IAEA
SAFETY
STANDARDS
SERIES

Safety Assessment and Verification for Nuclear Power Plants

SAFETY GUIDE

No. NS-G-1.2

INTERNATIONAL
ATOMIC ENERGY AGENCY
VIENNA

SAFETY ASSESSMENT AND VERIFICATION FOR NUCLEAR POWER PLANTS

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

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

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

Printed by the IAEA in Austria
November 2001
STI/PUB/1112

SAFETY STANDARDS SERIES No. NS-G-1.2

SAFETY ASSESSMENT AND VERIFICATION FOR NUCLEAR POWER PLANTS

SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2001

VIC Library Cataloguing in Publication Data

Safety assessment and verification for nuclear power plants : safety guide. —
Vienna : International Atomic Energy Agency, 2001.
p. ; 24 cm. — (Safety standards series, ISSN 1020–525X ; no. NS-G-1.2)
STI/PUB/1112
ISBN 92–0–101601–8
Includes bibliographical references.

1. Nuclear power plants — Risk assessment. 2. Nuclear power plants — Safety measures. I. International Atomic Energy Agency. II. Series.

VICL 01–00267

FOREWORD

by Mohamed ElBaradei
Director General

One of the statutory functions of the IAEA is to establish or adopt standards of safety for the protection of health, life and property in the development and application of nuclear energy for peaceful purposes, and to provide for the application of these standards to its own operations as well as to assisted operations and, at the request of the parties, to operations under any bilateral or multilateral arrangement, or, at the request of a State, to any of that State's activities in the field of nuclear energy.

The following bodies oversee the development of safety standards: the Commission for Safety Standards (CSS); the Nuclear Safety Standards Committee (NUSSC); the Radiation Safety Standards Committee (RASSC); the Transport Safety Standards Committee (TRANSSC); and the Waste Safety Standards Committee (WASSC). Member States are widely represented on these committees.

In order to ensure the broadest international consensus, safety standards are also submitted to all Member States for comment before approval by the IAEA Board of Governors (for Safety Fundamentals and Safety Requirements) or, on behalf of the Director General, by the Publications Committee (for Safety Guides).

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA. Any State wishing to enter into an agreement with the IAEA for its assistance in connection with the siting, design, construction, commissioning, operation or decommissioning of a nuclear facility or any other activities will be required to follow those parts of the safety standards that pertain to the activities to be covered by the agreement. However, it should be recalled that the final decisions and legal responsibilities in any licensing procedures rest with the States.

Although the safety standards establish an essential basis for safety, the incorporation of more detailed requirements, in accordance with national practice, may also be necessary. Moreover, there will generally be special aspects that need to be assessed on a case by case basis.

The physical protection of fissile and radioactive materials and of nuclear power plants as a whole is mentioned where appropriate but is not treated in detail; obligations of States in this respect should be addressed on the basis of the relevant instruments and publications developed under the auspices of the IAEA. Non-radiological aspects of industrial safety and environmental protection are also not explicitly considered; it is recognized that States should fulfil their international undertakings and obligations in relation to these.

The requirements and recommendations set forth in the IAEA safety standards might not be fully satisfied by some facilities built to earlier standards. Decisions on the way in which the safety standards are applied to such facilities will be taken by individual States.

The attention of States is drawn to the fact that the safety standards of the IAEA, while not legally binding, are developed with the aim of ensuring that the peaceful uses of nuclear energy and of radioactive materials are undertaken in a manner that enables States to meet their obligations under generally accepted principles of international law and rules such as those relating to environmental protection. According to one such general principle, the territory of a State must not be used in such a way as to cause damage in another State. States thus have an obligation of diligence and standard of care.

Civil nuclear activities conducted within the jurisdiction of States are, as any other activities, subject to obligations to which States may subscribe under international conventions, in addition to generally accepted principles of international law. States are expected to adopt within their national legal systems such legislation (including regulations) and other standards and measures as may be necessary to fulfil all of their international obligations effectively.

EDITORIAL NOTE

An appendix, when included, is considered to form an integral part of the standard and to have the same status as the main text. Annexes, footnotes and bibliographies, if included, are used to provide additional information or practical examples that might be helpful to the user.

The safety standards use the form 'shall' in making statements about requirements, responsibilities and obligations. Use of the form 'should' denotes recommendations of a desired option.

The English version of the text is the authoritative version.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. This publication supports the Safety Requirements on the Safety of Nuclear Power Plants: Design [1].

1.2. This Safety Guide was prepared on the basis of a systematic review of all the relevant publications including the Safety Fundamentals [2], Safety of Nuclear Power Plants: Design [1], current and ongoing revisions of other Safety Guides, INSAG reports [3, 4] and other publications that have addressed the safety of nuclear power plants. This Safety Guide also provides guidance for Contracting Parties to the Convention on Nuclear Safety in meeting their obligations under Article 14 on Assessment and Verification of Safety.

OBJECTIVE

1.3. The Safety Requirements publication entitled Safety of Nuclear Power Plants: Design [1] states that a comprehensive safety assessment and an independent verification of the safety assessment shall be carried out before the design is submitted to the regulatory body (see paras 3.10–3.13). This publication provides guidance on how this requirement should be met.

1.4. This Safety Guide provides recommendations to designers for carrying out a safety assessment during the initial design process and design modifications, as well as to the operating organization in carrying out independent verification of the safety assessment of new nuclear power plants with a new or already existing design. The recommendations for performing a safety assessment are suitable also as guidance for the safety review of an existing plant. The objective of reviewing existing plants against current standards and practices is to determine whether there are any deviations which would have an impact on plant safety. The methods and the recommendations of this Safety Guide can also be used by regulatory bodies for the conduct of the regulatory review and assessment. Although most recommendations of this Safety Guide are general and applicable to all types of nuclear reactors, some specific recommendations and examples apply mostly to water cooled reactors.

1.5. Terms such as ‘safety assessment’, ‘safety analysis’ and ‘independent verification’ are used differently in different countries. The way that these terms have been

used in this Safety Guide is explained in Section 2. The term 'design' as used here includes the specifications for the safe operation and management of the plant.

SCOPE

1.6. This Safety Guide identifies the key recommendations for carrying out the safety assessment and the independent verification. It provides detailed guidance in support of Ref. [1], particularly in the area of safety analysis. However, this does not include all the technical details which are available and reference is made to other IAEA publications on specific design issues and safety analysis methods.

1.7. Specific deterministic or probabilistic safety targets or radiological limits can vary in different countries and are the responsibility of the regulatory body. This Safety Guide provides some references to targets and limits established by international organizations. Operators, and sometimes designers, may also set their own safety targets which may be more stringent than those set by the regulator or may address different aspects of safety. In some countries operators are expected to do this as part of their 'ownership' of the entire safety case.

1.8. This Safety Guide does not include specific recommendations for the safety assessment of those plant systems for which dedicated Safety Guides exist.

STRUCTURE

1.9. Section 2 defines the terms 'safety assessment', 'safety analysis' and 'independent verification' and outlines their relationship. Section 3 gives the key recommendations for the safety assessment of the principal and plant design requirements. Section 4 gives the key recommendations for safety analysis. It describes the identification of postulated initiating events (PIEs), which are used throughout the safety assessment including the safety analysis, the deterministic transient analysis and severe accident analysis, and the probabilistic safety analysis. Section 5 gives the key recommendations for the independent verification of the safety of the plant.

2. SAFETY ASSESSMENT, SAFETY ANALYSIS AND INDEPENDENT VERIFICATION

SAFETY ASSESSMENT AND SAFETY ANALYSIS

2.1. In this context, safety assessment is the systematic process that is carried out throughout the design process to ensure that all the relevant safety requirements are met by the proposed (or actual) design of the plant. This would include also the requirements set by the operating organization and the regulators. Safety assessment includes, but is not limited to, the formal safety analysis (see Section 4). The design and the safety assessment are part of the same iterative process conducted by the plant designer which continues until a design solution which meets all the safety requirements, which may also include those developed during the course of the design, has been reached.

2.2. The scope of the safety assessment is to check that the design meets the requirements for management of safety, the principal technical requirements, the plant design and plant system design requirements given in Sections 3–6 of Safety of Nuclear Power Plants: Design [1], and that a comprehensive safety analysis has been carried out.

2.3. The requirements for management of safety (Section 3 in Ref. [1]) address the issues which relate to proven engineering practice, operating experience and safety research.

2.4. The principal technical requirements (Section 4 in Ref. [1]) include those which ensure that sufficient defence in depth has been provided and that the highest consideration is given to accident prevention and radiation protection.

2.5. The plant design requirements (Section 5 in Ref. [1]) relate to issues such as equipment qualification, ageing and the reliability of safety systems through the provision of redundancy, diversity and physical separation.

2.6. The plant system design requirements (Section 6 in Ref. [1]) address the issues which relate to the design of the reactor core, the reactor coolant system and the safety systems such as containment and emergency core cooling systems.

2.7. Regarding safety analysis, para. 5.69 in Ref. [1] states that “A safety analysis of the plant design shall be conducted in which methods of both deterministic and probabilistic analysis shall be applied. On the basis of this analysis, the design basis for

items important to safety shall be established and confirmed. It shall also be demonstrated that the plant as designed is capable of meeting any prescribed limits for radioactive releases and acceptable limits for potential radiation doses for each category of plant states, and that defence in depth has been effected." The scope and objectives of the deterministic and probabilistic safety analyses are outlined in paras 4.17–4.22 below.

INDEPENDENT VERIFICATION

2.8. Paragraph 3.13 in Ref. [1] states that "The operating organization shall ensure that an independent verification of the safety assessment is performed by individuals or groups separate from those carrying out the design, before the design is submitted to the regulatory body."

2.9. The independent verification should be carried out under the responsibility of the operating organization by a team of experts who are, as far as possible, independent of the designers and those performing the safety assessment. Personnel are considered independent if they have not participated in any part of the design and safety assessment. This independent verification is in addition to the quality assurance (QA) reviews carried out within the design organization.

2.10. Whereas the safety assessment is a comprehensive study carried out by the designers throughout the design process to address all relevant safety requirements, the independent verification would be carried out by or on behalf of the operating organization and may only relate to the design as delivered to the regulatory body for approval.

2.11. Owing to the complexity of the design and safety assessment issues that need to be addressed by the independent verification, this would typically be partly carried out in parallel with the design process rather than left to the end.

2.12. A separate independent review would be carried out by the regulators to check that the design meets their requirements.

RELATIONSHIP BETWEEN THE DESIGN, SAFETY ASSESSMENT AND INDEPENDENT VERIFICATION

2.13. Figure 1 shows the relationship between the safety assessment, independent verification, safety analysis and the other activities carried out during the design of a

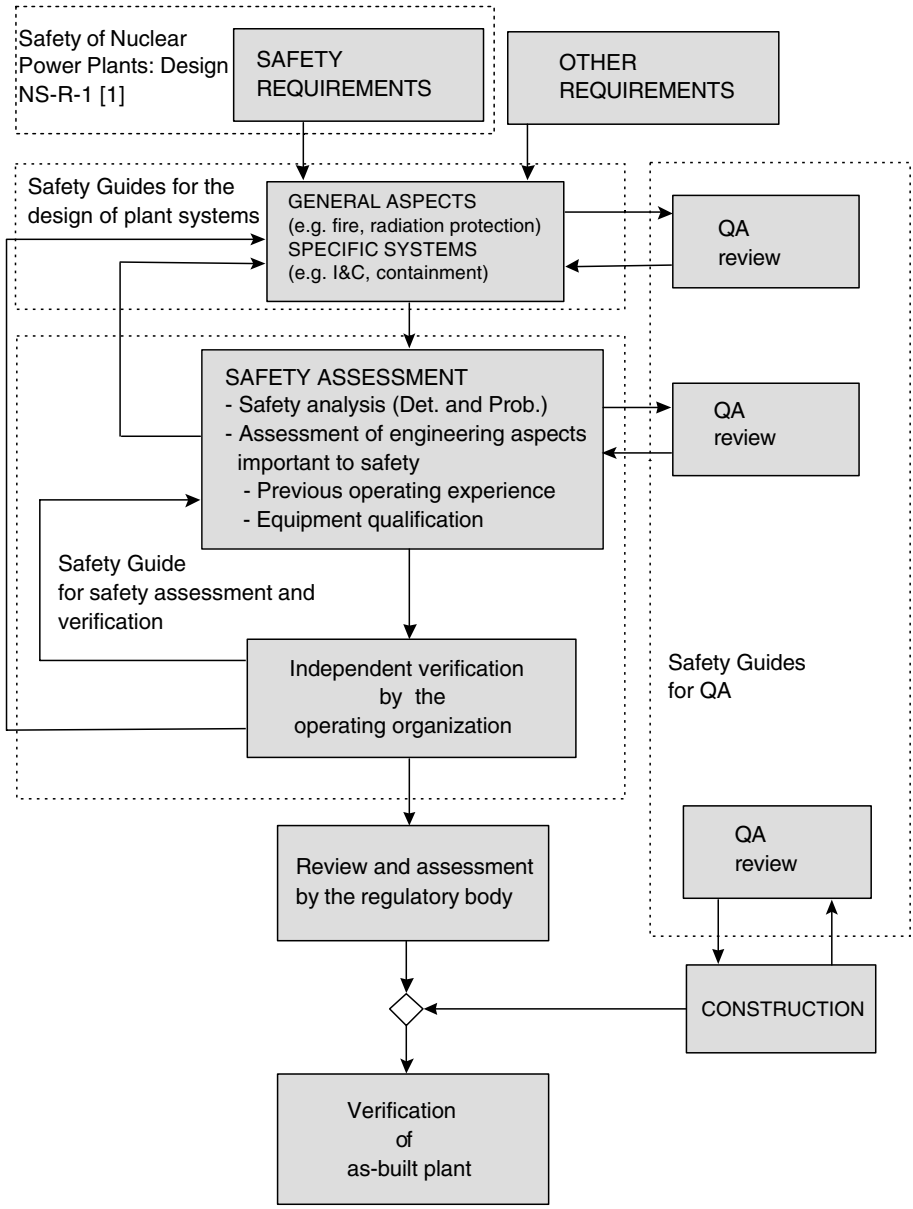

FIG. 1. Areas covered by the IAEA safety standards for the design of nuclear power plants [1] (Det.: deterministic; Prob.: probabilistic).

nuclear power plant. This figure also shows how the present Safety Guide relates to other IAEA publications relevant to the design process.

2.14. As the design is developed from a preliminary concept through to a complete design, the designer needs to take into account all the safety and other requirements defined by both the plant operator and the regulator. For developing nuclear programmes and the introduction of new designs, the design requirements may be revised or clarified during the design process. In the case of novel designs, detailed requirements may be developed while the design is in progress.

2.15. Throughout the design process, the safety assessment and independent verification are carried out by different groups or organizations. However, they are integral parts of an iterative design process and both have the main objective of ensuring that the plant meets the safety requirements. For this reason, both topics are addressed in the same Safety Guide. In some cases, the regulatory body is also involved during the design phase.

2.16. At various stages during the course of the design process (for example, before the start of construction or operation at power) the status of the design will be frozen and a safety analysis report will be produced that will describe the design and safety assessment that has been carried out up to that point. This provides input for the review and assessment of the regulatory body.

2.17. The independent verification is more effective if it is carried out in parallel with the design and safety assessment since early discussion and clarification of safety issues speeds up and facilitates their resolution. Any recommendations made to improve the design or safety assessment are most easily accommodated while the design work is still in progress. On the other hand, too close a relation will call into question the independence of the verification and a balance should be struck between effectiveness and independence.

2.18. Major design decisions to be taken in the course of the design may require special independent design reviews by the operating organization which are limited to the scope of the decision to be taken, and which may consider compliance with the safety requirements applicable to the matter to be decided.

2.19. The design work should be performed according to a QA programme which includes independent reviews of all design documents. The general QA process is addressed in Safety Guide SG-Q-10 [5].

3. ENGINEERING ASPECTS IMPORTANT TO SAFETY

GENERAL

3.1. This section includes recommendations and important considerations for assessing the compliance of the design with the requirements of Sections 3–5 of Ref. [1]. These requirements cover general engineering aspects important to safety and apply to all systems of the nuclear plant. While the assessment of the correct implementation of the requirements for such aspects may not be explicitly addressed in the safety analysis, it constitutes a relevant part of the safety assessment. For some of these aspects, no well-defined acceptance criteria are available and therefore the assessment of the compliance with the safety requirements is largely based on good engineering judgement.

PROVEN ENGINEERING PRACTICES AND OPERATIONAL EXPERIENCE

3.2. For reactors of an evolutionary type, wherever possible, the design should use structures, systems and components (SSCs) with previous successful applications in operating plants, or at least take due account of relevant operational experience which has been gained at other plants.

3.3. Available operating experience should be taken into account in the safety assessment with the aim of ensuring that all relevant lessons in the area of safety have been adequately considered in the design. Operating experience should be a fundamental source of information to improve the defence in depth of the plant.

3.4. The operational experience feedback on design and safety assessment should make full use of the large amount of operating information which is, in most part, openly available to interested organizations and individuals. The data on operating experience should be drawn from: (i) the national data bank; (ii) the incident reporting systems of the World Association of Nuclear Operators (WANO) and the IAEA–OECD Nuclear Energy Agency (OECD NEA); and (iii) the reports of IAEA ASSET (Assessment of Safety Significant Events Team) missions.

3.5. Extrapolative analysis from a real event sequence to what might ultimately have happened in a plant if there had been additional malfunctions (compared with the malfunctions which happened in the real situation) has been demonstrated to be a useful design tool.

3.6. The results of general safety research programmes may also provide useful support to designers and reviewers in their evaluation tasks. The results of safety research are generally available in open meetings, the literature and computer databases. The IAEA generic safety issues databases and IAEA technical documents (IAEA-TECDOCs) are examples of international results in the area of safety research.

INNOVATIVE DESIGN FEATURES

3.7. Based on lessons learned from operating experience, safety analysis and safety research, it is necessary to allow for consideration of the need for and value of design improvements beyond established practice. Where an innovative or non-proven design or design feature is introduced, compliance with the safety requirements should be demonstrated by an appropriate supporting demonstration programme and the features should be adequately tested before being put into service.

3.8. For example, passive safety systems are independent from external support systems such as electric power and have the potential for being simpler and more reliable than active systems. However, the actual performance and reliability of passive systems should be convincingly proven by appropriate and thorough development, testing and analysis programmes.

3.9. Another example of application of modern technology is the use of computer based safety and control systems. Computerized systems have potential advantages compared to classical hard wired systems, including greater functionality, better capability for testing and higher reliability of the hardware. These advantages, however, may have been gained in some embodiments at the expense of simplicity and transparency, and hence extensive assessment and testing should be performed to prove the performance and the overall reliability of the computerized systems, including the software, under conditions as close as possible to the real operating conditions. Further guidance in this area can be found in Ref. [6].

IMPLEMENTATION OF DEFENCE IN DEPTH

3.10. The objective of the defence in depth strategy as indicated in para. 2.10 of Ref. [1] is twofold: first, to prevent accidents and second, if prevention fails, to detect and limit their potential consequences and to prevent any evolution to more serious conditions.

TABLE I. OBJECTIVE OF EACH LEVEL OF PROTECTION AND ESSENTIAL MEANS OF ACHIEVING THEM

Level	Objective	Essential means
Level 1	Prevention of abnormal operation and of 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 emergency 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

3.11. Defence in depth is generally structured in five levels. Should one level fail, it would be compensated for or corrected by the subsequent level. The levels of defence are implemented so as to be independent of the effectiveness of higher and lower levels of defence. The objective of each level of protection and the essential means of achieving them are shown in Table I. Measures on the first three levels of defence should be considered within the design basis in order to ensure maintenance of the structural integrity of the core and to limit potential radiation hazards to members of the public. By contrast, measures on the fourth level of defence should be considered beyond the design basis in order to keep the likelihood and the radioactive releases of severe plant conditions as low as reasonably achievable (ALARA), taking economic and social factors into account.

3.12. The highest priority should be given to the prevention of: undue challenges to the integrity of physical barriers; failure or bypass of a barrier when challenged; failure of a barrier as a consequence of failure of another barrier; and significant releases of radioactive materials.

3.13. The design should be assessed to verify that specific measures are implemented to ensure the effectiveness of defence levels 1 to 4.

3.14. The assessment of the implementation of defence in depth should be achieved through the demonstration of compliance with a large number of requirements supported by the complete safety analysis. This assessment should confirm that possible initiating events are adequately dealt with on the respective defence in depth level by ensuring that the fundamental safety functions are performed and that the release of radioactive materials is controlled.

3.15. The assessment process should pay special attention to internal and external hazards which could have the potential to adversely affect more than one barrier at once or to cause simultaneous failures of redundant equipment of safety systems.

3.16. The design should have provisions to detect the failure or bypass of each level of defence as far as applicable. The requested levels of defence should be specified for each operational mode (for example, an open containment may be allowed in certain shutdown modes, and the specified levels of defence should be available at all times when in that mode).

RADIATION PROTECTION

3.17. Detailed recommendations on design aspects of radiation protection are given in a specific IAEA Safety Guide[1]. The designer should consider these recommendations for the plant design. The subject of the assessment is the demonstration of the compliance with the Radiation Protection Objective as it is stated in the Safety Fundamentals. Some significant aspects of the radiation protection design are discussed below.

3.18. Two design objectives should be considered for normal operation and anticipated operational occurrences: (1) keep the radiation doses below prescribed limits, and (2) keep the radiation doses as low as reasonably achievable. The compliance with the first objective should be demonstrated by comparing the calculated equivalent dose with the prescribed limit specified in the national legislation. The relevant design calculations should be assessed by the designer to ensure the correctness of the input data and the validity of the methodology used (see Section 4).

---

[1] Safety Series No. 50-SG-D9, Design Aspects of Radiation Protection for Nuclear Power Plants (1985).

3.19. The second design objective (meeting the ALARA principle) implies that all doses should be kept as low as reasonably achievable, taking economic and social factors into account. The process of optimization of radiation protection should involve some degree of balancing detriments (costs) and benefits (safety gains). In this optimization process, orientation values for radiation exposures and related design measures could be derived from similar existing plants with good operating records. The safety assessment should take into account the operational experience and consider additional design provisions or improvements to further reduce the radiation exposure to workers and members of the public. Such measures could be either direct (improved shielding) or indirect (reduction of equipment maintenance time).

3.20. The exposures should be kept low through practices such as minimization of cladding defects, use of corrosion resistant materials, reduction of formation of long lived corrosion and activation isotopes, very low primary circuit coolant leakage, minimization of maintenance in high radiation areas and use of remote handling tools and robots.

3.21. Provisions such as sufficient space for inspection and maintenance, adequacy of shielding for radiation protection, and correct installation of plant equipment should be systematically assessed during the design.

3.22. The plant designer and safety assessor should also take into account the operational doses during the final decommissioning. Choice of materials and space for access to dismantle equipment and tools are among the subjects deserving attention, as is the use of 'sacrificial layers' in structures subject to high radiation doses, e.g. concrete shields around the pressure vessel to minimize the amount of highly active waste and to facilitate its removal.

3.23. The design of spaces and equipment such as spent fuel storage and handling facilities, and radioactive waste storage should account for provisions to minimize the release that could result from their failure.

3.24. The designer should show that sufficient design measures have been effected to allow adequate monitoring for radiation protection in accordance with Ref. [1].

3.25. The adequacy of design provisions for protection against accident conditions should be assessed by comparing the releases and the doses calculated in the safety analysis with the limits specified or accepted by the regulatory body. The mitigation of the radiological consequences of beyond design basis accidents may require special actions on the site and around the plant (accident management and emergency