

DS348 Draft 8  
Date:

# **IAEA SAFETY STANDARDS**

**for protecting people and the environment**

**Status: Draft for comments by Member States.**  
**Comments due by 30 November 2007.**

## **Safety Assessment for Facilities and Activities**

**DRAFT SAFETY REQUIREMENT  
DS348**

New Safety Requirement

**IAEA**  
International Atomic Energy Agency

**DRAFT**

**by Mohamed ElBaradei**

**Director General**

**(To be added in the final version)**

**DRAFT**



## CONTENTS

1. INTRODUCTION.....	1
BACKGROUND .....	1
OBJECTIVE .....	1
STRUCTURE .....	3
2. BASIS FOR REQUIRING A SAFETY ASSESSMENT .....	5
3. GRADED APPROACH TO SAFETY ASSESSMENT .....	7
4. SAFETY ASSESSMENT .....	8
OVERALL REQUIREMENTS .....	8
SPECIFIC REQUIREMENTS .....	9
Preparation for the safety assessment .....	10
Assessment of the potential radiation risks.....	12
Assessment of safety functions .....	12
Assessment of site characteristics .....	12
Assessment of the radiological protection provisions.....	13
Assessment of the engineering aspects .....	13
Assessment of human factors.....	14
Assessment of long term safety .....	15
DEFENCE IN DEPTH AND SAFETY MARGINS .....	15
REQUIREMENTS RELATING TO SAFETY ANALYSIS .....	16
Scope of safety analysis .....	16
Approaches to safety analysis .....	17
Criteria for judging safety .....	17
Uncertainty and sensitivity analysis.....	17
Use of computer codes .....	18
Use of data from operating experience .....	18
DOCUMENTATION .....	18
INDEPENDENT VERIFICATION.....	19
5. MANAGEMENT, USE AND MAINTENANCE OF THE SAFETY ASSESSMENT .....	20
REFERENCES.....	21
CONTRIBUTORS TO DRAFTING AND REVIEW .....	23



# 1. INTRODUCTION

## BACKGROUND

1.1. The Fundamental Safety Principles [1] specify principles to ensure the protection of workers, the public and the environment, now and in the future, from harmful effects of ionizing radiation. These principles apply to all situations involving exposure to, or the potential for exposure to, ionizing radiation.

1.2. Safety assessments<sup>1</sup> are to be undertaken as a means of evaluating compliance with these safety requirements (and thereby the application of these principles) for all facilities and activities and to determine the measures that need to be taken to achieve safety. The safety assessment needs to be produced and documented by the organization responsible for operating the facility or conducting the activity, to be independently verified and to be submitted to the regulatory body as part of the licensing process.

## OBJECTIVE

1.3. The objective of this Safety Requirements publication is to establish the generally applicable requirements to be fulfilled in the safety assessment of facilities and activities, with special attention to defence in depth, quantitative analyses and the application of a graded approach to the range of facilities and activities that are addressed. The publication also addresses the independent verification of the safety assessment that needs to be carried out by the producers and users of the safety assessment. It is the intention of this publication to provide a consistent and coherent basis for safety assessment across all facilities and activities. This will promote discussion and transfer of good practices between organizations implementing safety assessments and assist in enhancing public confidence that an adequate level of safety has been achieved for facilities and activities.

1.4. The set of requirements established in this publication will be supported by more detailed guidance on particular aspects of the safety assessment and safety analysis for specific types of facilities and activities. This publication is aimed at achieving a consistent terminology and identifying differences in the requirements for different facilities and activities.

1.5. Implementation of the comprehensive set of requirements established in this publication will ensure that all the safety relevant issues are considered. However, a graded approach must be made to implementation of the requirements to provide flexibility. Hence, although it is anticipated that all the safety requirements are to be complied with, it is recognized that the level of effort applied in carrying out the necessary safety assessment needs to be commensurate with the potential radiation risks and the uncertainties associated with the facility or activity.

---

<sup>1</sup> In general, safety assessment is the assessment of all aspects of a practice that are relevant to protection and safety. For an authorized facility, this includes siting, design and operation of the facility. The safety assessment is the systematic process that is carried out throughout the lifetime of the facility or activity to ensure that all the relevant safety requirements are met by the proposed or actual design. Safety assessment includes, but is not limited to, the formal safety analysis.

## SCOPE

1.6. The requirements derived from the Fundamental Safety Principles [1] relate to any human activity that may cause people to be exposed to radiation risks<sup>2</sup> arising from facilities and activities as follows:<sup>3</sup>

‘Facilities’ includes:

- (a) Enrichment and fuel fabrication facilities;
- (b) Nuclear power plants;
- (c) Other reactors (such as research reactors and critical assemblies);
- (d) Spent fuel reprocessing plants;
- (e) Conversion facilities used to generate UF<sub>6</sub>;
- (f) Radioactive waste management facilities (such as processing, storage and disposal facilities) and any other places where radioactive materials are produced, processed, used, handled, stored or disposed of;
- (g) Irradiation facilities for medical, industrial, research and other purposes, and any places where radiation generators are installed; and
- (h) Facilities where the mining and processing of radioactive ores (such as uranium and thorium) are carried out.

‘Activities’ includes:

- (a) The production, use, import and export of sources of ionizing radiation for industrial, research, medical and other purposes;
- (b) The transport of radioactive material;
- (c) Decommissioning of facilities and the closure of repositories for the disposal of radioactive waste;
- (d) The close-out of facilities where the mining and processing of radioactive ore was carried out;
- (e) Radioactive waste management activities such as the discharge of effluents; and
- (f) The remediation of sites affected by residues from past activities.

---

<sup>2</sup> ‘Radiation risks’ means:

- Detrimental health effects of exposure to radiation (including the likelihood of such effects occurring).
- Any other safety related risks (including those to ecosystems in the environment) that might arise as a direct consequence of:
  - Exposure to radiation;
  - The presence of radioactive material (including radioactive waste) or its release to the environment;
  - A loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation.

<sup>3</sup> The list of facilities and activities given here has been compiled from the lists provided in the Fundamental Safety Principles [1] and the Safety Requirements publication on Legal and Governmental Infrastructure for Nuclear, Radiation, Radioactive Waste and Transport Safety [2].

1.7. Safety assessment plays an important role throughout the lifetime of the facility or activity whenever decisions on safety issues are made by the designers, the operating organization or the regulatory body. The initial development and use of the safety assessment provides the framework for the production of the necessary information to demonstrate compliance with the relevant safety requirements, and for the development and maintenance of the safety assessment over the lifetime of the facility or activity.

1.8. Stages in the lifetime of a facility or activity where the safety assessment is carried out, updated and used by the designers, the operating organization and the regulatory body include:

- (a) Site evaluation for the facility or activity<sup>4</sup>;
- (b) Development of the design;
- (c) Construction of the facility or implementation of the activity;
- (d) Commissioning of the facility or activity;
- (e) Commencement of the operation of the facility or the conduct of the activity;
- (f) Normal operation of the facility (including startup, shutdown and outages);
- (g) Modification of the design or operation;
- (h) Periodic safety reviews;
- (i) Life extension of the facility beyond its original design life;
- (j) Changes in the ownership or management of a facility;
- (k) Decommissioning of a facility;
- (l) Closure of a repository for the disposal of radioactive waste; and
- (m) Remediation of a site and release from regulatory control.

1.9. For many facilities and activities, environmental impact assessments and non-radiological risk assessments will be required before the construction or implementation can commence. The assessment of these aspects will, in general, have many commonalities with the safety assessment that is carried out to address the risks from ionizing radiation. Therefore, these different assessments may be combined to save resources and increase the credibility and acceptability of their results. However, this publication does not establish requirements for such a combined assessment or make recommendations on how to assess non-radiological hazards.

## STRUCTURE

1.10. Section 2 provides the basis for requiring a safety assessment to be carried out, derived from the Fundamental Safety Principles [1]. Section 3 describes the graded approach for the implementation of the requirements for safety assessment for different facilities and activities. Section 4 establishes the overall requirements for a safety assessment and specific requirements that relate to the assessment of features relevant to safety. Section 4 also establishes the requirements to address defence in depth and safety margins, to perform safety analysis, to document the safety assessment and to carry out an independent verification. Section 5 establishes the requirements for the management, use and maintenance of the safety assessment.

---

<sup>4</sup> For transport related activities, the requirements are given in Ref [3].

**DRAFT**

## 2. BASIS FOR REQUIRING A SAFETY ASSESSMENT

2.1. The Fundamental Safety Principles [1] states that “The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation”. This objective applies to all facilities and activities as identified in Section 1, and has to be achieved for all stages in their lifetime without unduly limiting the application of technology.

2.2. The Fundamental Safety Principles also defines ten principles that apply in achieving this fundamental safety objective. This leads, inter alia, to the requirement for a safety assessment to be carried out.

2.3. Principle 3 on leadership and management for safety states that:

“Safety has to be assessed for all facilities and activities, consistent with a graded approach. Safety assessment involves the systematic analysis of normal operation and its effects, of the ways in which failures might occur and of the consequences of such failures. Safety assessments cover the safety measures necessary to control the hazard, and the design and engineered safety features are assessed to demonstrate that they fulfill the safety functions required of them. Where control measures or operator actions are called on to maintain safety, an initial safety assessment has to be carried out to demonstrate that the arrangements made are robust and that they can be relied on. A facility may only be constructed and commissioned or an activity may only be commenced once it has been demonstrated to the satisfaction of the regulatory body that the proposed safety measures are adequate” (para. 3.15, Ref. [1]).

2.4. Principle 3 also states that:

“The process of safety assessment for facilities and activities is repeated in whole or in part as necessary later in the conduct of operations in order to take into account changed circumstances (such as the application of new standards or scientific and technological developments), the feedback of operating experience, modifications and the effects of ageing. For operations that continue over long periods of time, assessments are reviewed and repeated as necessary. Continuation of such operations is subject to these reassessments demonstrating to the satisfaction of the regulatory body that the safety measures remain adequate” (para. 3.16, Ref. [1]).

2.5. Principle 5 on the optimization of protection recognizes the need for a graded approach so that:

“The resources devoted to safety by the licensee, and the scope and stringency of regulations and their application, have to be commensurate with the magnitude of the radiation risks and their amenability to control. Regulatory control may not be needed where this is not warranted by the magnitude of the radiation risks” (para. 3.24, Ref. [1]).

The concept of the graded approach applies to all considerations of safety including the scope and level of detail of the safety assessment required. This is addressed in Section 3.

2.6. The safety assessment also provides input into applying other fundamental principles as follows:

- Principle 4 on the justification of facilities and activities: to identify the risks that must be compensated for by the benefits provided by the facility or activity.
- Principle 5 on the optimization of protection: to determine whether the risks that arise from the facility or activity have been reduced to a level that is as low as reasonably achievable when economic and social factors have been taken into account.

- Principle 6 on the limitation of the risks to individuals: to determine whether the applicable dose and risk limits have been met.
- Principle 7 on the protection of present and future generations: to determine whether adequate protection has been provided for all population groups and the environment now and in the future. A safety assessment will provide input to any necessary environmental impact assessment.
- Principle 8 on accident prevention: to determine whether all practicable efforts have been made to prevent a loss of control that could give rise to a radiation risk.
- Principle 9 on emergency preparedness and response: to identify the full range of foreseeable events for which emergency response arrangements need to be made.
- Principle 10 on the reduction of existing or unregulated risks: to determine the magnitude of these risks and to provide an input into the determination of whether any proposed protective actions are justified.

2.7. Principle 8 on accident prevention also states that the usual approach to ensuring high levels of safety is to apply defence in depth, where a number of levels of protection or physical barriers are provided such that, if one level of protection or barrier were to fail, the subsequent level or barrier would be available. Requirements on the assessment of defence in depth are established in paras 4.45 to 4.48.

### 3. GRADED APPROACH TO SAFETY ASSESSMENT

3.1. Principle 5 of the Fundamental Safety Principles [1] is that the resources devoted to safety are to be commensurate with the magnitude of the potential radiation risks. To apply this principle, a graded approach needs to be taken in carrying out the safety assessments for the wide range of facilities and activities identified in Section 1 owing to the very different levels of potential radiation risks that they pose. This allows flexibility in the way that the radiation risks are assessed and controlled without unduly limiting the operation of facilities or the conduct of activities.

3.2. A graded approach shall be used in determining the scope, extent, level of detail and effort that needs to be devoted to the safety assessment carried out for any particular facility or activity.

3.3. The main factor taken into consideration in the application of a graded approach to the safety assessment shall be the magnitude of the potential radiation risks arising from the facility or activity. This needs to take into account any releases of radioactive material in normal operation, the potential consequences of anticipated operational occurrences and accidents, and the possibility of occurrence of very low probability events with potentially high consequences..

3.4. A graded approach to safety assessment shall also take into account other relevant factors such as the maturity or complexity of the facility or activity. The maturity relates to the use of proven practices and procedures, proven designs, data on operational performance of similar facilities or activities, uncertainties in the performance of the facility or activity, and the availability of experienced manufacturers and constructors. The complexity relates to the extent and difficulty of the effort required to construct a facility or implement an activity, the number of the related processes for which control is necessary, the extent to which radioactive material has to be handled, the longevity of the radioactive material, the reliability and complexity of systems and components and their accessibility for maintenance inspection, testing and repair.

3.5. At the start of the safety assessment, a judgement shall be made on the scope, extent, level of detail and the effort that needs to be applied to the safety assessment for the facility or activity.

3.6. The application of the graded approach shall be reassessed as the safety assessment progresses and a better understanding is obtained of the potential radiation risks arising from the facility or activity. The scope, extent and level of detail of the safety assessment and the effort applied shall be adjusted accordingly.

3.7. A graded approach shall also be applied to the requirements for updating the safety assessment (para 5.10).

## 4. SAFETY ASSESSMENT

### OVERALL REQUIREMENTS

- 4.1. As specified in the Fundamental Safety Principles [1], a safety assessment shall be carried out for all applications of technology that give rise to radiation risks – that is, for the facilities and activities identified in Section 1.
- 4.2. The responsibility for carrying out the safety assessment shall be with the legal person responsible for the facility of activity — generally the person or organization authorized (licensed) to operate the facility or conduct the activity – referred to as the ‘responsible legal person’. The operating organization shall be responsible for the way in which the safety assessment is carried out and for the quality of the results. If the operating organization changes, the responsibility for the safety assessment shall be transferred to the new operating organization.
- 4.3. The primary purpose of a safety assessment shall be to determine whether an adequate level of safety has been achieved for a facility or activity and whether the basic safety objectives and safety criteria established by the designer, the operating organization and the regulatory body, reflecting the radiation protection requirements as established in the Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources [4], have been complied with. This includes the requirements in respect of radiation exposure of workers and the public, and any other requirements to help ensure the safety of facilities and activities.
- 4.4. The safety assessment shall include an assessment of the radiological protection provisions in place to determine whether the radiological risks are being controlled within specified limits and whether they have been reduced to a level that is as low as reasonably achievable. This will also provide an input into applying the other principles as indicated in Section 2.
- 4.5. The safety assessment shall address all the radiation risks that arise from normal operation<sup>5</sup>, anticipated operational occurrences and accident conditions. The safety assessment for anticipated operational occurrences and accident conditions shall also address the way in which failures might occur and the consequences of any such failures.
- 4.6. A safety assessment shall be carried out at the design stage of a new facility or activity as early as possible in the lifetime of an existing facility or activity, and shall be updated as necessary as the facility or activity passes through the stages of its lifetime. Updating of the safety assessment shall take account of possible changes in circumstances (such as the application of new standards or scientific and technological developments), changes in the site characteristics, modifications in the design or operation and the effects of ageing.
- 4.7. The updating of the safety assessment shall also take account of operating experience including data relating to anticipated operational occurrences, accident conditions and accident precursors both from the facility or activity itself and from other similar facilities or activities.
- 4.8. For facilities and activities that continue over long periods of time, the safety assessment shall be updated as necessary. The frequency at which this is done shall be related to radiation risks associated with the facility or activity, and the extent to which changes are made to the facility or activity. Continuation of operation of such facilities and conduct of

---

<sup>5</sup> Normal operation includes all the modes of operation of the facility or activity including commissioning, startup, shutdown, outages, etc.

such activities is subject to the reassessment being able to demonstrate to the satisfaction of the operating organization and the regulatory body that the safety measures in place remain adequate.

4.9. The safety assessment shall identify all the safety measures necessary to control radiation risks. It shall be determined whether the design and engineered safety features fulfil the safety functions required of them. It shall also be determined whether adequate measures have been taken to prevent anticipated operational occurrences or accident conditions and whether the radiation risks would be mitigated should they occur.

4.10. The safety assessment shall address the radiation risks arising from the facility or activity to all the individuals and population groups who might be affected. This shall include the local population and population groups that are geographically remote from the facility or activity giving rise to the radiation risks, including those in other States as appropriate.

4.11. The safety assessment shall address the radiation risks now and in the future. This is particularly important for activities such as the long term management of radioactive waste where the effects could span many generations.

4.12. The safety assessment shall determine whether adequate defence in depth has been provided, as appropriate, through a combination of several layers of protection (i.e. physical barriers, systems to protect the barriers and administrative procedures), that would have to fail or be bypassed before harm could be caused to people or the environment.

4.13. In most cases, the safety assessment includes a safety analysis, which consists of a set of different analyses for quantitatively evaluating and assessing challenges to safety under various operational states, anticipated operational occurrences and accident conditions, using deterministic and probabilistic methods as appropriate. The safety analysis shall be an integral part of the safety assessment.

4.14. The computer codes that are used to carry out the safety analysis shall be verified and validated and this shall form part of the supporting evidence presented in the documentation. As part of the management system, the operating organization and the regulatory body shall seek improvements to the tools and data that are used.

4.15. The results of the safety assessment shall be used to identify appropriate safety related improvements to the design and operation of the facility or conduct of the activity. These results allow assessment of the safety significance of unremedied shortcomings or of planned modifications and may be used to determine their priority. They may also be used to provide the basis for continued operation of the facility or conduct of the activity.

## SPECIFIC REQUIREMENTS

4.16. Figure 1 shows the main elements of the safety assessment and verification process. This requires that a systematic evaluation of all features of the facility or activity relevant to safety is carried out and includes: the preparation for the safety assessment in terms of assembling the expertise, tools and information required to carry out the work; the identification of the potential radiation risks as a result of normal operation, anticipated operational occurrences or accident conditions; the identification and assessment of a comprehensive set of safety functions; the assessment of the site characteristics that relate to the radiological risk; the assessment of the radiological protection provisions; the assessment of the engineering aspects to determine whether the design safety requirements relevant to the facility or activity have been met; the assessment of the human factor aspects of the design and operation; and the assessment of safety in the longer term, which is a particular concern when ageing effects might develop and influence safety margins, the decommissioning of facilities and the closure of repositories for the disposal of radioactive waste. The

requirements associated with the main elements of safety assessment and verification are given in this section.

4.17 All the requirements given in this section shall be considered within the context of the complexity and the potential radiation risks associated with the facility or activity. The safety assessment shall incorporate a graded approach reflecting these considerations as indicated in para. 1.5 and described in Section 3.

#### **Preparation for the safety assessment**

4.18. As the first stage in carrying out the safety assessment, the necessary preparations shall be made to ensure that:

- (a) There are sufficient skilled and expert people available to carry out the work;
- (b) The relevant background information relating to the siting, design and operation of the facility or activity is available along with any other evidence that is required to support the safety assessment;
- (c) The necessary tools for carrying out the safety assessment are available. This includes the computer codes needed for carrying out the safety analysis; and
- (d) The safety criteria defined in national regulations or approved by the regulatory body to be used for judging whether the safety of the facility or activity is adequate have been identified.

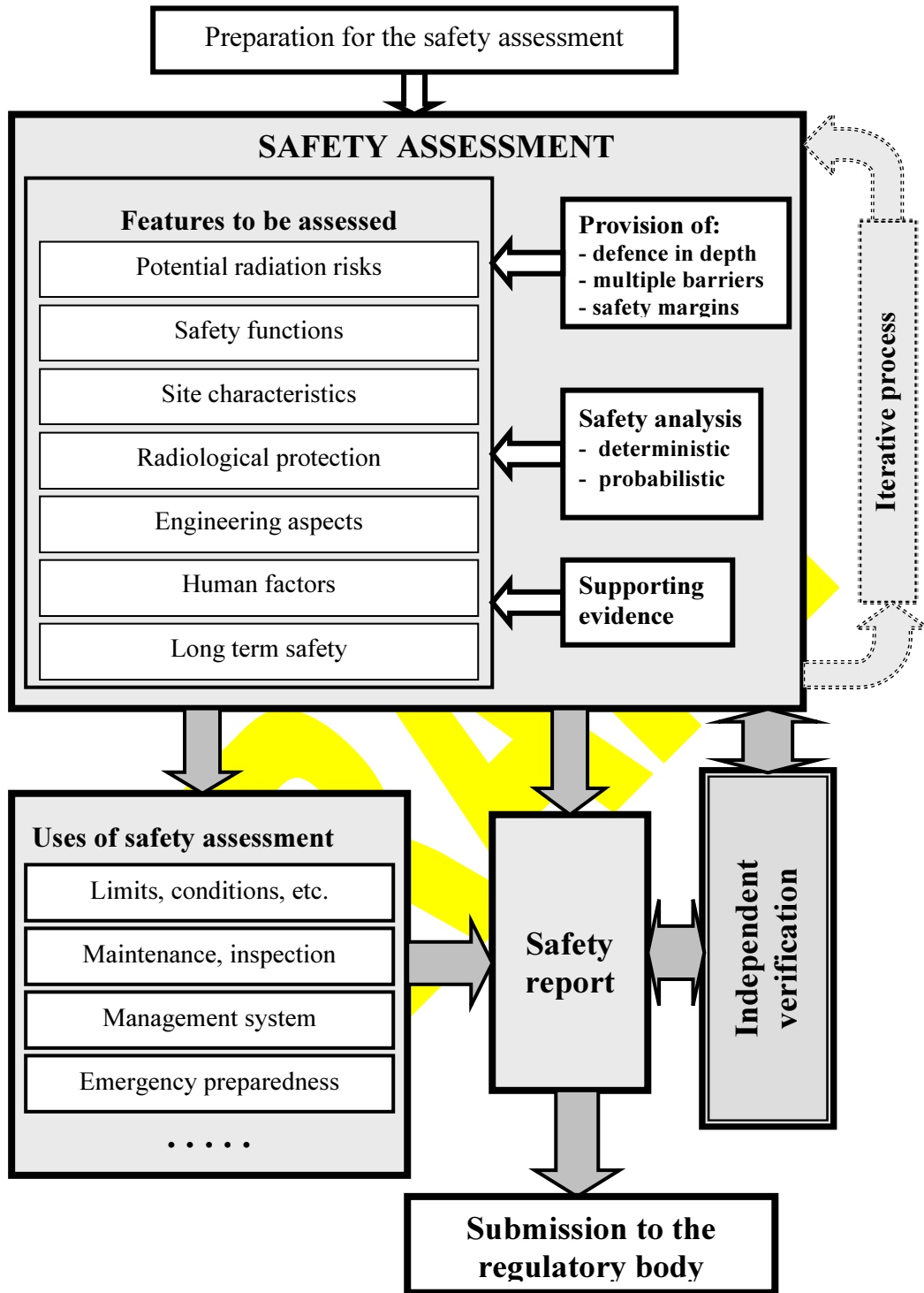


FIG 1: Overview of the safety assessment process<sup>1</sup>

### **Assessment of the potential radiation risks<sup>6</sup>**

4.19. The potential radiation risks associated with the facility or activity shall be identified and assessed. This includes the radiation exposure of workers and the public and the release of radioactive material to the environment associated with anticipated operational occurrences or accidents that lead to a loss of control.

### **Assessment of safety functions**

4.20. All safety functions<sup>7</sup> associated with a facility or activity shall be identified and assessed. This shall include the safety functions associated with the engineered structures, systems and components, any physical or natural barriers and inherent safety features as applicable, and any human actions necessary to ensure the safety of the facility or activity. This is a key aspect of assessment and is vital to the assessment of the application of defence in depth (see paras 4.45 to 4.48). An assessment shall be undertaken to determine whether the safety functions can be achieved for all normal operational modes (including startup and shutdown where appropriate), all anticipated operational occurrences and the accident conditions that need to be taken into account.

4.21. The assessment of the safety functions shall determine whether they will be carried out with an adequate level of reliability consistent with the graded approach (see Section 3). The assessment shall determine whether vulnerabilities that could lead to a single failure or to a common cause failure for engineered equipment are present. The assessment shall determine whether the structures, systems, components or barriers provided to carry out a safety function have adequate levels of redundancy, diversity, separation, segregation, equipment qualification, etc. as appropriate.

### **Assessment of site characteristics**

4.22. An assessment of the site characteristics related to the safety of the facility or activity shall be carried out and shall include:

- (a) The physical and chemical characteristics that will affect the dispersion or migration of radioactive material released in normal operation or due to anticipated operational occurrences or accident conditions;
- (b) The identification of the natural and human induced hazards of the region that have the potential to affect the safety of the facility or activity; and
- (c) The distribution of the population around the site and its characteristics with regard to any siting policy of the State, the potential to affect neighbouring States and the need to develop an emergency plan.

4.23. The scope and level of detail of the site assessment shall be consistent with the potential radiation risks associated with the facility or activity, the type of facility or activity to be carried out and the purpose of the assessment (e.g. to determine whether a new site is suitable for a facility or activity, to evaluate the safety of an existing site or to assess the long

---

<sup>6</sup> The term 'potential radiation risks' relates to the radiological consequences that would occur when no credit is taken for any of the safety systems or protective measures incorporated for the facility or activity.

<sup>7</sup> Safety functions are those design or operational features of the facility or activity that are relied upon to prevent or mitigate the radiological consequences of normal operation, anticipated operational occurrences and accident conditions.

term suitability of a site for waste disposal). The site assessment shall be reviewed periodically during the lifetime of the facility or activity (see para. 5.10).

#### **Assessment of the radiological protection provisions**

4.24. The safety assessment shall determine whether adequate measures are in place for a facility or activity to protect people and the environment from the harmful effects of ionising radiation as required by the fundamental safety objective [1].

4.25. The safety assessment shall determine whether adequate measures are in place to control the radiation exposure of workers and members of the public within any relevant dose limit (as required by Principle 6 [1]) and that the protection is optimized such that the magnitude of individual doses, the number of people exposed and the likelihood of incurring exposures have all been kept as low as reasonably achievable, economic and social factors being taken into account (see Principle 5 [1]).

4.26. The safety assessment of the radiological protection provisions shall address normal operation of the facility or activity, anticipated operational occurrences and accident conditions.

#### **Assessment of the engineering aspects**

4.27. The safety assessment shall determine whether a facility or activity uses, to the extent reasonable, structures, systems and components of robust and proven design. Relevant operational experience, including results of root cause analysis of anticipated operational occurrences and accidents where appropriate, shall be taken into account.

4.28. The safety assessment shall identify the design principles that have been applied to the facility and shall determine whether these principles have been met. The design principles applied would depend on the type of facility but could include requirements to incorporate application of defence in depth, multiple barriers to the release of radioactive material, safety margins, and the provision of redundancy, diversity and equipment qualification in the design of safety systems.

4.29. Where innovative improvements beyond current practices have been incorporated in the design, the safety assessment shall determine whether compliance with the safety requirements has been demonstrated by an appropriate programme of research, analysis and testing complemented by a subsequent programme of monitoring during operation.

4.30. The safety assessment shall determine whether a suitable safety classification scheme has been formulated and applied to the structures, systems and components. It shall determine whether it adequately reflects their importance to safety, the severity of the consequences of their failure, the need for them to be available following anticipated operational occurrences and accident conditions, and the need for them to be adequately qualified. The safety assessment shall also determine whether the scheme identifies the appropriate industry codes and standards and the regulatory requirements that need to be applied in the design, manufacturing, construction and inspection of the engineered features or for the development of procedures and in the management system of the facility or activity.

4.31. The safety assessment shall address the external hazards that could arise for a facility or activity, and shall determine whether an adequate level of protection is provided. This could include natural external events (such as extreme weather conditions, earthquakes and external flooding) and human induced events (such as aircraft crashes and hazards arising from transport and industrial activities) depending on the radiation risks associated with the facility or activity. Where applicable, the magnitude of the external events that the facility must be able to withstand (sometimes referred to as design basis external events) shall be

established for each of the external hazards on the basis of historical data for a site. Where there is more than one facility or activity at the same location, the safety assessment shall take account of the effect of a single external event such as an earthquake or a flood on all of them and of the hazard potential presented by each facility or activity to the others.

4.32. The safety assessment shall address the internal hazards that could arise for a facility and shall demonstrate whether the structures, systems and components are able to perform their safety function under the loads induced by normal operation, anticipated operational occurrences and accident conditions that have been taken into account explicitly in the design of the facility. This could include consideration of specific loads and load combinations, and environmental conditions (of temperature, pressure, humidity and radiation) imposed on structures and components by internal events such as pipe breaks, impingement forces, internal flooding and spraying, internal missiles, load drop, internal explosions and fire, depending on the radiation risks associated with the facility or activity.

4.33. The safety assessment shall determine whether the materials used are suitable for their purpose with regard to the standards specified in the design and for the operational conditions that arise during normal operation and following anticipated operational occurrences or accidents that have been taken into account explicitly in the design of the facility or activity.

4.34. The safety assessment shall determine whether preference has been given to a fail-safe design or, if this is not practicable, whether a means of detecting the failures that have occurred has been incorporated wherever appropriate.

4.35. The safety assessment shall determine whether any time related aspects such as ageing, wear-out or life limiting factors, such as cumulative fatigue, embrittlement, corrosion, chemical decomposition and radiation induced damage, have been adequately addressed.

4.36. The safety assessment shall determine whether the equipment essential to safety has been qualified to a sufficiently high level so that it will be able to perform its safety function in the conditions that it would experience in normal operation and following the anticipated operational occurrences and accidents that have been taken into account in the design.

4.37. The provisions made for the decommissioning of a facility or the closure of a repository for the disposal of radioactive waste shall be specified and the safety assessment shall determine whether they are adequate.

#### **Assessment of human factors**

4.38. The safety of facilities or activities will rely on actions carried out by operators. The safety assessment shall address all the human interactions with the facility or activity and shall determine whether the procedures and measures that are provided for all normal operational activities, in particular those necessary for implementation of the identified operational limits and conditions, and those required in response to anticipated operational occurrences and to accidents, ensure an adequate level of safety.

4.39. The safety assessment shall determine whether personnel competences, associated training and minimum staffing levels for maintaining safety are adequate.

4.40. The safety assessment shall determine whether the design and operation of the facility and the procedures for activities have addressed the requirements for human factors, including those related to the ergonomic design of all the areas, human-machine interfaces where operator actions are carried out, and future decommissioning and closure activities.

4.41. For existing facilities and activities, the safety assessments shall include aspects of safety culture where appropriate.

## Assessment of long term safety<sup>8</sup>

4.42. The safety assessment shall address the long term aspects of the safety of facilities and activities to ensure that the applicable regulations will continue to be met.

4.43. In the case of a repository for the disposal of significant quantities of radioactive waste, the radiation risks shall be considered for the post-closure phase. Radiation risks following closure of the repository may arise from gradual processes such as the degradation of barriers, and from discrete events that could affect waste isolation such as inadvertent human intrusion or abrupt changes in geological conditions.

4.44. In view of the uncertainties inherent in predicting events, according to the Safety Requirements publication on the Geological Disposal of Radioactive Waste [5], reasonable assurance of compliance with the safety requirements relating to long term hazards shall be achieved by the use of multiple lines of reasoning. This shall be achieved by supplementing the quantitative estimates of repository performance with qualitative evidence that the repository will provide isolation of the wastes as designed.

### DEFENCE IN DEPTH AND SAFETY MARGINS

4.45. The assessment of defence in depth shall determine whether adequate provisions have been made at each of the levels of defence in order to ensure that the system can:

- (a) Address deviations from normal operation and, in the case of a repository, from its desirable long term evolution;
- (b) Detect and intercept safety related deviations from normal operation and the desirable long term evolution should they occur;
- (c) Control accidents within the limits established for the design;
- (d) Identify measures to mitigate the consequences of accidents that exceed design limits; and
- (e) Mitigate the radiation risks of possible radioactive releases.

4.46. The safety assessment shall identify the necessary layers of protection including physical barriers to confine radioactive material at specific locations and the need for supporting administrative controls to achieve defence in depth. This shall include the identification of:

- (a) Safety functions that must be fulfilled;
- (b) Potential challenges to these safety functions;
- (c) Mechanisms giving rise to these challenges and the responses to them;
- (d) Provisions made to prevent these mechanisms from occurring; and
- (e) Provisions to mitigate the consequences if the safety function fails.

4.47. In order to determine whether defence in depth has been adequately implemented, the safety assessment shall determine whether:

- (a) The priority has been given to: reducing the number of challenges to the integrity of layers of protection and physical barriers; preventing the failure or bypass of a barrier when challenged; preventing the failure of one barrier leading to the failure of another

---

<sup>8</sup> In this context, 'long term' relates to the post-closure phase of a repository for the disposal of significant quantities of radioactive material.

one; and preventing significant releases of radioactive material if failure of the barriers does occur;

- (b) The layers of protection and physical barriers are independent of each other as far as practicable;
- (c) Special attention has been paid to internal and external hazards that have the potential to adversely affect more than one barrier at once or to cause simultaneous failures of safety systems; and
- (d) Specific measures have been implemented to ensure the reliability and effectiveness of the required levels of defence.

4.48. The safety assessment shall determine whether there are adequate safety margins in the design and operation of the facility or activity in normal operation and under anticipated operational occurrences or accident conditions so that there is a wide margin to failure of any structures, systems or components for any of the anticipated operational occurrences or accident conditions that could occur. Safety margins are typically specified in codes and standards as well as by the regulatory body. The safety assessment shall determine whether acceptance criteria for each aspect of the safety analysis are such that an adequate margin is ensured.

## REQUIREMENTS RELATING TO SAFETY ANALYSIS

### **Scope of safety analysis<sup>9</sup>**

4.49. The safety analysis shall assess the performance of a facility or activity in all operational states and, as necessary, in the post-operational phase and shall determine whether there is compliance with the safety requirements and regulatory requirements.

4.50. The safety analysis shall address both the consequences arising from all normal operational conditions (including startup and shutdown where appropriate) and the frequencies and consequences associated with all anticipated operational occurrences and accident conditions. The degree of detail of the analysis shall depend on the magnitude of the radiation risks associated with the facility or activity, the frequency of the events included in the analysis, the complexity of the facility or activity and the uncertainties inherent in the processes that are included in the analysis.

4.51. The safety analysis shall identify the anticipated operational occurrences and accident conditions that challenge safety. This needs to include all internal and external events and processes that may impact on physical barriers to confine the radioactive material or otherwise give rise to radiation risks.<sup>10</sup> The selection of events and processes to be considered in the safety analysis shall be based on a systematic, logical and structured approach and shall provide justification that the identification of all scenarios relevant for safety is sufficiently comprehensive.<sup>11</sup> The analysis shall be based on an appropriate grouping and bounding of the events and processes and shall consider partial failures of components or barriers as well as complete failures.

---

<sup>9</sup> Safety analysis is the subset of the safety assessment that is aimed at the quantification of any aspect of the safety of the facility or activity.

<sup>10</sup> It should be noted that different terms are used for the internal and external events and processes for different types of facilities and activities. For example, for nuclear reactors, the term used is postulated initiating events (PIEs) whereas for radioactive waste safety, the usual term is features, events and processes (FEPs).

<sup>11</sup> In accordance with the IAEA Safety Glossary [5], the term scenario is used here to describe “a postulated or assumed set of conditions and/or events”.

4.52. The safety analysis shall address the experience of operating the facility or conducting the activity. This shall include consideration of the anticipated operational occurrences and accident conditions that have arisen during operation of the facility or conduct of the activity where the aim will be to determine the cause of the anticipated operational occurrences or accident conditions, their possible effects, their significance and the effectiveness of the proposed corrective action.

### **Approaches to safety analysis**

4.53. The safety analysis shall incorporate deterministic and probabilistic approaches, as required by the graded approach. These approaches have been shown to complement each other and both shall be used together to provide input into an integrated decision making process.

4.54. The aim of the deterministic approach shall be to define and apply a set of conservative deterministic rules and requirements for the design and operation of facilities or the planning and conduct of activities. If these rules and requirements are met, they are expected to provide a high degree of confidence that the level of radiation risks to workers and members of the public arising from the facility or activity will be acceptably low. This conservative approach provides a way of compensating for uncertainties in the performance of equipment and humans with the aim of providing a large safety margin.

4.55. The aim of a probabilistic safety analysis shall be to determine all significant contributors to the radiation risk from a facility or activity and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria where they have been defined. In the area of reactor safety, the probabilistic safety analysis that is carried out uses a comprehensive, structured approach to identify failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk. The probabilistic approach uses realistic assumptions whenever possible and provides a framework for addressing many of the uncertainties explicitly. Probabilistic approaches may provide insights into system performance, reliability, interactions and weaknesses in the design, defence in depth and risk that it may not be possible to derive from a deterministic approach.

4.56. Improvements in the overall approach to safety analysis have achieved a better integration of deterministic and probabilistic approaches. With increasing quality of models and data it is possible to develop more realistic deterministic analysis and to make use of probabilistic information in selecting accident scenarios. Increasing emphasis is also being given to probabilistically specifying how compliance with the deterministic safety criteria is demonstrated, e.g. by specifying confidence intervals, and how safety margins are defined.

### **Criteria for judging safety**

4.57. Criteria for judging safety that are sufficient to meet the fundamental safety objective and the fundamental safety principles established in Ref. [1] and the requirements of the designer, the operating organization and the regulatory body shall be defined for the safety analysis. In addition, detailed criteria may be developed to assist in assessing compliance with these higher level objectives, principles and requirements, including risk criteria that relate to the likelihood of anticipated operational occurrences or accidents occurring with significant radiation risks.

### **Uncertainty and sensitivity analysis**

4.58. The safety analysis incorporates, to varying degrees, predictions of the circumstances that will prevail in the operational or post-operational stages of a facility or activity. There

will always be uncertainties<sup>12</sup> associated with such predictions that depend on the exact nature of the facility or activity and the complexity of the safety analysis. To the extent practicable the results of a safety analysis shall be robust, i.e. tolerant to uncertainties.

4.59. Uncertainties in the safety analysis shall be characterized with respect to their source, nature and degree, using quantitative methods, professional judgment or both. Uncertainties that may have implications for the outcome of the safety analysis and decisions made on that basis shall be addressed in uncertainty and sensitivity analyses. Uncertainty analysis mainly refers to the statistical combination and propagation of uncertainties in data, whereas sensitivity analysis refers to the sensitivity of results to major parameter, scenario or modelling assumptions.

#### **Use of computer codes**

4.60. The computer codes used in the safety analysis shall undergo verification and validation to a sufficient degree. Verification refers to the process of determining whether the controlling physical equations and data have been correctly translated into the computer code. Validation refers to the process of determining whether the mathematical model is an adequate representation of the real system being modelled by comparing the predictions of the model with observations of the real system or experimental data. The validation process shall identify the uncertainties, the approximations in the models, and shortcomings in the models and the underlying data basis and how these are to be taken into account in the safety analysis. In addition, users of the code shall have sufficient experience in the application of the code to the facility or activity being addressed.

#### **Use of data from operating experience**

4.61. If warranted by the potential radiation risks associated with a facility or activity, data on operational safety performance shall be collected and assessed, including records of incidents such as human errors, performance of safety systems, radiation doses, generation of radioactive waste and effluents. The scope of the data collection shall be commensurate with the graded approach. For complex facilities, the collection of data shall be based on a set of safety performance indicators that have been established for the facility. Operational safety experience shall be used, as appropriate, to update the safety assessment and to review the management systems; this is further described in Section 5.

### **DOCUMENTATION**

4.62. The results and findings of the safety assessment shall be documented, as appropriate, in the form of a safety report, reflecting the complexity of the facility or activity and the radiation risks associated with it. The purpose of the safety report is to present the assessment and the analyses that have been carried out to demonstrate that the facility or activity is in compliance with the fundamental safety principles and the requirements established here and any other safety requirements set out in national laws and regulations.

---

<sup>12</sup> There are two facets to uncertainty: aleatory (or stochastic) and epistemic uncertainty. Aleatory uncertainty has to do with events or phenomena that occur in a random manner such as random failures of equipment. These aspects of uncertainty are inherent in the logic structure of the probabilistic model. Epistemic uncertainty is associated with the state of knowledge relating to a given problem under consideration. In any analysis or analytical model of a physical phenomenon, simplifications and assumptions are made. Even for relatively simple problems, a model may leave out some aspects that are deemed unimportant to the solution. Additionally, the state of knowledge within the scientific and engineering disciplines may be incomplete. Simplifications and lack of knowledge lead to uncertainties in the prediction of outcomes for a specified problem.

4.63. The quantitative and qualitative outcomes of the safety assessment form the basis of the safety report. These are supplemented by supporting evidence for and reasoning about the robustness and reliability of the safety assessment and its assumptions, including information on the performance of individual system components as appropriate.

4.64. The safety report shall document the safety assessment with sufficient scope and detail to support the conclusions reached. The safety report shall include:

- (a) A justification for the selection of anticipated operational occurrences and accident conditions addressed in the analysis;
- (b) An overview and necessary details of the collection of data, the modelling, the computer codes and the assumptions made;
- (c) Criteria used for the evaluation of the modelling results;
- (d) Results of the analysis addressing the performance of the facility or activity, incurred risks and a discussion of the underlying uncertainties; and
- (e) Conclusions on the acceptability of the level of safety achieved and the identification of necessary improvements and additional measures.

4.65. The safety report shall be updated as necessary. This safety report shall be retained until the facility has been fully decommissioned or the activity has been terminated. For a repository for radioactive waste, the safety report shall be retained for an extended period after it has been closed.

#### INDEPENDENT VERIFICATION

4.66. The operating organization shall carry out an independent verification to increase the level of confidence in the safety assessment before it is used by the operating organization or submitted to the regulatory body.

4.67. The independent verification shall be performed by individuals or a group of people different from those who carried out the safety assessment. The aim shall be to determine whether the safety assessment has been carried out in an acceptable way.

4.68. Decisions about the scope and level of detail of the independent verification are subject to a graded approach and shall reflect the potential radiation risk, and the maturity and complexity of the facility or activity.

4.69. The independent verification shall combine an overall review to determine whether the safety assessment carried out is comprehensive with spot checks where a much more detailed review is carried out that focuses on those aspects of the safety assessment that have the highest impact on the radiation risks arising from the facility or activity. The independent verification shall also consider whether there are any contributions to the radiation risks that have not been taken into account.

4.70. The independent verification shall determine whether the models and data used are accurate representations of the design and operation.

4.71. In addition, the regulatory body shall carry out a separate independent verification to satisfy itself that the safety assessment is acceptable and to determine whether it provides an adequate demonstration of whether the legal and regulatory requirements are met.<sup>13</sup>

---

<sup>13</sup> It is accepted that the scope and extent of the independent verification carried out by the regulatory body is at the discretion of each Member State.

## 5. MANAGEMENT, USE AND MAINTENANCE OF THE SAFETY ASSESSMENT

5.1. The safety assessment is key to enabling the operating organization to manage facilities and activities safely. It is also a vital input to the safety report required to demonstrate compliance with regulatory requirements.

5.2. The safety assessment in itself cannot achieve safety. Safety is only achieved if the input assumptions are valid, the derived limits and conditions are implemented and maintained and the assessment reflects the facility or activity as it actually is at any point in time. Facilities and activities evolve in their lifetimes (e.g. through construction, commissioning, operation and decommissioning or closure) and with modifications, improvements and ageing. Knowledge and understanding also develop with time and experience. In order to remain valid, therefore, the safety assessment shall be updated to reflect such changes. The updating of the safety assessment is also important in order to provide a baseline for the future evaluation of monitoring data and performance indicators and, for radioactive waste facilities, to provide an appropriate record for future site use. On this basis, the following additional requirements for the implementation and maintenance of the safety assessment are established.

5.3. The safety assessment shall be reviewed to identify the input assumptions that need to be complied with by appropriate safety management controls.

5.4. The safety assessment shall provide one of the inputs into defining the limits and conditions that need to be implemented through suitable procedures and controls. These shall include a means for monitoring to ensure that the limits and conditions are complied with at all times.

5.5. Input from the safety assessment shall be used to define the maintenance and inspection programme that needs to be established using procedures and controls that are auditable in order to ensure that:

- (a) Any necessary conditions are maintained; and
- (b) Any structures, systems and components maintain their integrity and functional capability over their required lifetime.

5.6. Input from the safety assessment shall be used to define the procedures that need to be put in place for all operational activities significant to safety and for responding to anticipated operational occurrences and accidents. The safety assessment shall also be used as an input for planning of the on-site and off-site accident management and emergency response.

5.7. Input from the safety assessment shall be used to define the necessary competences for the staff involved with the facility or activity and this shall be used to inform their training, control and supervision.

5.8. Input from the safety assessment shall be used to make decisions in an integrated risk informed approach.

5.9. Since the safety assessment provides such an important input to the management system of facilities and activities, the processes by which it is produced shall be planned, organized, applied, audited and reviewed in a way that is commensurate with the graded approach. Consideration shall also be given to the ways in which results and insights from the safety assessment may best be communicated to a wide range of interested parties, including the designers, the operating organization, the regulatory body, other safety professionals and, as appropriate, the public. Communication of the results from the safety assessment to interested parties shall be commensurate with the radiation risks arising from the facility or activity and the complexity of the models and tools used.

5.10. The safety assessment and management systems by means of which it is conducted shall be periodically reviewed at predefined intervals in accordance with regulatory requirements. In addition to such periodic reviews, they shall be reviewed and updated:

- (a) When there is any significant change that particularly affects the safety of the facility or activity;
- (b) When there are significant developments in knowledge and understanding (such as those arising from research or operational experience);
- (c) When there is an emerging safety issue due to a regulatory concern or an incident; and
- (d) When there have been significant improvements in the computer codes or the input data used in the safety analysis.

## **REFERENCES**

- [1] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles: Safety Fundamentals, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Legal and Governmental Infrastructure for Nuclear, Radiation, Radioactive Waste and Transport Safety, IAEA Safety Standards Series No. GS-R-1, IAEA, Vienna (2000).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material, 2005 Edition, IAEA Safety Standards Series No. TS-R-1, IAEA, Vienna (2005).
- [4] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANISATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, IAEA Safety Series No. 115, IAEA, Vienna (1996).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, OECD NUCLEAR ENERGY AGENCY, Geological Disposal of Radioactive Waste, IAEA Safety Standards Series No. WS-R-4, IAEA, Vienna (2006).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna (2007).

**DRAFT**

## CONTRIBUTORS TO DRAFTING AND REVIEW

Aeberli, W.	HSK, Switzerland
Bester, P.J.	National Nuclear Regulator, South Africa
De Monk, P.J.	Ministry of Housing, Spatial Planning and the Environment, Netherlands
El-Shanawany, M.	International Atomic Energy Agency
Goldammer, W.	Representing NSRW, Germany
Kanwar R	Bhabha Atomic Research Centre, India
Kondo, S.	Japan Nuclear Energy Safety Organization, Japan
Mayfield, M.	Nuclear Regulatory Commission, USA
Niehaus, F.	Private consultant, Germany
Ogiso, Z.	Japan Nuclear Energy Safety Organization, Japan
Prasad, S.S.	Bhabha Atomic Research Centre, India
Raze-ur-Rehman, X	Pakistan Atomic Energy Commission, Pakistan
Saint Raymond, P.	DSIN, France
Sajaroff, P.M.	Nuclear Regulatory Authority, Argentina
Sallit, G.	Department for Transport, UK
Sharma, D.N.	Bhabha Atomic Research Centre, India
Shepherd, C.H.	Corporate Risk Associates, United Kingdom
Vaughan, G.J.	Nuclear Installations Inspectorate, United Kingdom
Waker, C.	Nuclear Installations Inspectorate, United Kingdom