exposure to large amounts of radiation in a range still below levels that may cause death in a few days has been seen to have other deleterious effects that can show up soon afterwards. Radiation exposure at the upper end of this range could lead to temporary illness, with some symptoms resembling those of a severe burn and others associated with a change in blood physiology and chemistry.

Extreme amounts of nuclear radiation contributed to many deaths following the atomic bombing of Hiroshima and Nagasaki. Twenty-eight of the thirty fire fighters and workers who died at Chernobyl were killed by radiation from the damaged reactor, and others were very ill for a long time afterwards. In the decades since nuclear fission was discovered, several workers engaged in experimental activities have been killed in accidents that exposed them to very high levels of radiation.

## II.10. CANCER AND NUCLEAR RADIATION

There is also evidence that the high levels of radiation received by many at Hiroshima and Nagasaki caused a small but definite increase in the natural rate at which some forms of cancer occurred. Similar results have been found among some patients who were exposed a number of years ago to large amounts of radiation in the course of their medical treatment.

In recent years a great deal has been learned about the ways in which processes in living cells can lead to the development of cancer. It is now known that cancer may develop some time after injury to a part of some single cell of the many forming

living tissue. The injury can be caused in many different ways: by heat, by incompatible chemicals, by bacterial or viral invasion, or by nuclear or other ionizing radiation, or it may even be spontaneous, apparently a result of an inherent susceptibility in the cell's structure. The cancer grows as uncontrolled replication of the injured cell.

A large fraction of the cells in the human body are injured in such ways in the course of a lifetime. In a great many cases injured cells repair themselves by a natural internal process. Frequently the injured cell will die and perhaps be replaced by another. The development of a cancerous state where the cell begins to reproduce itself in an uncontrolled fashion is a rare event. About four out of five people escape the development of fatal cancer even though a great many of the cells in their bodies have at one time or another gone through the precancerous stage of injury.

Since most by far of the injured cells do not develop into cancers, such an act of development appears as a purely random event. A small exposure to a condition that has been linked to the induction of cancer is most unlikely to cause a cancer to develop. The cells that are injured are much more likely to be repaired or to die and be removed by the body.

Much remains to be learned about the specific means by which cells are injured, repair takes place and cancer sometimes develops. The importance of nuclear radiation in cancer induction is far better understood than that of other causes of cancer. This is partly because the effects of nuclear radiation have been studied more and partly because they are so much easier to study.

These effects of radiation are so well understood that radiation protection specialists and biologists have been able to show conclusively that at most a small fraction of the normal cancer incidence rate can be caused by natural levels of radiation. In fact, studies seeking to evaluate the effects of living in parts of the world with high natural levels of radiation have not revealed any effects on natural cancer rates. This is at least partly because the natural cancer rate is so high generally as to mask any expected and much smaller effect of increased radiation levels.

As for man-made radiation, protective practices are implemented to ensure that any effects of radiation are even smaller. Then man-made radiation cannot lead to a discernible increase in the huge number of naturally occurring cancers.

## II.11. IONIZING RADIATION AND MUTATIONS

The processes that cause mutations are identical to those that lead to precancerous states in cells, i.e. they are injuries to individual cells. In the case of mutations, the cell is of the specific type involved in reproduction, the ovum of a female or the spermatozoon of a male. The injury that causes the mutation leads to changes in one or more genes that are components of the chromosomal matter in the cell.

Most people believe that mutations lead to offspring which are deformed, sometimes hideously so. This is a gross misunderstanding, because such an extreme

result is most improbable. Instead, the most frequent result of a mutation in germ tissue is either non-viability of the germ cell or loss of its ability to participate in reproduction. When a germ cell bearing a mutation in its genetic code is still so viable that it does participate in fertilization with the result being a human birth, the usual result is change that is difficult to perceive because it is part of the variability of the human species. It is estimated that about 5-10% of all human births are of offspring with one or more genetic mutations representing variation from their ancestral germ tissue. These are not easy to distinguish from other birth defects that are caused by injury to the foetus during critical periods of its growth. Such injuries can be the result of exposure to certain chemicals or to exceptionally high levels of ionizing radiation, or physical injury to the mother. Some mutations can be harmful, with results such as reduced resistance to certain diseases<sup>4</sup>. Some mutations may be beneficial, but this is probably a rarer event. Some simply cause differences, such as in eye colour or hair characteristics.

The cell changes that lead to mutations in germ cells resemble those that cause the precancerous stages of other cells. Similar causes are at work in the two cases. The role of radiation in causing mutations is much better understood than that of other contributors, because it has been studied more and because it is easier to study. It is well established that very little of the natural rate of incidence of mutations can be due to naturally occurring nuclear radiation.

Classic experiments with insects have led to occasional radiation induced mutations causing such changes as altered eye colouring. Experiments with large numbers of mice have also shown radiation effects on their heredity. No mutations have ever been observed in larger animals as a result of radiation, though numerous studies have been conducted to isolate such effects. The study of survivors of the atomic bombings of Hiroshima and Nagasaki has failed to reveal any mutations attributable to irradiation. Yet it is believed that large enough experiments would show some effect, and most geneticists believe that some small fraction of the naturally occurring human mutation rate must be the result of exposure to natural levels of radiation. They believe that the inability to find such a connection when it has been sought must be attributed to the fact that other, predominantly natural, sources of mutations have been so dominant as to conceal the effects of radiation.

## II.12. RADIATION PROTECTION PRACTICES

The limitations that have been set on nuclear radiation exposure in connection with nuclear energy and other activities are those that have been recommended by the International Commission on Radiological Protection (ICRP). The ICRP was

<sup>4</sup> For example, a mutation in a germ cell of Queen Victoria of England led to haemophilia in her male descendants among the Bourbons of France and the Romanovs of Russia.

formed about 70 years ago in response to a recognized need for internationally accepted standards for exposure to ionizing radiation. The ICRP's recommendations on radiation dose limits and on protective practices have evolved as more has been learned about the subject. The latest revisions to the recommendations, published in 1991, reflect increases that have been found in the numbers of leukaemia cases due to later incidence in survivors of the atomic bombing of Hiroshima and Nagasaki, and changes in estimates of the radiation exposures of these survivors. Radiation protection at nuclear plants around the world is generally in conformance with these new recommendations, and where it is not, it is expected that the practices will be modified accordingly.

ICRP recommends that radiation practices follow the principles of justification, optimization and limitation. By justification is meant avoidance of activities that lead to unnecessary radiation exposure. Optimization means maintaining radiation exposures as low as reasonably achievable. Limitation means that exposures above recommended limits are to be avoided if at all possible.

On the basis of these recommendations as to practices, limits are proposed by the ICRP on radiation exposures for workers in the industries in which ionizing radiation is generated, and for any of the general public who might be affected. These limits are chosen to restrict risks from radiation exposures to low values.

The objective in the field of nuclear energy is to keep the risks low compared to the limits recommended by the ICRP. As was pointed out earlier, if natural radiation has harmful effects, they are at levels so low that careful study has not been able to identify them. It was also pointed out that cancer rates have been seen to be increased slightly but measurably by high doses of radiation. Modern cell biology concludes that the same processes which lead to occasional development of cancer at high levels of radiation should also act at lower levels, but at a probability that is lower as the radiation dose is reduced. It is also believed that any tendency to cancer induction decreases at a rate faster than the reduction in the dose level, so that the effect at low levels is correspondingly smaller.

Because modern biology includes the assumption that any amount of ionizing radiation has some chance, however small, of inducing cancer, radiation protection practices are recommended by ICRP for all sources and uses of man-made ionizing radiation. These protective measures are aimed at keeping exposures to man-made ionizing radiation well below natural exposure levels, and as low as is practicable. It is recognized, however, that some workers must occasionally be subjected to higher doses, and special limits are set for these situations such that the workers are not submitted to risks that would be exceptional in industrial practice.

It is also recognized that no industrial enterprise is guaranteed to be free of the possibility of an accident. The protective measures established for and by the nuclear power industry are directed at making sure that no member of the public would undergo a high risk of harm even if an accident occurred at some nearby nuclear plant. Modern practice extends this objective to the workers at the nuclear plant.

## Appendix III

### RELATIVE HEALTH RISKS IN ELECTRICITY GENERATION

#### INTRODUCTION

The following discussion of the relative risks of generating electricity by different means is not based on any work by INSAG or its members, but is taken from well known available international sources<sup>5</sup>.

#### III.1. GENERAL

Although the generation of electricity bestows many benefits, it also carries with it certain health risks. So that the implications of these risks may be understood and compared, they must be objectively quantified. These risks originate in many parts of the cycle associated with whatever means of generating electricity is considered. They are diverse in character and involve different people at different stages. It is necessary, therefore, to discriminate between aspects of risk so that only similar categories are compared.

##### III.1.1. Energy cycle

Each means of producing electricity requires an infrastructure of supporting activities without which it could not exist. Most consume fuel of one kind or another, which must be extracted from the earth, processed and transported to the place of use. All depend on manufacturing of the equipment used for mining, refining and transportation, and on the manufacture and construction of the plants in which the electricity is generated. The totality of the generating activity and the support systems is called an energy cycle.

The major health risks of different energy options can occur in quite different parts of their energy cycles, and in order to compare the risks it becomes necessary to consider entire cycles. The energy production process itself is, of course, an important step in the cycle, which finally ends with the processing and disposal of all wastes generated in the production of the electricity and the supporting cycle. The health risk of a particular energy option is the sum of the risks of all the individual steps of the cycle. A comparison of the risks of only a single step such as the actual

<sup>5</sup> Appendix III draws extensively on material from Refs [9, 10], much of which is summarized in Ref. [11].

generation of electricity would give quite a misleading picture if the major risks were elsewhere.

The electrical energy systems to be compared include: (1) the fossil fuel combustion cycle; (2) renewable energy systems; and (3) the nuclear fuel cycle.

#### III.1.2. Health risks

Health risks are generally divided into the categories of immediate and delayed effects. Immediate effects consist of severe physical injury or death. Delayed effects are those that would not be felt until some time after the occurrence of an event contributing to them. The event could be a single incident or it might be an accumulation of several incidents, even a continuing situation. In the case of a chronic exposure to a noxious substance or to radiation, such as the exposure of a miner to dust or the exposure of a member of the public to the emissions from a power plant, there is a cumulative risk of contracting a disease which might be fatal. Among such health effects, the risk of cancer is important.

A discussion of the risks of energy production to human health must therefore differentiate between immediate effects due to accidents and delayed effects such as disease, and this both for occupational activities on the one hand and for the general public on the other.

#### III.1.3. Severe accidents

Events discussed so far refer to the routine conduct of operations forming parts of an energy cycle. This also includes all faults, accidents and diseases which, as experience shows, must be expected to accompany routine operations. They do not, however, include the possibility of a very severe event, which may be so unlikely that it has only rarely if ever occurred. Examples of severe events of this kind are a disastrous mine accident, an explosion or fire, the failure of a hydropower dam or a severe reactor accident. These are generally perceived as occurrences of special significance. They usually excite more concern than routine events, even though these events may, over the years, be responsible for a death toll far in excess of that from the spectacular rare events.

#### III.1.4. Risk assessment

Analyses of comparative risk available in the literature show large differences due to different data and assumptions. Furthermore, these studies provide only incomplete views of the complex health risks associated with the generation and supply of electrical energy. For example, no study thus far has included a quantitative



treatment of near term health effects of nitrogen oxides, trace metals and hydrocarbons, or an analysis of the long term health consequences of release of these agents or of carbon dioxide.

For the determination of the risks resulting from the emission of toxic substances, computational models of the relevant processes must be set up which draw on statistical information on such topics as atmospheric diffusion, population distribution and dose-effect relationships. These models are far less well established for electricity production by fossil fuelled plants than for nuclear plants.

Probabilistic risk analysis is used to estimate the probable frequency and effects of accidents to nuclear plants. The probabilities of all failures and combinations of failures of components and systems of the plant are combined and analysed to provide overall probabilities of failure sequences and their consequences. This leads to estimates of the corresponding risks. In practice, the analysis has been done only for nuclear plants, since the required data are not known for fossil fuelled plants.

### III.1.5. Perception and assessment of risks

Hazardous situations of different kinds are perceived in different ways, depending usually on many subjectively experienced circumstances. This subjective relative perception of the risk due to a given situation can vary individually to a high degree. The result is that individuals and society often act in ways inconsistent with an objective ranking. As a result of the subjectivity of reaction to risks, it frequently happens that behaviour in the face of a hazard is ambiguous or even counter-productive. In countless cases society undertakes costly safety measures to ward off small or even trivial risks when these stir up emotions, while far greater risks are ignored if they do not loom as threatening.

INSAG is concerned here with objective indications of the probability that harm will ensue and of the magnitude of that harm. Subjective risk decisions are political and not technical.

## III.2. ESTIMATED RISKS EXCLUDING SEVERE ACCIDENT RISKS

Risks can involve quite different sections of the population. Hazards at work and public risks must be treated separately since one would tend to judge these various hazardous situations differently. Workers are or should be aware of their occupational risks, which depend to a considerable extent on the behaviour of the person concerned. In contrast, the public is only vaguely aware of the hazards resulting from industrial processes and must trust the organizations responsible that these risks have been reduced to an acceptable level.

### III.2.1. Occupational risk

#### III.2.1.1. Immediate occupational risk

For the group of fossil fuel systems, this aspect of risk is quoted as between 0.1 and 3.2 fatalities/GW·a (the unit gigawatt-year, GW·a, represents operation of a station to produce 1000 MW(e) of electricity over an entire year). The risk is distinctly higher for the coal cycle than for oil and gas. If the coal is mined under bad working conditions in an out of date mine, the risk can be higher by at least a factor of ten. Table II shows the data.

The risk in the case of the renewable energy systems is perhaps surprisingly high, quoted with a range of up to a few fatalities/GW·a. This is due to the large materials requirements of these systems. In the case of solar and wind energy, it is suggested that a reduction by a factor of perhaps four might be hoped for after further development has reduced the materials requirements. Hydropower energy production remains comparatively risky with respect to acute occupational hazard.

The nuclear power systems clearly show the lowest risks in this category (0.07–0.5 fatalities/GW·a), principally because the requirements for fuel and construction materials are less. Table II shows the comparison with fossil fuelled electricity generation.

#### III.2.1.2. Delayed occupational risk

The risks quoted are 0.02–1.1 fatalities/GW·a (coal) and 0.07–0.37 fatalities/GW·a (nuclear); see Table II. These fatalities arise mainly in the mining of coal and uranium ores. The other energy systems also incur some occupational risks in

TABLE II. OCCUPATIONAL FATALITIES (per GW·a)

	Immediate	Delayed
Coal	0.16–3.2	0.02–1.1
Oil	0.20–1.35	?
Gas	0.10–1.0	?
Nuclear (LWRs) <sup>a</sup>	0.07–0.5	0.07–0.37
Renewable (solar, wind)	0.07–0.5	?
Renewable (hydropower)	0.5–4.0	?

<sup>a</sup> LWR: Light water reactor.



TABLE III. PUBLIC FATALITIES (per GW·a)

	Immediate	Delayed
Coal	0.1-1.0	2.0-6.0
Oil	0.001-0.1	2.0-6.0
Gas	0.2	0.004-0.2
Nuclear	0.001-0.01	0.005-0.2
Renewable (solar, wind)	0.05-2.0	0.05-2.0
Hydropower	?	?

the course of the production of base materials for the various installations but they are generally small and have rarely been assessed. For coal and uranium ore mining, the risks depend on whether the mining is performed underground or at the surface. Underground coal mining is more dangerous than underground uranium ore mining and the risk can be higher by a factor of more than ten under bad working conditions in an out of date mine. The use of surface mined coal leads to fewer late fatalities than the nuclear option, whereas other parts of the fuel cycle, particularly the operation of the power station, contribute more to this aspect of risk.

Adding acute and late effects gives a total occupational risk for nuclear power in the range 0.14-0.87 fatalities/GW·a, compared with the equivalent figure for coal, 0.18-4.3 fatalities/GW·a.

### III.2.2. Public risk

#### III.2.2.1. Immediate public risk

The immediate risk of death for the general public is given in Table III. It is due mainly to rail and highway accidents or to accidents involving other means of transport such as pipelines. These risks are usually dependent on the transport distances. Because of the much lower quantities of materials that have to be transported, the risk for nuclear systems, quoted as 0.001-0.01 fatalities/GW·a, is far lower than for any of the other energy options.

The coal cycle is at the greatest disadvantage here, because such large quantities of materials must be transported (0.1-1.0 fatalities/GW·a). The risk from the transportation of fuel oil, large quantities of which also are needed, can vary considerably, depending on the site of the power station and the means of transportation (0.001-0.1 fatalities/GW·a). The rather high value for natural gas (0.2 fatalities/GW·a) is a result of pipeline transport and includes relatively rare but very high consequence accidents with explosions and fires.

Information on the risks of renewable energy systems based on use of the Sun and wind reflects the need for transport of large quantities of materials. The expected reduction in material requirements following further development should reduce these risks.

No information is available on transport risks in connection with the construction of hydropower dams.

#### III.2.2.2. Delayed public risk

Immediate risks previously discussed are founded directly on accident and mortality statistics.

The situation is rather different for the late mortality risks for the public. These risks are a consequence of routine emissions of noxious chemical or radioactive substances, not only during the operation of the power stations, but also in the course of producing the materials required for the construction of all necessary installations. The consequences of these emissions are difficult to distinguish from those of many other influences that can have identical effects. Therefore these consequences are difficult to measure directly and are not well known on a statistical basis. They have to be estimated on the basis of the corresponding dose-effect relationships. Here two difficulties are encountered.

Knowledge about the biological effects of ionizing radiation is relatively good. In contrast, far less is known of the health effects of chemical substances, which are present in the environment in enormous variety. Of the noxious substances produced during the combustion of fossil fuels and emitted from power plants, the effects of sulphur dioxide have been studied most extensively. Exhaust gases contain many other components, such as nitrogen oxides, carbon monoxide, carbonyls and many other organics identified as carcinogenic, and many heavy metals. The health effects of these have been studied only very little. In an analysis such as that reported here, the health effects are usually correlated with the sulphur dioxide content of the exhaust gases. How far this use of sulphur as an indicator can reproduce the effects of the other components is an open question.

The second difficulty is of a more fundamental nature. The doses resulting from the emissions are low and are frequently very low, but they may be shared by large groups of the population. It is thus necessary to extrapolate the health detriment, which is better known at high doses, down to the doses of interest, usually many orders of magnitude lower. It is generally agreed among risk assessors that a linear extrapolation without a threshold down to zero dose is a conservative assumption. This assumption is made by the ICRP for ionizing radiation and it forms the basis for the radiation protection regulations in most countries. In addition, it is almost unanimously accepted for the assessment of the risks from noxious chemicals.

It is important to note, however, that this assumption is a hypothesis, whose validity may perhaps never be statistically confirmed or disproved, just because the

effects are so small at low doses. Thus the fatalities determined on the basis of this hypothesis are calculated hypothetical fatalities, which cannot be directly compared with statistically registered actual fatalities.

Such low doses due to emissions from energy systems and their effects must also be related to doses of the same substances due to other sources. In the case of ionizing radiation, the population is exposed continually both to natural radiation, which varies considerably from place to place, and to radiation from medical and other activities. In contrast, for most of the chemical substances emanating from fossil fuelled power stations, there is at most an insignificant natural background dose. The levels of sulphur and nitrogen oxides and ozone measured today originate from industry, energy production and particularly from motor traffic.

Table III quotes estimates of the late mortality risk to the public due to electricity production. This risk is similar for the nuclear and natural gas options (0.004–0.2 fatalities/GW·a). For the options based on burning coal and fuel oil it is much higher (2.0–6.0 fatalities/GW·a).

Emissions in connection with the production of base materials for the renewable energy options also lead to relatively high risks. No figures are available for the risks of hydropower energy production.

The addition of acute and late risks gives a total public risk for nuclear energy in the range 0.006–0.21 fatalities/GW.a. The equivalent figure for coal and oil is in the range 2.0–7.0 and for natural gas 0.2–0.4.

### III.3. SEVERE ACCIDENTS

#### III.3.1. Case histories

Table IV lists potential severe accidents to which energy production is subject, and Table V lists selected cases and their consequences (Tables XV and XVI of Ref.[11]). Table VI reproduces the summary from Table XVII of Ref.[11]. These data show only too clearly that energy production, whatever the means, can be subject to severe accidents that in some cases are not even so infrequent.

In the coal cycle there is a potential for severe accidents during underground mining operations. In the course of the stated 18 year period there were at least 62 mine disasters worldwide, with from 10 to 434 fatalities each and a total of 3600 fatalities. On an average there were 200 such fatalities per year. In the first half of 1989 there were additional accidents in the Federal Republic of Germany with 47 fatalities and in China with 44.

The extraction of petroleum and natural gas from under the sea has led to the capsizing of 6 oil platforms with a loss of from 6 to 123 lives at a time. A further 166 deaths were caused in July 1987 by an explosion on a platform in the North Sea.

TABLE IV. NATURE OF POTENTIAL ACCIDENTS WITH DIFFERENT ENERGY SOURCES<sup>a</sup>

Energy source	Accident description
Coal	Explosions or fires in underground coal mines; collapse of roofs or walls in underground or surface mines; tailings dam collapse; haulage/vehicular accidents
Oil/gas	Offshore rig accidents; fires or explosions from leaks or process plant failures; well blowouts causing leaks; transport accidents resulting in fires or explosions; loss of content in storage farms resulting in fires or explosions
Nuclear	Loss of coolant water and reactor meltdown; accidents during shipment of high level radioactive waste
Hydropower	Rupture or overtopping of dam
Geothermal	Well blowouts, resulting in release of toxic gases
Solar, thermal	Release of toxic working fluids

<sup>a</sup> Table XV of Ref.[11].

An explosion or a large fire is possible in a number of steps in the fuel cycles based on use of oil and natural gas, especially in a refinery, an oil or gas tank, or during transportation, particularly over the seas. In the case of oil, at least 15 such events occurred during the 18 years to 1986. They were responsible for a total of 450 fatalities. At least 24 such events took place in the natural gas cycle (excluding local distribution and use). These caused a total of 1440 fatalities, almost 100 per year.

Hydropower dams have historically been the cause of a number of particularly disastrous events. It is difficult to determine from the available literature which of the accidents that occurred were to dams devoted to electricity production. In the interval from 1969 to 1986, at least 8 severe dam accidents fell into this category, caused mostly by overtopping due to floods. These caused a total of 3839 fatalities, an average of over 200 per year.

TABLE V. SELECTED SEVERE ENERGY RELATED ACCIDENTS<sup>a</sup>

Source	Location	Country	Year: event	Immediate fatalities		Environmental effects
				Occupational	Public	
Coal						
Waste storage	Aberfan	South Wales, UK	1966: Spoil slag heap slippage		144	
Mining	Yubari	Japan	1981: Gas explosion	93		
	?	China	1982: Avalanche	284		
	Natal	S. Africa	1983: Fire damp	63		
	Omuta	Japan	1984: Fire	83		
	Mei Shan	Taiwan (China)	1984: Pit fire	121		
	Taipeh	Taiwan (China)	1984: Explosion	93		
	Hokkaido	Japan	1985: Mine disaster	62		
Oil						
Exploration/production	Piper Alpha	UK	1988: Fire and explosion	187		
Transport	Amoco Cadiz	France	1978: Oil spill			367 km coastline
	Betelgeuse	Ireland	1979: Fire and explosion	48	2	
	Exxon Valdez	USA	1989: Oil spill			1600 km coastline
Pipeline	Cubatão	Brazil	1964: Explosion and fire		500	

<b>Gas</b>						
Storage	San Juanico	Mexico	1984: Fire and explosions		> 500	
Pipeline	Ash-Ufa	Urals, USSR	1969: Explosion		> 500	
	Huimanquilla	Mexico	1976: Fracture		58	
	Gahri Ohoda	Pakistan	1984: Explosion		80	
	Urals	USSR	1989: Explosion		650-800	
Transport	San Carlos	Spain	1978: Explosion		216	
	Xilatopec	Mexico	1976: Explosion		100	
<b>Hydropower dam</b>						
	Vaiont	Italy	1963 Overtopping		1989	
	Koyona	India	1967		180	
	Canyon Lake	USA	1972		240	
	Macchu 2	India	1979		2500	
	Gujarati	India	1979		15000	
	Orissa	India	1980		1000	
	?	Liberia	1982		200	
	Cundinamarca	Colombia	1983		150	
<b>Nuclear</b>						
	Chernobyl	USSR	1986	30	Late effects(?) (130 000 evacuated)	Large area of land contaminated

<sup>a</sup> Table XVI of Ref. [11].

TABLE VI. NORMALIZED FATALITY RATES FOR SEVERE ACCIDENTS (1969-1986) (after Ref. [9])<sup>a</sup>

	No. of events	Fatalities per event	Total fatalities	Energy produced (GW·a)	Fatalities/energy (fat./GW·a)
<b>Coal</b>					
Mine disaster	62	10-434	3600	10 000	0.34
<b>Oil</b>					
Capsizing	6	6-123	NA <sup>b</sup>	21 000	0.02
Refinery fire	15	5-145	450		
During transport	42	5-500	1620		
<b>Natural gas</b>					
Fire/explosion	24	6-452	1440	8 600	0.17
<b>Hydropower</b>	8	11-2500	3839	2 700	1.41
<b>Nuclear</b>	1	31	31	1 100	0.03

<sup>a</sup> Table XVII of Ref. [11].

<sup>b</sup> NA: Not available.

Note: Reported fatalities are in terms of immediate fatalities; delayed fatalities, which are particularly relevant for the Chernobyl accident, are not included.

The only severe accident to a nuclear plant since the start of commercial nuclear energy production about 35 years ago was the one at Chernobyl. This caused 30 fatalities among workers and there is a possibility of a number of late fatalities among the public which cannot at present be estimated with any certainty.

### III.3.2. Immediate mortality risks

The foregoing discussion does not yet give a clear idea of the relative risks of the alternative ways of producing electrical power. To do this, it is necessary to relate the number of fatalities due to the production of electricity by a given means to the amount of electrical energy produced in those ways.

Hydropower and nuclear energy are used only to produce electricity, so the mortality risk attached to these can be compared directly. During the period to which Table VI refers (1969 to 1986) a total of about 2722 GW·a of electricity were produced worldwide by hydropower. Since this led to at least 3839 fatalities, the risk was 1.41 fatalities/GW·a or greater (Table VI).

In the same period, 1035 GW·a of electricity were produced by nuclear energy. The only immediate fatalities were the 31 at Chernobyl. The corresponding risk was therefore 0.03 fatalities/GW·a, 50 times lower than that for hydropower. It may also be asked whether the inclusion of the Chernobyl accident among the data is meaningful. That reactor was of a type very different from the ones used in the rest of the world, and the design has even been abandoned in the USSR for future plant construction. Furthermore, the operating practices that led to the Chernobyl accident have been severely modified. It is more valuable to estimate the corresponding risk of immediate fatalities for the nuclear plants used in most of the world, and to compare this risk to that of hydropower. There have been no fatalities from operation of these types of nuclear plants, however, and to obtain an estimate of relative risks it is necessary to resort to probabilistic risk assessments, which seek to evaluate such information from the characteristics of the plants and their operating modes. Such probabilistic risk assessments have been performed for many of the types of nuclear plants used in most of the world. These assessments have been used in the following comparisons.

Figure 1 shows the immediate mortality risk due to severe accidents in the nuclear power (LWR), fossil fuel and hydropower energy cycles. It is seen that severe accidents with a specific number of acute fatalities are expected to occur about 10 000 times more frequently in mines to produce coal for the coal electric cycle than would occur at nuclear power plants producing the same amount of energy.

Refining of oil is only one of the major processes in the oil-electricity cycle. Yet severe accidents at oil refineries are about a factor of 1000 times more frequent than is expected for accidents of the same severity at nuclear plants.

According to the estimates in Ref.[11], for equivalent severity, an accident to a hydropower dam is more likely by a factor of about 1000 than an accident to a nuclear plant.

Converting these data to a basis which allows for the quantities of electricity generated leads to a risk of 0.0001 fatalities/GW·a for the nuclear option. The corresponding figures for the fossil fuelled cycles are given in Table VI as:

Coal	0.34
Oil	0.10
Gas	0.17

In this connection, the renewable energy systems, solar, wind and biomass (excluding wood), are exceptional. In contrast to all other energy options they have practically no potential for severe accidents or for catastrophic failure in the actual production of electricity. The corresponding risks in their support cycles have not been evaluated.

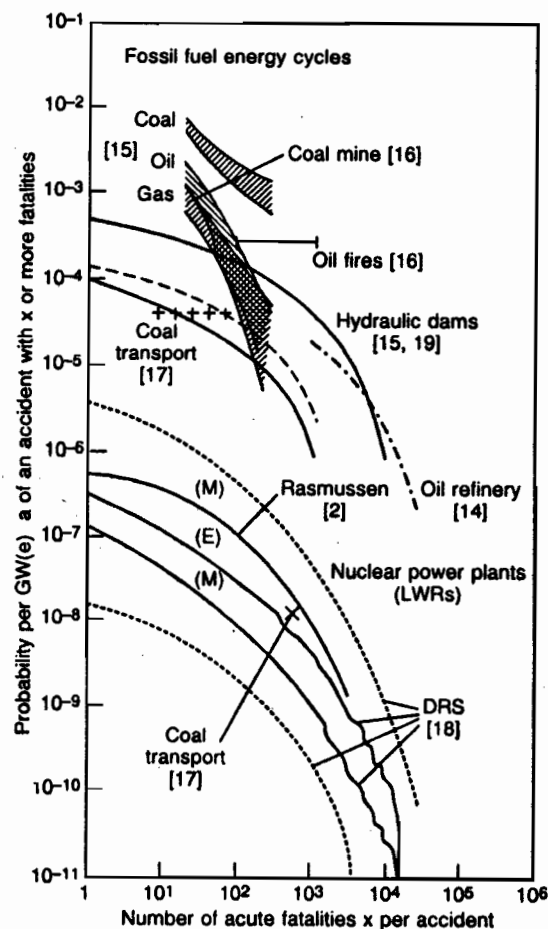


FIG. 1. Probabilities per gigawatt-year of electricity production of immediate fatalities due to severe accidents for nuclear power, hydropower and fossil fuel options. ((E) is the reference curve determined on the basis of the mean values of the expected release category frequencies; (M) is the curve determined on the basis of the median values of the expected release category frequencies; LWR: light water reactor; DRS: German Risk Study [12]) (after Refs [9, 13]).

### III.3.3. Late mortality risks

The production of nuclear electricity is the only cycle that has thus far been analysed for the late mortality risk from severe accidents, and such results have only recently been published in the USA. The topic is not covered in the references drawn on so far in Appendix III. One of these results has already been quoted in the main report, however. This states the probability that an accident will occur at a light water reactor causing one or more subsequent cancer fatalities as between 0.1 and 2.0 per 100 000 plant-years. To a degree, this form of statement disguises the fact that accidents with very low probabilities could lead to a large number of health effects to the public. When these are taken into account, an average expected value for latent cancer fatalities of between 0.001 and 0.01 delayed fatalities/GW·a is obtained. Added to the total risk to the public from routine energy production (0.006–0.21 fatalities/GW·a) and from the immediate effects of severe accidents (0.0001 fatalities/GW·a), this does not change significantly the overall estimates of the risks from the nuclear option.

Corresponding events that might occur in the other energy cycles but whose consequences have not yet been calculated are a refinery accident that might lead to a spread of carcinogens, or an explosion in a future large scale factory for producing photovoltaic devices, that might result in a widespread distribution of gallium arsenide. In both cases the dispersion mechanisms of toxic products in the environment would be quite similar to those taken into account in the nuclear risk studies, and potential harmful consequences must be assumed.

Therefore, even if no meaningful comparisons of this aspect of risk are available at present owing to the lack of evaluation of the late health effects to be expected after a large non-nuclear accident, the probability of nuclear accidents with large health effects at water reactors is still so low that they do not make a large contribution to the overall risk.

### III.4. CONCLUSION

On the basis of, first, the mortality risks during routine energy production, excluding severe accidents, nuclear energy presents a very low risk for the public. The occupational risk, stemming from ore mining and operation of the power plant, is not negligible. But one must keep in mind that the fossil fuel energy cycles exhibit much higher risks for the personnel who harvest the large quantities of fuel needed. Moreover, the general public is also subjected to a relatively high risk from the noxious products of the combustion process; natural gas, a very clean fuel, is an exception in this latter respect.

Most people believe that renewable energy systems are risk free. This is not the case. They require large amounts of materials, and thus are associated with appreciable occupational accident risks, as well as non-negligible public risks.

The risks originating from severe accidents are small or negligible for some types of renewable energy systems for which severe accidents are hardly imaginable. But the fossil fuel energy systems and hydropower have relatively large probabilities of severe accidents. By contrast, the risk is low for the nuclear energy cycle.

## REFERENCES

- [1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, Safety Series No. 75-INSAG-3, IAEA, Vienna (1988).
- [2] RASMUSSEN, N.C., Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, Main Report, Rep. WASH-1400-MR (NUREG-75/014), United States Nuclear Regulatory Commission, Washington, DC (1975).
- [3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Safety Culture, Safety Series No. 75-INSAG-4, IAEA, Vienna (1991).
- [4] UNITED STATES NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, Rep. NUREG-1150, 3 vols, Washington, DC (1989).
- [5] MURLEY, T.E., "Nuclear power plant safety experience in the United States", Aspectos de Segurança de Usinas Nucleares na América Latina (Proc. Symp. Rio de Janeiro, June 1991), Latin American Section/American Nuclear Society, Rio de Janeiro (1991) I3-I13.
- [6] UNITED NATIONS, Sources, Effects and Risks of Ionizing Radiation (Report to the General Assembly), Scientific Committee on the Effects of Atomic Radiation (UNSCEAR), UN, New York (1988).
- [7] ELECTRIC POWER RESEARCH INSTITUTE, Advanced Light Water Reactor — Utility Requirements Document, Rep. NP-6780, EPRI, Palo Alto, CA (1990).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, The Structure and Content of Agreements between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons, INFCIRC/153 (corrected), IAEA, Vienna (1972).
- [9] FRITZSCHE, A.F., The health risks of energy production, Risk Anal. 9 4 (1989) 565-577.
- [10] KALLENBACH, A., THÖNE, E., VOSS, A., "Comparative risks of different electricity generating systems", Envrisk 88 (Proc. Int. Workshop, Como, 1988) (1988).
- [11] INTERNATIONAL EXPERT GROUP, "Comparative environmental and health effects of different energy systems for electricity generation", Key Issues Paper No. 3, Senior Expert Symposium on Electricity and the Environment (Proc. Symp. Helsinki, 1991), IAEA, Vienna (1991) 91-141.
- [12] BUNDESMINISTER FÜR FORSCHUNG UND TECHNOLOGIE, Deutsche Risiko-studie: Kernkraftwerke, TÜV Rheinland, Cologne (1979).
- [13] FRITZSCHE, A.F., Gesundheitsrisiken von Energieversorgungssystemen: von der Kohle bis zu Energien der Zukunft und den Rohstoffen bis zur Entsorgung, Technischer Überwachtungsverein Rheinland, Cologne (1988).
- [14] COHEN, A.V., PRITCHARD, D.K., Comparative Risks of Electricity Production Systems: A Critical Survey of the Literature, Health and Safety Executive, HMSO, London (1980).
- [15] NORGES OFFENTLIGE UTREDNINGER, Nuclear Power and Safety, Rep. NOU 1978, 35C, Universitetsforlaget, Oslo (June 1978).



- [16] SMITH, K.R., WEYANT, J., HOLDREN, J.P., Evaluation of Conventional Power Systems, Rep. ERG 75-5, NASA Energy and Resources Program, Washington, DC (July 1975).
- [17] COHEN, A.V., Comparative risks of electricity generating systems, J. Soc. Radiol. Prot. 3 (1983-1984) 9-14.
- [18] BAYER, A., et al., The German Risk Study: Accident consequence model and results of the study, Nucl. Technol. 59 (1982) 20-50.
- [19] SCHNITTER, N., Statistische Sicherheit der Talsperren, Wasser-Energie-Luft 68 5 (1976) 126-129.

## MEMBERS OF THE INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

Beninson, D.  
Birkhofer, A.  
Bukrinski, A.M.  
Chatterjee, S.K.  
Domaratzki, Z.  
Edmondson, B.  
González-Gómez, E.

Höhn, J.  
Kouts, H.J.C. (*Chairman*)  
Lepecki, W.  
Li, Deping  
Sato, K.  
Sidorenko, V.A.  
Tanguy, P.  
Vuorinen, A.P.

Note: A.M. Bukrinski deputized for V.A. Sidorenko.

## WORKING GROUP EXPERTS

Doos, B.  
Kouts, H.J.C. (*Chairman of INSAG*)  
Manowitz, B.

Pershagen, B.  
Sennis, C.  
Thadani, A.C.