INSAG-10

Defence in Depth in Nuclear Safety

INSAG-10

A REPORT BY THE
INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

INSAG

IAEA

DEFENCE IN DEPTH IN NUCLEAR SAFETY

INSAG-10

A report by the International Nuclear Safety Advisory Group

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

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

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

Printed by the IAEA in Austria
June 1996
STI/PUB/1013

INSAG-10

DEFENCE IN DEPTH IN NUCLEAR SAFETY

INSAG-10

A report by the
International Nuclear Safety Advisory Group

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 1996

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 indentify 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 PUBLICATION IS ALSO ISSUED IN FRENCH, RUSSIAN AND SPANISH

VIC Library Cataloguing in Publication Data

Defence in depth in nuclear safety : INSAG–10 / a report by the International Nuclear Safety Advisory group.
– Vienna : International Atomic Energy Agency, 1996.
p. ; 24 cm. — (INSAG series, ISSN 1025–2169 ;)
STI/PUB/1013
ISBN 92-0-103295-1
Includes bibliographical references.

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

VICL 96-00150

FOREWORD
by the Director General

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

With the intention of strengthening the IAEA's contribution to ensuring the safety of nuclear power plants, 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 research on nuclear safety and operational experience. It advises on areas where additional efforts are required. Where possible, it seeks to formulate common safety concepts.

The present report deals with the concept of defence in depth in nuclear and radiation safety, discussing its objectives, strategy, implementation and future development. The report is intended for use by governmental authorities and by the nuclear industry and its supporting organizations. It is intended to stimulate discussion and to promote practical action at all levels to enhance safety.

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

CONTENTS

1. INTRODUCTION AND HISTORICAL DEVELOPMENT

1. The concept of defence in depth, which concerns the protection of both the public and workers, is fundamental to the safety of nuclear installations. As was stated in Basic Safety Principles for Nuclear Power Plants (INSAG-3) [1] in relation to the safety of nuclear power plants, "*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...*"

2. The report is structured as follows:

- Section 1 summarizes the historical development of safety concepts, focusing on defence in depth;
- Section 2 discusses the concept of defence in depth in terms of objectives, strategy, physical barriers and levels of protection;
- Section 3 describes the implementation of defence in depth and illustrates how its various elements interrelate;
- Section 4 indicates how defence in depth can be enhanced for the nuclear power plants that are currently operating;
- Section 5 proposes a development of defence in depth which could be applied systematically for plants to be built in the future.

3. The development of nuclear safety goes back to the earliest use of nuclear energy. The means of ensuring safety in the peaceful uses of nuclear energy have progressed from early simple concepts and methods into a methodology resting on a firm foundation of experience. From the original small experimental nuclear facilities, progressively larger units have been constructed that produce correspondingly larger amounts of energy and of radioactive materials, thereby increasing the potential risk and prompting additional safety measures. Concurrently, the continuous growth in knowledge, the development of safety concepts and the increasing expertise and experience gained from operating nuclear power plants under normal and abnormal conditions and from accidents have led to more comprehensive and systematic approaches to safety.

4. The concept of placing multiple barriers between radioactive materials and the environment was gradually developed. However, application of this concept alone cannot provide the necessary assurance of safety, since it does not include the means to provide the barriers themselves with successive layers or levels of protection. In fact, the approach was intended to provide redundant means to ensure the fulfilment

of the basic safety functions of controlling the power, cooling the fuel and confining radioactive material.

5. The concept of defence in depth was therefore gradually refined to constitute an increasingly effective approach combining both prevention of a wide range of postulated incidents and accidents and mitigation of their consequences. Incidents and accidents were postulated on the basis of single initiating events selected according to the order of magnitude of their frequency, estimated from general industrial experience.

6. In this early stage, the concept of defence in depth generally included three levels:

— conservative design, providing margins between the operating conditions foreseen (covering normal operation as well as postulated incidents and accidents) and the failure conditions of equipment;
— control of operation, including response to abnormal operation or to any indication of system failure, by the use of control, limiting and protection systems to prevent the evolution of such occurrences into postulated incidents and accidents;
— engineered safety features, to control postulated incidents or accidents in order to prevent them from progressing to severe accidents or to mitigate their consequences, as appropriate.

7. Later, the concept of defence in depth was further refined to include consideration of external hazards, quality assurance, automation, monitoring and diagnostic tools. Furthermore, additional severe accidents were considered in studies and probabilistic safety analyses.

8. The Three Mile Island accident in the United States of America in 1979, which led to a severe core melt, bore out many of the results of the first theoretical studies of severe accidents and probabilistic safety analyses. The accident illustrated the importance of human factors, the human–machine interface and long term effective containment. It resulted in advances in the physical understanding of potential severe accidents due to extensive research work. Moreover, it demonstrated the importance of effective analysis and feedback of operating experience, to identify and eliminate possible weaknesses in defence in depth, including weaknesses in design, operating procedures and training.

9. Investigation of the progression of severe accidents has indicated that, in most cases, there is a substantial period of time from the initiating event of an accident up to the point at which core damage can no longer be prevented. It was appreciated that this time span can be used for taking on-site measures for accident management before core degradation occurs. Measures for accident management were developed

in order to prevent severe damage to the reactor core, or to mitigate, as far as possible, the consequences of severe core damage. It was realized that such measures have the potential to reduce the risk associated with severe core damage accidents provided that all the teams or individuals involved (from operating staff to external crisis teams) are adequately prepared to act according to appropriate procedures in the event of an emergency.

10. Feedback of experience and investigation of severe accidents resulted in new extensions of the concept of defence in depth:

- additional measures were introduced in order to cope with significant multiple failures such as a complete loss of redundant systems (such as the scram system, the electrical power supply, the steam generator feedwater systems, or the ultimate heat sink);
- accident management was implemented in order to prevent accidents or, in the event of non-postulated accidents, to mitigate their consequences;
- symptom oriented emergency procedures were developed;
- provision was made for on-site and off-site emergency response to mitigate the effects on the public and the environment of the release of radioactive materials.

11. In parallel to the lessons learned from the accident at Three Mile Island, timely feedback of operating experience helped to strengthen each level of defence in depth, and to identify weaknesses in the design, construction, operation and testing of equipment, as well as in the related analyses.

12. The Chernobyl accident in the Ukrainian Republic of the Union of Soviet Socialist Republics in 1986 demonstrated the possible consequences of inadequate defence in depth and the importance of organizational issues such as the need for an effective regulatory regime and for a safety culture. It also focused attention on medium and long term contamination due to radioactive releases and the role of off-site emergency planning.

13. In summary, the historical development of the concept of defence in depth led to a general structure of four physical barriers and five successive levels, which were described in INSAG-3 [1] and are elaborated in Section 2.

14. An assessment of the effectiveness of defence in depth has become an important means of assessing general plant safety. Reference to this concept is of particular importance in the assessment of the safety of nuclear power plants built to earlier standards (see A Common Basis for Judging the Safety of Nuclear Power Plants Built to Earlier Standards (INSAG-8) [2]).

2. THE APPROACH TO DEFENCE IN DEPTH

15. Defence in depth consists in a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant. Defence in depth is implemented through design and operation to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within the plant and events initiated outside the plant.

16. For a consistent implementation, account needs to be taken of the risk represented by the amount and type of radioactive material present in the installation; the potential for its dispersion due to the physical and chemical nature of these products; and the possibility of nuclear, chemical or thermal reactions that could occur under normal or abnormal conditions and the kinetics of such events. These characteristics influence the required number and strength of lines of defence, depending on the reactor type.

2.1. OBJECTIVES OF DEFENCE IN DEPTH

17. Basic Safety Principles for Nuclear Power Plants (INSAG-3) [1] discusses the implementation of a defence in depth concept centred on several levels of protection, including successive barriers preventing the release of radioactive material to the environment. The objectives are as follows:

— to compensate for potential human and component failures;
— to maintain the effectiveness of the barriers by averting damage to the plant and to the barriers themselves; and
— to protect the public and the environment from harm in the event that these barriers are not fully effective.

2.2. STRATEGY FOR DEFENCE IN DEPTH

18. The strategy for defence in depth is twofold: first, to prevent accidents and, second, if prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions. Accident prevention is the first priority. The rationale for the priority is that provisions to prevent deviations of the plant state from well known operating conditions are generally more effective and more predictable than measures

aimed at mitigation of the consequences of such a departure, because the plant's performance generally deteriorates when the status of the plant or a component departs from normal conditions. Thus preventing the degradation of plant status and performance generally will provide the most effective protection of the public and the environment, as well as of the productive capacity of the plant. Should preventive measures fail, however, mitigatory measures, in particular the use of a well designed confinement function, can provide the necessary additional protection of the public and the environment.

19. Defence in depth is generally structured in five levels. Should one level fail, the subsequent level comes into play. The objective of the first level of protection is the prevention of abnormal operation and system failures. If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection. Should the second level fail, the third level ensures that safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response.

20. In order to reflect defence in depth as described here, the levels of protection can be named according to their objective or the primary means of achieving the objectives. Basic Safety Principles for Nuclear Power Plants (INSAG-3) [1] adopted for the most part the second approach. In the present report, preference is given to recognizing both the objectives of each level of protection and the means of achieving them. These objectives and means are shown in Table I.

21. For the effective implementation of defence in depth, some basic prerequisites apply to all measures at Levels 1 to 5. These prerequisites, which are interrelated and are fulfilled as part of policy for safe design and operation, are appropriate conservatism, quality assurance and safety culture.

22. The general objective of defence in depth is to ensure that a single failure, whether equipment failure or human failure, at one level of defence, and even combinations of failures at more than one level of defence, would not propagate to jeopardize defence in depth at subsequent levels. The independence of different levels of defence is a key element in meeting this objective.

23. The existence of several elements of defence in depth does not justify continued operation in the absence of one element. Thus all the elements of defence in depth are normally available when a plant is at power and an appropriate number of available elements is required at other times.

TABLE I. LEVELS OF DEFENCE IN DEPTH

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

24. The primary way of preventing accidents is to achieve a high quality in design, construction and operation of the plant, and thereby to ensure that deviations from normal operation are infrequent. Operating systems are designed to counter in a straightforward manner events which, as expected by the plant's designers, are likely to occur during the operating lifetime of the plant, owing to equipment as well as human failures. The availability of the fundamental safety functions — controlling the power, cooling the fuel and confining the radioactive material — is normally ensured through the use of automatic control and safety systems and prepared staff actions.

25. In-service surveillance such as non-destructive testing or functional periodic testing contribute to the prevention of incidents and accidents. In addition, these measures are necessary to contribute to the control of accidents. Due consideration of these activities at the design stage is essential.

26. The boundary conditions for designing the safety and protection systems are determined by well defined postulated incidents and accidents that are representative of groups of events with similar plant responses and attendant loads. The choice of these postulated conditions is justified on the basis of analysis supported by operating

experience from both nuclear power plants and industry generally. The effectiveness and reliability of the safety systems to cope with these incidents and accidents have to be clearly demonstrated during the safety assessment process. The design of the safety systems focuses on the prevention of core damage and the assurance of the retention capability of the containment to prevent uncontrolled releases of radioactive materials to the environment after a postulated event or to mitigate the consequences of such releases.

27. Hazards such as fire, flooding or earthquakes could potentially impair several levels of defence (for example, they could bring about accident situations and, at the same time, inhibit the means of coping with such situations). Special attention is paid to such hazards, precautions are taken against them, and the plant and its safety systems are designed to cope with them. For example, protection against fire requires prevention of fires, detection of fires and the limitation of consequences by the design of fire zones and physical separation for the redundant lines of safety systems.

28. If it is not feasible to have independent levels of defence against some events (such as sudden reactor pressure vessel failure), several levels of precautions are introduced into the design and operation. Such precautions may be taken, for instance, in the selection of materials, in periodic inspection or in siting, or in design by incorporating additional margins of safety.

29. The precautions described in the foregoing may also defend against some complex failures and some human errors. Other complex failures that are not explicitly taken into account in the design of currently operating plants can be investigated through safety studies and reactor research, which can suggest additional preventive and mitigatory measures. Since such measures anticipate potential events of low estimated frequency, they are generally subject to specific and less stringent rules than those for the safety systems, such rules being defined on a case by case basis. For example, such events are analysed using best estimate models and data.

30. Irrespective of these efforts, there can be no guarantee that conditions that exceed design basis accident conditions will not occur. Such conditions are anticipated by both preventive measures and mitigatory measures (for accident management). Should engineered safety features fail to protect the integrity of barriers, and should accident conditions arise with consequences exceeding those anticipated in the design, the next line of defence would be to manage an accident so as to prevent progression of the accident, to limit radioactive releases from the plant or to mitigate the consequences of such releases.

31. Owing to the relatively slow development from most initiating events to severe accident conditions, it is in principle possible for plant personnel to diagnose the status

of the plant and to restore failed safety related functions. This may be done, for example, by reactivating operational or safety systems or by activating other systems. These measures have priority over mitigatory measures. Nevertheless, measures to protect the population in the short and long term (such as monitoring of activity levels, sheltering, evacuation and control of foodstuffs) in the event of significant releases need to be planned and ready to be applied within a specified time frame by the competent authorities.

2.3. BARRIERS

32. Generally, several successive physical barriers for the confinement of radioactive material are put in place. Their specific design may vary depending on the activity of the material and on the possible deviations from normal operation that could result in the failure of some barriers. For water reactors at power operation, the barriers confining the fission products are typically:

— the fuel matrix;
— the fuel cladding;
— the boundary of the reactor coolant system;
— the containment system.

33. The public and the environment are protected primarily by means of these barriers, which may serve operational and safety purposes or safety purposes only. The defence in depth concept applies to the protection of their integrity against internal and external events that may jeopardize it. Situations in which one or more barriers are breached (such as during shutdown) necessitate special attention.

2.4. LEVELS OF DEFENCE

34. Measures relative to defence in depth are generally ranked in five levels of defence. The first four levels are oriented towards the protection of barriers and mitigation of releases; the last level relates to off-site emergency measures to protect the public in the event of a significant release. Even though implementation of the concept of defence in depth may differ from country to country and may to a certain degree depend on plant design, the main principles are common.

Level 1: Prevention of abnormal operation and failures

35. Measures at Level 1 include a broad range of conservative provisions in design, from siting through to the end of plant life, aimed at confining radioactive material and minimizing deviations from normal operating conditions (including transient

conditions and plant shutdown states). The safety provisions at Level 1 are taken through the choice of site, design, manufacturing, construction, commissioning, operating and maintenance requirements such as:

— the clear definition of normal and abnormal operating conditions;
— adequate margins in the design of systems and plant components, including robustness and resistance to accident conditions, in particular aimed at minimizing the need to take measures at Level 2 and Level 3;
— adequate time for operators to respond to events and appropriate human–machine interfaces, including operator aids, to reduce the burden on the operators;
— careful selection of materials and use of qualified fabrication processes and proven technology together with extensive testing;
— comprehensive training of appropriately selected operating personnel whose behaviour is consistent with a sound safety culture;
— adequate operating instructions and reliable monitoring of plant status and operating conditions;
— recording, evaluation and utilization of operating experience;
— comprehensive preventive maintenance prioritized in accordance with the safety significance and reliability requirements of systems.

36. Furthermore, Level 1 provides the initial basis for protection against external and internal hazards (e.g. earthquakes, aircraft crashes, blast waves, fire, flooding), even though some additional protection may be required at higher levels of defence.

Level 2: Control of abnormal operation and detection of failures

37. Level 2 incorporates inherent plant features, such as core stability and thermal inertia, and systems to control abnormal operation (anticipated operational occurrences), with account taken of phenomena capable of causing further deterioration in the plant status. The systems to mitigate the consequences of such operating occurrences are designed according to specific criteria (such as redundancy, layout and qualification). The objective is to bring the plant back to normal operating conditions as soon as possible.

38. Diagnostic tools and equipment such as automatic control systems can be provided to actuate corrective actions before reactor protection limits are reached; examples are power operated relief valves, automatic limitation systems on reactor power and on coolant pressure, temperature or level, and process control function systems which record and announce faults in the control room. Ongoing surveillance of quality and compliance with the design assumptions by means of in-service inspection and periodic testing of systems and plant components is also necessary to

detect any degradation of equipment and systems before it can affect the safety of the plant.

Level 3: Control of accidents within the design basis

39. In spite of provisions for prevention, accident conditions may occur. Engineered safety features and protection systems are provided to prevent evolution towards severe accidents and also to confine radioactive materials within the containment system. The measures taken at this level are aimed at preventing core damage in particular.

40. Engineered safety features are designed on the basis of postulated accidents representing the limiting loads of sets of similar events. Typical postulated accidents are those originating in the plant, such as the breach of a reactor coolant pipe (a loss of coolant accident) or in a main steam line or feedwater line, or loss of control of criticality, such as in a slow uncontrolled boron dilution or a control rod withdrawal.

41. Design and operating procedures are aimed at maintaining the effectiveness of the barriers, especially the containment, in the event of such a postulated accident. Active and passive engineered safety systems are used. In the short term, safety systems are actuated by the reactor protection system when needed.

42. To ensure a high reliability of the engineered safety systems, the following design principles are adhered to:

— redundancy;
— prevention of common mode failure due to internal or external hazards, by physical or spatial separation and structural protection;
— prevention of common mode failure due to design, manufacturing, construction, commissioning, maintenance or other human intervention, by diversity or functional redundancy;
— automation to reduce vulnerability to human failure, at least in the initial phase of an incident or an accident;
— testability to provide clear evidence of system availability and performance;
— qualification of systems, components and structures for specific environmental conditions that may result from an accident or an external hazard.

Level 4: Control of severe conditions including prevention of accident progression and mitigation of the consequences of a severe accident

43. For the concept of defence in depth as applied to currently operating plants, it is assumed that the measures considered at the first three levels will ensure maintenance of the structural integrity of the core and limit potential radiation hazards for

members of the public. Nevertheless, additional efforts are made in order to further reduce the risks. The broad aim of the fourth level of defence is to ensure that the likelihood of an accident entailing severe core damage, and the magnitude of radioactive releases in the unlikely event that a severe plant condition occur, are both kept as low as reasonably achievable, economic and social factors being taken into account. Accident management may not be used to excuse design deficiencies at prior levels.

44. Consideration is given to severe plant conditions that were not explicitly addressed in the original design (Levels 1 to 3) of currently operating plants owing to their very low probabilities. Such plant conditions may be caused by multiple failures, such as the complete loss of all trains of a safety system, or by an extremely unlikely event such as a severe flood. Some of these conditions bear a potential that radioactive materials could be released to the environment. The thermal inertia of the plant provides time to deal with some of these conditions by means of additional measures and procedures. Ancillary and support systems are designed, manufactured, constructed, commissioned and operated consistent with the required reliability of engineered safety systems.

45. Measures for accident management[1] are also aimed at controlling the course of severe accidents and mitigating their consequences. In terms of core damage, accident management comprises both preventive and mitigatory measures. With regard to off-site emergency response, the measures are essentially preventive. Essential objectives of accident management are:

— to monitor the main characteristics of plant status;
— to control core subcriticality;
— to restore heat removal from the core and maintain long term core cooling;
— to protect the integrity of the containment by ensuring heat removal and preventing dangerous loads on the containment in the event of severe core damage or further accident progression;
— regaining control of the plant if possible and, if degradation cannot be stopped, delaying further plant deterioration and implementing on-site and off-site emergency response.

46. The most important objective for mitigation of the consequences of an accident in Level 4 is the protection of the confinement. For most reactor designs there exists a containment structure which withstands pressure, with strict design limits on permissible leakage under a specified pressure. Functions that protect the containment,

---

[1] The term used depends on the country and the plant design: typical expressions are "complementary measures", "emergency procedures" and "on-site accident management". In the present text, the term "accident management" is used.

such as containment cooling and penetration control, are typically designed and analysed to the same conservative standards as engineered safety features. Such design provides the possibility of maintaining effective functioning of the containment under more severe plant conditions. Specific measures for accident management are established on the basis of safety studies and research results. These measures fully utilize existing plant capabilities, including available non-safety-related equipment. For example, any source of fresh water could be used in the event of loss of the ultimate heat sink or in order to feed the secondary side of the steam generators. Measures for accident management can also include hardware changes. Examples are the installation of filtered containment venting systems and the inerting of the containment in boiling water reactors in order to prevent hydrogen burning in severe accident conditions. For such additional measures specific design rules can be applied in a pragmatic way.

47. The role of the operators is vital in actuating hardware features for accident management and in taking actions beyond the originally intended functions of systems or using temporary or ad hoc systems. Adequate staff preparation and training for such conditions is a prerequisite for effective accident management. Managerial provisions such as an on-site emergency plan are also necessary.

Level 5: Mitigation of the radiological consequences of significant external releases of radioactive materials

48. Even if the efforts described in the foregoing are expected to be effective in limiting the consequences of severe accidents, it would be inconsistent with defence in depth to dismiss off-site emergency plans. These plans cover the functions of collecting and assessing information about the levels of exposures expected to occur in such very unlikely conditions, and the short and long term protective actions that constitute intervention. The responsible authorities take the corresponding actions on the advice of the operating organization and the regulatory body.

49. Off-site emergency procedures are prepared in consultation with the operating organization and the authorities in charge and must comply with international agreements. Both on-site and off-site emergency plans are exercised periodically to the extent necessary to ensure the readiness of the organizations involved.

Basic prerequisites

50. As stated in para. 21, an effective implementation of defence in depth has certain prerequisites which apply to all measures considered at all the levels. These are appropriate conservatism, quality assurance and safety culture.

Conservatism

51. Conservatism is broadly applied at the first three levels of defence. Conservative assumptions are made for site selection, design and construction, commissioning and operation. Appropriate conservative assumptions and safety margins are also considered in the review of modifications, the assessment of ageing effects, periodic safety reassessment, and the development of emergency plans, as well as in regulatory review and subsequent licensing decisions. At Levels 4 and 5, best estimate considerations are increasingly important.

Quality assurance

52. Each level of defence can be effective only if the quality of design, materials, structures, components and systems, operation and maintenance can be relied upon. Quality assurance programmes can ensure the development of a safe design (including site evaluation, design of process and safety systems, design of barriers, design of modifications and safety analysis). They can also ensure that the intent of the design is achieved in the plant as built and that the plant is being operated as intended and maintained as designed.

Safety culture

53. Organizations and individuals involved in activities that may have an impact at each level of defence need to be committed to a strong safety culture (see Safety Culture, INSAG-4 [3]). The operating organization and the governmental organization, as well as organizations involved in design, manufacturing, construction, maintenance, testing and in-service inspection and emergency interventions, must ensure that appropriate prerequisites are met and that appropriate methods are used.

3. IMPLEMENTATION OF DEFENCE IN DEPTH

54. The concepts of barriers and levels of protection that constitute defence in depth as well as some common elements of these barriers and levels were discussed in Section 2. Section 3 deals with the more detailed elements and practices used for putting into practice the concepts of defence in depth. The practices can be viewed as "tools" that are used to devise, maintain and improve barriers and defences at different levels.

55. In defence in depth, a wide diversity of specific measures are called upon, both at the design stage and in operation. These design and operational measures are complementary.

3.1. DETERMINISTIC DESIGN

56. A fundamental component of defence in depth is a plant design that provides an effective means to perform safety functions under normal and abnormal operating conditions and in accidents. The design relies on deterministic assumptions and procedures without explicit consideration of probabilities. Design provides the following:

- high quality and reliability, achieved by means of proven technology and appropriate standards, suitable safety margins and due consideration of site characteristics (Level 1 of defence);
- systems to prevent departure from normal operating conditions or to monitor any deviation and to restore normal operating conditions (Level 2 of defence);
- safety systems to prevent and/or mitigate postulated accidents and to prevent further degradation (Level 3 of defence).

57. As stated earlier, conservatism, including safety margins, is part of all these steps. It applies to the processes of site selection, system design and material specification, and the setting of quality requirements, acceptance criteria for qualification tests and for commissioning tests, in-service inspection requirements and technical specifications, and to safety assessment. Design rules such as segregation, redundancy and diversification provide a high degree of protection against potential functional failures.

58. A deterministic approach that makes greater use of best estimate assumptions also provides support and procedures for control of more severe plant conditions and for the management of severe accidents (Level 4 of defence).

3.2. PROBABILISTIC STUDIES AND DEFENCE IN DEPTH

59. Probabilistic safety assessment (PSA) is an effective means of enhancing understanding of plant vulnerabilities, including complex situations due to several equipment and/or human failures. The results can be used to improve defence in depth. PSA is also a useful tool for optimizing efforts in implementing defence in depth. Probabilistic Safety Assessment, INSAG-6 [4], provides a general view on the techniques and methods of PSA.

60. For a plant design that leads to a well established defence, including several independent levels of defence, the uncertainties in PSA results will be diminished. In this case, the reliability requirements for individual components or systems can be moderate and failure rates are thus observable, permitting derivation of data from past experience. Where levels of defence are fewer or are not fully independent, the reliability requirement is more stringent, and data from past experience will be difficult to obtain and highly uncertain.

61. Some aspects of plant safety are difficult to assess quantitatively by probabilistic methods. Examples include the influence of plant organization and safety culture, as well as aspects such as common cause effects, reliability of software, some types of human error, and internal and external hazards. It is therefore an essential task of deterministic plant design to limit the influence of such aspects of safety.

3.3. MEANS OF ACHIEVING OPERATIONAL SAFETY

Technical specifications and operating procedures

62. Technical specifications and operating procedures are usually derived from deterministic design, but probabilistic studies as well as operating experience are used for further enhancement of safety. The operational tools for accident prevention are the operating procedures for normal operation; that is, the general procedures for each plant state and transient, as well as specific procedures for systems related to operational safety. All these procedures are developed in advance of operation and made available to the operators for training. Periodic checking of such procedures, and their subsequent modification and approval for use, is an iterative process that continues throughout plant life, following developments in plant features (particularly safety features in the process of upgrading).

63. The normal operating procedures take into account limits and conditions set by the design and also cover shutdown conditions. Procedures are also set up to cope with incident and accident conditions.

The human factor and training of plant personnel

64. While human error bears a potential for jeopardizing defence, human actions are crucial to safe operation and professionalism and safety culture allow the staff to contribute to ensuring reliable operation and detecting and preventing anomalies at the initial stage. Moreover, if sufficient time and information are available, a person is able to react constructively in situations that cannot be completely planned for and

therefore cannot be controlled by automatic actions. However, successful human action requires a high level of qualification and training, including simulator training for a wide range of operational situations.

65. Training programmes include provisions for periodic checking of competence as well as refresher training. These programmes take into account all relevant changes within systems and components due to backfitting measures as well as changes in procedures. They also include recent sequences of significant events that have occurred at other plants or possible sequences from theoretical investigations. The actions to be taken in accident and emergency conditions are covered in the training.

66. Similar requirements are applied to the extent necessary to all plant personnel, including maintenance personnel and personnel permitted to work on site, whose actions might affect plant safety (including, for example, contractors and corporate level personnel). Training needs to cover technical and interpersonal managerial skills. Staff need to have both an adequate understanding of their work and a broad understanding of their contribution to plant safety.

Maintenance and surveillance

67. Prevention of the degradation of plant equipment that may be of significance for safety is a basic objective of maintenance. Of particular importance is preventive maintenance, which has the object of preventing undue degradation, malfunction or unavailability rather than restoring plant systems. Maintenance, testing and examination and inspection of structures, systems and components important to safety need to be of such a standard and frequency as to ensure that levels of reliability and effectiveness remain in accordance with the design assumptions and intent and that the safety of the plant has not been compromised since the beginning of operation. The operating organization ensures that periodic tests, examinations and inspections are carried out by qualified personnel using appropriate equipment and techniques. Maintenance is carefully planned and executed, by organizations with adequate qualification, safety culture, quality assurance programmes and work authorization procedures, and is independently verified with subsequent appropriate requalification tests.

68. The operating organization ensures that detailed instructions and procedures for maintenance, testing, examination and in-service inspection of those structures, systems and components that are necessary for safe operation are set out in writing and are consistent with the design assumptions. The ancillary and support systems such as electrical sources, compressed air supplies and lubricants are recognized as safety related and are subjected to appropriate surveillance.

69. Ageing, without appropriate countermeasures, can affect most plant components to a significant extent, with possible implications for safety. For instance, significant corrosion could induce a sudden rupture which would bring about an accident condition. Therefore measures need to be taken to ensure that age related degradation does not reduce the operational readiness of equipment, resulting in a degradation of defence in depth. Measures include the replacement of components with limited endurance before the performance of the components deteriorates. Surveillance is intended to prevent such an evolution by detecting anomalies of this type early enough that appropriate corrective actions may be initiated. Limitations on operating conditions or equipment replacement may be considered.

70. The design of equipment allows for in-service tests without major disturbance to plant operation. In-service testing is performed with the required working load on the equipment, if possible.

71. Any intervention for maintenance, testing or modification of a safety related system is conducted in accordance with the concept of defence in depth. In order to ensure that the daily operations of the plant are consistent with the global approach to safety, such interventions are conducted as follows:

— Degradation of defence in depth is prevented by: careful preparation of the work; evaluation of the risk; detailed preparation of each action and the relevant documents; verification of the compatibility between the plant condition and the intended intervention in accordance with the technical specifications related to system unavailability; identification of appropriate ways to mitigate possible consequences; use of qualified personnel; strict application of and compliance with the prepared documentation during the intervention; and implementation of a requalification process.
— Surveillance consists in periodic verification of continuing activities by means of check points, controls, visual inspections, rounds, comparisons with expected results, detection of anomalies and assessment of any observed deviation;
— Limitation of the possible consequences of anomalies or incidents, should they occur, is achieved by reaching an identified plant status preselected during the preparation of the activity, with the aid of preinstalled automatic or manual equipment or systems.

Management and safety culture

72. Safety culture is defined in INSAG-4 [3] as "that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance."

73. Safety culture is broadly relevant to all areas related to defence in depth and is particularly important for operational safety. One of the most important lessons learned from severe accidents is that there is a need to encourage a questioning and learning attitude to protection and safety and to discourage complacency in order to ensure that:

(a) policies and procedures be established that assign high priority to the protection and safety of workers and the public;
(b) problems affecting protection and safety be promptly detected and corrected in a manner commensurate with their importance;
(c) the responsibilities of each individual, including senior managers, for protection and safety be clearly identified and each individual be suitably trained and qualified;
(d) clear lines of authority for decisions on protection and safety be established;
(e) organizational arrangements and lines of communication be established that result in an appropriate flow of information on protection and safety, at and between the various levels in the operating organization;
(f) the organization has a real commitment to enhance the safety culture through the participation of staff at all levels.

74. Direct responsibility for plant safety always remains with the plant management. The operating organization delegates to the plant management all necessary authority for safe operation. The plant management ensures that the installation is operated in a safe manner, and in particular in accordance with the operational limits and conditions. The senior management of the operating organization has a major responsibility for fostering safety culture and reviewing the plant management's performance and the performance of the plant in terms of safety.

75. The operating organization sets up a detailed structure, with a description of the technical and managerial functions at the different levels of the hierarchy as well as unambiguous accountabilities for the different tasks. In addition, the work organization defines the means of internal communication and feedback as well as the relations with subcontracting companies. The use of technical support is clearly established for all modes of operation. The processes for detection, in depth analysis and corrective measures with regard to deviations and events are also clearly defined. The necessary financial and human resources are provided, including those for research and development and for engineering support.

76. For accident conditions, the organizational structure can be adapted to provide the operators with additional support and instructions. The management of accident conditions and emergencies under this organizational structure is exercised periodically.

3.4. ENHANCEMENT OF SAFETY

Operating experience

77. Information gained in operating activities such as periodic testing and maintenance and from incidents permits the design assumptions relating to equipment availability and human performance, as well as procedures, to be compared with observed performance. This essential basis for improving defence in depth generally requires internal written procedures and data handling capabilities.

78. Feedback of operating experience helps to ensure and enhance safety in operating plants and to prevent severe accidents, such as by use of the lessons learned from accident precursors.[2] Operating experience indicates the significance of events for various levels of defence in depth. The evaluation of operating experience is a continuous process to check the assumptions made during the design, the quality of the construction and the adequacy of plant operation. The results of this evaluation have significantly influenced the design of the current generation of nuclear power plants and also backfitting measures taken in operating plants, and will influence the design of future plants.

79. The operating organization maintains an effective system to ensure that operating experience is exchanged, reviewed and analysed with respect to the lessons to be learned and actions to be taken. Operating experience and lessons learned through actual incidents and accidents are also widely exchanged through communication systems with other operators. Prompt and open reporting is an obligation for mutual assistance.

80. Although operators are trained to deal with unexpected occurrences, reliance on defence in depth is no substitute for a thorough search for the root causes of incidents so that surveillance can detect incipient faults, as far as possible before they endanger the plant. It is of particular importance to identify events that indicate hidden deficiencies in defence, such as events with a potential for failures affecting more than one level. Methods of incident analysis have been progressively improved in this respect.

---

[2] An accident precursor is an equipment failure or an error that could have been the cause of an accident, in another plant condition or in the event of an additional failure, if it had not been compensated for or corrected. One way to identify significant precursors is to use PSAs to evaluate the increase in the core melt probability linked to a specific incident.

Analysis of the safety impact of plant modifications

81. Design changes to improve certain aspects of safety are carefully reviewed and their implementation carefully planned in order to ensure that they are not detrimental to safety. Particular attention is given to activities performed while the reactor is at power to prevent mishaps from jeopardizing the availability of safety functions. When a modification has been made, systems or components are requalified as nec-essary to verify that they are functioning as intended. The modification is promptly reflected in all affected features of plant operation, such as in plant documents, procedures and personnel training.

3.5. ACCIDENT CONTROL

82. Measures needed for accident control comprise specific procedures and staff training. Accident procedures are aimed at controlling the accident, with priority given to restoring safe conditions and preventing further degradation of the plant condition. Furthermore, accident procedures are reviewed and improved to take into account new knowledge and progress in research and development.

83. Two alternative approaches have been followed in developing procedures for dealing with accidents. The traditional approach most widely used is based on event analysis. Symptom based procedures are now gaining increasing support. A balanced combination of the two methods provides possibilities for further improving accident control.

3.6. MANAGEMENT OF SEVERE ACCIDENTS

84. As explained in relation to Level 4 of defence in depth (see Section 2.4), there are some means to control severe accidents and/or to mitigate their consequences.

85. Since there are generally many uncertainties about the actual course of a severe accident, it is advisable to develop a flexible approach for helping the operating staff to cope with it, including providing adequate information on plant status and support in decision making. Efficient management of severe accidents also requires careful preparation of the operating staff and the availability of specific technical support such as technical crisis teams. One feature of such situations is that the operating team is guided by a senior manager with appropriate competence and training.

86. It is essential to develop and install adequate instrumentation qualified for the radiological and accident conditions in order to diagnose the threats to the core

cooling and confinement functions as well as to monitor radiological conditions inside the plant.

3.7. EMERGENCY RESPONSE

87. On-site and off-site emergency responses are integrated, with each other and with accident management, with account taken of the size and nature of the possible source terms.

88. Emergency planning is done on the basis of deterministic considerations which may be complemented by probabilistic studies. Planning is based on a reasonable selection of scenarios and account is taken of the measures taken at Levels 2, 3 and 4 and the results of research. The on-site emergency plan addresses the issues of accident management: the protection of site workers and the provision of information to and communication with the crisis team and off-site support personnel.

89. To ensure preparedness for intervention, plans are drawn up and tested prior to starting operation and are in force throughout the plant life. Periodic rehearsal is necessary to check the effectiveness of such plans and as a training opportunity for the organization. Emergency planning also includes consideration of intervention measures such as those addressed in the International Commission on Radiological Protection's Publication No. 63 on Principles for Intervention for Protection of the Public in a Radiological Emergency [5] and in the International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources [6].

3.8. SAFETY ASSESSMENT AND VERIFICATION OF DEFENCE IN DEPTH

90. The safety assessment for the plant serves:

(a) to identify the ways in which normal and potential exposures could be incurred;
(b) to assess the quality and extent of the protection and safety provisions;
(c) to determine the expected magnitudes of normal exposures, and to estimate the probabilities and magnitudes of potential exposures.

91. Safety assessment focuses on possible challenges to levels of defence. An essential element of such an assessment is a judgement of whether and to what extent the safety functions (controlling the power, cooling the fuel and confining the radioactive material) are ensured by different levels of defence.

92. Systematic assessment of the implementation of defence in depth is performed throughout the lifetime of the plant, and account is taken of operating experience and

significant new safety information from all relevant sources. Such assessments are based on: the definition of the initial safety requirements for the plant; demonstration of compliance with these requirements; insights about deficiencies from incidents or investigations (e.g. from operating experience and the use of probabilistic evaluations); consideration of equipment ageing; and the general extension of knowledge.

93. The verification process takes into account data relating to design, manufacture, construction, commissioning, maintenance, tests, in-service inspections, modifications, component failures, component replacements, operator actions, incidents, plant and systems availability, radiation doses and radioactive releases, as appropriate. Trend analysis is a useful tool; the results of trend analyses are reviewed not only to verify that relevant parameters remain as expected but also to demonstrate that they remain within design safety limits and will remain within these limits throughout the planned life of the equipment.

94. The verification process takes advantage of two complementary methods, the deterministic method and the probabilistic method. These methods each have inherent strengths and weaknesses. The demonstration of an efficient implementation of defence in depth requires their appropriate application, with account taken of their merits and limitations.

Deterministic method

95. In the deterministic method, postulated events are chosen to encompass a range of related possible initiating events that could challenge the safety of the plant, in order to define design parameters for engineered safety features. Analyses are made to investigate the effectiveness of the safety functions in the event of the accidents they are intended to control or mitigate. Conservative assumptions are made at all steps of such calculations of accidental sequences to show that the response of the plant and its safety systems to postulated events allows the plant to meet safety targets and to ensure that the end result in terms of potential releases of radioactive materials is acceptable.

96. In calculations of the radiological consequences of postulated incidents and accidents, consideration must be given to the different pathways in the transfer of radioactive materials to the environment (via air, surface water and underground water) as well as the pathways to humans (by irradiation or by radionuclide intake by ingestion or inhalation).

97. In the safety demonstration, single initiating events are either "dealt with" or "excluded from consideration" by examining their consequences in a deterministic

way. Single initiating events can be categorized according to their estimated frequencies. More severe potential radiological consequences may be deemed tolerable for categories of very low estimated frequency.

98. The exclusion of some single initiating events from consideration has to be justified. For events that could have serious consequences, this exclusion implies preventive measures of very high reliability that can be demonstrated convincingly. These preventive measures include design conditions and criteria, selection of materials, initial and periodic inspection and testing, operational limits and conditions, and protective devices. For example, the exclusion of control rod ejection in boiling water reactors has been treated in this way.

99. In addition to single initiating events, the safety demonstration has to deal with the possibility of multiple failures and with internal and external hazards. A plant simulator may be used to demonstrate complex procedures. This part of the safety demonstration can be supported by probabilistic assessments.

Probabilistic safety assessment

100. Probabilistic safety assessment is an effective tool for identifying vulnerabilities in design and operational practices, complementary to traditional deterministic assessment. A PSA, which makes use of assumptions and data that are as realistic as possible, is also an essential tool for assessing the completeness and the balance of efforts undertaken within defence in depth.

101. The assessment of PSA results in comparison with probabilistic targets (see para. 25 of INSAG-3 [1]) can provide useful guidance. However, quantitative probabilistic targets are generally not viewed as regulatory requirements. They are intended as a guide for checking and evaluating the design, but not as the only criteria for evaluating a plant. The strengths and weaknesses of PSA are elaborated in Probabilistic Safety Assessment (INSAG-6) [4].

3.9. THE REGULATORY BODY

102. In the context of a clear allocation of responsibilities between an operating organization and the regulatory body, the latter plays a role in implementing defence in depth by setting safety objectives and by its own independent review and technical assessment of the safety justifications provided by the operating organization. This review is to check the consistency and the completeness of these justifications. Deficiencies in the implementation of defence in depth may also be detected by regulatory inspections.

103. These actions increase general confidence in the safety of plants and may be considered a contribution to defence in depth. The regulatory body, in addition, investigates safety culture within relevant organizations.

3.10. INTERNATIONAL PEER REVIEW PROCESSES

104. The implementation of defence in depth can also be improved by international co-operation. International peer reviews, as anticipated under the Convention on Nuclear Safety, will also contribute to this improvement by providing opportunities for discussing and monitoring national approaches and practices, and thereby introducing a means of learning and self-education consistent with a high level of safety culture.

4. ENHANCEMENT OF DEFENCE IN DEPTH FOR PLANTS CURRENTLY OPERATING

105. The extension of knowledge due to the accumulation of operating experience, continuing research and technological development allows for cost effective improvements in enhancing defence in depth. Section 4 discusses opportunities for such improvements in plants currently operating.

4.1. FEEDBACK OF OPERATING EXPERIENCE

106. The feedback of operating experience is a fundamental means of enhancing defence in depth, and improvements in the means of feedback are particularly important. In the following some aspects are described in which progress seems both desirable and possible.

107. Determination of the safety significance of events requires a root cause analysis. Methods for such detailed analysis have been developed and the use of root cause analysis is becoming widespread. The further development of such methods could enhance the effectiveness of the feedback of operating experience.

108. In principle, all events are assessed for whether they can be regarded as precursors of accidents. A detailed assessment of incidents will determine their safety significance (including both their direct causes and their root causes) and the appropriateness of the response of the plant systems and the personnel. Systematic analysis of

precursors will provide insights into potential deficiencies and challenges to defence in depth and might indicate the need for improvement. Some precursors of severe accidents may require urgent and effective corrective actions.

4.2. LOW POWER AND SHUTDOWN CONDITIONS

109. As the main efforts were initially devoted to postulated incidents and accidents occurring mainly under full power conditions, the implementation of the different levels of defence was for a long time less systematic, and is partly still so, for low power and shutdown conditions. The search for initiating events during shutdown was less methodical, meaning that some operating conditions were inadequately investigated, and there was a lack of well designed monitoring and protective devices, and possibly also of some automatic prevention and mitigatory systems and of well defined operating procedures.

110. The unavailability of safety systems due to maintenance activities can contribute to the development of incidents under shutdown conditions; less comprehensive confinement requirements linked to these activities may also increase the potential for external consequences. Specific operating procedures are prepared for these situations.

111. Recent systematic studies have led to the identification of sequences linked to the introduction of non-borated water into the reactor core of pressurized water reactors under specific conditions as possible initiators of criticality accidents. Owing to the potentially significant contributions of these sequences to the probability of criticality accidents, complementary preventive measures were taken.

112. Some PSAs have included systematic investigations of the relative contributions of plant shutdown conditions to the probability of core damage. These PSAs provided evidence that shutdown conditions could make significant contributions to this probability. The contribution to the frequency of core damage for the shutdown state was shown to be of the same order of magnitude as that for operation. In the light of current information, a broader and more systematic consideration of the shutdown state could improve defence in depth.

4.3. HUMAN FACTORS

113. Initiatives on the part of operators that have been based on adequate understanding and safety culture have been beneficial in some abnormal circumstances not covered clearly by operating procedures. On the other hand, human errors bear a potential for jeopardizing defence in depth. This ambivalent human role has in some

countries stimulated the organization of a kind of human redundancy and diversity, with a safety engineer acting during abnormal occurrences in parallel with the operating staff.

114. The need for continuous questioning about improvements in safety includes questions relating to automation and the human–machine interface in order to support the beneficial contributions of the staff and to reduce the possibilities and consequences of human errors. However, even though the contribution of human error to risk has been reduced in absolute terms, it remains an important relative contributor since the reliability of technical equipment is constantly being improved.

115. With regard to the potential degradation of defence in depth, one major concern is errors of commission: erroneous actions either not anticipated or differently foreseen in operating or maintenance procedures rather than omissions of required steps. Examples are selecting wrong controls, issuing wrong commands or information, changing sequences of tasks, and performing tasks too early or too late. Such errors can occur as a result of errors in decision making by the operators; misinterpreted or vague procedures; misleading instrumentation; misunderstandings; or simply errors by an operator. They bear a considerable potential to trigger common cause failures, as has been seen in some safety significant events, including the accidents at Three Mile Island in the USA in 1979 and at Chernobyl in the Ukrainian Republic in 1986. The large variety of possible actions adds to the considerable difficulty in taking such errors into account, so they need continuing attention in both the evaluation of operating experience and safety analyses (including PSA).

5. DEVELOPMENT OF DEFENCE IN DEPTH FOR FUTURE NUCLEAR POWER PLANTS

116. Several concepts for advanced reactors are being considered, and the achievement of improvements in safety and reliability is the primary incentive for these developments. Among the features of general interest are technical advances in areas relevant to reactor technology (such as information technology) and a significant reduction in system complexity with corresponding improvement in operability, including the ability to monitor the plant and to respond to system degradation.

117. The various advanced plant designs differ considerably with regard to technical principles, plant size and the time-scale considered for industrial application. From a general point of view, two approaches can be distinguished:

— The first approach aims at an improvement through an evolution from currently operating plants that takes into account results from safety research and from plant operation. This approach makes maximum use of proven technology and operating experience but may nevertheless include new safety features, some of which can be passive features. In the corresponding designs there are "large evolutionary" plants, typically water cooled, which are generally assumed to require no prototype for proof of performance and expected to be available for extensive industrial application around the end of the century; this category also includes mid-sized light water reactor designs based primarily on proven technology but incorporating more new passive safety features that can be separately tested.
— The second approach implies more fundamental changes in comparison with present designs, often with strong emphasis on specific passive features to protect fuel integrity. Owing to the nature and capability of these passive features, such "innovative designs" are mostly of smaller power output. Among these are small liquid metal reactors and high temperature gas cooled reactors, and certain advanced light water reactors that will require a prototype before industrial use and will be available later than the evolutionary designs.

118. In relation to the power output, the use of advanced reactor concepts will not reduce the amount of radioactive material in the reactor core. Defence in depth must therefore continue to be the basis for the safety of future plants and it is assumed that its improvement will continue to be the essential basis for further advances in safety. In this regard, two complementary means can be explored and put into effect:

— further reduction of the probability of severe core damage;
— strengthening the function of confinement of the radioactive products in the event of an accident.

119. Prevention of accidents remains the highest priority among the safety provisions for future plants. As already indicated in INSAG-3 [1], concerning the estimated probability of severe core damage, figures below 10^{-5} per plant year ought to be achievable. However, values that are much smaller than this would, it is generally assumed, be difficult to validate by methods and with operating experience currently available. Improved mitigation is therefore an essential complementary means to ensure public safety.

120. The optimum technical solutions for such objectives naturally depend on the specific design. For the next generation of nuclear power plants, severe accident scenarios will be considered explicitly and systematically in the design. Section 5 focuses on the next generation of plants, i.e. on designs of the evolutionary type that are intended to be available for extensive full scale application around the turn of the

century. Nevertheless, many of the approaches could apply to a broader class of concepts for future reactors.

5.1. IMPROVEMENTS IN DEFENCE IN DEPTH

121. The approach for further improvement of defence in depth is similar for existing and for future plants. However, for future plants such improvements can be achieved in a more systematic and complete way. This includes:

— improving accident prevention, in particular by optimizing the balance between the measures taken at different levels of defence in depth and by increasing their independence;
— improving the confinement function.

122. One main basis for strengthening accident prevention and the confinement function is the general consensus on the safety targets of INSAG-3 [1] for future plants, namely a probability of severe core damage below 10^{-5} per plant operating year combined with a further reduction by a factor of at least ten in the probability of a major release requiring a short term off-site response.

123. Possible means for strengthening accident prevention are:

— increased thermal inertia;
— optimized human–machine interfaces;
— extended use of information technology;
— reduced complexity;
— improved maintainability;
— expanded use of passive features;
— more systematic consideration of the possibilities of multiple failures in the original plant design.

124. The confinement function for advanced reactors will be strengthened by approaches and initiatives consistent with the following concepts:

— For advanced designs, it would be demonstrated, by deterministic and probabilistic means, that hypothetical severe accident sequences that could lead to large radioactive releases due to early containment failure are essentially eliminated with a high degree of confidence.
— Severe accidents that could lead to late containment failure would be considered explicitly in the design process for advanced reactors. This applies to both the prevention of such accidents and mitigation of their consequences, and includes a careful, realistic (best estimate) review of the confinement function and opportunities for improvement in such scenarios.

— For accident situations without core melt, it will need to be demonstrated for advanced designs that there is no necessity for protective measures (evacuation or sheltering) for people living in the vicinity of a plant. For those severe accidents that are considered explicitly in the design, it would be demonstrated by best estimate analysis that only protective measures that are very limited in scope in terms of both area and time would be needed (including restrictions in food consumption).

5.2. LEVELS OF DEFENCE IN DEPTH FOR THE NEXT GENERATION OF PLANTS

125. Meeting the safety objectives set for the next generation of nuclear power plants will necessitate improving the strength and independence of the different levels of defence. The aim is to strengthen the preventive aspect and to consider explicitly the mitigation of the consequences of severe accidents consistent with the initiatives stated in Section 5.1. This development would include the following trends:

— Level 1, for the prevention of abnormal operation and failures is to be extended by considering in the basic design a larger set of operating conditions based on general operating experience and the results of safety studies. The aims would be to reduce the expected frequencies of initiating failures and to deal with all operating conditions, including full power, low power and all relevant shutdown conditions.
— Level 2, for the control of abnormal operation and the detection of failures, is to be reinforced (for example by more systematic use of limitation systems, independent from control systems), with feedback of operating experience, an improved human–machine interface and extended diagnostic systems. This covers instrumentation and control capabilities over the necessary ranges and the use of digital technology of proven reliability.
— Level 3, for the control of accidents within the design basis, is to consider a larger set of incident and accident conditions including, as appropriate, some conditions initiated by multiple failures, for which best estimate assumptions and data are used. Probabilistic studies and other analytical means will contribute to the definition of the incidents and accidents to be dealt with; special care needs to be given to reducing the likelihood of containment bypass sequences.
— Level 4, for the prevention of accident progression, is to consider systematically the wide range of preventive strategies for accident management and to include means to control accidents resulting in severe core damage. This will include suitable devices to protect the containment function such as the capability of the containment building to withstand hydrogen deflagration, or improved protection of the basemat for the prevention of melt-through.

— Level 5, for the mitigation of the radiological consequences of significant releases, could be reduced, owing to improvements at previous levels, and especially owing to reductions in source terms. Although less called upon, Level 5 is nonetheless to be maintained.

REFERENCES

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

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, A Common Basis for Judging the Safety of Nuclear Power Plants Built to Earlier Standards, INSAG Series No 8, IAEA, Vienna (1995).

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Safety Culture, Safety Series No. 75-INSAG-4, IAEA, Vienna (1991).

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

[5] INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, Principles for Intervention for Protection of the Public in a Radiological Emergency, ICRP Publication No. 63, Ann. ICRP **22** 4, Pergamon Press, Oxford and New York (1991).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Interim Edition, Safety Series No. 115-I, IAEA, Vienna (1994).

MEMBERS OF THE INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

Beninson, D.	Matsuura, S.
Birkhofer, A.	Quéniart, D.
Chang, S.H.	Sidorenko, V.A.
Clarke, R.H.	Soman, S.D.
Domaratzki, Z. *(Chairman)*	Taylor, J.J.
Gonzalez-Gomez, E.	Velona, F.
Högberg, L.	Wang, C.

D. Quéniart replaced D. Vignon in May 1993. Z. Križ resigned from INSAG in June 1993. S. Matsuura replaced K. Sato in February 1994.

A. Bukrinski, J. Libmann and A. Schäfer also contributed to the drafting and review of this report.

A. Karbassioun of the IAEA Secretariat is responsible for matters relating to INSAG in the Division of Nuclear Safety.

PUBLICATIONS OF THE INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

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

HOW TO ORDER IAEA PUBLICATIONS

No. 2, January 1996

☆ ☆ **In the United States of America and Canada**, the exclusive sales agents for IAEA publications, to whom all orders and inquiries should be addressed, is:

UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA

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

AUSTRALIA	Hunter Publications, 58A Gipps Street, Collingwood, Victoria 3066
BELGIUM	Jean de Lannoy, 202 Avenue du Roi, B-1060 Brussels
CHINA	IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing
CZECH REPUBLIC	Artia Pegas Press Ltd., Palác Metro, Narodni tř. 25, P.O. Box 825, CZ-111 21 Prague 1
DENMARK	Munksgaard International Publishers Ltd., P.O. Box 2148, DK-1016 Copenhagen K
EGYPT	The Middle East Observer, 41 Sherif Street, Cairo
FRANCE	Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05
GERMANY	UNO-Verlag, Vertriebs- und Verlags GmbH, Dag Hammarskjöld-Haus, Poppelsdorfer Allee 55, D-53115 Bonn
HUNGARY	Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
INDIA	Viva Books Private Limited, 4325/3, Ansari Road, Darya Ganj, New Delhi-110002
ISRAEL	YOZMOT Literature Ltd., P.O. Box 56055, IL-61560 Tel Aviv
ITALY	Libreria Scientifica Dott. Lucio di Biasio "AEIOU", Via Coronelli 6, I-20146 Milan
JAPAN	Maruzen Company, Ltd., P.O. Box 5050, 100-31 Tokyo International
NETHERLANDS	Martinus Nijhoff International, P.O. Box 269, NL-2501 AX The Hague Swets and Zeitlinger b.v., P.O. Box 830, NL-2610 SZ Lisse
POLAND	Ars Polona, Foreign Trade Enterprise, Krakowskie Przedmieście 7, PL-00-068 Warsaw
SLOVAKIA	Alfa Press Publishers, Hurbanovo námestie 3, SQ-815 89 Bratislava
SPAIN	Díaz de Santos, Lagasca 95, E-28006 Madrid Díaz de Santos, Balmes 417, E-08022 Barcelona
SWEDEN	Fritzes Customer Service, S-106 47 Stockholm
UNITED KINGDOM	HMSO, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR

☆ ☆ Orders (except for customers in Canada and the USA) and requests for information may also be addressed directly to:

Sales and Promotion Unit
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria

Telephone: +43 1 2060 22529 (or 22530)
Facsimile: +43 1 2060 29302
Electronic mail: SALESPUB@ADPO1.IAEA.OR.AT

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 1996
ISBN 92–0–102596–3
ISSN 1025–2169