SAFETY SERIES No. 110

SAFETY FUNDAMENTALS

safety series

The Safety of Nuclear Installations

INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1993

CATEGORIES IN THE IAEA SAFETY SERIES

A new hierarchical categorization scheme has been introduced, according to which the publications in the IAEA Safety Series are grouped as follows:

Safety Fundamentals (silver cover)

Basic objectives, concepts and principles to ensure safety.

Safety Standards (red cover)

Basic requirements which must be satisfied to ensure safety for particular activities or application areas.

Safety Guides (green cover)

Recommendations, on the basis of international experience, relating to the fulfilment of basic requirements.

Safety Practices (blue cover)

Practical examples and detailed methods which can be used for the application of Safety Standards or Safety Guides.

Safety Fundamentals and Safety Standards are issued with the approval of the IAEA Board of Governors; Safety Guides and Safety Practices are issued under the authority of the Director General of the IAEA.

An additional category, **Safety Reports** (purple cover), comprises independent reports of expert groups on safety matters, including the development of new principles, advanced concepts and major issues and events. These reports are issued under the authority of the Director General of the IAEA.

There are other publications of the IAEA which also contain information important to safety, in particular in the Proceedings Series (papers presented at symposia and conferences), the Technical Reports Series (emphasis on technological aspects) and the IAEA-TECDOC Series (information usually in a preliminary form).

THE SAFETY OF NUCLEAR INSTALLATIONS

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

AFGHANISTAN
ALBANIA
ALGERIA
ARGENTINA
AUSTRALIA
AUSTRIA
BANGLADESH
BELARUS
BELGIUM
BOLIVIA
BRAZIL
BULGARIA
CAMBODIA
CAMEROON
CANADA
CHILE
CHINA
COLOMBIA
COSTA RICA
COTE D'IVOIRE
CROATIA
CUBA
CYPRUS
DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA
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
KENYA
KOREA, REPUBLIC OF
KUWAIT
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LUXEMBOURG
MADAGASCAR
MALAYSIA
MALI
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
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
THAILAND
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
VENEZUELA
VIET NAM
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
July 1993
STI/PUB/938

SAFETY SERIES No. 110

THE SAFETY OF NUCLEAR INSTALLATIONS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 1993

THIS SAFETY SERIES PUBLICATION IS ALSO ISSUED IN CHINESE, FRENCH, RUSSIAN AND SPANISH

VIC Library Cataloguing in Publication Data

The safety of nuclear installations. — Vienna : International Atomic Energy Agency, 1993.
p. ; 24 cm. — (Safety series, ISSN 0074–1892 ; 110)
STI/PUB/938
ISBN 92–0–101893–2
Includes bibliographical references.

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

VICL 93-00062

FOREWORD

The development of nuclear safety standards is one of the tasks authorized in the Statute of the IAEA. The Secretariat seeks to establish standards of safety, assisted by Member States with experience of nuclear power programmes. A broad consensus of opinion is sought to provide assurance that the safety objectives and standards thus defined and developed are acceptable to all Member States. The publication of such consensus opinions with the approval of the IAEA Board of Governors establishes them as rules for the IAEA's own activities.

This Safety Fundamentals publication presents an international consensus on the basic concepts underlying the principles for the regulation, management of safety and operation of nuclear installations. It forms a top level publication in the hierarchy of the IAEA Safety Series. In conjunction with this publication, Safety Standards, Safety Guides and Safety Practices provide detailed requirements and recommendations for activities relating to siting, design, quality assurance, operation and regulation for nuclear installations. The totality of measures taken to ensure nuclear safety is both detailed and technically complex. This publication explains the basis for those measures and provides an insight for those who make decisions relating to the use of nuclear energy but who may not be specialists in nuclear science and technology.

The publication has been prepared by drawing on material from other IAEA publications. Particular benefit was gained from the work of the International Nuclear Safety Advisory Group (INSAG), and in particular its publication Basic Safety Principles for Nuclear Power Plants (IAEA Safety Series No. 75-INSAG-3).

The IAEA is grateful to all those who assisted in drafting and review.

CONTENTS

1. INTRODUCTION

BACKGROUND

101. The implementation of safety standards for nuclear installations, including those of the IAEA's Nuclear Safety Standards (NUSS) programme, has indicated a need for a separate publication to present the fundamental principles of nuclear safety. The Safety Series publications form a hierarchy of four levels with Safety Fundamentals at the highest level. Other levels correspond to Safety Standards, Safety Guides and Safety Practices. This Safety Fundamentals publication is intended not only for those people who are interested in the more detailed Safety Standards and Safety Guides, but also for those technical and political decision makers who may need a concise explanation of the fundamental safety principles.

OBJECTIVE

102. Nuclear technology can contribute to the well-being of people but, as with other industrial activities, may also have detrimental effects. The purpose of this publication is to define those fundamental safety principles which, when effectively applied, contribute to the reduction to very low levels of any detrimental effects from the use of nuclear technology.

103. This Safety Fundamentals publication sets out basic objectives, concepts and principles for ensuring safety that can be used both by the Agency in its international assistance operations and by a Member State in its national nuclear programme. Guidance on the application of these fundamental safety principles is given in the Agency's Safety Series publications, such as the NUSS Codes and Safety Guides and the Research Reactor Codes and Safety Guides.

SCOPE

104. These Safety Fundamentals apply primarily to those nuclear installations in which the stored energy or the energy developed in certain situations could potentially result in the release of radioactive material from its designated location with the consequent risk of radiation exposure of people. These principles, since they are fundamental in nature, are applicable to a broad range of nuclear installations, but their detailed application will depend on the particular technology and the risks posed by it. In addition to nuclear power plants, such installations may include: research reactors and facilities; fuel enrichment, manufacturing and reprocessing plants; and certain facilities for radioactive waste treatment and storage. Activities at

these installations may also include industrial processes that pose additional hazards to site personnel and the environment. These industrial hazards are outside the scope of this publication, but must also be considered.

STRUCTURE

105. This publication is structured so that Section 2 covers the Safety Objectives and Sections 3–6 cover the supporting basic principles. Sections 3–6 are structured so that the background and general safety implications of the particular subject are dealt with first and the safety issues are then condensed into safety principles. These constitute the nucleus of safety requirements necessary to ensure adequate protection from the hazards of ionizing radiation. For this reason they are phrased as imperatives with the word 'shall' to distinguish them as fundamental requirements.

2. SAFETY OBJECTIVES

201. Any industrial activity both yields benefits and incurs risks. For the purpose of this publication, risk is taken to be the probability that a specified harmful effect will occur within a specified period. Complex industrial activities, such as the operation of nuclear installations, usually have associated risks of various types. The risks may be borne by the site personnel, by people living near the installation and by the whole of society. The environment may also suffer harm if radioactive materials are released, particularly under accident conditions. Consequently, it is necessary to limit the risks to which people and the environment are subject for all reasonably foreseeable circumstances. A further discussion of the concept of risk and of various methods for risk evaluation and limitation is found in the Annex.

202. The principles in this publication apply to the measures necessary to minimize the risks to site personnel, the public and the environment from the effects of ionizing radiation. These risks must be strictly controlled. The principles are derived from the following Safety Objectives.

203. **General Nuclear Safety Objective:** *To protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defences against radiological hazards.*

204. This General Nuclear Safety Objective is supported by two complementary Safety Objectives dealing with radiation protection and technical aspects. They are interdependent: the technical aspects in conjunction with administrative and procedural measures ensure defence against hazards due to ionizing radiation.

205. **Radiation Protection Objective:** *To ensure that in all operational states radiation exposure within the installation or due to any planned release of radioactive material from the installation is kept below prescribed limits and as low as reasonably achievable, and to ensure mitigation of the radiological consequences of any accidents.*

206. **Technical Safety Objective:** *To take all reasonably practicable measures to prevent accidents in nuclear installations and to mitigate their consequences should they occur; to ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and to ensure that the likelihood of accidents with serious radiological consequences is extremely low.*

207. Safety Objectives require that nuclear installations are designed and operated so as to keep all sources of radiation exposure under strict technical and administrative control. However, the Radiation Protection Objective does not preclude limited exposure of people or the release of legally authorized quantities of radioactive materials to the environment from installations in operational states. Such exposures and releases, however, must be strictly controlled and must be in compliance with operational limits and radiation protection standards.

208. To achieve the Safety Objectives, measures need to be taken to control radiation exposure in all operational states to levels as low as reasonably achievable and to minimize the likelihood of an accident that might lead to the loss of normal control of the source of radiation. Nevertheless, accidents can happen. Measures are therefore required to ensure that any radiological consequences are mitigated. Such measures include on-site accident management procedures and off-site intervention measures in order to mitigate radiation exposure after an accident has occurred. The greater the potential hazard from an uncontrolled release of radioactive material, the lower the likelihood must be of its occurrence.

ACHIEVEMENT OF SAFETY OBJECTIVES

209. Countries that are operating nuclear installations now or that may be doing so in the future need to apply the fundamental principles set out in this publication, as appropriate, taking into account the hazards for each type of installation. On the basis of the areas and issues addressed, the principles have been grouped into four sections (Sections 3–6).

210. Section 3 clarifies the responsibilities of the major parties: governmental, legislative and regulatory responsibilities on the one hand and the responsibilities of the operating organization on the other.

211. Section 4 defines the basic requirements for safety management for organizations that have important responsibilities in connection with safety. In particular, the requirements on the operating organization are addressed, because of its prime responsibility for safety.

212. Sections 5 and 6 present the fundamental technical principles that must be applied to achieve and verify safety.

3. LEGISLATIVE AND REGULATORY FRAMEWORK

LEGISLATIVE REQUIREMENTS

301. A legal framework needs to be established that provides for the regulation of nuclear activities and for the clear assignment of safety responsibilities. Government is responsible for the adoption of legislation which assigns the prime responsibility for safety to the operating organization and establishes a regulatory body responsible for a system of licensing (see definition of licence), for the regulatory control of nuclear activities and for enforcing the relevant regulations.

302. In the application of these fundamental principles, differences between Member States' legal systems, cultures and practices may lead to differences in approach to the regulation of safety within the overall legislative framework.

RESPONSIBILITIES OF THE REGULATORY BODY

303. It is the responsibility of the regulatory body to set safety objectives and standards, and to monitor and enforce them within the established legislative and statutory framework. No other responsibility is to jeopardize or conflict with safety, its prime mission.

304. An important condition for the proper functioning of the regulatory body in discharging its responsibilities is its effective independence from organizations or bodies that promote nuclear activities. This is necessary so that its judgements may

be made, and enforcement actions taken, without undue pressure from interests that may compete with safety. An additional important function of the regulatory body is to communicate independently its regulatory decisions and opinions and their bases to the public.

305. The organizational framework of a regulatory body may vary from country to country, but in all cases the regulatory body must have the statutory authority, competence and resources:

- to set safety standards;
- to license and inspect installations;
- to set, monitor and enforce licence conditions; and
- to ensure that corrective actions are taken wherever unsafe or potentially unsafe conditions are detected.

None of these functions should be interpreted as reducing or relieving the operating organization of its responsibility for safety.

RESPONSIBILITIES OF THE OPERATING ORGANIZATION

306. The prime responsibility for the safety of the installation rests with the operating organization. It is responsible for specifying its safety criteria and assuring itself that the design, construction and operation of the installation meet the relevant safety standards. Subsequently, it is responsible for the establishment of procedures and arrangements to ensure the safe control of the installation under all conditions, for the establishment and maintenance of a competent and fully trained staff, and for the control of fissile and radioactive materials utilized or generated. The fulfilment of these responsibilities is to be in accordance with applicable safety objectives and requirements established or approved by the regulatory body.

307. Other bodies may have professional or legal responsibilities that are significant to safety; for example, designers, manufacturers and constructors. Such bodies are also required to meet quality standards and specifications. Although the operating organization may delegate authority to carry out functions on its behalf, it cannot delegate the prime responsibility for safety.

Principles

(1) *The government shall establish a legislative and statutory framework for the regulation of nuclear installations. There shall be a clear separation of responsibilities between the regulatory body and the operating organization.*

(2) *The prime responsibility for safety shall be assigned to the operating organization.*

(3) *The regulatory body shall be effectively independent of the organization or body charged with the promotion or utilization of nuclear energy. It shall have licensing, inspection and enforcement responsibilities and shall have adequate authority, competence and resources to fulfil its assigned responsibilities. No other responsibility shall jeopardize or conflict with its responsibility for safety.*

4. MANAGEMENT OF SAFETY

401. Safety management is the term used for the measures required to ensure that an acceptable level of safety is maintained throughout the life of an installation, including decommissioning. The starting point for the management of safety is the senior managers of all organizations involved. The role of each organization should be specific and defined and may extend throughout the life of the installation or be limited to a particular phase. Whichever the case, it is a management responsibility to recognize the safety significance of the organization's activities. Management must ensure that its organization is well structured with clear lines of authority and communication and well defined responsibilities; and that its safety policies, requirements and procedures are established, understood and observed by all involved. However, the assignment of tasks among organizations must not reduce or divide the prime responsibility for safety, which lies with the operating organization. As a result, the operating organization remains in a supervisory position for delegated tasks.

402. The principles of safety management broadly apply to all organizations. Thus, the practices described for the operating organization apply, where relevant, to other organizations with safety responsibilities.

RESPONSIBILITIES IN MANAGEMENT

403. The operating organization has the responsibility to assure itself of and to maintain the quality of the installation as designed, constructed, commissioned and operated; to ensure that it is operated in accordance with the design specifications and safety analysis; and to make the necessary safety improvements. Thus, the operating organization must:

— establish and implement safety policies;
— have a clear division of responsibilities with corresponding lines of authority and communication;
— ensure that it has sufficient staff with appropriate levels of education and training;
— develop and strictly adhere to sound procedures; and
— review, monitor and audit all safety related matters on a regular basis.

404. The sum of these measures is intended to create an atmosphere of rigour and thoroughness throughout the operating organization to ensure that all safety objectives are achieved. However, the management of safety at the installation will not be effective unless the operating organization has a very high level of commitment to safety. The lead in safety matters must come from the top, from the highest levels of management. Their safety policies and attitudes need to permeate the operating organization on every level and to extend to other organizations performing delegated tasks. There can be no complacency at any level about the continuous attention demanded by safety. Safety management implies a learning attitude to safety matters and the open exchange of information both upwards and downwards in the organization.

405. The operating organization will usually delegate operating authority to the on-site management of the installation which has the direct day to day control. Accordingly, the operating organization has a responsibility to monitor the effectiveness of safety management at the installation and to take necessary measures to ensure that safety is maintained at the desired level.

QUALITY ASSURANCE

406. Quality assurance practices are an essential part of good management and are to be applied to all activities affecting the quality of items, processes and services important to safety. Inherent in the achievement of quality is the adoption of a quality assurance programme, which includes the planned and systematic actions necessary to provide adequate confidence that specified requirements are satisfied. Implementation of the quality assurance programme involves managers, performers of tasks, and those responsible for verification and assessment of the effectiveness of the programme. It is not the sole domain of a single group. However, management has the key responsibility to ensure that the programme functions properly and to establish and cultivate principles that integrate quality assurance practices with daily work activities.

407. Quality needs to be verified by a disciplined approach. Thus, quality assurance practices include:

— a detailed analysis of the objectives to be achieved;
— an analysis of the tasks to be performed;
— the identification of skills required;
— the selection and training of personnel;
— the use of appropriate equipment and procedures;
— the use of document control and record systems;
— the creation of a satisfactory working environment; and
— a recognition of individual responsibilities.

The extent and type of quality verification need to reflect the safety significance and nature of the individual tasks. Such verification methods include audits, checks and examinations to ensure that each task has been satisfactorily performed or that any necessary corrective actions have been taken. However, the basic responsibility for achieving quality remains with the performer of the task, not the verifier.

HUMAN FACTORS

408. An important factor in safety management is the recognition of the influence of human behaviour. The possibility of the occurrence of human errors directly affecting safety needs to be recognized and the probability reduced to the minimum practically achievable. The effects of such errors must, where practicable, be eliminated or mitigated by a systematic approach, in order to achieve a high tolerance of human errors in the installation. Additionally, functional requirements for personnel need to be defined and met through appropriate staff selection and training.

ACCIDENT MANAGEMENT AND EMERGENCY PREPAREDNESS

409. Accident prevention is the first safety priority of designers and the operating organization. There can be no guarantee that the prevention of accidents will be totally successful. However, the rigorous application of safety principles provides confidence that the likelihood of an accident that leads to a significant release of radioactive materials from an installation is extremely low. Nevertheless, the operating organization and regulatory body need to make preparations to cope with accident situations. In particular, the operating organization must prepare accident management procedures and on-site emergency plans before the commencement of operation. Off-site emergency procedures must also be prepared with the involvement of the operating organization and competent authorities, and be consistent with national and international agreements. Both on-site and off-site emergency plans

need to be exercised periodically to the extent necessary to ensure the preparedness of responsible organizations.

Principles

(4) *Organizations engaged in activities important to safety shall establish policies that give safety matters the highest priority, and shall ensure that these policies are implemented within a managerial structure having clear divisions of responsibility and clear lines of communication.*

(5) *Organizations engaged in activities important to safety shall establish and implement appropriate quality assurance programmes which extend throughout the life of the installation, from siting and design through to decommissioning.*

(6) *Organizations engaged in activities important to safety shall ensure that there are sufficient numbers of adequately trained and authorized staff working in accordance with approved and validated procedures.*

(7) *The capabilities and limitations of human performance shall be taken into account at all stages in the life of the installation.*

(8) *Emergency plans for accident situations shall be prepared and appropriately exercised by all organizations concerned. The capability to implement emergency plans shall be in place before an installation commences operation.*

5. TECHNICAL ASPECTS OF SAFETY

SITING

501. Potential sites need to be evaluated for man-made and natural factors that could adversely affect the safety of the installation. The effects the installation may have on the surrounding population and on the environment, such as by the utilization of land and water, should also be evaluated. Relevant site related factors must be taken into account in the design of the installation and the adequacy of the design in this respect needs to be demonstrated before the acceptability of the site can be confirmed. An evaluation of all site related factors must be made by the operating organization as part of the licensing application, and reviewed by the regulatory body. Population density and distribution over the lifetime of the installation are of

particular importance and need to be evaluated periodically to ensure the continued feasibility of emergency plans.

Principle

(9) *The site selection shall take into account relevant features that might affect the safety of the installation, or be affected by the installation, and the feasibility of carrying out emergency plans. All aspects shall be evaluated for the projected lifetime of the installation and re-evaluated as necessary to ensure the continued acceptability for safety of site related factors.*

DESIGN AND CONSTRUCTION

502. To comply with the Safety Objectives presented in Section 2, the design of the installation and the operational procedures need to ensure:

- the limitation of radiation exposures, of radioactive releases and of the production of radioactive wastes during all operational states, as far as is reasonably achievable;
- the prevention of accidents that could affect site personnel, the public and the environment; and
- the limitation and mitigation of the consequences of accidents if they do occur.

503. Consequently, there is a need for:

- components, systems and structures with high reliability;
- technology that is proven or qualified by experience or testing or both, meeting conservative regulations or criteria with appropriate safety margins;
- appropriate inherent and engineered safety features; and
- specific consideration in design to minimizing personnel exposures.

Additionally, components, structures and systems need to be classified on the basis of their safety significance and to be designed, manufactured and installed to a level of quality commensurate with that classification.

504. Since engineered systems may fail despite all careful precautions, it is a basic design concept to provide backup features so that either a function is performed by another system or another design feature mitigates the consequences associated with the failure of the system. Consequently, design principles have been formulated to achieve the goal of accident prevention and mitigation with high confidence. For example:

- no single equipment failure or single maintenance action or any other single human action should disable a safety function;

— the possibility of failures due to a common cause should be minimized by diversity of equipment;
— redundant systems should function independently of each other to achieve reliability; and
— where practicable, design concepts should be used which place the installation in a safe state on failure of components or systems.

The proper application of such design principles creates a design based on defence in depth, centred on several levels of protection and multiple barriers to prevent the release of radioactive materials. The levels of protection are designed firstly, to prevent the breach of any barrier, and secondly, to mitigate the consequences of a breach. The levels of protection include not only engineered control and protection systems, but also aspects such as conservative design, quality assurance, accident management strategies and emergency response.

505. The design also needs to take account of the performance capabilities of the operating and maintenance personnel. Attention to human factors will ensure that the installation is tolerant of human errors. Among the appropriate elements in minimizing human error is the systematic application of ergonomic principles to:

— engineered systems;
— the provision of automatic control, protection and alarm systems;
— the elimination of human actions that jeopardize safety;
— the clear presentation of data; and
— reliable communication within the installation.

506. A comprehensive safety analysis of the behaviour of the installation under a wide range of conditions is necessary. It must include an assessment of a wide spectrum of events to ensure that accidents, including those of low probability, can be effectively dealt with and their consequences mitigated by means of installed safety systems, sound procedures and accident management.

507. The responsibility for ensuring that the safety of the design is acceptable lies with the operating organization. The task of producing a safe design lies with the design organization. However, a group responsible for safety assessment, and separate from those carrying out the design, needs to provide an independent verification that all safety requirements and objectives have been met. The operating organization is responsible for making sure that this provision is effective. Moreover, the operating organization must ensure that there is appropriate liaison with the design group in order to ensure that the design meets the operating staff's requirements and is consistent with anticipated operating procedures.

508. Construction of an installation may start only after the operating organization has satisfied itself that the main safety issues have been resolved and the regulatory body has satisfied itself of the adequacy of the safety analysis submitted and the adequacy of the proposed arrangements, procedures and quality assurance programmes to implement the design throughout construction. In this regard the responsibility for ensuring that the construction is acceptable lies with the operating organization.

Principles

(10) *The design shall ensure that the nuclear installation is suited for reliable, stable and easily manageable operation. The prime goal shall be the prevention of accidents.*

(11) *The design shall include the appropriate application of the defence in depth principle so that there are several levels of protection and multiple barriers to prevent releases of radioactive materials, and to ensure that failures or combinations of failures that might lead to significant radiological consequences are of very low probability.*

(12) *Technologies incorporated in a design shall be proven or qualified by experience or testing or both.*

(13) *The systematic consideration of the man–machine interface and human factors shall be included in all stages of design and in the associated development of operational requirements.*

(14) *The exposure to radiation of site personnel and releases of radioactive materials to the environment shall be made by design as low as reasonably achievable.*

(15) *A comprehensive safety assessment and independent verification shall be carried out to confirm that the design of the installation will fulfil the safety objectives and requirements, before the operating organization completes its submission to the regulatory body.*

COMMISSIONING

509. The purpose of commissioning is to demonstrate that the design specifications of the installation have been met and that the completed installation is satisfactory for service. The operating organization is responsible for the preparation and

documentation of the commissioning programme with the full participation of the design organization. The programme needs to provide for the sequential testing of elements of systems and completed systems and of the correct functioning of interrelated systems in a progressive manner. The installation needs to be proven for all foreseeable operational states and, where practicable, all foreseeable accident conditions, including all operator actions that are required for systems to function under normal or accident conditions. The commissioning programme, including relevant limits and conditions, must be approved in advance by the regulatory body. The regulatory body must satisfy itself that the safety analysis is valid for the commissioning programme and for continued operations.

Principle

(16) *Specific approval by the regulatory body shall be required before the start of normal operation on the basis of an appropriate safety analysis and a commissioning programme. The commissioning programme shall provide evidence that the installation as constructed is consistent with design and safety requirements. Operating procedures shall be validated to the extent practicable as part of the commissioning programme, with the participation of the future operating staff.*

OPERATION AND MAINTENANCE

510. The operation of the installation must be controlled in accordance with a set of operational limits and conditions, derived from the safety analysis, which identify safe boundaries of operation. These limits and conditions must be revised as necessary in the light of experience from commissioning and operation. Minimum requirements must be set for the availability of staff and equipment. Competent technical support for the operating organization and its operating staff has to be available throughout the lifetime of the installation. Operations must be carried out by adequately trained and authorized personnel in accordance with detailed, validated and approved procedures and in accordance with a quality assurance programme.

511. The installation must be regularly inspected, tested and maintained in accordance with approved procedures to ensure that components, structures and systems continue to be available and to operate as intended, and that they retain their capability to meet the design objectives and the requirements of the safety analysis. Modifications to the installation must be controlled in accordance with approved procedures. Where modifications alter the operational limits and conditions, there needs to be a safety analysis to justify the new limits and conditions.

512. Operating procedures must provide staff with instructions for the response to anticipated operational occurrences. Procedures are also needed to manage, as far as practicable, accidents that could lead to severe consequences, even if the probability of these is extremely low. The principal objectives of such procedures are to restore prime safety functions, to facilitate long term recovery from an accident and to mitigate its radiological consequences.

513. The operating organization must establish a programme for the collection and analysis of operating experience. Safety significant information needs to be disseminated to its staff and to relevant national and international organizations. Lessons learned from operating experience need to be considered by both the operating organization and the regulatory body in order to determine whether equipment, procedures and/or training or related safety requirements need to be modified.

Principles

(17) *A set of operational limits and conditions derived from the safety analysis, tests and subsequent operational experience shall be defined to identify safe boundaries for operation. The safety analysis, operating limits and procedures shall be revised as necessary if the installation is modified.*

(18) *Operation, inspection, testing and maintenance and supporting functions shall be conducted by sufficient numbers of adequately trained and authorized personnel in accordance with approved procedures.*

(19) *Engineering and technical support, with competence in all disciplines important for safety, shall be available throughout the lifetime of the installation.*

(20) *The operating organization shall establish documented and approved procedures as a basis for operator response to anticipated operational occurrences and accidents.*

(21) *The operating organization shall report incidents significant to safety to the regulatory body. The operating organization and the regulatory body shall establish complementary programmes to analyse operating experience to ensure that lessons are learned and acted upon. Such experience shall be shared with relevant national and international bodies.*

RADIOACTIVE WASTE MANAGEMENT AND DECOMMISSIONING

514. The generation of radioactive waste needs to be limited, in terms of both activity and volume, by design measures and operating practices, as far as is

reasonably achievable. Radioactive waste treatment and interim storage need to be provided and strictly controlled in a manner that is also consistent with final disposal requirements.

515. The fact that a nuclear installation will cease operation and may be dismantled and removed has to be recognized and appropriate precautions taken. The design of the installation needs to address the limitation of radiation exposures to site personnel and of release of radioactive material to the environment as far as is reasonably achievable during dismantling. A suitable decommissioning programme needs to be approved by the regulatory body prior to the initiation of decommissioning.

Principles

(22) *The generation of radioactive waste, in terms of both activity and volume, shall be kept to the minimum practicable by appropriate design measures and operating practices. Waste treatment and interim storage shall be strictly controlled in a manner consistent with the requirements for safe final disposal.*

(23) *The design of an installation and the decommissioning programme shall take into account the need to limit exposures during decommissioning to as low as is reasonably achievable. Prior to the initiation of decommissioning activities, the decommissioning programme shall be approved by the regulatory body.*

6. VERIFICATION OF SAFETY

601. Verification of the safety of a nuclear installation over its lifetime includes many activities, such as:

- application of quality assurance principles at all stages;
- independent assessment of the safety of the design;
- review of site related factors;
- review of tests during construction and commissioning;
- continuing monitoring and inspection of the installation during operation, including environmental monitoring;
- assessment of the need for and the control of modifications.

602. Safety verification also means that the operating organization has the responsibility to ensure that events important to safety are reviewed in depth and that, when necessary, equipment is modified, procedures are revised and training is given to prevent recurrence. Access to information and relevant experience from similar installations worldwide is essential in such reviews.

603. The operating organization additionally must carry out systematic reviews of safety to confirm that the safety analysis for the installation remains valid, or, if necessary, to implement safety improvements. Such reviews need to consider the cumulative effects of modifications, changes to procedures, the ageing of components, operating experience and technical developments. Operational limits and conditions need to be reviewed at the same time and modified, as required, with account taken of operating experience and technological developments. Special safety reviews of the installation must be conducted before operation beyond the design life. Such reviews are needed as a basis for a decision on reissuing or extending the operating licence for the installation.

604. The regulatory body, after consultation with the operating organization, specifies the programme for systematic safety reassessment of the installation. The combination of day to day and year to year surveillance and systematic safety reassessment is aimed at verifying that the installation is operated within the bounds of its safety analysis at all times.

Principles

(24) *The operating organization shall verify by analysis, surveillance, testing and inspection that the physical state of the installation and its operation continue in accordance with operational limits and conditions, safety requirements and the safety analysis.*

(25) *Systematic safety reassessments of the installation in accordance with the regulatory requirements shall be performed throughout its operational lifetime, with account taken of operating experience and significant new safety information from all relevant sources.*

DEFINITIONS

Accident Conditions

Deviations[1] from Operational States in which the releases of radioactive materials are kept to acceptable limits by appropriate design features. These deviations do not include Severe Accidents.

Accident Management

The taking of a set of actions

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

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

Anticipated Operational Occurrences[2]

All operational processes deviating from Normal Operation that are expected to occur once or several times during the operating life of the installation and which, in view of appropriate design provisions, do not cause any significant damage to items important to safety or lead to Accident Conditions.

Commencement of Operation

The beginning of initial fuel loading.

---

[1] A deviation may be a major fuel failure, a loss of coolant accident (LOCA), etc.

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

Commissioning[3]

The process during which components and systems of nuclear installations, having been constructed, are made operational and verified to be in accordance with design assumptions and to have met the performance criteria; this includes both non-nuclear and nuclear tests.

Construction[3]

The process of manufacturing and assembling the components of a nuclear installation, the erection of civil works and structures, the installation of components and equipment, and the performance of associated tests.

Decommissioning[3]

The process by which a nuclear installation is permanently taken out of Operation.

Design[3]

The process and the result of developing the concept, detailed plans, supporting calculations and specifications for a nuclear installation and its parts.

Enforcement

Legal actions by the Regulatory Body, intended to correct and, as appropriate, penalize non-compliance.

Inspection

Actions which by means of examination, observation or measurement determine the conformance of materials, parts, components, systems and structures, as well as processes and procedures, with defined requirements.

---

[3] The terms Siting, Design, Construction, Commissioning, Operation and Decommissioning are used to delineate the six major stages of the licensing process. Several of the stages may coexist; for example, Construction and Commissioning, or Commissioning and Operation.

Licence

Authorization issued to the applicant by the Regulatory Body to perform specified activities related to the Siting, Design, Construction, Commissioning, Operation and Decommissioning of a nuclear installation.

Normal Operation

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

Operating Organization

The organization authorized by the Regulatory Body to operate the nuclear installation.

Operation (see footnote 3)

All activities performed to achieve the purpose for which the nuclear installation was constructed, including maintenance, refuelling, in-service inspection and other associated activities.

Operational Limits and Conditions

A set of rules which set forth parameter limits, the functional capability and the performance levels of equipment and personnel approved by the Regulatory Body for safe operation of the nuclear installation.

Operational States

States defined under Normal Operation or Anticipated Operational Occurrences.

Prescribed Limits[4]

Limits established or accepted by the Regulatory Body.

---

[4] The term 'authorized limits' is sometimes used in IAEA publications.

Quality Assurance

All those planned and systematic actions necessary to provide adequate confidence that an item or service will satisfy given requirements for quality.

Regulatory Body

A national authority or a system of authorities designated by a Member State, assisted by technical and other advisory bodies, and having the legal authority for conducting the licensing process, for issuing Licences and thereby for regulating Siting, Design, Construction, Commissioning, Operation and Decommissioning, or specified aspects thereof, for nuclear installations.

Severe Accidents

States of nuclear installations beyond Accident Conditions, including those causing significant core degradation.

Site Personnel

All persons working on the site, either permanently or temporarily.

Siting (see footnote 3)

The process of selecting a suitable site for a nuclear installation, including appropriate assessment and definition of the related design bases.

Annex

THE CONCEPT OF RISK: METHODS OF RISK EVALUATION AND LIMITATION

A1. In para. 201 risk was taken to be the probability that a specified harmful effect will occur within a specified period. It was furthermore noted that complex industrial activities, such as the operation of nuclear installations, usually have associated risks of various types, relating to different types of harm to individuals, society and the environment. Therefore, any evaluation of risk starts with a definition of the types of harmful effects that need to be taken into account.

A2. One commonly used type of risk evaluation is that of the increment in probability that an individual will suffer a fatal injury or illness as a result of radiation exposure (the increment in individual health risk). However, an evaluation of the consequences of a potential major accident at a nuclear installation may have to consider types of harmful effects other than just increments in individual health risks. Such effects may include the potential total number of fatalities or injuries attributable to radiation exposure, long term restrictions on land use, disruption of normal life, damage to the installation and other property, and loss of production. These, collectively, may be referred to as societal risk.

A3. The aim of the specification of safety objectives is to reduce the risks associated with nuclear installations to levels considered tolerable by the appropriate national bodies, in the light of international practice. Thus, the risks to be addressed in the safety analysis of a specific nuclear installation and the safety objectives to be achieved need to be specified or endorsed in a national context. One of the purposes of the safety analysis is to demonstrate that the specified safety objectives have been met.

A4. Present international practice implies that risks from nuclear installations ought to contribute only a small increment to the risk to which people are subject owing to other comparable industrial activities. This applies to risks from exposures relating to operational states as well as risks relating to potential exposures should an accident occur.

A5. The seriousness of the consequences of a nuclear accident is to a large extent dependent on the magnitude and content of the accidental radioactive release, often referred to as the source term. This is true whether the consequences considered are individual health risks or other types of harm, such as restrictions on land usage. Increments in individual health risks can, however, be substantially influenced by

intervention measures after an accident has occurred, such as evacuation and restrictions on food and water.

A6. As stated in para. A3, the attainment of the safety objectives for a particular nuclear installation is demonstrated by means of a safety analysis. Ideally, this safety analysis should include all events, sequences and processes where failures or combinations of failures could potentially have radiological consequences. In practical applications, it is not possible or necessary to achieve this degree of completeness. Whether the safety analysis is carried out by probabilistic methods or by the conventional methods of detailed engineering analyses (deterministic methods) it will, of necessity, be based on a selected set of scenarios (combinations of events, sequences and processes). The selection must be made in such a way that the major contributors to risk are covered as far as is reasonably achievable. Safety analysis, i.e. the demonstration that the types of risks to be considered have been reduced to tolerable levels, as discussed in para. A3, should be performed using proven methods and with appropriate peer review.

A7. The deterministic methods for safety analysis start by specifying scenarios in terms of initiating events and the component failures that are assumed to occur. The scenarios are specified to include even remotely likely events, and acceptance criteria (including safety margins) are specified in such a way that the end result will meet the national safety objectives.

A8. A probabilistic safety analysis (PSA) starts by defining the detrimental end effects for which probability estimates are sought. Such detrimental effects may, for example, be specified as potential damage states or potential source terms characterizing different types of radioactive releases in the event of an accident. The next step is to identify relevant initiating events. For each initiating event, potential event sequences are mapped, modelling potential paths to the detrimental end effect. A systematic evaluation of the event sequences is made, usually by computer. The end result will typically be an estimate of the overall probability of occurrence of the chosen detrimental end effect, and the identification of the initiating events and sequences that dominate for this outcome.

A9. Risk reduction targets may be specified as estimated probabilities for defined detrimental effects, such as installation damage, radioactive release or health effects on the public. For example, in INSAG-3[5] the following targets are given:

> "The target for existing nuclear power plants consistent with the technical safety objective is a likelihood of occurrence of severe core damage that is

---

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

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."

These INSAG targets may be interpreted as what may be reasonably achievable with existing technology and practices.

A10. Both the deterministic and the probabilistic methods have inherent strengths and weaknesses. Demonstration of a high level of safety in a complex industrial activity, such as nuclear power production, requires careful application of both methods as appropriate, and recognition of the strengths and weaknesses of each method.

CONTRIBUTORS TO DRAFTING AND REVIEW

Consultants Meetings

Vienna, Austria: 27–29 August 1990, 25–27 February 1991, 9–11 March 1992

Fischer, J.	International Atomic Energy Agency
Giuliani, P. *(first meeting only)*	Ente per le Nuove Tecnologie, l'Energia e l'Ambiente, Italy
Harrison, J. *(first meeting only)*	Central Electricity Generating Board, United Kingdom
Heltemes, C.J., Jr. *(third meeting only)*	Nuclear Regulatory Commission, United States of America
Högberg, L.	Swedish Nuclear Power Inspectorate, Sweden
Karbassioun, A.	International Atomic Energy Agency
Reed, J.	Nuclear Installations Inspectorate, United Kingdom
Versteeg, J.	Ministry of Social Affairs and Employment, Netherlands

Nuclear Safety Standards Advisory Group Meetings

8–10 April 1991, 20–22 May 1992

Addison, P.	International Atomic Energy Agency
Barber, P.	Ministère de l'industrie, France
Brooks, G.	Atomic Energy of Canada Ltd, Canada
Bystedt, P.	Swedish Nuclear Power Inspectorate, Sweden
Delgado, J.L.	Comisión Nacional de Seguridad Nucleár y Salvaguardias, Mexico
Gast, K.	Federal Ministry for the Environment, Nature Protection and Nuclear Safety, Germany
Harbison, A.S.	Nuclear Installations Inspectorate, United Kingdom

Heltemes, C.J., Jr.	Nuclear Regulatory Commission, United States of America
Herttrich, M.	Gesellschaft für Reaktorsicherheit, Germany
Isaev, A.	I.V. Kurchatov Institute of Atomic Energy, Russian Federation
Ishikawa, M.	University of Hokkaido, Japan
Karbassioun, A.	International Atomic Energy Agency
Kee, S.H.	Institute of Nuclear Safety, Republic of Korea
Klonk, H.	Bundesamt für Strahlenschutz, Germany
Kovalevich, O.M.	Gosatomgonadzor, Russian Federation
Křiž, Z.	Atomic Energy Commission, Czechoslovakia
Lei, Y.	National Nuclear Safety Administration, China
López-Menchero, M.E.	Commission of the European Communities, Brussels
Medina, M.	Comisión Nacional de Seguridad Nucleár y Salvaguardias, Mexico
Mucskai, G.	National Atomic Energy Commission, Hungary
Pelé, J.P.	Commission of the European Communities, Brussels
Reed, J.	Nuclear Installations Inspectorate, United Kingdom
Ryder, E.	Nuclear Installations Inspectorate, United Kingdom
Sarma, M.S.R.	Atomic Energy Regulatory Board, India
Scherrer, J.	Direction de la Sureté des installations nucléaires, France
Szönyi, Z.	National Atomic Energy Commission, Hungary
Versteeg, J.	Ministry of Social Affairs and Employment, Netherlands
Yamamoto, K.	Nuclear Safety Bureau, Japan

HOW TO ORDER IAEA PUBLICATIONS

An exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, has been appointed for the following countries:

CANADA UNITED STATES OF AMERICA	UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA

In the following countries IAEA publications may be purchased from the sales agents or booksellers listed or through major local booksellers. Payment can be made in local currency or with UNESCO coupons.

ARGENTINA	Comisión Nacional de Energía Atómica, Avenida del Libertador 8250, RA-1429 Buenos Aires
AUSTRALIA	Hunter Publications, 58 A Gipps Street, Collingwood, Victoria 3066
BELGIUM	Service Courrier UNESCO, 202, Avenue du Roi, B-1060 Brussels
CHILE	Comisión Chilena de Energía Nuclear, Venta de Publicaciones, Amunategui 95, Casilla 188-D, Santiago
CHINA	IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing IAEA Publications other than in Chinese: China National Publications Import & Export Corporation, Deutsche Abteilung, P.O. Box 88, Beijing
FRANCE	Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05
HUNGARY	Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
INDIA	Oxford Book and Stationery Co., 17, Park Street, Calcutta-700 016 Oxford Book and Stationery Co., Scindia House, New Delhi-110 001
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
PAKISTAN	Mirza Book Agency, 65, Shahrah Quaid-e-Azam, P.O. Box 729, Lahore 3
POLAND	Ars Polona, Foreign Trade Enterprise, Krakowskie Przedmieście 7, PL-00-068 Warsaw
ROMANIA	Ilexim, P.O. Box 136-137, Bucharest
RUSSIAN FEDERATION	Mezhdunarodnaya Kniga, Sovinkniga-EA, Dimitrova 39, SU-113 095 Moscow
SLOVAK REPUBLIC	Alfa, Publishers, Hurbanovo námestie 3, 815 89 Bratislava
SOUTH AFRICA	Van Schaik Bookstore (Pty) Ltd, P.O. Box 724, Pretoria 0001
SPAIN	Díaz de Santos, Lagasca 95, E-28006 Madrid Díaz de Santos, Balmes 417, E-08022 Barcelona
SWEDEN	AB Fritzes Kungl. Hovbokhandel, Fredsgatan 2, P.O. Box 16356, S-103 27 Stockholm
UNITED KINGDOM	HMSO, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR
YUGOSLAVIA	Jugoslovenska Knjiga, Terazije 27, P.O. Box 36, YU-11001 Belgrade

Orders from countries where sales agents have not yet been appointed and requests for information should be addressed directly to:

Division of Publications
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria