IAEA SAFETY STANDARDS AND APPROACH TO SAFETY OF ADVANCED REACTORS

M. Gasparini
International Atomic Energy Agency
Division of Nuclear Installation Safety
M.Gasparini@iaea.org

ABSTRACT

The paper presents an overview of the IAEA safety standards including their overall structure and purpose. A detailed presentation is devoted to the general approach to safety that is embodied in the current safety requirements for the design of nuclear power plants. A safety approach is proposed for the future. This approach can be used as reference for a safe design, for safety assessment and for the preparation of the safety requirements. The method proposes an integration of deterministic and risk informed concepts in the general frame of a generalized concept of safety goals and defence in depth. This methodology may provide a useful tool for the preparation of safety requirements for the design and operation of any kind of reactor including small and medium sized reactors with innovative safety features.

1 INTRODUCTION

There is a large number of proposed advanced nuclear reactors and there are also different definitions of the term “advanced”. According to the definitions proposed by the Agency [1], an advanced plant design is a design of current interest for which improvements over its predecessors and/or existing designs are expected. Advanced designs consist of evolutionary designs and designs requiring substantial development efforts. The latter can range from moderate modifications of existing designs to entirely new design concepts. They differ from evolutionary designs in that a prototype or a demonstration plant is required, or that work is still needed to establish whether such a plant is required. Most designs proposed for new small and medium size reactors are either evolutionary or innovative.

The different design approaches, technologies and safety features of advanced concepts indicate that the full application of existing safety requirements, mostly developed for large water cooled reactors may need, in some cases, interpretation or adaptation. For some innovative concepts there is a need to develop a tailored set of safety requirements derived from the general consolidated principles of nuclear safety, which better incorporates the specific characteristic of a given concept. The IAEA Safety Standards and the ongoing work on implementation of defence in depth for different type of reactors provide a useful starting point and a suitable framework for this purpose.

2 THE IAEA SAFETY STANDARDS

While safety is a national responsibility, international standards and approaches to safety promote consistency and facilitate international technical co-operation and trade, and help to provide assurance that nuclear and radiation related technologies are used safely.

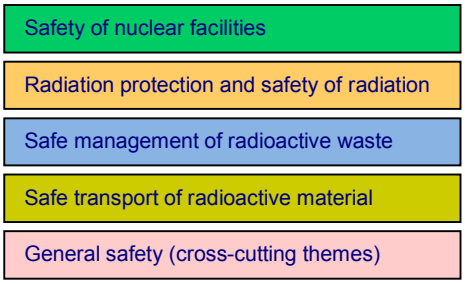
Under the terms of its Statute, the Agency is authorized to establish standards of safety for protection against ionizing radiation. The IAEA publications of a regulatory nature are issued in the IAEA Safety Standards Series, covering nuclear safety, radiation safety, transport safety and waste safety.

Safety standards are intended for regulatory bodies and governmental agencies as well as organizations that design and use nuclear and radiation related technologies, and users of radioactive material in industry medicine, agriculture, research and education.

An extensive process was established some years ago to review all NUSS publications to produce a better-organized and consistent set of documents.

The new overall structure of the safety standards developed during the revision process is represented in Figure 1. Full text of all safety standards that have been prepared since the revision project was initiated are now available on the web site of the Agency (http://www-ns.iaea.org/standards/).

The IAEA safety standards cover safety in five areas:



Some IAEA safety standards address matters that are relevant to safety in a range of facilities and activities (thematic areas); other address different aspects of safety for a specific type of facility or activity.

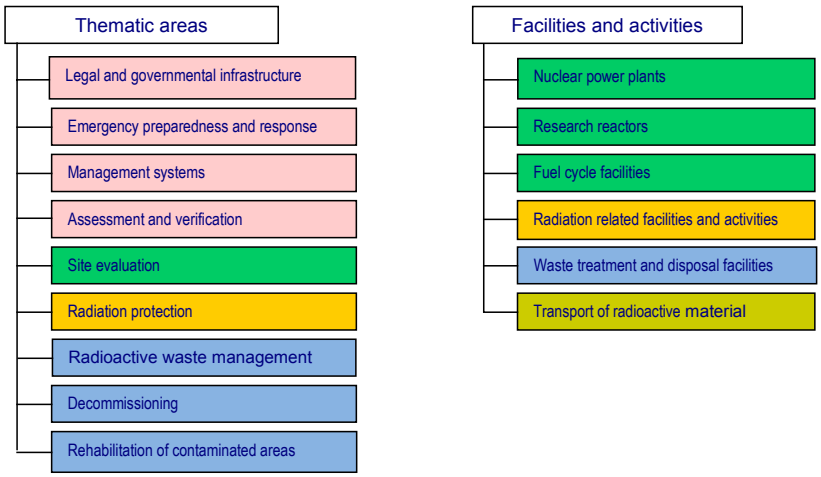


Figure 1. Overall structure of the IAEA safety standards series.

For each thematic area and each type of facility and activity, there are three categories of Standards, schematically depicted in Figure 2, with the following aims:

Safety Fundamentals: present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements: establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides: recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

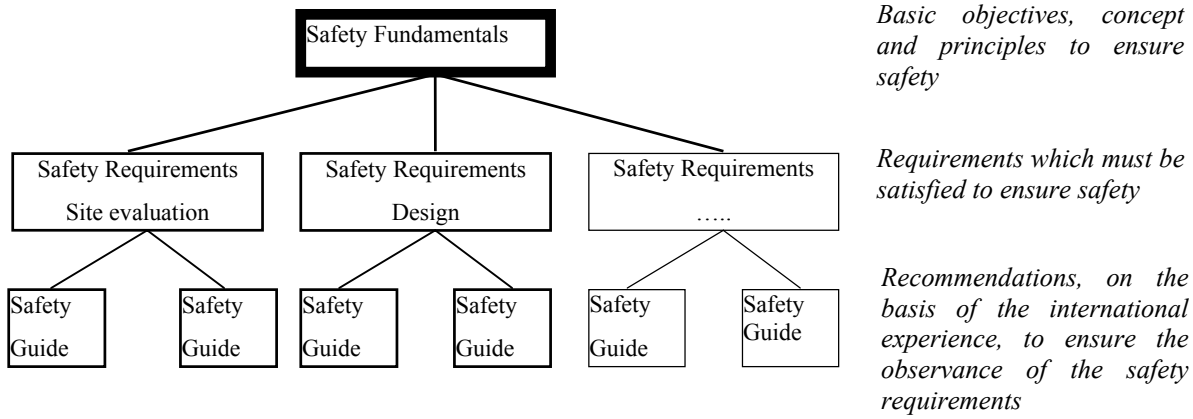


Figure 2. Hierarchy of the IAEA Safety Standards Series.

3 CURRENT AND FUTURE SAFETY APPROACH

The safety approach on which the design of the current nuclear power plants are based, has been developed in several years and it is reflected in the current regulatory structure. This structure has been developed mainly to respond to the challenges presented by the current technology for water cooled reactors.

The large number of new designs and different technologies proposed for new reactors pose several challenges to the preparation of regulations that should be addressed starting with a new and fresh consideration of the entire safety philosophy and its main pillars.

It is necessary to reconstruct the rationale behind the current rules and from this prepare a new approach more technology neutral and safety performance based without any preconditioned notion purely technology dependent. The new approach should also take advantage of the advances in PSA and include the risk informed notion.

A recent work done at the IAEA has identified the main pillars underpinning the current safety approach and has showed that they may also be suitable for new plants, if properly interpreted and formulated. The main pillars are the safety objectives, the fundamental safety functions and the concept of defence in depth.

General safety objectives

The IAEA publication The Safety of Nuclear Installations [2] sets out basic objectives, concepts and principles for ensuring the safety of nuclear installations in which the stored energy or the energy developed in certain situations could potentially result in the release of radioactive material from its designated location with the consequent risk of radiation exposure of people. The principles are derived from the following three fundamental safety objectives (the following five paragraphs are reproduced from Ref. [2].

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

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

consequences of any accidents.

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

The three safety objectives as described above are expressed in general qualitative terms. There is no evidence, for the time being, of any need for substantial changes to these objectives — they still represent the starting point for the preparation of safety requirements for any advanced or future reactor.

These qualitative safety objectives can generate a safety goal (curve of the acceptable risk) expressed in quantitative terms such as the example showed in Figure 3. This curve (or step line) on the diagram "Frequency of events-Radiological consequences" separates acceptable and non-acceptable plant conditions and provides a quantitative indicator of the overall plant safety level. It does provide the designer with a target to establish the safety architecture of the plant and to design safety systems.

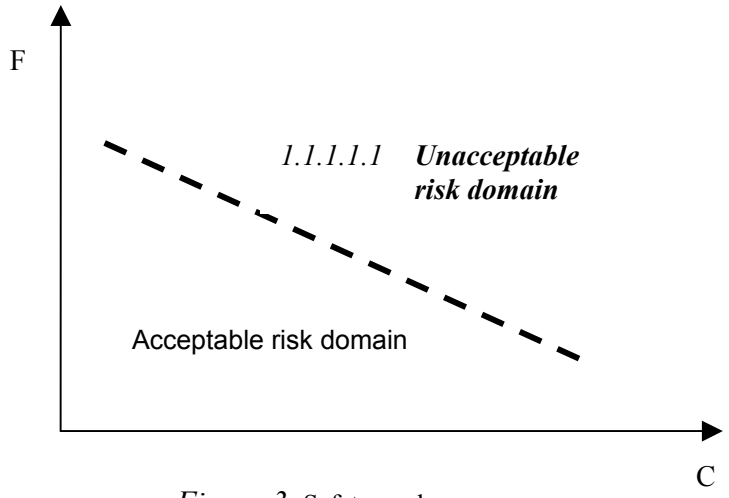


Figure 3. Safety goal

The curve Frequency-Consequences derived from the safety performance of a modern LWR design (e.g. EPR) can be used to tentatively establish the general safety goal for innovative reactors, with the assumption that the safety level of a future reactor should be at least, if not better, equivalent to the safety level of this reactor.

The fundamental safety functions

To ensure safety (i.e. to meet allowable radiological consequences during all foreseeable plant conditions), the following fundamental safety functions shall be performed in operational states, in and following a design basis accident and in and after the occurrence of severe plant conditions:

— control of the reactivity;

— removal of heat from the core; and

— confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

The possible challenges to the safety functions are dealt with by the provisions of a given level of defence. All mechanisms that can challenge the successful achievement of the safety functions are identified for each level of defence. These mechanisms are used to determine the set of initiating events that encompass the possible initiations of sequences.

The defence in depth strategy

The implementation of the concept of defence in depth in the design of a plant provides a series of levels of defence (essential means of each level of defence are inherent characteristics, safety margins, systems, procedures) aimed at preventing failures and abnormal operations and ensuring appropriate protection in the event that prevention fails.

Accident prevention is the first priority. The rationale for the priority is that provisions to prevent deviations of the plant state from well-known operating conditions are generally more effective and more predictable than measures aimed at mitigation of such departure, because the plant's performance generally deteriorates when the status of the plant or a component departs from normal conditions. Thus preventing the degradation of plant status and performance generally will provide the most effective protection of the public and the environment.

Defence in depth, according to the definition of the IAEA [3], is structured in five levels. Should one level fail, the subsequent level comes into play. Table 1 summarizes the objectives of each of the five levels and the primary means of achieving them. The correct implementation of defence in depth ensures that a failure, whether mechanical or human, at one level of defence, and even combinations of failures at more than one level of defence, will not propagate to jeopardize defence in depth at subsequent levels. This requires the independence of the different levels of defence.

As the objective of the first level of protection is the prevention of abnormal operation and system failures, if it fails, an Initiating Event comes into play. Then the second level of protection will detect the failures and control the abnormal operation. Should the second level fail, the third level ensures that the safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response. Some off-site measures should be taken preventively and independently from the success of the provisions of the fourth level of defence.

Table 1. Levels of defence in depth (from INSAG-10)

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

The general concept of defence in depth as articulated by the IAEA is now widely known and adopted, even though, in some cases, defence in depth is still solely interpreted as the availability of multiple physical barriers to the release of fission products.

Operating NPPs are largely designed according to a safety architecture dictated by the implementation of the defence in depth strategy. The defence in depth is applied in a deterministic way. This means that the plant is deterministically designed against a set of normal and accident situations according to well-established deterministic design criteria in order to meet the radiological targets. The deterministic approach is complemented by probabilistic evaluations with the main purpose of verifying that the design is well balanced and there are no weak areas or systems that would allow the possibility of risky sequences. This safety approach is reflected in the existing IAEA Safety Requirements for the design of NPPs [4].

For innovative reactors an effort is necessary to achieve a more satisfactory integration of deterministic and risk informed considerations in the frame of a generalized concept of defence in depth. Each level of defence in depth could be associated with the events in a given range of probability and probabilistic success criteria could be defined together with deterministic success criteria for each level of defence in depth. The probabilistic success criteria will provide input to the utilization and design of the features of each level of defence indicating the necessary reliability to comply with the general safety goal.

Figure 4 summarizes the safety approach described so far and shows the link between the safety approach and the derivation of the safety requirements. In this scheme the preparation of safety requirements is intended as establishing a set of rules for the implementation of each level of defence in depth to comply with the general safety goal.

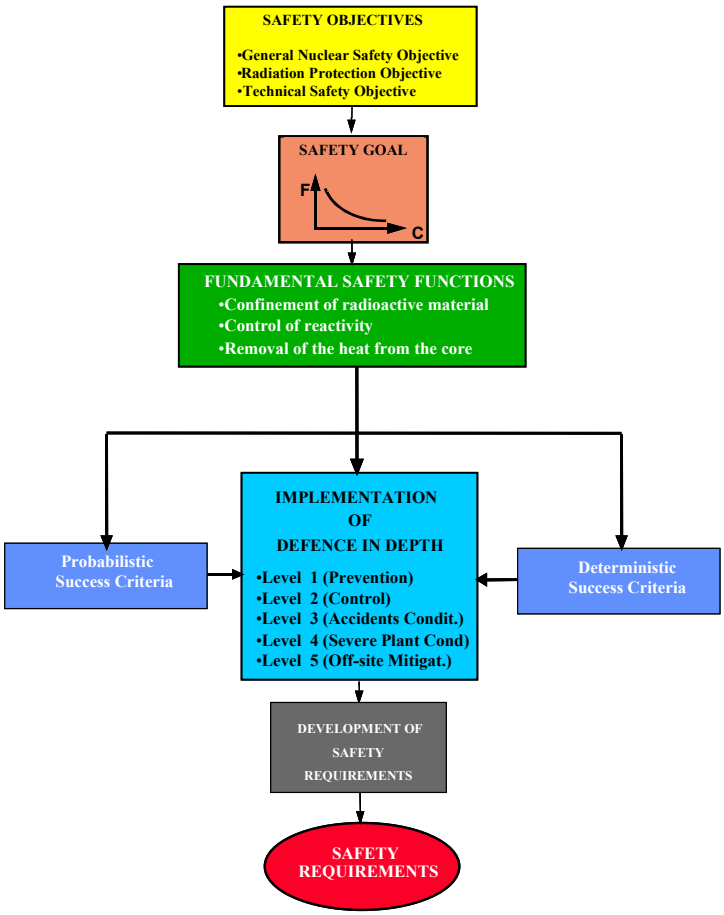


Figure 4. Logical process underpinning the safety requirements.

4 THE TOP-DOWN APPROACH

The safety requirements for NPPs have reached the current status through a long development process, which has incorporated the results of extensive plant operating experience and the experience gained from the lessons of the past. The current safety requirements [4] define the safety approach developed and refined over the course of many years. Although they have mostly been developed for large water cooled reactors, it is reasonable to assume that they are a good starting point for the preparation of the design requirements for any advanced reactor, provided the rational behind each requirement is fully understood in the logic of a generalised concept of defence in depth. The criterion for judging the applicability or adequacy of a requirement for an existing NPP to a different reactor should be based on the full understanding of the contribution of the requirement to defence in depth.

The proposed top-down approach consists of a systematic review of the existing requirements for the design of nuclear power plants [4] starting from the most general (applicable to all NPPs) and down to the most specific and more technology dependent. This process is schematically presented in Fig. 5.

The Requirements for a specific type of reactor are generated through a critical interpretation of the 'objectives' and 'essential means' associated with each level of defence in depth (see Table 1), and the full understanding of the safety features of the specific reactor.

The 'transfer function' (central box in Fig. 5) that establishes the requirements for a generic nuclear reactor plant from the requirements for an existing NPP should not simply be interpreted as a filter to accept or not a requirement, but as a mechanism to generate new requirements if they are necessary because of the features of the specific nuclear reactor plant. For example, an inherent feature that fulfils a safety function in a very reliable way could allow for a relaxation of the requirements for a safety system or even to the possible elimination of the safety system that normally performs that function in water reactors. On the other hand, specific features or materials could possibly introduce failures that could initiate events for which adequate preventive or mitigative measures could be necessary.

This process will lead to the compilation of a consistent set of requirements organized in a hierarchical way with the general requirements at the top and the more specific at the bottom. Moving from the top down, the requirements will become more specific and more dependent on the particular technology.

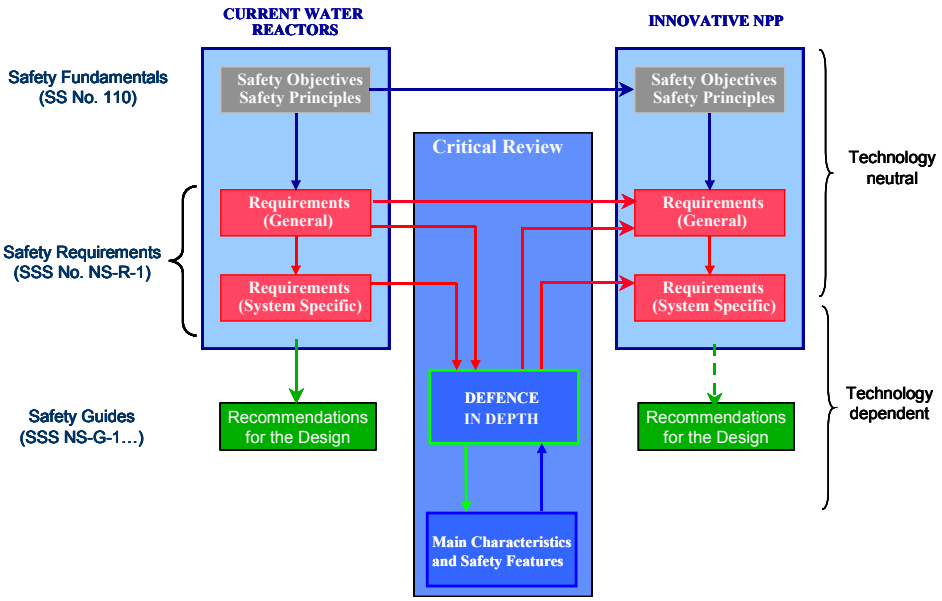


Figure 5. Generation of Requirements for Advanced NPPs.

5 THE OBJECTIVE-PROVISIONS TREE

The method of the objective-provisions tree described below represents a preliminary attempt to systematically address the 'critical review' of the implementation of the defence in depth as indicated in Fig. 5.

The logical framework of the objective-provisions method is graphically depicted in terms of a tree such as shown in Fig. 6. At the top of this tree is the level of defence in depth that is of interest, followed by both the objectives to be achieved and the safety functions to perform.

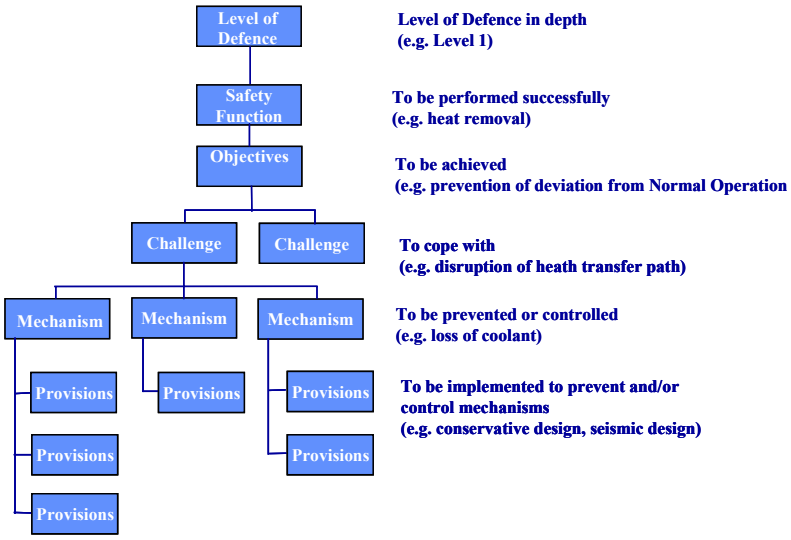


Figure 6. Defence in depth objective-provisions tree

For each function or subfunction the challenges to their fulfilment can be identified. These challenges are general processes or situations that can prevent adequate performance of the safety functions (e.g. reactivity excursions that could damage the fuel before shutdown). The challenges arise from a variety of mechanisms that have also to be identified. The identification of the mechanisms that can challenge the achievement of a safety function is an essential task in the development of the logical framework for inventorying the defence in depth capabilities of an NPP. Once the mechanisms are known, it is possible to determine the provisions necessary to prevent and/or control them.

This methodology has been applied at the Division of Nuclear Installation Safety of the IAEA as case study for the development of Safety Requirements for Modular High Temperature Gas Cooled Reactors [5].

6 CONCLUDING REMARKS

There is a large worldwide interest on innovative reactors. The IAEA INPRO program has developed the user requirements for reactors to be built in the coming decades. The Generation IV Roadmap project has selected some promising concepts of innovative reactors and defined the research necessary to finalize their design.

New reactors, in particular small and medium sized will adopt innovative safety approaches and features. For these reactors there are no established international agreed design rules or regulatory guides. There is a need for designs licensable in several countries and the need to simplify the licensing procedures.

The IAEA is carrying out a project to develop an international agreed safety approach for innovative reactors and to achieve consensus on a scheme of safety compliance check. This work will eventually lead to a proposal of guidance for the design and to a set of safety requirements similar to that existing for current NPPs.

The approach proposed is technology neutral, risk informed and performance based. It is based on the definition of a safety goal expressed in terms of risk and adoption of a generalized implementation of defence in depth.

The exiting safety requirements for the design of nuclear power plants may be used as major reference to generate the requirements for advanced reactors through a review process. This process will be based on a critical application of the strategy of defence in depth.

The challenge for the future is to develop more confidence in the PSA tools and to demonstrate that sufficient defence in depth can be achieved through simpler and cheaper technological solutions. Risk informed decision making will play an important role in the development of future reactors of any kind. It will help to achieve high levels of safety and reduce costs; in particular through simplification of safety systems and a sound and well balanced safety classification of structures, systems and components.

Benefits can be obtained through harmonizing licensing criteria and procedures used by the nuclear community to the greatest possible extent, based on worldwide scientific resolution of technical issues and accepted standards of safety adequacy.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Terms for Describing New, Advanced Nuclear Power Plants, IAEA-TECDOC-936, Vienna (1997)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, Vienna (2000).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations in the development of safety requirements for innovative reactors: Application to modular high temperature gas cooled reactors, IAEA-TECDOC-1366, Vienna (2003).