IAEA-TECDOC-1235

Safety aspects of nuclear plants coupled with seawater desalination units

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

August 2001

The originating Section of this publication in the IAEA was:

Engineering Safety Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

SAFETY ASPECTS OF NUCLEAR PLANTS COUPLED WITH SEAWATER DESALINATION UNITS
IAEA, VIENNA, 2001
IAEA-TECDOC-1235
ISSN 1011–4289

Printed by the IAEA in Austria
August 2001

FOREWORD

The worldwide demand for potable water is steadily growing and water shortages are already reaching serious proportions in many regions of the world. Because of the abundance of seawater, desalination is a good alternative. However, desalination is an energy intensive process. Therefore, the increasing demand for desalted water creates a collateral demand for increased production of energy.

The use of nuclear fission as an energy source for desalination is technically and economically very attractive. In particular, co-generation allows for the energy to be harnessed in a very efficient way. The considerations on feasibility and economics should be, however, associated with and supported by safety considerations.

The 42nd IAEA General Conference in 1998 requested the IAEA to "take appropriate measures and concrete actions, on the basis of the technical and economic feasibility of seawater desalination using nuclear energy, with a view to the effective development and practical application of nuclear technologies for producing potable water economically." The General Conference further stressed the importance of safety and urged the IAEA to continue its "work regarding the safety and security aspects of desalination using nuclear energy."

The purpose of this publication is to address the specific safety and licensing aspects of nuclear plants for use in heat utilization applications and to establish the basis for safety assessment of such plants.

This publication also proposes a general approach for the preparation of safety requirements for reactors with special safety features or of a smaller size compared with nuclear power plants. This approach (top-down approach) is aimed at generating the safety design requirements for any kind of nuclear reactor starting from those for nuclear power plants, which are covered by the IAEA's well established corpus of safety standards.

The IAEA is grateful to the experts who contributed to this publication. The responsible IAEA officer was M. Gasparini of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. Nuclear desalination and other heat utilization applications

In many regions of the world, the supply of renewable water resources is inadequate to meet current needs, and that from non-renewable sources is being rapidly depleted. Since the worldwide demand for potable water is steadily growing, the result is water shortages that are already reaching serious proportions in many regions. To mitigate the stress being placed on water resources, additional freshwater production capability must be developed. Because of the abundance of seawater, desalination is a good alternative. However desalination is an energy intensive process. Therefore, the increasing demand for desalted water creates a collateral demand for increased production of energy.

Because of the proven capability of nuclear power for large scale energy generation, and at the request of its Member States, in 1989 the International Atomic Energy Agency (IAEA) initiated a programme aimed at evaluating the use of nuclear power as an energy source for seawater desalination. Under the umbrella of its "potable water programme" the IAEA and a number of its Member States have carried out studies of nuclear desalination[1]. The results of these studies have consistently shown that nuclear desalination is technically viable and can be economically competitive. As a result of the positive outcome of studies to date and the increasing level of interest among Member States, Resolution GC(42)/35 of the 42nd IAEA General Conference requested that the IAEA "take appropriate measures and concrete action, on the basis of the technical and economic feasibility of seawater desalination using nuclear energy, with a view to the effective development and practical application of nuclear technologies for producing potable water economically." The resolution further urged the IAEA to continue its "work regarding the safety and security aspects of desalination using nuclear energy."

In addition to desalination, there has been a resurgence of interest in other heat utilization applications. The temperature requirements for these applications vary greatly from low temperature heat for district heating to high temperature process heat for coal gasification and hydrogen production.

The purpose of this publication is to address the safety and licensing aspects of nuclear plants for which a significant portion of the heat energy produced by the reactor is intended for use in heat utilization applications. Although intended to cover the broad spectrum of nuclear heat applications, the focus of the discussion will be the desalination of sea water using nuclear power plants as the energy source for the desalination process.

1.2. Desalination processes

The choice of desalination technology determines the manner in which the desalination plant is coupled with the reactor. The two technologies that are most commonly considered for coupling with nuclear reactors are thermal processes, such as multi-stage flash (MSF)

[1] As defined in IAEA-TECDOC-898, "nuclear desalination" is taken to mean the production of potable water from sea water in an integrated facility in which both the nuclear reactor and the desalination system are located on a common site, there is some sharing of common systems and/or facilities, and the energy used for the desalination system is supplied by the nuclear reactor.

distillation or multi-effect distillation (MED), and mechanical processes such as reverse osmosis (RO) or vapour compression (VC).

With the distillation processes, MSF and MED, the coupling between the desalination plant and the reactor is primarily thermal, although some electrical energy is required for the operation of pumps for the system. The thermal coupling may take the form of steam extraction, for example from the cross-over from high pressure to low pressure turbines, or it may be as cooling water from a condensing turbine. In this latter case, the need to provide thermal conditions that satisfy the requirements for the desalination process may impose special design requirements or constraints on the turbine and/or condenser. Intermediate loops may be included to provide isolation of the reactor from the desalination plant.

Reverse osmosis systems may be "contiguous" systems or may make use of "preheated" feedwater. With contiguous RO, the desalination system will share some common facilities or systems with the reactor plant (e.g. seawater intake and outfall structures), however the only energetic coupling required is electrical. For preheat systems, the primary coupling is electrical, although there is also a very "loose" thermal coupling through the use of condenser cooling water discharged from the reactor as feedwater for the RO system.

1.3. Reactors for desalination applications

Many of the various reactor types currently in use or under development have been considered for nuclear desalination. All reactors produce energy in the form of heat, which may be used directly in a heat application or converted to electricity through a secondary steam generator-turbine-condenser circuit. In some cases, the system is designed to produce both heat and electricity as products.

The most common reactor type considered for desalination is the water reactor, either light water reactor or pressurized heavy water reactor. Such reactors can be either heat-only reactors, providing low temperature heat directly for use in thermal desalination processes, or co-generation reactors providing both electricity and heat. Liquid metal cooled and gas cooled reactors can also be considered for desalination, but are more likely to be used in other heat applications where high temperatures are required.

1.4. Safety and licensing considerations

The overall safety and licensing issues associated with an integrated nuclear desalination facility consisting of a nuclear energy system coupled to a desalination system are primarily those associated with the nuclear plant itself. Nevertheless, it is in fact the safety and licensing of the integrated system that must be addressed and this may introduce particular considerations related to the coupling between the reactor and the desalination plant. These could include, for example, the potential for introduction of radioactive material into the potable water being produced by the facility, the possibility of interaction effects between the nuclear plant and the desalination plant, environmental issues arising from the discharge of concentrated brine from the facility, the potential impact of shared resources such as intake and outfall structures, and the "backfitting" of desalination systems with already existing nuclear plants. There may also be issues that arise if siting of the facility near population centres is considered.

2. SAFETY STANDARDS AND THEIR APPLICABILITY TO NUCLEAR DESALINATION AND OTHER HEAT UTILIZATION APPLICATIONS

2.1. Existing IAEA safety standards

The development and publication of standards, requirements and design guidelines for the safety of nuclear installations is one of the activities of the IAEA. These have been published as the Safety Series of publications, including the well-known Nuclear Safety Standards (NUSS). However, it is recognized that technology and scientific knowledge evolve, that nuclear safety and what is considered adequate protection are not static entities, and that safety requirements must change with time to reflect these ongoing developments. Therefore these publications are currently being updated and revised, and are being published as a part of the new Safety Standards Series (SSS). The Safety Standards Series embodies and international consensus on objectives, concepts, principles, logic, methods and facts which is necessary to promote a common approach to ensuring safety in peaceful applications of nuclear energy. The Standards are written for use by organizations designing, manufacturing, constructing and operating nuclear power plants as well as by regulatory bodies.

The Safety Standards Series is organized into a hierarchy of three categories: Safety Fundamentals, Safety Requirements and Safety Guides. More specifically, this hierarchy of three categories includes:

2.1.1. Safety Fundamentals

The Safety Fundamentals category is the primary category in the hierarchy. Publications in this category *present basic objectives, concepts and principles to ensure safety* in the development and application of nuclear energy for peaceful purposes.

Three basic safety objectives are defined for nuclear power plants. The first is very general in nature. The other two are complementary objectives that interpret the general objective, dealing with radiation protection and the technical aspects of safety, respectively. These objectives are:

- **General 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.*

For the safety of nuclear installations, these objectives are achieved through the application of 25 fundamental principles grouped into four main areas:

- Legislative and regulatory framework;
- Management of safety;
- Technical aspects of safety; and
- Verification of safety.

The Safety Fundamentals apply to all nuclear installations. Hence by definition the fundamental principles apply to nuclear desalination facilities, to district heating facilities, and to facilities designed for other heat utilization applications.

2.1.2. Safety Requirements

Publications in the Safety Requirements category specify *basic requirements that must be satisfied to ensure safety for particular activities or application areas.* These requirements are governed by the basic objectives, concepts and principles that are presented in the Safety Fundamentals. The publications in this category do not present recommendations on, or explanations of, how to meet the requirements.

The Safety Requirements for nuclear power plants (NPPs) cover five main areas:

- Siting;
- Design;
- Operation;
- Governmental Organization;
- Quality assurance.

The field of applicability is described in each set of Requirements. For example, "The Safety of Nuclear Power Plants: Design" includes the following paragraph (**bold** added here for emphasis):

> "103. The publication is a compilation of nuclear safety requirements aimed at defining the elements necessary to ensure nuclear safety. These requirements are applicable to safety functions and the associated structures, systems and components, as well as to procedures important to safety in nuclear power plants, with emphasis on what safety requirements shall be met rather than on specifying how these requirements can be met. **It is expected that this publication will be used primarily for nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (district heating, desalination, etc.).** It is recognised that in the case of other reactor types, including innovative developments in future systems, some of the requirements may not be applicable, or may need some judgment to be made in their interpretation."

A separate set of safety requirements exists for the design and operation of research reactors. The Safety Standards for research reactors reflect the fact that "there are important differences between power reactors and research reactors that must be taken into account to

ensure that the design and operation of a research reactor lead to adequate safety of the facility. For example, most research reactors have an obviously small potential for hazard to the public compared with power reactors but may pose a greater potential for hazard to operators; also, the need for greater flexibility in their use for individual experiments requires a different approach to achieving or managing safety."

2.1.3. Safety Guides

Publications in the Safety Guides category supplement Safety Requirements by presenting *recommendations, on the basis of international experience, of safety measures to ensure the observance of safety standards.* "Safety measures" means any action that might be taken, condition that might be applied, or procedure that might be followed to fulfil the basic Safety Requirements. Safety measures must be effective as a means of ensuring the observance of applicable safety standards.

2.2. Concerns arising from the use of existing IAEA safety standards

The application of power reactor safety standards to the nuclear portion of desalination and district heating plants will in most cases be obvious and appropriate. However, some reactor designs may be considered for district heating or desalination for which the application of power reactor standards, in their entirety, may not be appropriate. In these cases there may be a desire to use standards and requirements applicable to research reactors.

However, the application of research reactor requirements may not necessarily be appropriate either. Paragraph 109 of the "Code on the Safety of Nuclear Research Reactors: Design" [4] states that:

> "109. The requirements given in this publication form the basis for the safety of research reactors with limited hazard potential to the public and typical characteristics. Research reactors with powers of several tens of megawatts, fast neutron spectrum research reactors or small prototype power reactors, for example, may require additional safety measures and the use of codes for power reactors may be more appropriate for a number of aspects. No specifications for such a transition to other codes are presented. These specifications should be agreed upon between the regulatory body and the operating organization and should be acceptable to the former."

On the basis of power level, a 10, 20, or perhaps 30 MW desalination reactor could conceivably fall within the range of applicability of the research reactor standards. However, "typical characteristics" is subject to interpretation, and a high pressure cooling system (15-25 atm), would not be considered a "typical characteristic" even for research reactors. This is also the case in the 100-200 MW power range, for which the research reactor standards clearly do not apply based on power level. Therefore, even though on first examination research reactor standards may appear to be applicable to reactors for district heating and low power nuclear desalination systems, the conditions of their operation are such that the application of these standards, in their entirety, may not be acceptable.

Hence, even though the safety considerations that must be addressed for reactors to be used for the various heat utilization applications are, in general terms, very similar to those of reactors for other uses there may be instances in which currently existing IAEA safety

standards are not specifically applicable. Furthermore, it is not considered practicable (or necessary) to prepare a different set of publications in the IAEA Safety Standards Series specifically to provide guidance for the safety of reactors used in these applications in those few instances where the existing standards are not considered to be applicable.

2.3. Specific requirements applicable to nuclear desalination and other heat utilization applications

As previously mentioned all of the current safety standards (NUSS and research reactor) are being subjected to a comprehensive review and revision process. Since the safety requirements applicable to nuclear desalination, district heating and other heat utilization applications will, in general, be those applicable to nuclear power plants, it should be possible during this revision process to incorporate within the revised publications any new or unique requirements specific to these systems. For example, the standard entitled "The Safety of Nuclear Power Plants: Design" (NS-R-1) incorporates the following new requirement:

> **Power plants used for co-generation, heat generation, desalination.**
>
> 5.59. Nuclear power plants coupled with heat utilization units (such as for district heating) and/or water desalination units shall be designed to prevent transport of radioactive material from the nuclear plant to the desalination or district heating unit under any condition of normal operation, anticipated operational occurrences, design basis accidents and selected severe accidents.

Requirements of this type, and similar requirements addressing other considerations specific to the use of reactors for desalination, district heating or other heat utilization applications, should be considered for inclusion in updated/revised publications in the Safety Standards Series.

It is also suggested that a logical, unified approach to the application of the IAEA Safety Standards Series be developed for such "non-traditional" applications. A hierarchical, "top-down" approach should allow the designers of nuclear desalination installations to systematically identify an appropriate set of comprehensive site/country specific requirements for their particular application, based on the IAEA standards and national regulatory requirements. Such a hierarchical, top-down approach is described in the Section 4 below.

3. SAFETY CONSIDERATIONS SPECIFIC TO NUCLEAR DESALINATION (AND OTHER HEAT UTILIZATION APPLICATIONS)

As previously stated, the overall safety considerations associated with an integrated nuclear desalination facility consisting of a nuclear power plant coupled to a desalination plant are primarily those associated with the nuclear plant itself. (In general this is also the case for reactors intended for coupling to other heat utilization units.) Nevertheless, it is in fact the safety of the integrated facility as a whole that must be addressed. The design, operation and performance of a nuclear desalination plant (or other heat utilization unit) must be such as to ensure the safety of the nuclear reactor as well as the protection of the public and the

environment. Specific safety related considerations pertinent to nuclear desalination plants are discussed below. In many cases these can be generalized to include other heat utilization applications, although that has not been done in the following discussions.

3.1. Coupling

Nuclear desalination installations consist of a reactor and a co-located desalination system coupled to the reactor in one of variety of ways, and sharing many common systems and facilities. This may introduce particular considerations related to the design impact of coupling the reactor plant to the desalination plant and to the transient interactions between the two. These factors must be considered under various coupling situations to determine their effect on the safety of the facility both in normal operation and accident situations.

The choice of desalination technology is a major factor in determining the manner in which the desalination plant is coupled with the reactor. In coupling a nuclear plant with a distillation process, such as multi-stage flash (MSF) or multi-effect distillation (MED), the coupling is primarily thermal, although some electrical energy is required for the operation of pumps for the system. Operational transients in either the nuclear plant or desalination plant could have a direct effect on the operation of the other system. Such transients could have safety implications, which need to be assessed.

In case of a contiguous (co-located) desalination plant using an electrically driven process such as reverse osmosis (RO) or vapor compression (VC), the desalination system may draw its electrical energy either from the grid or by direct connection to the nuclear plant with an auxiliary connection to the grid. If the desalination plant draws part or all of its feedwater from the condenser cooling water discharge of the nuclear plant, as in the RO preheat configuration, there is also a limited thermal coupling between the nuclear plant and the desalination plant. The possibility of interaction effects between the nuclear plant and the desalination plant are likely to be minimal in such cases, but nevertheless must be assessed for potential safety impact.

In any of the coupling configurations involving the transfer of thermal energy between the heat source and the desalination plant, there is a direct coupling via heat transfer circuit(s), introducing the potential for the transfer of radioactive material from the nuclear plant to the product water.

The safety considerations related to the various coupling schemes that must be taken into account are discussed below.

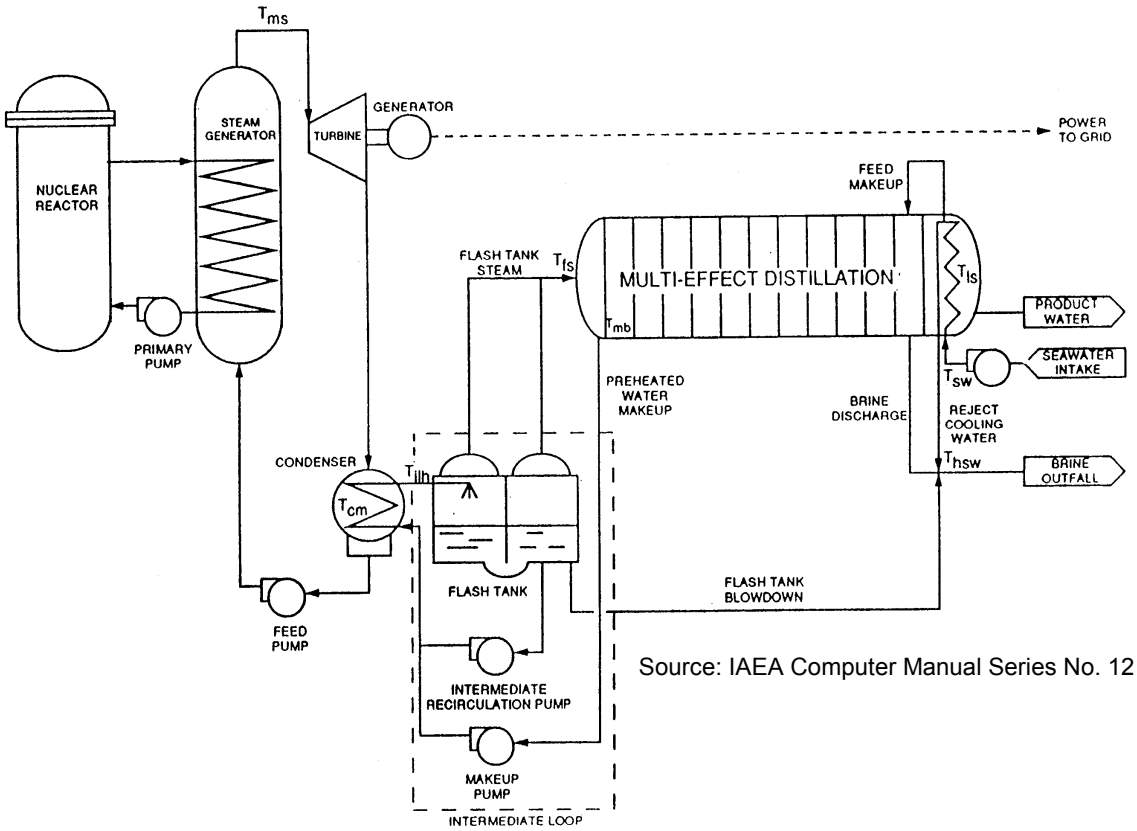
3.1.1. Thermal coupling to distillation systems (MED or MSF)

In dual-purpose[2] plants, one mechanism by which thermal energy can be supplied to the desalination unit is via an intermediate heat transfer loop that serves as the condenser cooling circuit. Heat removed from the condenser is transferred to the flash tank of an MED system or the first stage of an MSF system, as illustrated schematically in Figures 1 and 2, respectively. In such configurations, there is a direct fluid coupling between the reactor and desalination

[2] A “dual-purpose” plant, as understood in the context of nuclear desalination, is one that supplies heat for a thermal desalination unit and produces electricity for distribution to the electrical grid.

system, introducing the risk of contamination of the product water. Coolant loops are normally maintained at pressures such that leakage will not transfer contamination to the product stream. However, constraints imposed by operating temperatures and pressures necessary for effective desalination system design may preclude such precautions without the introduction of additional intermediate loops. Scenarios involving failure mechanisms in materials, systems or components that could lead to carry over of radioactive materials to the product water must to be assessed in order to establish the level of risk. Design measures necessary to reduce the risk to a level that falls within prescribed limits must be implemented and their effectiveness demonstrated by analysis.

Another mechanism by which thermal energy can be supplied to MED and MSF desalination systems is by steam extraction directly from the nuclear power plant. "Live" steam extracted from the reactor's secondary circuit either upstream, from within, or downstream of the turbine would normally be passed through an intermediate heat exchanger, which in turn provides hot water at conditions suitable for the desalination process. An example of this approach is shown schematically in Figure 3, which illustrates the use of extraction steam either with or without the use of a backpressure turbine in the circuit. (The blocks labelled "Nuclear Heat Supply System" in Figure 3 represent the steam generator in the nuclear power plant. The condenser cooling system is not shown since there is no coupling to the desalination plant through the condenser cooling water.) As in the previous example, the potential for carryover of radioactive materials from the reactor system to the desalination system must be assessed and catered for in the design.



Source: IAEA Computer Manual Series No. 12

Fig. 1: Thermal coupling to a multi-effect distillation (MED) system.

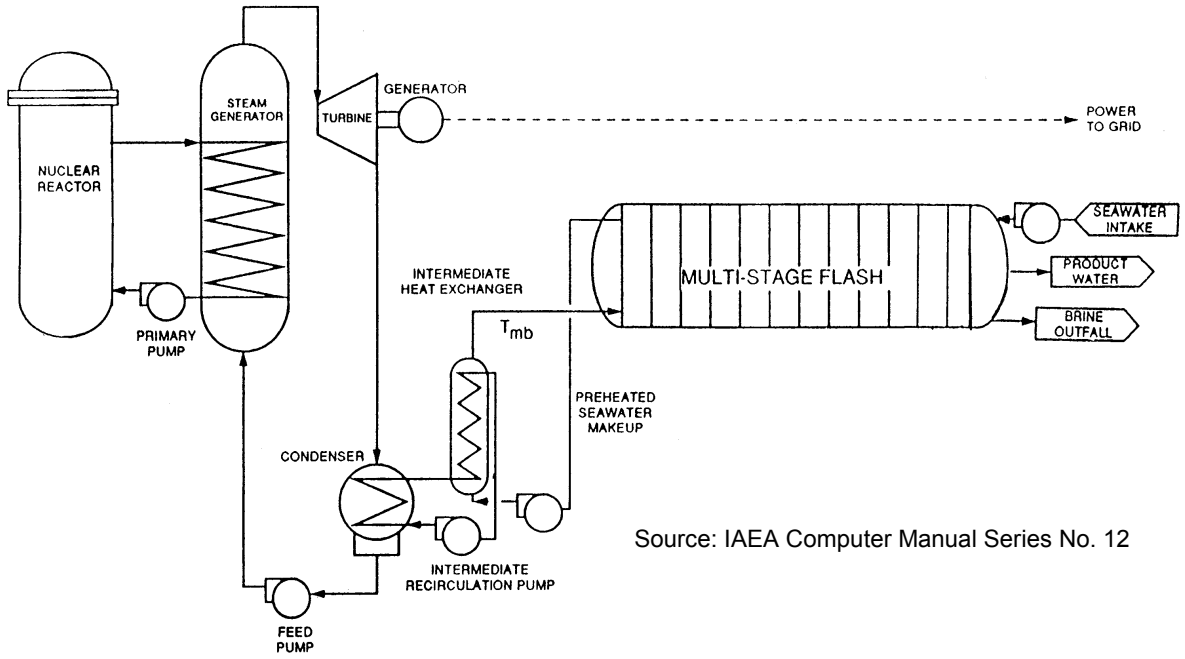


Fig. 2: Thermal coupling to a multi-stage flash (MSF) distillation system.

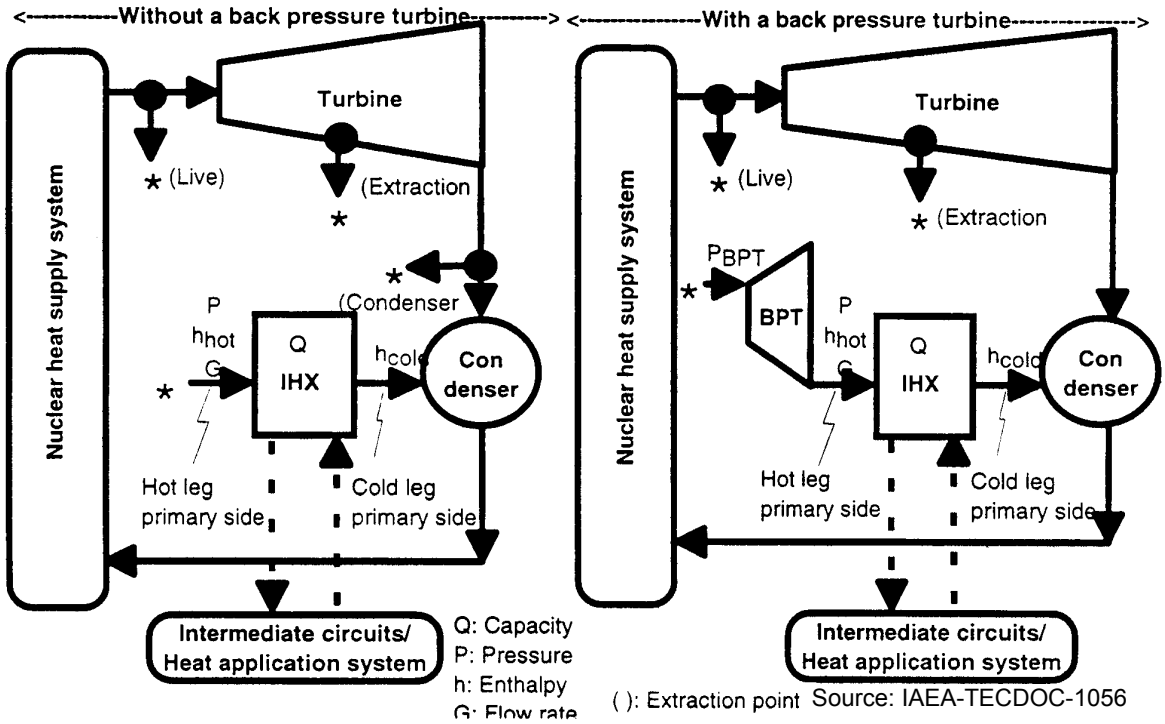


Fig. 3: Thermal coupling using steam extraction from a nuclear power plant.

In addition, since there is a direct coupling between the reactor and the desalination plant, transients between the two systems during normal operation and under accident conditions must be considered. Transients are discussed in more detail in Section 3.2.

3.1.2. Thermal coupling to distillation systems from a heat-only reactor

In the case of a single purpose nuclear plant designed solely for the production of heat for nuclear desalination (or other heat utilization applications), heat is supplied by the reactor through one or more intermediate circuits to either an MED or MSF desalination system. An example of such a system is shown in Figure 4, which illustrates a 200 MWt heating reactor supplying thermal energy to an MED plant in the form of steam, produced by a steam generator in the intermediate circuit. Heat may also be supplied in the form of hot water, depending on the temperature and pressure conditions specific to the desalination plant design. As in the previous examples, the transient behaviour and the potential for carry-over of radioactive materials from the reactor system to the desalination system must be assessed and catered for in the design.

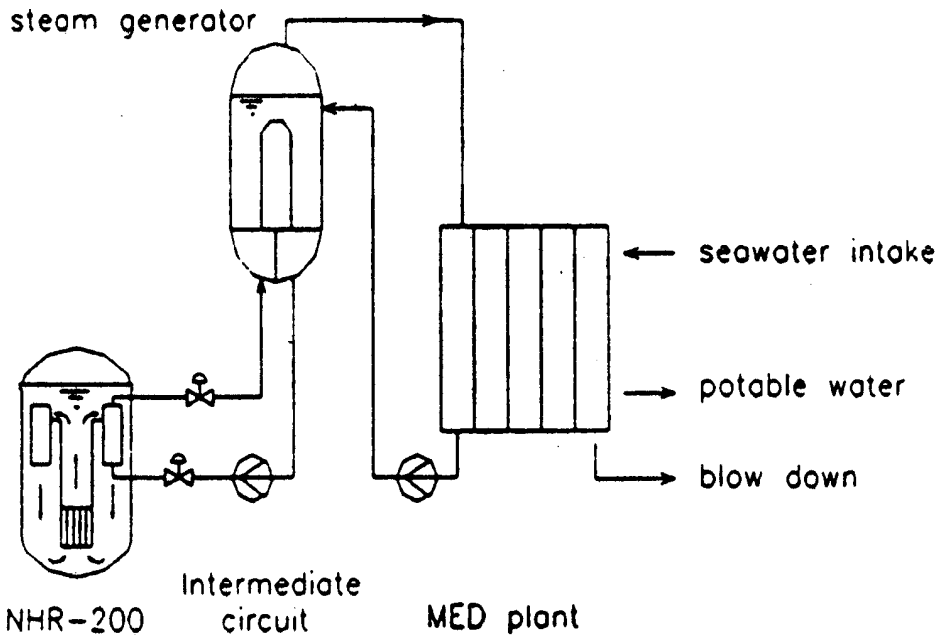


Fig. 4: Thermal coupling to an MED plant from a single purpose nuclear plant.

3.1.3. Electrical and thermal coupling to an RO preheat system

The generation of electricity is a relatively inefficient process with only about one-third of the thermal energy produced in a nuclear reactor being converted to electricity. Hence even for the case of a nuclear power plant in which the design is optimized for the production of electricity, there is a large amount of low-grade thermal energy available in the form of waste heat discharged from the nuclear plant through the condenser cooling system. Figure 5 illustrates schematically an "RO preheat" system, in which part or all of the feedwater to the RO system is taken from the condenser cooling water discharge stream. The RO system, which uses electricity as its primary energy input, may draw either from the electrical grid or by direct connection to the nuclear plant with an auxiliary connection to the grid. Since the

desalination plant draws its feedwater from the condenser cooling water discharge stream, there is also a thermal coupling between the nuclear plant and the desalination plant. As in the previous examples, the potential for carry-over of radioactive materials from the reactor system to the desalination system must be assessed and catered for in the design. The possibility of interaction effects between the nuclear plant and the desalination plant are likely to be minimal in such a configuration, but nevertheless must be assessed for potential safety impact.

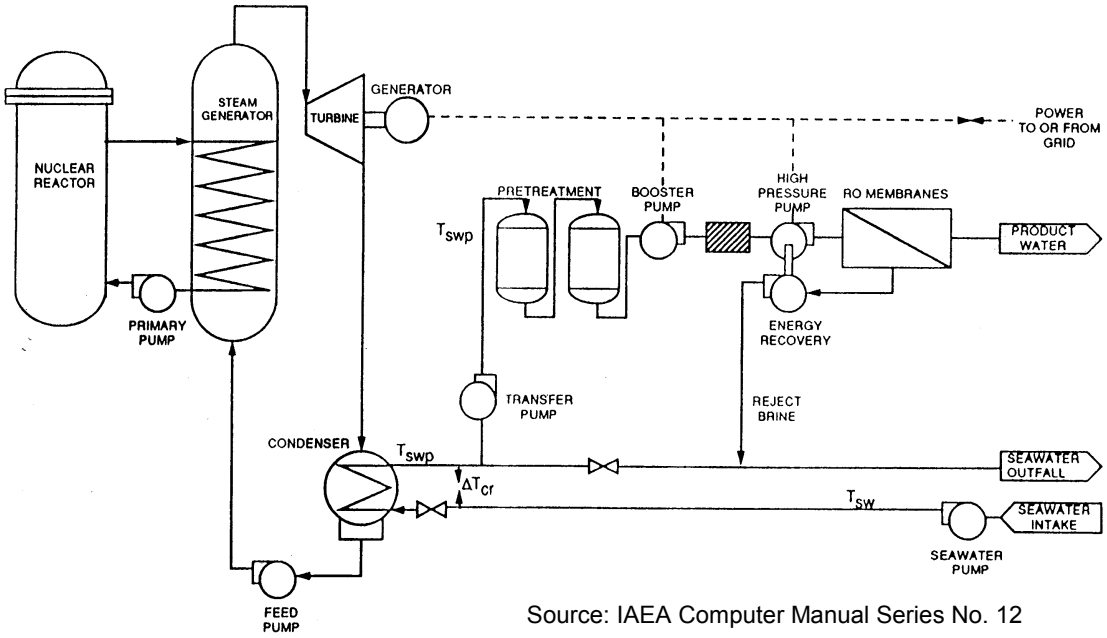


Fig. 5: Electrical and thermal coupling to a reverse osmosis (RO) preheat system.

3.1.4. Electrical only coupling to a contiguous RO system

Contiguous RO systems constitute "nuclear desalination" only in the sense that they are located on the nuclear plant site and share commons resources, such as the seawater intake and outfall structures. Such a configuration is illustrated schematically in Figure 6. In the case of contiguous RO (or vapor compression) desalination systems, the only energy supplied by the nuclear plant is electricity to operate the desalination system pumps. This may be drawn either from the electrical grid or by direct connection to the nuclear plant with an auxiliary connection to the grid. Since there is no thermal coupling between the reactor and the desalination plant, there is no direct path for carry-over of radioactive materials from the reactor to the product water. However, where the RO plant shares common resources with the desalination plant, the effect of this on operation of the reactor must be evaluated.

3.1.5. Coupling nuclear power plants to hybrid desalination systems

More complex coupling arrangements can also be considered. Figure 7 illustrates schematically the coupling of a nuclear power plant to a hybrid desalination system consisting of an MED plant (coupled as in Figure 1) followed by an RO plant which takes reject cooling water from the last effect of the MED system as feedwater to the RO system. A similar hybrid system could be considered based on the use of an MSF distillation plant followed by an RO plant. The safety considerations in such coupling schemes are the same as those discussed above.

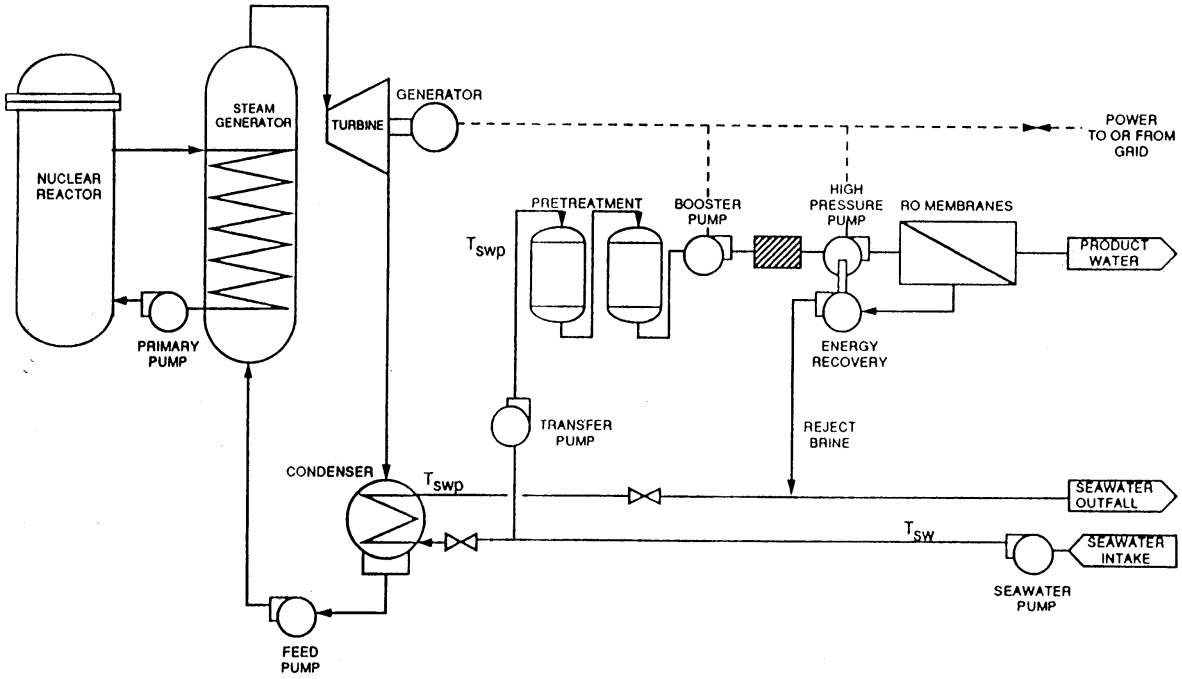
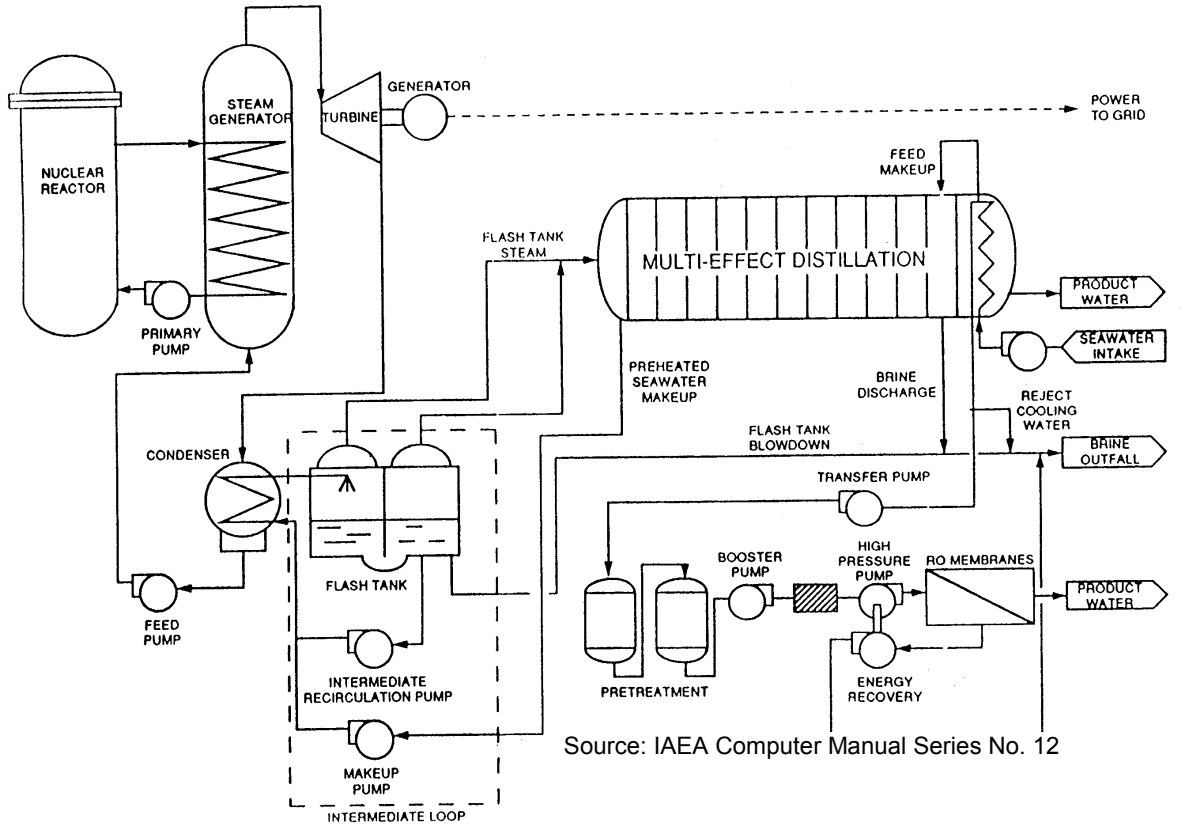


Fig. 6: Electrical only coupling to a contiguous reverse osmosis (RO) system.



Source: IAEA Computer Manual Series No. 12

Fig. 7: Coupling of a nuclear power plant to a hybrid MED-RO desalination system.

3.1.6. Carry-over of radioactive material into the product water

As noted above, one of the consequences of any coupling scheme that involves the transfer of thermal energy from the nuclear plant to the desalination plant is that it introduces the risk of carry-over into the product water stream. Failure scenarios can be postulated that could lead to the possibility of radioactive materials being transported from the reactor core into the primary coolant system, and from there through various tube leaks or failures in secondary and subsequent intermediate systems into the product water stream. Normally, operating pressures in the intermediate loops are controlled to prevent leakage towards the product water. For example, condensers normally operate under a high vacuum, hence any failures in the condenser/seawater boundary would be expected to result in leakage into the condenser, not into the feedwater stream to the desalination system. Even if radioactive isotopes did enter the desalination system feedwater stream, they are sufficiently large that they would have a very high rate of rejection (97–99%) by an RO system, or would be left behind in the concentrate in MED or MSF distillation systems. Hence the likelihood of radioactive material entering the desalination system product water stream is considered to be very low.

Nevertheless such scenarios do need to be addressed, with for example probabilistic safety analysis techniques, during the design implementation phase of a project. Provisions must be included in the design to ensure that the radiological risk posed by the addition of a desalination system to the nuclear plant remains within prescribed regulatory limits.

3.1.7. Sharing of resources

In cases where the coupling of the nuclear plant to the desalination system includes shared resources and systems, such as intake and outfall structures, these must be taken into account in the reactor design. For example it is important to locate intake and outfall structures such that any radioactivity discharged by the reactor plant is not likely to be sucked into the intake stream. This precaution is taken in order to ensure that the risk of radioactive contamination reaching the potable water produced is negligible.

3.1.8. Brine discharge

An additional consideration in the case of a nuclear desalination facility, not normally encountered in a nuclear installation, is the discharge of concentrated brine from the desalination plant. The environmental considerations are quite different from those normally encountered in a nuclear installation, as the brine is heavier than sea water and hence tends to settle towards the ocean floor, creating different problems for distribution and dilution than for the heated water normally discharged from the reactor's condenser cooling system. This must be taken into consideration in the integrated plant design.

3.2. Transients

3.2.1. Accident scenarios

No transients more severe than those usually addressed in the reactor design process are expected to occur as a result of the addition of a desalination (or other heat utilization) plant to the facility. Nevertheless, transients in the desalination plant, either during normal operation

or as a result of an accident scenario, could result in the feedback of transients to the reactor system. While these transients are not expected to be more constraining than those normally postulated, they must nevertheless be taken into account during the reactor design process. The number and severity of such transients must be assessed during the design and discussed within the safety report. In the unlikely event of such a transient having a potential safety impact greater than that normally anticipated in the nuclear plant, specific provisions must be included in the design to accommodate it. Examples of transients that must be considered include, but are not limited to, the following:

- **Loss of heat sink:** For thermal couplings such as those illustrated schematically in Figures 1, 2, 4 and 7, the desalination plant serves as the primary heat sink for the reactor system. Shutdown of the desalination plant, either for scheduled maintenance or as a result of an accident, will result in the complete loss of normal heat removal capability. Loss of heat sink accident analyses and provisions for reactor shutdown and emergency heat removal capability are included in nuclear plant design.
- **Loss of load:** For thermal, electrical/thermal and electrical couplings such as those illustrated schematically in Figures 3, 5 and 7, the normal heat removal function of the condenser is not affected by shutdown of the desalination plant. However, the sudden cessation of demand for electricity in RO systems (or in MSF systems, which may have nearly as high a pumping power requirement as an RO system, and to a lesser extent in MED systems) creates a loss of electrical load. In thermal plants based on steam extraction, the sudden cessation of a requirement for steam may create thermal transients in the secondary circuit similar to those resulting from a loss of electrical load. The loss of load is a transient that is catered for in the design and analysis of a nuclear plant.
- **Steam line break:** For thermal couplings based on steam extraction, such as those illustrated schematically in Figure 3, there is a potential for partial or complete breakage in the steam extraction piping. Such a transient could be expected to be similar to the steam line break accident considered in the nuclear plant design.

3.2.2. Operational transients

In addition to the anticipated operational transients normally considered in the design of a nuclear power plant, the addition of a desalination plant to the facility may introduce additional transient effects that need to be considered. Operational transients in the desalination plant could have a direct physical feedback into the reactor system. Such transients could have safety implications that would need to be assessed. Likewise, transients in the reactor could have an impact on operation of the desalination plant. (This is more likely to be an economic concern than a safety concern.)

In the case of a dual-purpose nuclear desalination plant, producing both electricity for the grid and heat for potable water production in a distillation plant, the turbines have to satisfy simultaneously the requirements of both systems. The power plant is the heat source for the desalination plant, and the desalination plant is the heat sink for the power plant. In this arrangement, the safety implications of balancing the energy needs of both plants must be assessed. Such an assessment must consider both base load operation and potential load follow scenarios involving fluctuations in demand for either or both products. In cases where the desalination plant represents a significant fraction of the load on the power plant, shutdown of either power plant or desalination plant for scheduled maintenance may interrupt

the operation of the other unit. Alternative heat sinks and/or alternative thermal energy supplies may need to be considered under these conditions, and any potential safety impact must be addressed.

In the case of an integrated facility in which feedwater to an RO system is taken from the condenser cooling water, as illustrated in Figure 5, the operational and physical interactions between the reactor and desalination plants are kept to a minimum. Shutdown of the reactor does not interrupt water production capability, if electrical energy can be drawn from the grid during that time, although it would affect the availability of RO feedwater preheat and accordingly influence the efficiency of water production. Shutdown of the desalination plant does not compromise the heat sink for the reactor as long as the discharge stream can be set to bypass the RO system.

While operational transients are not expected to pose a significant safety concern, they must nevertheless be considered in the safety analyses.

3.3. Water quality and monitoring

The limits for discharge of radioactivity to the environment are normally specified by national regulatory bodies, often based on internationally agreed values. Brine discharges, cooling water discharges and product water must be evaluated with respect to possible radionuclide contamination. The quantities of radioactivity allowable in the product water or in the heat distribution circuits for other heat utilization applications may depend upon the usage of the water. The allowable limit, for example, in a district heating system may be higher than that in a system producing drinking water.

For nuclear desalination, the target is to comply with national and international (e.g. World Health Organization) drinking water standards based on state of the art technology and the ALARA[3] principle. The value may be so low that continuously monitoring the distribution stream at this value is not technically possible. In this case, state of the art continuous radiation monitoring close to the limit of detectability could be utilized to shut down the process before radiologically significant quantities of water have been released. Monitoring at other locations may also be considered, for example in an intermediate loop, where the concentration of contaminates may be higher during a malfunction.

While continuous monitoring in the product stream may be difficult because of sensitivity limitations, supplemental periodic batch monitoring will usually be possible for radionuclides with low detectability thresholds. To allow for batch monitoring, the product water may need to be collected in storage tanks or reservoirs prior to its release to the distribution system. The hold up time must be sufficient to enable completion of monitoring before certifying that the product water is safe for public distribution.

Radiological limits for drinking water are available in some national regulations and international guide publications. However, due to the advances in Radiological Protection technology over the years, the existing limits may no longer be generally considered acceptable and it may be necessary to re-evaluate proposed limits.

[3] As low as reasonably achievable, social and economic consequences taken into account.

3.4. Availability of product water

Since the supply of fresh water (or of heating fluid) to the population cannot be interrupted except for very short time periods, the plant design has to provide alternative means to assure the continuity of the service, while preventing any constraint on the operation of the nuclear plant. To achieve a high availability[4] target, the discrepancy between the potential availability of the reactor and the desalination plant must be addressed by adopting appropriate design solutions (i.e. redundancy, water storage reservoirs, backup energy supply). Notwithstanding the existence of such provisions, from a safety perspective the operating procedures for the nuclear reactor and the desalination plant must anticipate both programmed maintenance shutdowns and unforeseen shutdowns requiring timely execution of inspections, tests and repairs.

There is one additional safety concern that must be addressed as a result of this discrepancy in availability between the nuclear plant and desalination plant. Because of the serious consequences of an interruption in water supply, there may be implied pressures on the operators of a nuclear desalination plant to keep the reactor operating under conditions that would not normally be considered acceptable in order to maintain water production capability. This pressure must be resisted, and plant management must ensure that a safety culture exists within the plant that places safety clearly above production capability. The availability of alternate sources of thermal or electrical energy to allow continued production when the reactor is shut down would help reduce this concern.

3.5. Siting and the proximity of population centres

As in the case of coupling, in general the siting issues of a reactor intended for desalination or other heat utilization applications are very similar to those of reactors for other uses. However, isolation from population centres is often preferable for a nuclear plant whereas proximity to population centres is an advantage for desalination plants from the point of view of water supply planning. There may be situations in which the design specification requires the location of the plant close to a populated zone (non-remote siting). This may occur, for example, if transportation costs[5] for water are deemed excessive, or in the case of reactors for district heating, where non-remote siting is intrinsic in their concept given the high costs of transporting hot water or steam over long distances [1]. Balancing these two competing factors is an essential element in the overall water and energy supply planning for a country.

In cases where the possibility of non-remote siting is specified, this must be taken into account in emergency planning. It may be necessary that the design assure that no planned evacuation be needed in order to prevent unacceptable health consequences for the population in case of design basis accidents, or even in the case of postulated beyond design basis events. Such increased safety requirements could compensate for the combined effect of proximity to a population center and of uncertainties in safety evaluations. Indeed, such requirements may be necessary in the case of quasi-urban siting, where population evacuation may not be practicable as a further defence against unexpected situations. Even in cases where it can be

[4] Experience with the operation of desalination plants has shown that availabilities in excess of 95% are frequently achieved. Nuclear plants are more likely to have an availability in the order of 80-85%.

[5] An estimate of transportation cost made for IAEA by an engineering firm indicates a cost of about 0.10–0.15 US $/m^3 for a 20 km distance. This point is discussed in more detail in IAEA-TECDOC-898.

demonstrated that non-remote siting is acceptable, off site emergency plans should not be dismissed.

As an additional measure, the safety aspects being enforced at every stage of the nuclear desalination project should be made apparent to the general public so that product acceptability by the public is ensured.

3.6. Licensing

There are a number of prerequisites that have been generally accepted as being essential for the safe utilization of nuclear power [2]. These include:

- A legislative and statutory framework for the regulation of nuclear facilities.
- A Regulatory Body that is independent of the organization or bodies charged with the promotion or utilisation of nuclear energy.
- The Regulatory Body should have responsibility for assessment, authorization (licensing), inspection and enforcement and adequate authority, competence and resources to discharge the same responsibilities; no other responsibility of the Regulatory Body should conflict with its responsibility for regulating safety.
- A clear separation of responsibilities between the Regulatory Body and the operating organisation or other interested organizations.
- Adequate provisions for the safe management of radioactive wastes.
- Governmental and non-governmental emergency response capabilities.
- Adequate physical protection arrangements.
- Technological infrastructure and financial means necessary to support the safety of facilities and radiation-related activities.
- A well-developed nuclear safety culture in all of the organizations involved in design, construction, operation and maintenance of the nuclear plant.

These basic requirements need to be established well in advance of constructing any nuclear facility and will need considerable resource commitment from any country presently not having a nuclear power plant.

In many cases, nuclear desalination plants or nuclear heat utilisation plants may be proposed for countries with very little experience with nuclear technology and in particular with nuclear safety. The creation of the necessary infrastructure requires time, human resources and long training.

There are a large number of new designs that have been proposed for small or medium size reactors and although they are mainly based on existing proven technology, they include innovative solutions and systems which require a careful safety evaluation, safety review and demonstration of licensability that in some cases can not be done by operator or local licensing authority because of lack of experience or capability.

Licensing of nuclear power plants involves considerable effort, expertise and good communication between the nuclear authority, the plant operator and other national authorities. In the case of nuclear desalination this will involve additional interactions dealing specifically with the authorities responsible water use. A joint effort and coordination is envisaged between the designer, the utility and the various national authorities.

4. A SYSTEMATIC APPROACH TO THE IDENTIFICATION OF COMPREHENSIVE REQUIREMENTS APPLICABLE TO A SPECIFIC NUCLEAR INSTALLATION

4.1. The hierarchical, or "top-down" approach

The main objective of this section is to describe a systematic approach to the identification of a comprehensive set of site/country specific requirements for the design and review of nuclear desalination installations that will be acceptable to both the plant designer and the national nuclear safety regulatory body. This description is based on the assumption that the national nuclear safety regulatory infrastructure for nuclear power plants in the country in which the plant is to be built and operated is (or will be, when implemented) in general accord with the Safety Standard Series (SSS) published by the IAEA. While the discussion that follows refers primarily to nuclear desalination facilities, it is also applicable to other nuclear heat utilization applications, or in general to other nuclear installations for which the provisions of the SSS for nuclear power plants need to be amended or augmented.

As discussed in Section 2, a hierarchical set of publications called the Safety Standards Series, consisting of Safety Fundamentals, Safety Requirements and Safety Guides, is published and promulgated by the IAEA for nuclear power plants. There is a general international consensus that the SSS represents an acceptable and comprehensive basis for the safe design, construction, operation and decommissioning of nuclear power plants. The discussion which follows is focused primarily on the design phase, but in general can be extended to encompass other phases in the life cycle of a nuclear plant.

As suggested in Section 2, the overall safety of a nuclear desalination installation will be primarily a function of the nuclear power plant itself. The application of the IAEA Safety Standards Series and the application of national licensing requirements to a site/country specific design will in most cases be obvious and appropriate.

The safety philosophy prevalent in most countries is one in which **the responsibility for safety of a nuclear installation lies solely with the owner/operator** of that facility. It is the responsibility of the national regulatory authority, acting on behalf of the public, to:

- Set standards for the protection of individuals, society and the environment.
- Establish acceptance criteria by which it can be determined whether these standards have been met.
- Carry out an independent assessment and make an independent judgement as to whether the owner/operator has adequately satisfied its obligation for safety.

Within the framework of this licensing philosophy, the nuclear desalination system designer, acting on behalf of the owner/operator, must articulate a set of project specific design requirements based on the national regulatory requirements for nuclear installations. These requirements, when agreed upon with the regulatory authority, constitute the safety design basis for the project and form the licensing basis on which a construction permit and operating licence are to be granted. In establishing these safety design requirements, it is the responsibility of the designer to determine whether there are any unique design features or operating characteristics of the specific nuclear desalination project that may require amendment to or augmentation of internationally accepted and/or nationally mandated safety or licensing requirements.

The need for some flexibility in the application of requirements to cover design configurations or operating conditions not specifically addressed is acknowledged in the IAEA safety standards. The standards for nuclear power plant design [3] and research reactor design [4] note, respectively, that:

> "It is recognised that in the case of … innovative developments … some of the requirements may not be applicable, or may need some judgment to be made in their interpretation."
> "…may require additional safety measures and the use of (other) codes … may be more appropriate for a number of aspects. No specifications for such a transition to other codes are presented. These specifications should be agreed upon between the regulatory body and the operating organization and should be acceptable to the former."

The systematic identification of a comprehensive set of safety design and licensing basis requirements applicable to a site/country specific nuclear installation can be achieved by a hierarchical "top-down" review and consideration of existing safety fundamentals, safety requirements and safety guides. Having been identified by the designer and adopted by the owner/operator as the basis for achieving a safe design, these safety design and licensing basis requirements must be found acceptable to the national nuclear safety regulatory body.

4.2. Guidelines for implementing a hierarchical, top-down approach to the systematic identification of a comprehensive set of safety requirements

The international and national safety requirements specified by the Safety Standards Series and by national regulatory documentation create a general framework for the design and assessment activities that will be required to meet the overall safety objectives for a nuclear desalination project. However, there is a considerable degree of interpretation necessary to translate these requirements into safety design requirements applicable to a specific project. It is in the implementation of this interpretative process that a hierarchical, top-down approach to the systematic identification of a comprehensive set of project specific safety design and licensing basis requirements can be taken.

4.2.1. The hierarchical, top-down approach as an iterative process

In order to be effective in identifying the safety design and licensing basis requirements that must be met in order for a design to satisfy the safety objectives described in Section 2.1.1, the approach taken to identify these requirements must:

- Be **systematic**[6] — it must be an approach that can be applied uniformly to all nuclear desalination installations (or other nuclear installations) under consideration.
- Result in a **comprehensive**[7] set of requirements — the framework of requirements must be sufficiently complete to cover all eventualities that can be conceived of at the time the requirements are established, and must be sufficiently broad so that new requirements identified at a later time can be readily incorporated into the existing framework. These "tests" for a systematic and comprehensive approach can be

[6] The Merriam Webster WWW Dictionary defines **systematic** as **"**methodical in procedure or plan" **"**marked by thoroughness and regularity".
[7] The Merriam Webster WWW Dictionary defines **comprehensive** as "covering completely or broadly".

satisfied through the application of an iterative process that includes the following basic steps:

- A hierarchical set of formalized requirements applicable in general to all nuclear installations is adopted. The SSS, with its hierarchy of Safety Fundamentals, Safety Requirements and Safety Guides can serve as an appropriate starting point.
- The system performance characteristics and other externally imposed requirements are established.
- A preliminary selection of technologies for the nuclear desalination system is made. This includes the preferred (or proposed) desalination technology, reactor technology and approach to coupling these two technologies.
- Detailed (but still preliminary) design features and performance characteristics of the preferred/proposed nuclear desalination facility are established by preliminary system design, performance analyses and safety analyses.
- A "top-down" review with respect to the hierarchy of requirements is carried out to identify potential conflicts with the detailed design features and performance characteristics of the preferred/proposed design:
  - The strategy of defence in depth is used during all process as a general tool for the assessment of the significance of each requirement. Table I summarizes the main concepts of defence in depth, the necessary design response and the assumptions and acceptance criteria for the safety assessment.
  - At the highest level, Safety Fundamentals are adopted that must be satisfied by the proposed design. If any of the safety fundamentals cannot be satisfied, design modifications must be introduced.
  - At the next lower tier, the design is assessed against established Safety Requirements. If any conflicts between the proposed design and established requirements are identified alternatives must be explored. This can include design modifications which allow the established requirements to be satisfied and/or amended/augmented requirements which can be shown to satisfy the intent of the Safety Fundamentals when the specific design features or operating characteristics of the proposed design are taken into consideration.
  - The next lower tier, at the level of Safety Guides, can be explored to help identify potential alternative solutions to conflicts between established requirements and the proposed design.
- This hierarchical review is repeated, as necessary, until all conflicts between established requirements and the proposed design configuration have been identified and resolved. The resolution of these conflicts will have resulted in the identification of a set of project specific safety design guides that is fully consistent with the Safety Fundamentals and with the identification of specific design features that satisfy the project specific safety design requirements.
- As a final step in this process, the designer/owner/operator must obtain agreement with the national regulatory authority. This, too, may be an iterative process. The final set of agreed upon safety design requirements serves as the licensing basis for the project.

TABLE I. IMPLEMENTATION OF DEFENCE IN DEPTH FOR FUTURE NPP DESIGN AND SAFETY ASSESSMENT
(basic table extracted from TECDOC-986, changes in italics)

Levels of defence in depth	Objective	Essential means	Category of representative events	Design response		Plant safety assessment	
				Systems/features	Design criteria	Assumptions and methods	Main acceptance criteria/ targets
1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Normal operation, *including operational transients induced by the coupling*	Operational features incl. control, surveillance features *specific for product water*	• Operational conditions • Robustness, design margins to meet all standards • High reliability *and availability*	• Best estimate methods and data wherever possible •Conservative assumptions as necessary to address uncertainties	• Operational radiological limits • Safety Operating Limits • *Radioactivity limits in potable water*
2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Anticipated operational occurrences (expected in the lifetime of the plant) *including those induced by the coupling*	• Reactor protection system • Engineered safety features • *Effective defences achieving the containment function*	• Redundancy (single failure) • Protection against specified internal/external hazards • Test-friendly • Qualification • Design margins • *Inspection, maintenance and repair* • *Functional independence*	• Bounding assumptions • Single failure criteria • Credit for safety-related equipment only	• Effectiveness/integrity of all barriers for confinement of radioactive material
3	Control of accidents within the design basis	Engineered safety features and accident procedures	Design basis accidents (not expected in the lifetime of the plant) *including those induced by the coupling*				• Minor radiological consequences • Effectiveness of at least one barrier for confinement of radioactive material
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents *See introductory remarks on "selected severe accidents" in Annex II.*	Complementary measures and accident management	*Combination of failures* without severe core damage *See introductory remarks on "selected severe accidents" in Annex II.*	Additional or diverse features for core damage prevention	• Functional independence • Survivability	• Best estimate (e.g. in-vessel and ex-vessel analysis, source terms, containment response, meteorology)	• Core damage frequency $< 10^{-5}a^{-1}$ (target**)
			Combination of failures with severe core damage *See introductory remarks on "selected severe accidents" in Annex II.*	*Effective defences achieving the containment function. Measures for accident management also including permanent features or temporary hardware connections*			• Frequency of large offsite release $< 10^{-6}a^{-1}$ (target**) • Other national criteria
5	Mitigation of radiological consequences of significant releases of radioactive materials	Offsite emergency response *without evacuation*	NA	NA	NA	NA	NA

**Targets according to INSAG 3 and TECDOC 801. *The figures calculated by the designers are significantly lower.*

4.2.2. Preliminary selection of technologies for the nuclear desalination installation

A wide range of possibilities can be considered in the selection of nuclear desalination plant technologies and their associated coupling configurations. As noted above, it is nevertheless considered necessary to have made a preliminary selection of technologies for these installations in order to establish project specific safety design requirements. Examples of the type of technical factors that must be considered include:

- Analysis of possible nuclear energy sources. (A review of the various proposals for nuclear desalination installations will provide an indication of the type and size of nuclear plants being considered as energy sources for desalination. An examination of the engineering features for the coupling with the desalination plant will provide additional information on possible transient feedback. External constraints on the water demand, such as for example the requested plant availability, will be considered to assess the potential of the current design to satisfy these requirements. The time delays available for various abnormal situations, the possibilities for on-line maintenance, and the duration of the programmed maintenance shutdowns shall be assessed to identify items that will require specific guidelines. The risk of product water contamination and the technological solutions that could be implemented will be reviewed to identify the "abnormal conditions" that shall be taken into account during the plant design..
- The nuclear plant "boundary conditions" (i.e. the use of the reactor for desalination or other heat utilization applications; whether the plant is intended as a single purpose or dual purpose plant; the coupling characteristics between the nuclear and conventional parts of the installation; the siting characteristics; etc.).
- Analysis of the desalination process and identification of the coupling parameters (The different process are reviewed to identify the parameters that characterise the interface with the nuclear installation. The plausible process transients are analysed to define the conditions that shall be taken into account, such as external PIEs[8], in the nuclear plant safety assessment. The possible sharing of plant resources such as control room and seawater intake/outfall structures shall also be identified and the related risks evaluated. The potential drawbacks due to the interaction with the environment due to effects such as heat pollution and brine discharge will also be assessed).

4.2.3. Review of the proposed design in relation to Safety Fundamentals for nuclear **p***ower plants*

As noted in Section 2.1.1, Safety Fundamentals are at the highest level in the safety hierarchy and their purpose is to *present basic objectives, concepts and principles to ensure safety* in the development and application of nuclear energy for peaceful purposes. The hierarchical, top-down review of a proposed design must start at this level. Any design feature that precludes the design from satisfying the Safety Fundamentals must be revised.

4.2.4. Review of the proposed design in relation to Safety Requirements for nuclear power plants

The second tier of review is at the Safety Requirements level. The process outlined above is intended to provide a framework within which that review can be carried out in order

[8] Postulated initiating events.

to identify project specific requirements that may be needed in addition to (or instead of) those for facilities that fit the traditional classification of "nuclear power plant". There may also be requirements for the nuclear desalination plant that can be less stringent than those of the SSS for nuclear power plants due to specific features of the proposed design that allow the Safety Fundamentals to be satisfied in an alternative manner. For example, there may be design characteristics that are similar to those of "research reactors", for which requirements applicable to such reactors could be considered.

4.2.5. Project specific safety design and licensing basis requirements

The hierarchical, top-down approach allows the systematic specification of a comprehensive set of project specific safety design and licensing basis requirements and guidelines based on currently available international and national standards. These requirements and guidelines can be tailored to meet the particular needs of specific nuclear installations intended for desalination, district heating or other heat utilization applications. When agreed upon with the nuclear safety regulatory authority, they provide the basis on which the detailed nuclear desalination system design can proceed. They also form the basis for an independent safety review by the regulatory authority, allowing the necessary licensing decisions to be made in support of the issuance of the construction permit and operating licence.

4.2.6. Exercise of application of the top-down methodology for the preparation of the Safety Requirements

Two reactors with quite different technical characteristics and features were selected for a preliminary exercise of application of the methodology for the preparation of dedicated safety requirements.

The first reactor was the NHR-10 [5, 6] proposed by China and the second was the Pebble Bed Modular Reactor (PBMR) [7] under development in South Africa. The main characteristics of these reactors are presented below.

1) NHR-10
Thermal power: 10 MW
Fuel: PWR fuel type
Moderator: light water
Coolant: light water in natural circulation
Operating pressure: 15–25 bars
In vessel heat exchangers
Primary vessel enveloped by a secondary vessel designed for the full accident pressure
Long grace period
Passive decay heat removal

2) PBMR
Thermal power: 300 MW
Fuel: coated particles TRISO type
Moderator: graphite
Coolant: helium
Operating pressure: 70 bars

Direct cooling cycle (no steam generators) Bryton type
The fuel can retain fission product up to a very high temperature (~1600°C)
Long grace period
Passive decay heat removal

The results of a critical examination of the existing requirements for NPPs for these two reactors in the frame of the defence in depth strategy are presented in Annex I.

5. CONCLUSIONS

The safety concerns and related regulatory implications of reactors used for nuclear desalination, district heating or other heat utilization applications are generally the same as those of other nuclear power plants. As such, the body of existing IAEA standards and guides contain requirements that are generally applicable to these plants. However, in particular cases the specific characteristics and intended application of these plants may allow the application project specific safety design standards that differ in some respects from the nuclear power plant standards on which they are based. In such cases, a logical unified approach must be applied to the systematic identification of a comprehensive set of safety design requirements. A hierarchical, top-down approach can be applied to develop of the project specific guides and criteria for the design and operation of these reactors.

Nuclear desalination installations consist of a reactor and a co-located desalination system coupled to the reactor in one of variety of ways, and sharing a number of common systems and facilities. The choice of desalination technology determines the manner in which the desalination plant is coupled with the reactor. This coupling between the reactor and desalination plant introduces a number of safety related considerations, including:

- In the case of distillation plants, the coupling between the heat source and the product water is made via heat transfer circuits, creating a potential for transfer of radioactivity to the product loop.
- For RO plants sharing common structures or facilities, or drawing preheated feedwater from the condenser cooling water discharge, the coupling is much less direct but must, nevertheless, be considered.
- The limits and measurement criteria for radioactivity in the product water should be set by national authorities, possibly using international guidance.
- The effect of possible transients introduced by the desalination plant, both as a result of normal operation and during accident scenarios, should be taken into account during the reactor design process.
- Because of the generally high availability of desalination plants, special provisions may be required to ensure continuity of water supply during planned or unplanned reactor outages.
- **W**ith respect to the siting of reactors for desalination, district heating or other heat utilization applications, there may be design or economic factors that lead to a decision to locate the plant near urban populations. in the event of such non-remote siting, there may be safety implications that impose limitations on the reactor design, or that affect emergency planning, particularly if planned evacuation of the population is not practicable.

REFERENCES

[1] SCHMOCKER, U., GILLI, R., Safety goals and design criteria for small heating reactors, Nuclear Engineering and Design **118** (1990) 17–20.

[2] CARNINO, A., GASPARINI, M., Safety Aspects of the Desalination of Seawater using Nuclear Energy, in Nuclear Desalination of Seawater (Proc. Symp. on Desalination of Seawater with Nuclear Energy, Taejon, 1997), IAEA, Vienna (1997).

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

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Research Reactors: Design, Safety Series No. 35-S1, Vienna (1992).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Design and Development Status of Small and Medium Reactor Systems 1995, IAEA-TECDOC-881, Vienna (1996).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Approaches for Heating Reactors, IAEA-TECDOC-965, Vienna (1997).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Current status and Future Development of Modular High Temperature Gas Cooled Reactor Technology, IAEA-TECDOC-1198, Vienna (2001).

Annex 1

EXAMPLE OF THE APPLICATION OF THE GENERAL METHODOLOGY FOR THE IDENTIFICATION OF COMPREHENSIVE REQUIREMENTS APPLICABLE TO THE DESIGN OF SPECIFIC NUCLEAR PLANTS

The following table below provides an example of the application of the general methodology for the identification of comprehensive requirements applicable to the design of specific nuclear plants. The requirements presented the left column are extracted from the draft Safety Standards Series on The Safety of Nuclear Power Plants: Design. The right column presents examples of how these requirements might be applied to the two specific cases of the PBMR and the NHR-10, which are innovative new designs being considered for nuclear desalination. These are only to be taken as an example of the application of a systematic review process, and not as a statement of acceptable criteria for these reactors. Where no comment is given in the right column, the corresponding SSS requirement is considered to be applicable without modification or special interpretation.

The Safety fundamentals given in IAEA Safety Series No. 110, The Safety of Nuclear Installations, have also been reviewed. The comments provided below are considered to be fully consistent with the provisions of that publication.

Interpretation of "selected severe accidents"

For the two reactors used in the example below, the designers have stated that severe accidents are not applicable, as they are defined by the IAEA safety publications. Nevertheless, the general principle that there are "bounding accidents" that must be considered remains valid, even in innovative new reactor designs. The detailed analysis and consideration of such accidents provides information to assist in the safety design for such reactors, and helps to assure the appropriate application of the defence in depth principle so that there are several levels of protection and multiple barriers to prevent releases of radioactive materials and to ensure that failures or combinations of failures that might lead to significant radiological consequences are of very low probability. The wording "selected severe accidents" has not been modified in the comments that follow, but should be understood to be taken within the framework of this context.

Safety of Nuclear Power Plants: Design, SSS No. NS-R-1	Comments on the applicability to NHR-10 and PBMR
INTRODUCTION	
BACKGROUND	
1.1. The present publication supersedes the Code on the Safety of Nuclear Power Plants: Design (Safety Series No. 50-C-D (Rev. 1), issued in 1988). It takes account of developments relating to the safety of nuclear power plants since the Code on Design was last revised. These developments include the issuing of the Safety Fundamentals publication, The Safety of Nuclear Installations [1], and the present revision of various safety standards and other publications relating to safety. Requirements for nuclear safety are intended to ensure adequate protection of site personnel, the public and the environment from the effects of ionizing radiation arising from nuclear power plants. It is recognized that technology and scientific knowledge advance, and nuclear safety and what is considered adequate protection are not static entities. Safety requirements change with these developments and this publication reflects the present consensus.	
OBJECTIVE	
1.2. This Safety Requirements publication takes account of the developments in safety requirements by, for example, including the consideration of severe accidents in the design process. Other topics that have been given more detailed attention include management of safety, design management, plant ageing and wearing out effects, computer based safety systems, external and internal hazards, human factors, feedback of operational experience, and safety assessment and verification.	
1.3. This publication establishes safety requirements that define the elements necessary to ensure nuclear safety. These requirements are applicable to safety functions and the associated structures, systems and components, as well as to procedures important to safety in nuclear power plants. It is expected that this publication will be used primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). It is recognized that in the case of other reactor types, including innovative developments in future systems, some of the requirements may not be applicable, or may need some judgement in their interpretation. Various Safety Guides will provide guidance in the interpretation and implementation of these requirements.	
1.4. This publication is intended for use by organizations designing, manufacturing, constructing and operating nuclear power plants as well as by regulatory bodies.	
SCOPE	
1.5. This publication establishes design requirements for structures, systems and components important to safety that must be met for safe operation of a nuclear power plant, and for preventing or mitigating the consequences of events that could jeopardize safety. It also establishes requirements for a comprehensive safety assessment, which is carried out in order to identify the potential hazards that may arise from the operation of the plant, under the various plant states (operational states and accident conditions). The safety assessment process includes the complementary techniques of deterministic safety analysis and probabilistic safety analysis. These analyses necessitate consideration of postulated initiating events (PIEs) which include many factors that, singly or in combination, may affect safety and which may:	
originate in the operation of the nuclear power plant itself;	
be caused by human action; and	
be directly related to the nuclear power plant and its environment.	

1.6. This publication also addresses events that are very unlikely to occur, such as severe accidents that may result in major radioactive releases, and for which it may be appropriate and practicable to provide preventive or mitigatory features in the design.	
1.7. This publication does not address:	
external natural or human induced events that are extremely unlikely (such as the impact of a meteorite or an artificial satellite);	
conventional industrial accidents that under no circumstances could affect the safety of the nuclear power plant; or	
non-radiological effects arising from the operation of nuclear power plants, which may be subject to separate national regulatory requirements.	
STRUCTURE	
1.8. This Safety Requirements publication follows the relationship between principles and objectives for safety, and safety requirements and criteria. Section 2 elaborates on the safety principles, objectives and concepts which form the basis for deriving the safety requirements that must be met in the design of the plant. The safety objectives (in italics in Section 2) are reproduced from the Safety Fundamentals publication, The Safety of Nuclear Installations [1].	
Section 3 covers the principal requirements to be applied by the design organization in the management of the design process, and also requirements for safety assessment, for quality assurance and for the use of proven engineering practices and operational experience.	
Section 4 provides the principal and more general technical requirements for defence in depth and radiation protection.	
Section 5 provides general plant design requirements which supplement the principal requirements to ensure that the safety objectives are met.	
Section 6 provides design requirements applicable to specific plant systems, such as the reactor core, coolant systems and containment systems.	
Appendix I elaborates on the definition of and application of the concept of a postulated initiating event. Appendix II discusses the application of redundancy, diversity and independence as measures to enhance reliability and to protect against common cause failures. The Annex elaborates on safety functions for reactors.	
SAFETY OBJECTIVES AND CONCEPTS	
SAFETY OBJECTIVES	
2.1. The Safety Fundamentals publication, The Safety of Nuclear Installations [1], presents three fundamental safety objectives, upon the basis of which the requirements for minimizing the risks associated with nuclear power plants are derived. The following paras 2.2–2.6 are reproduced directly from The Safety of Nuclear Installations, paras 203–207.	
2.2. **"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.*	
2.3. "This General Nuclear Safety Objective is supported by two complementary Safety Objectives dealing with radiation protection and technical aspects. They are interdependent: the technical aspects in conjunction with administrative and procedural measures ensure defence against hazards due to ionizing radiation.	
2.4. **"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.*	Radiological limits for drinking water are available in some national regulations and international guide documents. However, due to the advances in Radiological Protection technology over the years, the existing limits may no longer be

	generally considered acceptable and it may be necessary to re-evaluate proposed limits. Separate limits may need to be defined for water production and district heating. See Annex IV for additional information on the prevention of radioactive contamination of product water.
2.5. "**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 physical coupling of desalination systems to nuclear facilities will introduce specific, possibly unique, considerations that must be addressed.
2.6. "Safety Objectives require that nuclear installations are designed and operated so as to keep all sources of radiation exposure under strict technical and administrative control. However, the Radiation Protection Objective does not preclude limited exposure of people or the release of legally authorized quantities of radioactive materials to the environment from installations in operational states. Such exposures and releases, however, must be strictly controlled and must be in compliance with operational limits and radiation protection standards."	While continuous monitoring in the product stream may be difficult because of sensitivity limitations, supplemental periodic batch monitoring will usually be possible for radionuclides with low detectability thresholds. To allow for batch monitoring, the product water may need to be collected in storage tanks or reservoirs for a brief period prior to its release to the distribution system. The hold up time must be sufficient to enable completion of monitoring before certifying that the product water is safe for public distribution.
2.7. In order to achieve these three safety objectives, in the design of a nuclear power plant, a comprehensive safety analysis is carried out to identify all sources of exposure and to evaluate radiation doses that could be received by workers at the installation and the public, as well as potential effects on the environment (see para. 4.9). The safety analysis examines: (1) all planned normal operational modes of the plant; (2) plant performance in anticipated operational occurrences; (3) design basis accidents; and (4) event sequences that may lead to a severe accident. On the basis of this analysis, the robustness of the engineering design in withstanding postulated initiating events and accidents can be established, the effectiveness of the safety systems and safety related items or systems can be demonstrated, and requirements for emergency response can be established.	No transients more severe than those usually addressed in the reactor design process are expected to occur as a result of the addition of a desalination (or other heat utilization) plant to the facility. Nevertheless, transients in the desalination plant, either during normal operation or as a result of an accident scenario, could result in the feedback of transients to the reactor system. While these transients are not expected to be more constraining than those normally postulated, they must nevertheless be taken into account during the reactor design process. The number and severity of such transients must be assessed during the design and discussed within the safety report. In the unlikely event of such a transient having a potential safety impact greater than that normally anticipated in the nuclear plant, specific provisions must be included in the design to accommodate it.

2.8. Although measures are taken to control radiation exposure in all operational states to levels as low as reasonably achievable (ALARA) and to minimize the likelihood of an accident that could lead to the loss of normal control of the source of radiation, there is a residual probability that an accident may happen. Measures are therefore taken to ensure that the radiological consequences are mitigated. Such measures include: engineered safety features; on-site accident management procedures established by the operating organization; and possibly off-site intervention measures established by appropriate authorities in order to mitigate radiation exposure if an accident has occurred. The design for safety of a nuclear power plant applies the principle that plant states that could result in high radiation doses or radioactive releases are of very low probability (likelihood) of occurrence, and plant states with significant probability (likelihood) of occurrence have only minor or no potential radiological consequences. An essential objective is that the need for external intervention measures may be limited or even eliminated in technical terms, although such measures may still be required by national authorities.	In cases where the possibility of non-remote siting is specified, this must be taken into account in emergency planning. It may be necessary that the design include provisions to assure that no planned evacuation be needed in order to prevent unacceptable health consequences for the population in case of postulated accidents. Such design features could compensate for the combined effect of proximity to a population centre and of uncertainties in safety evaluations. Indeed, such features may be necessary in the case of quasi-urban siting, where population evacuation may not be practicable as a further defence against unexpected situations. Even in cases where it can be demonstrated that non-remote siting is acceptable, off site emergency plans should not be dismissed. For the two reactors under consideration the claim is made that no need exists for planned evacuations. For NRH-10, a 250 meter non-residential area and a 2 km area of restricted development surrounding the site are planned.
THE CONCEPT OF DEFENCE IN DEPTH	
2.9. The concept of defence in depth, as applied to all safety activities, whether organizational, behavioural or design related, ensures that they are subject to overlapping provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. The concept has been further elaborated since 1988 [2, 3]. Application of the concept of defence in depth throughout design and operation provides a graded protection against a wide variety of transients, anticipated operational occurrences and accidents, including those resulting from equipment failure or human action within the plant, and events that originate outside the plant.	
2.10. Application of the concept of defence in depth in the design of a plant provides a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.	
The aim of the first level of defence is to prevent deviations from normal operation, and to prevent system failures. This leads to the requirement that the plant be soundly and conservatively designed, constructed, maintained and operated in accordance with appropriate quality levels and engineering practices, such as the application of redundancy, independence and diversity. To meet this objective, careful attention is paid to the selection of appropriate design codes and materials, and to the control of fabrication of components and of plant construction. Design options that can contribute to reducing the potential for internal hazards (e.g. controlling the response to a PIE), to reduce the consequences of a given PIE, or to reduce the likely release source term following an accident sequence contribute at this level of defence. Attention is also paid to the procedures involved in the design, fabrication, construction and in-service plant inspection, maintenance	

and testing, to the ease of access for these activities, to the way the plant is operated and to how operational experience is utilized. This whole process is supported by a detailed analysis which determines the operational and maintenance requirements for the plant.	
The aim of the second level of defence is to detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions. This is in recognition of the fact that some PIEs are likely to occur over the service lifetime of a nuclear power plant, despite the care taken to prevent them. This level necessitates the provision of specific systems as determined in the safety analysis and the definition of operating procedures to prevent or minimize damage from such PIEs.	In addition to the anticipated operational transients normally considered in the design of a nuclear power plant, the addition of a desalination plant to the facility may introduce additional transient effects that need to be considered. Operational transients in the desalination plant could have a direct physical feedback into the reactor system. Such transients could have safety implications that would need to be assessed. Likewise, transients in the reactor could have an impact on operation of the desalination plant.
For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or PIEs may not be arrested by a preceding level and a more serious event may develop. These unlikely events are anticipated in the design basis for the plant, and inherent safety features, fail-safe design, additional equipment and procedures are provided to control their consequences and to achieve stable and acceptable plant states following such events. This leads to the requirement that engineered safety features be provided that are capable of leading the plant first to a controlled state, and subsequently to a safe shutdown state, and maintaining at least one barrier for the confinement of radioactive material.	Examples of transients that must be considered include, but are not limited to, loss of that sink, loss of load and steam line break.
The aim of the fourth level of defence is to address severe accidents in which the design basis may be exceeded and to ensure that radioactive releases are kept as low as practicable. The most important objective of this level is the protection of the confinement function. This may be achieved by complementary measures and procedures to prevent accident progression, and by mitigation of the consequences of selected severe accidents, in addition to accident management procedures. The protection provided by the confinement may be demonstrated using best estimate methods.	For the two reactors under consideration the designers claim that severe accidents, as defined in IAEA safety publications, are not possible. There must be a strong and supportable justification put forward to substantiate such a claim. Nevertheless, the requirement is considered to be applicable, using a set of plant conditions appropriate to the specific designs. See also introductory remarks.
The fifth and final level of defence is aimed at mitigation of the radiological consequences of potential releases of radioactive materials that may result from accident conditions. This requires the provision of an adequately equipped emergency control centre, and plans for the on-site and off-site emergency response.	Refer to remarks on 209.
2.11. A relevant aspect of the implementation of defence in depth is the provision in the design of a series of physical barriers to confine the radioactive material at specified locations. The number of physical barriers that will be necessary will depend on the potential internal and external hazards, and the potential consequences of failures. The barriers may, typically for water cooled reactors, be in the form of the fuel matrix, the fuel cladding, the reactor coolant system pressure boundary and the containment.	For NHR-10 a guard vessel plus a concrete structure is recognized by the designer as providing the equivalent function as a conventional containment. The containment is intended to cope with a break in the reactor vessel bottom. For PBMR containment as usually defined in not considered necessary by the designers.

	For both reactors, when dealing with containment there may need to be different requirements derived due the unique nature of the containment systems for these plants. Refer also remarks on containment system requirement, 643-667.
REQUIREMENTS FOR MANAGEMENT OF SAFETY	
RESPONSIBILITIES IN MANAGEMENT	
3.1. The operating organization has overall responsibility for safety. However, all organizations engaged in activities important to safety have a responsibility to ensure that safety matters are given the highest priority. The design organization shall ensure that the installation is designed to meet the requirements of the operating organization, including any standardized utility requirements; that it takes account of the current state of art for safety; that it is in accordance with the design specifications and safety analysis; that it satisfies national regulatory requirements, that it fulfils the requirements of an effective quality assurance programme; and that the safety of any design change is properly considered. Thus, the design organization:	
shall implement safety policies established by the operating organization;	
shall have a clear division of responsibilities with corresponding lines of authority and communication;	
shall ensure that it has sufficient technically qualified and appropriately trained staff at all levels;	
shall establish clear interfaces between the groups engaged in different parts of the design, and between designers, utilities, suppliers, constructors and contractors as appropriate;	
shall develop and strictly adhere to sound procedures;	
shall review, monitor and audit all safety related design matters on a regular basis; and	
shall ensure that a safety culture is maintained.	
MANAGEMENT OF DESIGN	
3.2. The design management for a nuclear power plant shall ensure that the structures, systems and components important to safety have the appropriate characteristics, specifications and material composition so that the safety functions can be performed and the plant can operate safely with the necessary reliability for the full duration of its design life, with accident prevention and protection of site personnel, the public and the environment as prime objectives.	
3.3. The design management shall ensure that the requirements of the operating organization are met and that due account is taken of the human capabilities and limitations of personnel. The design organization shall supply adequate safety design information to ensure safe operation and maintenance of the plant and to allow subsequent plant modifications to be made, and recommended practices for incorporation into the plant administrative and operational procedures (i.e. operational limits and conditions).	
3.4. The design management shall take account of the results of the deterministic and complementary probabilistic safety analyses, so that an iterative process takes place by means of which it shall be ensured that due consideration has been given to the prevention of accidents and mitigation of their consequences.	
3.5. The design management shall ensure that the generation of radioactive waste is kept to the minimum practicable, in terms of both activity and volume, by appropriate design measures and operational and decommissioning practices.	

PROVEN ENGINEERING PRACTICES	
3.6. Wherever possible, structures, systems and components important to safety shall be: designed according to the latest or currently applicable approved standards; shall be of a design proven in previous equivalent applications; and shall be selected to be consistent with the plant reliability goals necessary for safety. Where codes and standards are used as design rules, they shall be identified and evaluated to determine their applicability, adequacy and sufficiency and shall be supplemented or modified as necessary to ensure that the final quality is commensurate with the necessary safety function.	For the NHR-10 and PBMR currently approved codes and standards need to be carefully reviewed to examine their applicablity. The unique characteristics of these reactors should be considered in stipulating the codes and standards to be invoked in the design and construction of the facilities.
3.7. Where an unproven design or feature is introduced or there is a departure from an established engineering practice, safety shall be demonstrated to be adequate by appropriate supporting research programmes, or by examination of operational experience from other relevant applications. The development shall also be adequately tested before being brought into service and monitored in service, to verify that the expected behaviour is achieved.	Both NHR-10 and PBMR include several innovative design features and unproven technology. The provisions of this requirement must be given careful consideration in their application to these reactor designs.
3.8. In the selection of equipment, consideration shall be given to both spurious operation and unsafe failure modes (e.g. failure to trip when necessary). Where failure of a structure, system or component has to be expected and accommodated by the design, preference shall be given to equipment that exhibits a predictable and revealed mode of failure and facilitates repair or replacement.	
OPERATIONAL EXPERIENCE AND SAFETY RESEARCH	
3.9. The design shall take due account of relevant operational experience that has been gained in operating plants and of the results of relevant research programmes.	
SAFETY ASSESSMENT	
3.10. A comprehensive safety assessment shall be carried out to confirm that the design as delivered for fabrication, as for construction and as built meets the safety requirements set out at the beginning of the design process.	
3.11. The safety assessment shall be part of the design process, with iteration between the design and confirmatory analytical activities, and increasing in the scope and level of detail as the design programme progresses.	
3.12. The basis for the safety assessment shall be data derived from the safety analysis, previous operational experience, results of supporting research and proven engineering practice.	The lack of data concerning the reliability of innovative passive safety systems affect the uncertainty of the figures given for such characteristics as core melt frequency.
INDEPENDENT VERIFICATION OF THE SAFETY ASSESSMENT	
3.13. 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.	
QUALITY ASSURANCE[1]	
A quality assurance programme that describes the overall arrangements for the management, performance and assessment of the plant design shall be prepared and implemented. This programme shall be supported by more detailed plans for each structure, system and component so that the quality of the design is ensured at all times.	
3.15. Design, including subsequent changes or safety improvements, shall be carried out in accordance with established procedures that call on appropriate engineering codes and standards, and shall incorporate	

[1] For further guidance, see Ref. [4].

applicable requirements and design bases. Design interfaces shall be identified and controlled.	
3.16. The adequacy of design, including design tools and design inputs and outputs, shall be verified or validated by individuals or groups separate from those who originally performed the work. Verification, validation and approval shall be completed before implementation of the detailed design.	
PRINCIPAL TECHNICAL REQUIREMENTS	
REQUIREMENTS FOR DEFENCE IN DEPTH	
4.1. In the design process, defence in depth shall be incorporated as described in Section 2. The design therefore:	
shall provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment;	
shall be conservative, and the construction shall be of high quality, so as to provide confidence that plant failures and deviations from normal operations are minimized and accidents prevented;	
shall provide for control of the plant behaviour during and following a PIE, using inherent and engineered features, i.e. uncontrolled transients shall be minimized or excluded by design to the extent possible;	
shall provide for supplementing control of the plant, by the use of automatic activation of safety systems in order to minimize operator actions in the early phase of PIEs and by operator actions;	
shall provide for equipment and procedures to control the course and limit the consequences of accidents as far as practicable; and	
shall provide multiple means for ensuring that each of the fundamental safety functions, i.e. control of the reactivity, heat removal and the confinement of radioactive materials is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any PIEs.	
4.2. To ensure that the overall safety concept of defence in depth is maintained, the design shall be such as to prevent as far as practicable:	
challenges to the integrity of physical barriers;	
failure of a barrier when challenged;	
failure of a barrier as a consequence of failure of another barrier.	For NHR-10 this requirement is particularly stringent since one of the key design features is that the guard vessel does not fail as a consequence of failure of the primary pressure vessel.
4.3. The design shall be such that the first, or at most the second, level of defence is capable of preventing escalation to accident conditions for all but the most improbable PIEs.	
4.4. The design shall take into account the fact that the existence of multiple levels of defence is not a sufficient basis for continued power operation in the absence of one level of defence. All levels of defence shall be available at all times, although some relaxations may be specified for the various operational modes other than power operation.	
SAFETY FUNCTIONS	
4.5. The objective of the safety approach shall be: to provide adequate means to maintain the plant in a normal operational state; to ensure the proper short term response immediately following a PIE; and to facilitate the management of the plant in and following any design basis accident, and following those plant states beyond the design basis that are considered.	
4.6. To ensure safety, the following fundamental safety functions shall be performed in operational states, in and following a design basis accident and, to the extent practicable, in and after the occurrence of plant states considered that are beyond those of the design basis accidents:	

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.	When considering a nuclear desalination facility, this requirement applies to release of radioactive materials from the desalination plant as well as from the nuclear plant. Discharge limits specific for allowed releases in potable water must be specified.
An example of a detailed subdivision of these three fundamental safety functions is given in the Annex.	
4.7. A systematic approach shall be followed to identify the structures, systems and components that are necessary to fulfil the safety functions at the various times following a PIE.	
ACCIDENT PREVENTION AND PLANT SAFETY CHARACTERISTICS	
4.8. The plant design shall be such that its sensitivity to PIEs is minimized. The expected plant response to any PIE shall be those of the following that can reasonably be achieved (in order of importance):	
(1) a PIE produces no significant safety related effect or produces only a change in the plant towards a safe condition by inherent characteristics; or	
(2) following a PIE, the plant is rendered safe by passive safety features or by the action of safety systems that are continuously operating in the state necessary to control the PIE; or	
(3) following a PIE, the plant is rendered safe by the action of safety systems that need to be brought into service in response to the PIE; or	
(4) following a PIE, the plant is rendered safe by specified procedural actions.	
RADIATION PROTECTION AND ACCEPTANCE CRITERIA	
4.9. In order to achieve the three safety objectives given in paras 2.2–2.5 in the design of a nuclear installation, all actual and potential sources of radiation shall be identified and properly considered, and provision shall be made to ensure that sources are kept under strict technical and administrative control.	Refer to remarks on 2.4 and 2.5
4.10. Measures shall be provided to ensure that the radiation protection and technical safety objectives as given in paras 2.4 and 2.5 are achieved, and that radiation doses to the public and to site personnel in all operational states, including maintenance and decommissioning, do not exceed prescribed limits and are as low as reasonably achievable.	Refer to remarks on 4.6
4.11. The design shall have as an objective the prevention or, if this fails, the mitigation of radiation exposures resulting from design basis accidents and selected severe accidents. Design provisions shall be made to ensure that potential radiation doses to the public and the site personnel do not exceed acceptable limits and are as low as reasonably achievable.	
4.12. Plant states that could potentially result in high radiation doses or radioactive releases shall be restricted to a very low likelihood of occurrence, and it shall be ensured that the potential radiological consequences of plant states with a significant likelihood of occurrence shall be only minor. Radiological acceptance criteria for the design of a nuclear power plant shall be specified on the basis of these requirements.	
4.13. There is usually a limited number of sets of radiological acceptance criteria, and it is common practice to associate these with categories of plant states. These categories generally include those for normal operation, anticipated operational occurrences, design basis accidents and severe accidents. The radiological acceptance criteria for	Concerning severe accidents, refer to the introductory remarks and remarks on 2.10 (4)

these categories shall, as a minimum level of safety, meet the requirements of the regulatory body.	
REQUIREMENTS FOR PLANT DESIGN	
SAFETY CLASSIFICATION	
5.1. All structures, systems and components, including software for instrumentation and control (I&C), that are items important to safety shall be first identified and then classified on the basis of their function and significance with regard to safety. They shall be designed, constructed and maintained such that their quality and reliability is commensurate with this classification.	
5.2. The method for classifying the safety significance of a structure, system or component shall primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgement, with account taken of factors such as:	
the safety function(s) to be performed by the item;	
the consequences of failure to perform their function;	
the probability that the item will be called upon to perform a safety function; and	
the time following a PIE at which, or the period throughout which, it will be called upon to operate.	
5.3. Appropriately designed interfaces shall be provided between structures, systems and components of different classes to ensure that any failure in a system classified in a lower class will not propagate to a system classified in a higher class.	
GENERAL DESIGN BASIS	
5.4. The design basis shall specify the necessary capabilities of the plant to cope with a specified range of operational states and design basis accidents within the defined radiological protection requirements. The design basis shall include the specification for normal operation, plant states created by the PIEs, the safety classification, important assumptions and, in some cases, the particular methods of analysis.	In nuclear desalination facilities there may be transients introduced by the desalination plant that must be considered in the plant design. Refer to remarks in 2.10 (3).
5.5. Conservative design measures shall be applied and sound engineering practices shall be adhered to in the design bases for normal operation, anticipated operational occurrences and design basis accidents so as to provide a high degree of assurance that no significant damage will occur to the reactor core and that radiation doses will remain within prescribed limits and will be ALARA.	Refer to remarks on 2.10 (3).
5.6. In addition to the design basis, the performance of the plant in specified accidents beyond the design basis, including selected severe accidents, shall also be addressed in the design. The assumptions and methods used for these evaluations may be on a best estimate basis.	
Categories of plant states	
The plant states shall be identified and grouped into a limited number of categories according to their probability of occurrence. The categories typically cover normal operation, anticipated operational occurrences, design basis accidents and severe accidents. Acceptance criteria shall be assigned to each category that take account of the requirement that frequent PIEs shall have only minor or no radiological consequences, and that events that may result in severe consequences shall be of very low probability.	Concerning severe accidents, refer to the introductory remarks and remarks on 2.10(4).
Postulated initiating events	
5.8. In the design of the plant, it shall be recognized that challenges to all levels of defence in depth may occur and design measures shall be provided to ensure that the necessary safety functions are accomplished and the safety objectives can be met. These challenges stem from the PIEs, which are selected on the basis of deterministic or probabilistic techniques or a combination of the two. Independent events, each having a low probability, are normally not anticipated in the design to occur simultaneously.	

Internal events	
5.9. An analysis of the PIEs (see Appendix I) shall be made to establish all those internal events which may affect the safety of the plant. These events may include equipment failures or maloperation.	
Fires and explosions	
5.10. Structures, systems and components important to safety shall be designed and located so as to minimize, consistent with other safety requirements, the probabilities and effects of fires and explosions caused by external or internal events. The capability for shutdown, residual heat removal, confinement of radioactive material and monitoring of the state of the plant shall be maintained. These requirements shall be achieved by suitable incorporation of redundant parts, diverse systems, physical separation and design for fail-safe operation such that the following objectives are achieved:	For PBMR combustion of fuel or graphite matrix is a specific concern during maintenance or for an accident with breaks leading to air ingress. Specific criteria may be needed to guarantee an adequate margin of protection against this event.
to prevent fires from starting;	
to detect and extinguish quickly those fires which do start, thus limiting the damage;	
to prevent the spread of those fires which are not been extinguished, thus minimizing their effects on essential plant functions.	
5.11. A fire hazard analysis of the plant shall be carried out to determine the necessary rating of the fire barriers, and fire detection and fire fighting systems of the necessary capability shall be provided.	
5.12. Fire fighting systems shall be automatically initiated where necessary, and systems shall be designed and located so as to ensure that their rupture or spurious or inadvertent operation does not significantly impair the capability of structures, systems and components important to safety, and does not simultaneously affect redundant safety groups, thereby rendering ineffective the measures taken to comply with the 'single failure' criterion.	
5.13. Non-combustible or fire retardant and heat resistant materials shall be used wherever practicable throughout the plant, particularly in locations such as the containment and the control room.	
Other internal hazards	
5.14. The potential for internal hazards such as flooding, missile generation, pipe whip, jet impact, or release of fluid from failed systems or from other installations on the site shall be taken into account in the design of the plant. Appropriate preventive and mitigatory measures shall be provided to ensure that nuclear safety is not compromised. Some external events may initiate internal fires or floods and may lead to the generation of missiles. Such interaction of external and internal events shall also be considered in the design, where appropriate.	For NHR-10 the close proximity of the guard vessel and the primary vessel may introduce concerns for which specific criteria may need to be developed. Refer to remarks on 4.2(3).
5.15. If two fluid systems that are operating at different pressures are interconnected, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to preclude the design pressure of the system operating at the lower pressure from being exceeded, on the assumption that a single failure occurs.	The coupling of a desalination system to the nuclear plant may introduce fluid circuits that must be considered in this regard.
External events	
5.16. The design basis natural and human induced external events shall be determined for the proposed combination of site and plant. All those events with which significant radiological risk may be associated shall be considered. A combination of deterministic and probabilistic methods shall be used to select a subset of external events which the plant is designed to withstand, and the design bases are determined.	The desalination plant must be considered as a source of potential external events affecting the nuclear plant. For example, rupture of high pressure components in an RO system could lead to potential concerns.
5.17. Natural external events which shall be considered include those which have been identified in site characterisation, such as earthquakes, floods, high winds, tornadoes, tsunami (tidal waves) and extreme meteorological conditions. Human induced external events that shall be considered include those that have been identified in site characterisation and for which design bases have been derived. The list	

of these events shall be reassessed for completeness at an early stage of the design process.	
Site related characteristics[2]	
5.18. In determining the design basis of a nuclear power plant, various interactions between the plant and the environment, including such factors as population, meteorology, hydrology, geology and seismology, shall be taken into account. The availability of off-site services upon which the safety of the plant and protection of the public may depend, such as the electricity supply and fire fighting services, shall also be taken into account.	Refer to remark on 2.9
5.19. Projects for nuclear power plants to be sited in tropical, polar, arid or volcanic areas shall be assessed with a view to identifying special design features which may be necessary as a result of the characteristics of the site.	
Combinations of events	
5.20. Where combinations of randomly occurring individual events could credibly lead to anticipated operational occurrences or accident conditions, they shall be considered in the design. Certain events may be the consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original PIE.	
Design rules	
5.21. The engineering design rules for structures, systems and components shall be specified and shall comply with the appropriate accepted national standard engineering practices (see para. 3.6), or those standards or practices already used internationally or established in another country, and whose use is applicable and also accepted by the national regulatory body.	Refer to remark on 3.6
5.22. The seismic design of the plant shall provide for a sufficient safety margin to protect against seismic events.	
Design limits	
5.23. A set of design limits consistent with the key physical parameters for each structure, system or component shall be specified for operational states and design basis accidents.	
Operational states	
5.24. The plant shall be designed to operate safely within a defined range of parameters (for example, of pressure, temperature, power), and a minimum set of specified support features for safety systems (for example, auxiliary feedwater capacity and an emergency electrical power supply) shall be assumed to be available. The design shall be such that the response of the plant to a wide range of anticipated operational occurrences will allow safe operation or shutdown, if necessary, without the necessity of invoking provisions beyond the first, or at the most the second, level of defence in depth.	Refer to remark on 2.7
5.25. The potential for accidents to occur in low power and shutdown states, such as startup, refuelling and maintenance, when the availability of safety systems may be reduced, shall be addressed in the design, and appropriate limitations on the unavailability of safety systems shall be specified.	
5.26. The design process shall establish a set of requirements and limitations for safe operation, including:	
safety system settings;	
control system and procedural constraints on process variables and other important parameters;	
requirements for maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, with the ALARA principle taken into consideration; and	

[2] For further guidance, see Ref. [5].

clearly defined operational configurations, including operational restrictions in the event of safety system outages.	
These requirements and limitations shall be a basis for the establishment of operational limits and conditions under which the operating organization will be authorized to operate the plant.	
Design basis accidents	
5.27. A set of design basis accidents shall be derived from the listing of PIEs (see Appendix I) for the purpose of setting the boundary conditions according to which the structures, systems and components important to safety shall be designed.	
5.28. Where prompt and reliable action is necessary in response to a PIE, provision shall be made to initiate the necessary actions of safety system automatically, in order to prevent progression to a more severe condition that may threaten the next barrier. Where prompt action is not necessary, manual initiation of systems or other operator actions may be permitted, provided that the need for the action be revealed in sufficient time and that adequate procedures (such as administrative, operational and emergency procedures) be defined to ensure the reliability of such actions.	
5.29. The operator actions that may be necessary to diagnose the state of the plant and to put it into a stable long term shutdown condition in a timely manner shall be taken into account and facilitated by the provision of adequate instrumentation to monitor the plant status and controls for manual operation of equipment.	
5.30. Any equipment necessary in manual response and recovery processes shall be placed at the most suitable location to ensure its ready availability at the time of need and to allow human access for the anticipated environmental conditions.	
Severe accidents	
5.31. Certain very low probability plant states that are beyond design basis accident conditions and which may arise owing to multiple failures of safety systems leading to significant core degradation may jeopardize the integrity of many or all the barriers to the release of radioactive material. These event sequences are called severe accidents. Consideration shall be given to these severe accident sequences, using a combination of engineering judgement and probabilistic methods, to determine those sequences for which reasonably practicable preventive or mitigatory measures can be identified. Acceptable measures need not involve the application of conservative engineering practices used in setting and evaluating design basis accidents, but rather should be based upon realistic or best estimate assumptions, methods and analytical criteria. On the basis of operational experience, relevant safety analysis and results from safety research, design activities for addressing severe accidents shall take into account the following:	For the two reactors under consideration it has been stated that severe accidents are precluded by design features. A complete demonstration of this statement has to be provided as part of the safety assessment for these reactors. Refer to the introductory remarks and remarks on 2.10(4).
Important event sequences that may lead to a severe accident shall be identified using a combination of probabilistic methods, deterministic methods and sound engineering judgement.	
These event sequences shall then be reviewed against a set of criteria aimed at determining which severe accidents shall be addressed in the design.	
Potential design changes or procedural changes that could either reduce the likelihood of these selected events, or mitigate their consequences should these selected events occur, shall be evaluated and shall be implemented if reasonably practicable.	
Consideration shall be given to the plant's full design capabilities, including the possible use of some systems (i.e. safety and non-safety systems) beyond their originally intended function and anticipated operational states, and the use of additional temporary systems, to return the plant to a controlled state and/or to mitigate the consequences of a	

severe accident, provided that it can be shown that the systems are able to function in the environmental conditions to be expected.	
For multiunit plants, consideration shall be given to the use of available means and/or support from other units, provided that the safe operation of the other units is not compromised.	
Accident management procedures shall be established, taking into account representative and dominant severe accident scenarios.	
DESIGN FOR RELIABILITY OF STRUCTURES, SYSTEMS AND COMPONENTS	
5.32. Structures, systems and components important to safety shall be designed to be capable of withstanding all identified PIEs (see Appendix I) with sufficient reliability.	
Common cause failures	
5.33. The potential for common cause failures of items important to safety shall be considered to determine where the principles of diversity, redundancy and independence should be applied to achieve the necessary reliability.	
Single failure criterion	
5.34. The single failure criterion shall be applied to each safety group incorporated in the plant design.	
5.35. To test compliance of the plant with the single failure criterion, the pertinent safety group shall be analysed in the following way. A single failure (and all its consequential failures) shall be assumed in turn to occur for each element of the safety group until all possible failures have been analysed. The analyses of each pertinent safety group shall then be conducted in turn until all safety groups and all failures have been considered. (In this Safety Requirements publication, safety functions, or systems contributing to performing those safety functions, for which redundancy is necessary to achieve the necessary reliability have been identified by the statement 'on the assumption of a single failure'.) The assumption of a single failure in that system is part of the process described. At no point in the single failure analysis is more than one random failure assumed to occur.	
5.36. Spurious action shall be considered as one mode of failure when applying the concept to a safety group or system.	
5.37. Compliance with the criterion shall be considered to have been achieved when each safety group has been shown to perform its safety function when the above analyses are applied, under the following conditions:	
any potentially harmful consequences of the PIE for the safety group are assumed to occur; and	
the worst permissible configuration of safety systems performing the necessary safety function is assumed, with account taken of maintenance, testing, inspection and repair, and allowable equipment outage times.	
Non-compliance with the single failure criterion shall be exceptional, and shall be clearly justified in the safety analysis.	
5.39. In the single failure analysis, it may not be necessary to assume the failure of a passive component designed, manufactured, inspected and maintained in service to an extremely high quality, provided that it remains unaffected by the PIE. However, when it is assumed that a passive component does not fail, such an analytical approach shall be justified, with account taken of the loads and environmental conditions, as well as the total period of time after the initiating event for which functioning of the component is necessary.	

Fail-safe design	
5.40. The principle of fail-safe design shall be considered and incorporated into the design of systems and components important to safety for the plant as appropriate: if a system or component fails, plant systems shall be designed to pass into a safe state with no necessity for any action to be initiated.	
Auxiliary services	
5.41. Auxiliary services that support equipment forming part of a system important to safety shall be considered part of that system and shall be classified accordingly. Their reliability, redundancy, diversity and independence and the provision of features for isolation and for testing of functional capability shall be commensurate with the reliability of the system that is supported. Auxiliary services necessary to maintain the plant in a safe state may include the supply of electricity, cooling water and compressed air or other gases, and means of lubrication.	
Equipment outages	
5.42. The design shall be such as to ensure, by the application of measures such as increased redundancy, that reasonable on-line maintenance and testing of systems important to safety can be conducted without the necessity to shut down the plant. Equipment outages, including unavailability of systems or components due to failure, shall be taken into account, and the impact of the anticipated maintenance, test and repair work on the reliability of each individual safety system shall be included in this consideration in order to ensure that the safety function can still be achieved with the necessary reliability. The time allowed for equipment outages and the actions to be taken shall be analysed and defined for each case before the start of plant operation and included in the plant operating instructions.	
PROVISION FOR IN-SERVICE TESTING, MAINTENANCE, REPAIR, INSPECTION AND MONITORING	
5.43. Structures, systems and components important to safety, except as described in para. 5.44, shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored with respect to their functional capability over the lifetime of the nuclear power plant to demonstrate that reliability targets are being met. The plant layout shall be such that these activities are facilitated and can be performed to standards commensurate with the importance of the safety functions to be performed, with no significant reduction in system availability and without undue exposure of the site personnel to radiation.	
5.44. If the structures, systems and components important to safety cannot be designed to be able to be tested, inspected or monitored to the extent desirable, then the following approach shall be followed:	
other proven alternative and/or indirect methods such as surveillance of reference items or use of verified and validated calculational methods shall be specified; and	
conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures.	
EQUIPMENT QUALIFICATION	
5.45. A qualification procedure shall be adopted to confirm that the items important to safety are capable of meeting, throughout their design operational lives, the demands for performing their functions while being subject to the environmental conditions (of vibration, temperature, pressure, jet impingement, electromagnetic interference, irradiation, humidity or any likely combination thereof) prevailing at the time of need. The environmental conditions to be considered shall include the variations expected in normal operation, anticipated operational occurrences and design basis accidents. In the qualification programme, consideration shall be given to ageing effects caused by various	

environmental factors (such as vibration, irradiation and extreme temperature) over the expected lifetime of the equipment. Where the equipment is subject to external natural events and is needed to perform a safety function in or following such an event, the qualification programme shall replicate as far as practicable the conditions imposed on the equipment by the natural phenomenon, either by test or by analysis or by a combination of both.	
5.46. In addition, any unusual environmental conditions that can reasonably be anticipated and could arise from specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme. To the extent possible, equipment (such as certain instrumentation) that must operate in a severe accident should be shown, with reasonable confidence, to be capable of achieving the design intent.	
AGEING	
5.47. Appropriate margins shall be provided in the design for all structures, systems and components important to safety so as to take into account relevant ageing and wear-out mechanisms and potential age related degradation, in order to ensure the capability of the structure, system or component to perform the necessary safety function throughout its design life. Ageing and wear-out effects in all normal operating conditions, testing, maintenance, maintenance outages, plant states in a PIE and post-PIE shall also be taken into account. Provision shall also be made for monitoring, testing, sampling and inspection, to assess ageing mechanisms predicted at the design stage and to identify unanticipated behaviour or degradation that may occur in service.	
HUMAN FACTORS	
Design for optimal operator performance	
5.48. The design shall be 'operator friendly' and shall be aimed at limiting the effects of human errors. Attention shall be paid to plant layout and procedures (administrative, operational and emergency), including maintenance and inspection, in order to facilitate the interface between the operating personnel and the plant.	
5.49. The working areas and working environment of the site personnel shall be designed according to ergonomic principles.	
5.50. Systematic consideration of human factors and the human–machine interface shall be included in the design process at an early stage and shall continue throughout the entire process, to ensure an appropriate and clear distinction of functions between operating personnel and the automatic systems provided.	
5.51. The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, compatible with the necessary decision and action times. Similar provisions shall be made for the supplementary control room.	
5.52. Verification and validation of aspects of human factors shall be included at appropriate stages to confirm that the design adequately accommodates all necessary operator actions.	
5.53. To assist in the establishment of design criteria for information display and controls, the operator shall be considered to have dual roles: that of a systems manager, including accident management, and that of an equipment operator.	
5.54. In the system manager role, the operator shall be provided with information that permits the following:	
the ready assessment of the general state of the plant in whichever condition it is, whether in normal operation, in an anticipated operational occurrence or in an accident condition, and confirmation that the designed automatic safety actions are being carried out; and	
the determination of the appropriate operator initiated safety actions to be taken.	

5.55. As equipment operator, the operator shall be provided with sufficient information on parameters associated with individual plant systems and equipment to confirm that the necessary safety actions can be initiated safely.	
5.56. The design shall be aimed at promoting the success of operator actions with due regard for the time available for action, the physical environment to be expected and the psychological demands to be made on the operator. The need for intervention by the operator on a short time-scale shall be kept to a minimum. It shall be taken into account in the design that the necessity for such intervention is only acceptable provided that the designer can demonstrate that the operator has sufficient time to make a decision and to act; that the information necessary for the operator to make the decision to act is simply and unambiguously presented; and that following an event the physical environment in the control room or in the supplementary control room and on the access route to that supplementary control room is acceptable.	
OTHER DESIGN CONSIDERATIONS	
Sharing of structures, systems and components between reactors	
5.57. Structures, systems and components important to safety shall generally not be shared between two or more reactors in nuclear power plants. If in exceptional cases such structures, systems and components important to safety are shared between two or more reactors, it shall be demonstrated that all safety requirements are met for all reactors under all operational states (including maintenance) and in design basis accidents. In the event of a severe accident involving one of the reactors, an orderly shutdown, cooling down and removal of residual heat shall be achievable for the other reactor(s).	
Systems containing fissile or radioactive materials	
5.58. All systems within a nuclear power plant that may contain fissile or radioactive materials shall be designed to ensure adequate safety in operational states and in design basis accidents.	
Power plants used for cogeneration, heat generation or desalination	
5.59. Nuclear power plants coupled with heat utilization units (such as for district heating) and/or water desalination units shall be designed to prevent transport of radioactive materials from the nuclear plant to the desalination or district heating unit under any condition of normal operation, anticipated operational occurrences, design basis accidents and selected severe accidents.	
Transport and packaging for fuel and radioactive waste	
5.60. The design shall incorporate appropriate features to facilitate transport and handling of fresh fuel, spent fuel and radioactive waste. Consideration shall be given to access to facilities and lifting and packaging capabilities.	
Escape routes and means of communication	
5.61. The nuclear power plant shall be provided with a sufficient number of safe escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other building services essential to the safe use of these routes. The escape routes shall meet the relevant international requirements for radiation zoning and fire protection and the relevant national requirements for industrial safety and plant security.	
5.62. Suitable alarm systems and means of communication shall be provided so that all persons present in the plant and on the site can be warned and instructed, even under accident conditions.	
5.63. The availability of means of communication necessary for safety, within the nuclear power plant, in the immediate vicinity and to off-site agencies, as stipulated in the emergency plan, shall be ensured at all times. This requirement shall be taken into account in the design and the diversity of the methods of communication selected.	

Control of access	
5.64. The plant shall be isolated from the surroundings by suitable layout of the structural elements in such a way that access to it can be permanently controlled. In particular, provision shall be made in the design of the buildings and the layout of the site for personnel and/or equipment for the control of access, and attention shall be paid to guarding against the unauthorized entry of persons and goods to the plant.	
5.65. Unauthorized access to, or interference for any reason with, structures, systems and components important to safety shall be prevented. Where access is necessary for maintenance, testing or inspection purposes, it shall be ensured in the design that the necessary activities can be performed without significantly reducing the reliability of safety related equipment.	
Interactions of systems	
5.66. If there is a significant probability that it will be necessary for systems important to safety to operate simultaneously, their possible interaction shall be evaluated. In the analysis, account shall be taken not only of physical interconnections, but also of the possible effects of one system's operation, maloperation or failure on the physical environment of other essential systems, in order to ensure that changes in the environment do not affect the reliability of system components in functioning as intended.	Interaction between the desalination plant and the nuclear plant should be investigated. See also remarks on 2.7.
Interactions between the electrical power grid and the plant	
5.67. In the design of the plant, account shall be taken of power grid–plant interactions, including the independence of and number of power supply lines to the plant, in relation to the necessary reliability of the power supply to plant systems important to safety.	
Decommissioning	
5.68. At the design stage, special consideration shall be given to the incorporation of features that will facilitate the decommissioning and dismantling of the plant. In particular, account shall be taken in the design of:	
the choice of materials, such that eventual quantities of radioactive waste are minimized and decontamination is facilitated;	
the access capabilities that may be necessary; and	
the facilities necessary for storing radioactive waste generated in both operation and decommissioning of the plant.	
SAFETY ANALYSIS	
5.69. 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 (see para. 5.7), and that defence in depth has been effected.	
The computer programs, analytical methods and plant models used in the safety analysis shall be verified and validated, and adequate consideration shall be given to uncertainties.	
Deterministic approach	
5.71. The deterministic safety analysis shall include the following:	
confirmation that operational limits and conditions are in compliance with the assumptions and intent of design for normal plant operation;	
characterisation of the PIEs (see Appendix I) that are appropriate for the design and site of the plant;	
analysis and evaluation of event sequences that result from PIEs;	
comparison of the results of the analysis with radiological acceptance criteria and design limits;	

establishment and confirmation of the design basis; and	
demonstration that the management of anticipated operational occurrences and design basis accidents is possible by automatic response of safety systems in combination with prescribed actions of the operator.	
5.72. The applicability of the analytical assumptions, methods and degree of conservatism used shall be verified. The safety analysis of the plant design shall be updated with regard to significant changes in plant configuration, operational experience, and advances in technical knowledge and understanding of physical phenomena, and shall be consistent with the current or 'as built' state.	
Probabilistic approach	
5.73. A probabilistic safety analysis of the plant shall be carried out in order to do the following:	For innovative designs the higher level of uncertainties in the component failure database may require more caution in the application and interpretation of probabilistic safety analyses. This may be particularly relevant to PBMR.
to provide a systematic analysis to give confidence that the design will comply with the general safety objectives;	
to demonstrate that a balanced design has been achieved such that no particular feature or PIE makes a disproportionately large or significantly uncertain contribution to the overall risk, and that the first two levels of defence in depth bear the primary burden of ensuring nuclear safety;	
to provide confidence that small deviations in plant parameters that could give rise to severely abnormal plant behaviour ('cliff edge effects') will be prevented;	
to provide assessments of the probabilities of occurrence of severe core damage states and assessments of the risks of major off-site releases necessitating a short term off-site response, particularly for releases associated with early containment failure;	
to provide assessments of the probabilities of occurrence and the consequences of external hazards, in particular those unique to the plant site;	
to identify systems for which design improvements or modifications to operational procedures could reduce the probabilities of severe accidents or mitigate their consequences;	
to assess the adequacy of plant emergency procedures; and	
to verify compliance with probabilistic targets, if set.	
REQUIREMENTS FOR DESIGN OF PLANT SYSTEMS	
REACTOR CORE AND ASSOCIATED FEATURES	
General design	
6.1. The reactor core and associated coolant, control and protection systems shall be designed with appropriate margins to ensure that the specified design limits are not exceeded and that radiation safety standards are applied in all operational states and in design basis accidents, with account taken of the existing uncertainties.	
6.2. The reactor core and associated internal components located within the reactor vessel shall be designed and mounted in such a way that they will withstand the static and dynamic loading expected in operational states, design basis accidents and external events to the extent necessary to ensure safe shutdown of the reactor, to maintain the reactor subcritical and to ensure cooling of the core.	
6.3. The maximum degree of positive reactivity and its maximum rate of increase by insertion in operational states and design basis accidents shall be limited so that no resultant failure of the reactor pressure boundary will occur, cooling capability will be maintained and no significant damage will occur to the reactor core.	

6.4. It shall be ensured in the design that the possibility of recriticality or reactivity excursion following a PIE is minimized.	
6.5. The reactor core and associated coolant, control and protection systems shall be designed to enable adequate inspection and testing throughout the service lifetime of the plant.	For PBMR an annular core is envisaged without any physical separation between regions. In such a case there must be specific requirements to define the allowable geometric configuration of the core and the means for monitoring and verification of the core configuration.
Fuel elements and assemblies	No requirements are indicated for leaking fuel element management. For PBMR specific fuel management requirements must be stipulated to deal with radioactive fission products leaking into the primary coolant.
6.6. Fuel elements and assemblies shall be designed to withstand satisfactorily the anticipated irradiation and environmental conditions in the reactor core in combination with all processes of deterioration that can occur in normal operation and in anticipated operational occurrences.	For PBMR the fuel is expected to serve as one of the major barriers against release of radioactive materials, and the fuel is not configured in the form of "fuel elements and assemblies". Specific requirements will be necessary to ensure that the intent of this requirement is satisfied.
6.7. The deterioration considered shall include that arising from: differential expansion and deformation; external pressure of the coolant; additional internal pressure due to the fission products in the fuel element; irradiation of fuel and other materials in the fuel assembly; changes in pressures and temperatures resulting from changes in power demand; chemical effects; static and dynamic loading, including flow induced vibrations and mechanical vibrations; and changes in heat transfer performance that may result from distortions or chemical effects. Allowance shall be made for uncertainties in data, calculations and fabrication.	
6.8. Specified fuel design limits, including permissible leakage of fission products, shall not be exceeded in normal operation, and it shall be ensured that operational states that may be imposed in anticipated operational occurrences cause no significant further deterioration. Leakage of fission products shall be restricted by design limits and kept to a minimum.	
6.9. Fuel assemblies shall be designed to permit adequate inspection of their structure and component parts after irradiation. In design basis accidents, the fuel elements shall remain in position and shall not suffer distortion to an extent that would render post-accident core cooling insufficiently effective; and the specified limits for fuel elements for design basis accidents shall not be exceeded.	The intent of this requirement is to ensure that core cooling and fuel integrity are not compromised as the result of a design basis accident. For PBMR the lack of fuel assemblies necessitates special requirements to satisfy this intent.
6.10. The aforementioned requirements for reactor and fuel element design shall also be maintained in the event of changes in fuel management strategy or in operational states over the operational lifetime of the plant.	
Control of the reactor core	
6.11. The provisions of paras 6.3–6.10 shall be met for all levels and distributions of neutron flux that can arise in all states of the core, including those after shutdown and during or after refuelling, and those arising from anticipated operational occurrences and design basis	

accidents. Adequate means of detecting these flux distributions shall be provided to ensure that there are no regions of the core in which the provisions of paras 6.3–6.10 could be breached without being detected. The design of the core shall sufficiently reduce the demands made on the control system for maintaining flux shapes, levels and stability within specified limits in all operational states.	
6.12. Provision shall be made for the removal of non-radioactive substances, including corrosion products, which may compromise the safety of the system, for example by clogging coolant channels.	The example supplied with this requirement may not be applicable to the PBMR. However, the requirement should not be construed to be limited to blocking of flow channels. There must be provisions for removal of any substances that could compromise the safety of the system.
Reactor shutdown	
6.13. Means shall be provided to ensure that there is a capability to shut down the reactor in operational states and design basis accidents, and that the shutdown condition can be maintained even for the most reactive core conditions. The effectiveness, speed of action and shutdown margin of the means of shutdown shall be such that the specified limits are not exceeded. For the purpose of reactivity control and flux shaping in normal power operation, a part of the means of shutdown may be used provided that the shutdown capability be maintained with an adequate margin at all times.	
6.14. The means for shutting down the reactor shall consist of at least two different systems to provide diversity.	
6.15. At least one of the two systems shall be, on its own, capable of quickly rendering the nuclear reactor subcritical by an adequate margin from operational states and in design basis accidents, on the assumption of a single failure. Exceptionally, a transient recriticality may be permitted provided that the specified fuel and component limits are not exceeded.	The intent of this requirement is that the shutdown system be able to respond “quickly” with respect to the rate at which transients may proceed. In the case of PBMR, the design may be such that transients are relatively slow to develop and this may allow for some relaxation in the required reaction time, allowing for the use of an innovative shutdown system design.
6.16. At least one of these two systems shall be, on its own, capable of rendering the reactor subcritical from normal operational states, in anticipated operational occurrences and in design basis accidents, and of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the core.	
6.17. In judging the adequacy of the means of shutdown, consideration shall be given to failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or could result in a common cause failure.	
6.18. The means of shutdown shall be adequate to prevent or withstand inadvertent increases in reactivity by insertion during the shutdown, including refuelling in this state. In meeting this provision, deliberate actions that increase reactivity in the shutdown state (such as absorber movement for maintenance, dilution of boron content and refuelling actions) and a single failure in the shutdown means shall be taken into account.	
6.19. Instrumentation shall be provided and tests shall be specified to ensure that the shutdown means are always in the state stipulated for the given plant condition.	
6.20. In the design of reactivity control devices, account shall be taken of wear-out, and effects of irradiation, such as burnup, changes in physical properties and production of gas.	

REACTOR COOLANT SYSTEM	
Design of the reactor coolant system	
6.21. The reactor coolant system, its associated auxiliary systems, and the control and protection systems shall be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded in operational states. Provision shall be made to ensure that the operation of pressure relief devices, even in design basis accidents, will not lead to unacceptable releases of radioactive material from the plant. The reactor coolant pressure boundary shall be equipped with adequate isolation devices to limit any loss of radioactive fluid.	
6.22. The component parts containing the reactor coolant, such as the reactor pressure vessel or the pressure tubes, piping and connections, valves, fittings, pumps, circulators and heat exchangers, together with the devices by which such parts are held in place, shall be designed in such a way as to withstand the static and dynamic loads anticipated in all operational states and in design basis accidents. The materials used in the fabrication of the component parts shall be selected so as to minimize activation of the material.	
6.23. The reactor pressure vessel and the pressure tubes shall be designed and constructed to be of the highest quality with respect to materials, design standards, capability of inspection and fabrication.	
6.24. The pressure retaining boundary for reactor coolant shall be designed so that flaws are very unlikely to be initiated, and any flaws that are initiated would propagate in a regime of high resistance to unstable fracture with fast crack propagation, to permit timely detection of flaws (such as by application of the leak before break concept). Designs and plant states in which components of the reactor coolant pressure boundary could exhibit brittle behaviour shall be avoided.	
6.25. The design shall reflect consideration of all conditions of the boundary material in operational states, including those for maintenance and testing, and underdesign basis accidents conditions, with account taken of the expected end-of-life properties affected by erosion, creep, fatigue, the chemical environment, the radiation environment and ageing, and any uncertainties in determining the initial state of the components and the rate of possible deterioration.	
6.26. The design of the components contained inside the reactor coolant pressure boundary, such as pump impellers and valve parts, shall be such as to minimize the likelihood of failure and associated consequential damage to other items of the primary coolant system important to safety in all operational states and in design basis accidents, with due allowance made for deterioration that may occur in service.	
In-service inspection of the reactor coolant pressure boundary	
6.27. The components of the reactor coolant pressure boundary shall be designed, manufactured and arranged in such a way that it is possible, throughout the service lifetime of the plant, to carry out at appropriate intervals adequate inspections and tests of the boundary. Provision shall be made to implement a material surveillance programme for the reactor coolant pressure boundary, particularly in locations of high irradiation, and other important components as appropriate, for determining the metallurgical effects of factors such as irradiation, stress corrosion cracking, thermal embrittlement and ageing of structural materials.	Even in the event of designs with very low flux at the reactor coolant boundary this requirement needs to be considered in view of the importance of this boundary as one of the levels of defence in depth.
6.28. It shall be ensured that it is possible to inspect or test either directly or indirectly the components of the reactor coolant pressure boundary, according to the safety importance of those components, so as to demonstrate the absence of unacceptable defects or of safety significant deterioration.	

6.29. Indicators for the integrity of the reactor coolant pressure boundary (such as leakage) shall be monitored. The results of such measurements shall be taken into consideration in the determination of which inspections are necessary for safety.	
6.30. If the safety analysis of the nuclear power plant indicates that particular failures in the secondary cooling system may result in serious consequences, it shall be ensured that it is possible to inspect the relevant parts of the secondary cooling system.	
Inventory of reactor coolant	
6.31. Provision shall be made for controlling the inventory and pressure of coolant to ensure that specified design limits are not exceeded in any operational state, with volumetric changes and leakage taken into account. The systems performing this function shall have adequate capacity (flow rate and storage volumes) to meet this requirement. They may be composed of components needed for the processes of power generation or may be specially provided for performing this function.	
Cleanup of the reactor coolant	
6.32. Adequate facilities shall be provided for removal of radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel. The capability of the necessary systems shall be based on the specified fuel design limit on permissible leakage with a conservative margin to ensure that the plant can be operated with a level of circuit activity which is as low as reasonably practicable, and that radioactive releases meet the ALARA principle and are within the prescribed limits.	Refer to remarks on “Fuel elements and assemblies”, just prior to 6.6.
Removal of residual heat from the core	
6.33. Means for removing residual heat shall be provided. Their safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified fuel design limits and the design basis limits of the reactor coolant pressure boundary are not exceeded.	
6.34. Interconnections and isolation capabilities and other appropriate design features (such as leak detection) shall be provided to fulfil the requirements of para. 6.33 with sufficient reliability, on the assumptions of a single failure and the loss of off-site power, and with the incorporation of suitable redundancy, diversity and independence.	
Emergency core cooling	
6.35. Core cooling shall be provided in the event of a loss of coolant accident so as to minimize fuel damage and limit the escape of fission products from the fuel. The cooling provided shall ensure that:	
the limiting parameters for the cladding or fuel integrity (such as temperature) will not exceed the acceptable value for design basis accidents (for applicable reactor designs);	
possible chemical reactions are limited to an allowable level;	
the alterations in the fuel and internal structural alterations will not significantly reduce the effectiveness of the means of emergency core cooling; and	
the cooling of the core will be ensured for a sufficient time.	
6.36. Design features (such as leak detection, appropriate interconnections and isolation capabilities) and suitable redundancy and diversity in components shall be provided in order to fulfil these requirements with sufficient reliability for each PIE, on the assumption of a single failure.	
6.37. Adequate consideration shall be given to extending the capability to remove heat from the core following a severe accident.	Refer to introductory remarks and remarks on 2.10 (4)
Inspection and testing of the emergency core cooling system	
6.38. The emergency core cooling system shall be designed to permit appropriate periodic inspection of important components and to permit appropriate periodic testing to confirm the following:	

the structural integrity and leaktight integrity of its components;	
the operability and performance of the active components of the system in normal operation, as far as feasible; and	
the operability of the system as a whole under the plant states specified in the design basis, to the extent practicable.	
Heat transfer to an ultimate heat sink	
6.39. Systems shall be provided to transfer residual heat from structures, systems and components important to safety to an ultimate heat sink. This function shall be carried out at very high levels of reliability in operational states and in design basis accidents. All systems that contribute to the transport of heat (by conveying heat, by providing power or by supplying fluids to the heat transport systems) shall be designed in accordance with the importance of their contribution to the function of heat transfer as a whole.	
6.40. The reliability of the systems shall be achieved by an appropriate choice of measures including the use of proven components, redundancy, diversity, physical separation, interconnection and isolation.	
6.41. Natural phenomena and human induced events shall be taken into account in the design of the systems and in the possible choice of diversity in the ultimate heat sinks and in the storage systems from which fluids for heat transfer are supplied.	
6.42. Adequate consideration shall be given to extending the capability to transfer residual heat from the core to an ultimate heat sink so as to ensure that, in the event of a severe accident, acceptable temperatures can be maintained in structures, systems and components important to the safety function of confinement of radioactive materials.	
CONTAINMENT SYSTEM	
Design of the containment system	According to available design descriptions, for the reactors under consideration the notion of "containment system" as usually intended for water reactors is replaced by the notion of "effective defences" that achieve the containment function in order to protect the individual , society and the environment from harm due to radiological hazards. For PBMR these defences are represented by the SIC (silicon carbide) layer surrounding the fuel kernel, the RPV and the reactor building filtered ventilation system. For NHR-10 these defences are represented by the fuel matrix, the cladding, the RPV, the guard vessel and the reactor building filtered ventilation system. The following paragraphs indicate possible alternative wording for the containment system requirements to reflect these notions.
6.43. A containment system shall be provided in order to ensure that any release of radioactive materials to the environment in a design basis accident would be below prescribed limits. This system may include, depending on design requirements: leaktight structures; associated systems for the control of pressures and temperatures; and features for the isolation, management and removal of fission products, hydrogen, oxygen and other substances that could be released into the containment atmosphere.	*Effective defences shall be provided achieve containment function* to keep the release of radioactive materials to the environment below specified limits under design basis accidents. *These defences* may, depending on design requirements, include: leaktight structures,

	associated systems for the control of pressure and temperature, and features for isolation, management and removal of fission products, hydrogen, oxygen and other substances that may be released into the containment atmosphere.
6.44. All identified design basis accidents shall be taken into account in the design of the containment system. In addition, consideration shall be given to the provision of features for the mitigation of the consequences of selected severe accidents in order to limit the release of radioactive material to the environment.	The design of the *defences* shall take into account all identified design basis accidents. In addition, consideration shall be given to the provision of features for the mitigation of the consequences of selected severe accidents in order to limit the release of radioactive material to the environment. *Provisions for protection against external hazards must be provided.* [Refer to remarks on 2.10(4)]
Strength of the containment structure	
6.45. The strength of the containment structure, including access openings and penetrations and isolation valves, shall be calculated with sufficient margins of safety on the basis of the potential internal overpressures, underpressures and temperatures, dynamic effects such as missile impacts, and reaction forces anticipated to arise as a result of design basis accidents. The effects of other potential energy sources, including, for example, possible chemical and radiolytic reactions, shall also be considered. In calculating the necessary strength of the containment structure, natural phenomena and human induced events shall be taken into consideration, and provision shall be made to monitor the condition of the containment and its associated features.	
6.46. Provision for maintaining the integrity of the containment in the event of a severe accident shall be considered. In particular, the effects of any predicted combustion of flammable gases shall be taken into account.	It is to be understood here that it is the containment function that is to be maintained. Refer to the introductory remarks and remarks on 2.10(4).
Capability for containment pressure tests	This requirement is applicable for the RPV for PBMR and for the RPV and guard vessel for NHR.
6.47. The containment structure shall be designed and constructed so that it is possible to perform a pressure test at a specified pressure to demonstrate its structural integrity before operation of the plant and over the plant's lifetime.	This requirement is applicable for the RPV for PBMR and for the RPV and guard vessel for NHR.
Containment leakage	
6.48. The containment system shall be designed so that the prescribed maximum leakage rate is not exceeded in design basis accidents. The primary pressure withstanding containment may be partially or totally surrounded by a secondary confinement for the collection and controlled release or storage of materials that may leak from the primary containment in design basis accidents.	The defences that achieve the containment function should be designed so that the prescribed maximum leakage is not exceeded. For PBMR the SIC layer plays the role of primary containment and RPV plays the role of secondary containment.
6.49. The containment structure and equipment and components affecting the leaktightness of the containment system shall be designed and constructed so that the leak rate can be tested at the design pressure after all penetrations have been installed. Determination of the leakage rate of the containment system at periodic intervals over the service lifetime of the reactor shall be possible, either at the containment design pressure or at reduced pressures that permit estimation of the leakage rate at the containment design pressure.	

6.50. Adequate consideration shall be given to the capability to control any leakage of radioactive materials from the containment in the event of a severe accident.	
Containment penetrations	
6.51. The number of penetrations through the containment shall be kept to a practical minimum.	Refer to remarks on 6.48.
6.52. All penetrations through the containment shall meet the same design requirements as the containment structure itself. They shall be protected against reaction forces stemming from pipe movement or accidental loads such as those due to missiles, jet forces and pipe whip.	Refer to remarks on 6.48.
6.53. If resilient seals (such as elastomeric seals or electrical cable penetrations) or expansion bellows are used with penetrations, they shall be designed to have the capability for leak testing at the containment design pressure, independent of the determination of the leak rate of the containment as a whole, to demonstrate their continued integrity over the lifetime of the plant.	Refer to remarks on 6.48.
6.54. Adequate consideration shall be given to the capability of penetrations to remain functional in the event of a severe accident.	Refer to the introductory remarks and remarks on 2.10(4).
Containment isolation	
6.55. Each line that penetrates the containment as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of a design basis accident in which the leaktightness of the containment is essential to preventing radioactive releases to the environment that exceed prescribed limits. These lines shall be fitted with at least two adequate containment isolation valves arranged in series (normally with one outside and the other inside the containment, but other arrangements may be acceptable depending on the design), and each valve shall be capable of being reliably and independently actuated. Isolation valves shall be located as close to the containment as is practicable. Containment isolation shall be achievable on the assumption of a single failure. If the application of this requirement reduces the reliability of a safety system that penetrates the containment, other isolation methods may be used.	Refer to remarks on 6.48.
6.56. Each line that penetrates the primary reactor containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one adequate containment isolation valve. This valve shall be outside the containment and located as close to the containment as practicable.	Refer to remarks on 6.48.
6.57. Adequate consideration shall be given to the capability of isolation devices to maintain their function in the event of a severe accident.	Refer to the introductory remarks and remarks on 2.10(4).
Containment air locks	
6.58. Access by personnel to the containment shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor operations and in design basis accidents. Where provision is made for entry of personnel for surveillance purposes during certain low power operations, provisions for ensuring the safety of personnel in such operations shall be specified in the design. These requirements shall also apply to equipment air locks, where provided.	Refer to remarks on 6.48.
6.59. Adequate consideration shall be given to the capability of containment air locks to maintain their function in the event of a severe accident.	Refer to the introductory remarks and remarks on 2.10(4).
Internal structures of the containment	
6.60. The design shall provide for ample flow routes between separate compartments inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in design basis accidents do not result in damage to the	

pressure bearing structure or to other systems of importance in limiting the effects of design basis accidents.	
6.61. Adequate consideration shall be given to the capability of the internal structures to withstand the effects of a severe accident.	Refer to the introductory remarks and remarks on 2.10(4).
Removal of heat from the containment	
6.62. The capability to remove heat from the reactor containment shall be ensured. The safety function shall be fulfilled of reducing the pressure and temperature in the containment, and maintaining them at acceptably low levels, after any accidental release of high energy fluids in a design basis accident. The system performing the function of removing heat from the containment shall have adequate reliability and redundancy to ensure that this can be fulfilled, on the assumption of a single failure.	
6.63. Adequate consideration shall be given to the capability to remove heat from the reactor containment in the event of a severe accident.	Refer to the introductory remarks and remarks on 2.10(4).
Control and cleanup of the containment atmosphere	
6.64. Systems to control fission products, hydrogen, oxygen and other substances that may be released into the reactor containment shall be provided as necessary to do the following:	
to reduce the amount of fission products that might be released to the environment in design basis accidents; and	
to control the concentration of hydrogen, oxygen and other substances in the containment atmosphere in design basis accidents in order to prevent deflagration or detonation which could jeopardize the integrity of the containment.	
6.65. Systems for cleaning up the containment atmosphere shall have suitable redundancy in components and features to ensure that the safety group can fulfil the necessary safety function, on the assumption of a single failure.	
6.66. Adequate consideration shall be given to the control of fission products, hydrogen and other substances that may be generated or released in the event of a severe accident.	Refer to the introductory remarks and remarks on 2.10(4).
Coverings and coatings	
6.67. The coverings and coatings for components and structures within the containment system shall be carefully selected, and the methods of application shall be specified, to ensure fulfilment of their safety functions and to minimize interference with other safety functions in the event of the deterioration of the coverings and coatings.	
INSTRUMENTATION AND CONTROL	
General requirements for instrumentation and control systems important to safety	
6.68. Instrumentation shall be provided to monitor plant variables and systems over the respective ranges for normal operation, anticipated operational occurrences, design basis accidents and severe accidents in order to ensure that adequate information can be obtained on the status of the plant. Instrumentation shall be provided for measuring all the main variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems and the containment, and for obtaining any information on the plant necessary for its reliable and safe operation. Provision shall be made for automatic recording of measurements of any derived parameters that are important to safety, such as the subcooling margin of the coolant water. Instrumentation shall be environmentally qualified for the plant states concerned and shall be adequate for measuring plant parameters and thus classifying events for the purposes of emergency response.	
6.69. Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the course of design basis accidents and the status of essential equipment; and for predicting, as far as is necessary for safety, the locations and quantities	

of radioactive materials that could escape from the locations intended in the design. The instrumentation and recording equipment shall be adequate to provide information as far as practicable for determining the status of the plant in a severe accident and for taking decisions in accident management.	
6.70. Appropriate and reliable controls shall be provided to maintain the variables referred to in para. 6.68 within specified operational ranges.	
Control room	
6.71. A control room shall be provided from which the plant can be safely operated in all its operational states, and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of anticipated operational occurrences, design basis accidents and severe accidents. Appropriate measures shall be taken and adequate information provided to safeguard the occupants of the control room against consequent hazards, such as undue radiation levels resulting from an accident condition or the release of radioactive material or explosive or toxic gases, which could hinder necessary actions by the operator.	
6.72. Special attention shall be given to identifying those events, both internal and external to the control room, which may pose a direct threat to its continued operation, and the design shall provide for reasonably practicable measures to minimize the effects of such events.	
6.73. The layout of the instrumentation and the mode of presentation of information shall provide the operating personnel with an adequate overall picture of the status and performance of the plant. Ergonomics shall be taken into account in the design of the control room.	
6.74. Devices shall be provided to give in an efficient way visual and if appropriate also audible indications of operational states and processes that have deviated from normal and could affect safety.	
Supplementary control room	
6.75. Sufficient instrumentation and control equipment shall be available, preferably at a single location (supplementary control room) that is physically and electrically separate from the control room, so that the reactor can be placed and maintained in a shut down state, residual heat can be removed, and the essential plant variables can be monitored should there be a loss of ability to perform these essential safety functions in the control room.	
Use of computer based systems in systems important to safety	
6.76. If the design is such that a system important to safety is dependent upon the reliable performance of a computer based system, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the life cycle of the system, and in particular the software development cycle. The entire development shall be subject to an appropriate quality assurance programme.	
6.77. The level of reliability necessary shall be commensurate with the safety importance of the system. The necessary level of reliability shall be achieved by means of a comprehensive strategy that uses various complementary means (including an effective regime of analysis and testing) at each phase of development of the process, and a validation strategy to confirm that the design requirements for the system have been fulfilled.	
6.78. The level of reliability assumed in the safety analysis for a computer based system shall include a specified conservatism to compensate for the inherent complexity of the technology and the consequent difficulty of analysis.	

Automatic control	
6.79. Various safety actions shall be automated so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or design basis accidents. In addition, appropriate information shall be available to the operator to monitor the effects of the automatic actions.	
Functions of the protection system	
6.80. The protection system shall be designed to do the following:	
to initiate automatically the operation of appropriate systems, including, as necessary, the reactor shutdown systems, in order to ensure that specified design limits are not exceeded as a result of anticipated operational occurrences;	
to detect design basis accidents and to initiate the operation of systems necessary to limit the consequences of such accidents within the design basis; and	
to be capable of overriding unsafe actions of the control system.	
Reliability and testability of the protection system	
6.81. The protection system shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed. Redundancy and independence designed into the protection system shall be sufficient at least to ensure that:	
no single failure results in loss of protection function; and	
the removal from service of any component or channel does not result in loss of the necessary minimum redundancy, unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.	
6.82. The protection system shall be designed to ensure that the effects of normal operation, anticipated operational occurrences and design basis accidents on redundant channels do not result in loss of its function; or else it shall be demonstrated to be acceptable on some other basis. Design techniques such as testability, including a self-checking capability where necessary, fail-safe behaviour, functional diversity and diversity in component design or principles of operation shall be used to the extent practicable to prevent loss of a protection function.	
6.83. The protection system shall, unless its adequate reliability is ensured by some other means, be designed to permit periodic testing of its functioning when the reactor is in operation, including the possibility of testing channels independently to determine failures and losses of redundancy that may have occurred. The design shall permit all aspects of functionality from the sensor to the input signal to the final actuator to be tested in operation.	
The design shall be such as to minimize the likelihood that operator action could defeat the effectiveness of the protection system in normal operations and expected operational occurrences, but not to negate correct operator actions in design basis accidents.	
Use of computer based systems in protection	
6.85. Where a computer based system is intended to be used in a protection system, the following requirements shall supplement those of paras 6.76–6.78:	
the highest quality of and best practices for hardware and software shall be used;	
the whole development process, including control, testing and commissioning of the design changes, shall be systematically documented and reviewable;	
in order to confirm confidence in the reliability of the computer based systems, an assessment of the computer based system by expert personnel independent of the designers and suppliers shall be undertaken; and	

where the necessary integrity of the system cannot be demonstrated with a high level of confidence, a diverse means of ensuring fulfilment of the protection functions shall be provided.	
Separation of protection and control systems	
6.86. Interference between the protection system and the control systems shall be prevented by avoiding interconnections or by suitable functional isolation. If signals are used in common by both the protection system and any control system, appropriate separation (such as by adequate decoupling) shall be ensured and it shall be demonstrated that all safety requirements of paras 6.80–6.85 are fulfilled.	
EMERGENCY CONTROL CENTRE	
6.87. An on-site emergency control centre, separated from the plant control room, shall be provided to serve as meeting place for the emergency staff who will operate from there in the event of an emergency. Information about important plant parameters and radiological conditions in the plant and its immediate surroundings should be available there. The room should provide means of communication with the control room, the supplementary control room, and other important points in the plant, and with the on-site and off-site emergency response organizations. Appropriate measures shall be taken to protect the occupants for a protracted time against hazards resulting from a severe accident.	
EMERGENCY POWER SUPPLY	
6.88. After certain PIEs, various systems and components important to safety will need emergency power. It shall be ensured that the emergency power supply is able to supply the necessary power in any operational state or in a design basis accident, on the assumption of the coincidental loss of off-site power. The need for power will vary with the nature of the PIE, and the nature of the safety duty to be performed will be reflected in the choice of means for each duty; in respect of number, availability, duration, capacity and continuity, for example.	
6.89. The combined means to provide emergency power (such as by means of water, steam or gas turbine, diesel engines or batteries) shall have a reliability and form that are consistent with all the requirements of the safety systems to be supplied, and shall perform their functions on the assumption of a single failure. It shall be possible to test the functional capability of the emergency power supply.	
WASTE TREATMENT AND CONTROL SYSTEMS	
6.90. Adequate systems shall be provided to treat radioactive liquid and gaseous effluents in order to keep the quantities and concentrations of radioactive discharges within prescribed limits. The ALARA principle shall be applied.	
6.91. Adequate systems shall be provided for the handling of radioactive wastes and for storing these safely on the site for a period of time consistent with the availability of the disposal route on the site. Transport of solid wastes from the site shall be effected according to the decisions of competent authorities.	
Control of releases of radioactive liquids to the environment	
6.92. The plant shall include suitable means to control the release of radioactive liquids to the environment so as to conform to the ALARA principle and to ensure that emissions and concentrations remain within prescribed limits.	Refer to remarks on 2.4 and 2.6
Control of airborne radioactive material	
6.93. A ventilation system with an appropriate filtration system shall be provided to do the following:	
to prevent unacceptable dispersion of airborne radioactive substances within the plant;	
to reduce the concentration of airborne radioactive substances to levels compatible with the need for access to the particular area;	

to keep the level of airborne radioactive substances in the plant below prescribed limits, the ALARA principle being applied in normal operation, anticipated operational occurrences and design basis accidents; and	
to ventilate rooms containing inert or noxious gases without impairing the capability to control radioactive releases.	
Control of releases of gaseous radioactive material to the environment	
6.94. A ventilation system with an appropriate filtration system shall be provided to control the release of airborne radioactive substances to the environment and to ensure that it conforms to the ALARA principle and is within prescribed limits.	
6.95. Filter systems shall be sufficiently reliable and so designed that under the expected prevailing conditions the necessary retention factors are achieved. Filter systems shall be designed such that the efficiency can be tested.	
FUEL HANDLING AND STORAGE SYSTEMS	
Handling and storage of non-irradiated fuel	
6.96. The handling and storage systems for non-irradiated fuel shall be designed to do the following:	
to prevent criticality by a specified margin by physical means or processes, preferably by the use of geometrically safe configurations, even under plant states of optimum moderation;	
to permit appropriate maintenance, periodic inspection and testing of components important to safety; and	
to minimize the probability of loss of or damage to the fuel.	
Handling and storage of irradiated fuel	
6.97. The handling and storage systems for irradiated fuel shall be designed:	
to prevent criticality by physical means or processes, preferably by use of geometrically safe configurations, even under plant states of optimum moderation;	
to permit adequate heat removal in operational states and in design basis accidents;	
to permit inspection of irradiated fuel;	
to permit appropriate periodic inspection and testing of components important to safety;	
to prevent the dropping of spent fuel in transit;	
to prevent unacceptable handling stresses on the fuel elements or fuel assemblies;	
to prevent the inadvertent dropping of heavy objects such as spent fuel casks, cranes or other potentially damaging objects on the fuel assemblies;	
to permit safe storage of suspect or damaged fuel elements or fuel assemblies;	
to provide proper means for radiation protection;	
to adequately identify individual fuel modules;	
to control soluble absorber levels if used for criticality safety;	
to facilitate maintenance and decommissioning of the fuel storage and handling facilities;	
to facilitate decontamination of fuel handling and storage areas and equipment when necessary; and	
to ensure that adequate operating and accounting procedures can be implemented to prevent any loss of fuel.	
6.98. For reactors using a water pool system for fuel storage, the design shall provide the following:	
means for controlling the chemistry and activity of any water in which irradiated fuel is handled or stored;	
means for monitoring and controlling the water level in the fuel storage pool and for detecting leakage; and	

means to prevent emptying of the pool in the event of a pipe break (that is, antisyphon measures).	
RADIATION PROTECTION[3]	
General requirements	
6.99. Radiation protection is directed to preventing any avoidable radiation exposure and to keeping any unavoidable exposures as low as reasonably achievable. This objective shall be accomplished in the design by means of the following:	In the case of nuclear desalination facilities, these requirements extend to include the purity of water produced by the desalination plant.
appropriate layout and shielding of structures, systems and components containing radioactive materials;	
paying attention to the design of the plant and equipment so as to minimize the number and duration of human activities undertaken in radiation fields and reduce the likelihood of contamination of the site personnel;	
making provision for the treatment of radioactive materials in an appropriate form and condition, for either their disposal, their storage on the site or their removal from the site; and	
making arrangements to reduce the quantity and concentration of radioactive materials produced and dispersed within the plant or released to the environment.	
6.100. Full account shall be taken of the potential build-up of radiation levels with time in areas of personnel occupancy and of the need to minimize the generation of radioactive materials as wastes.	
Design for radiation protection	
6.101. Suitable provision shall be made in the design and layout of the plant to minimize exposure and contamination from all sources. Such provision shall include adequate design of structures, systems and components in terms of: minimizing exposure during maintenance and inspection; shielding from direct and scattered radiation; ventilation and filtration for control of airborne radioactive materials; limiting the activation of corrosion products by proper specification of materials; means of monitoring; control of access to the plant; and suitable decontamination facilities.	
6.102. The shielding design shall be such that radiation levels in operating areas do not exceed the prescribed limits, and shall facilitate maintenance and inspection so as to minimize exposure of maintenance personnel. The ALARA principle shall be applied.	
6.103. The plant layout and procedures shall provide for the control of access to radiation areas and areas of potential contamination, and for minimizing contamination from the movement of radioactive materials and personnel within the plant. The plant layout shall provide for efficient operation, inspection, maintenance and replacement as necessary to minimize radiation exposure.	
6.104. Provision shall be made for appropriate decontamination facilities for both personnel and equipment and for handling any radioactive waste arising from decontamination activities.	
Means of radiation monitoring	
6.105. Equipment shall be provided to ensure that there is adequate radiation monitoring in operational states, design basis accidents and, as practicable, severe accidents:	
(1) Stationary dose rate meters shall be provided for monitoring the local radiation dose rate at places routinely occupied by operating personnel and where the changes in radiation levels in normal operation or anticipated operational occurrences may be such that access shall be limited for certain periods of time. Furthermore, stationary dose rate meters shall be installed to indicate the general radiation level at appropriate locations in the event of design basis accidents and, as practicable, severe accidents. These instruments shall give sufficient	

[3] For further guidance, see Ref. [6].

information in the control room or at the appropriate control position that plant personnel can initiate corrective action if necessary.	
(2) Monitors shall be provided for measuring the activity of radioactive substances in the atmosphere in those areas routinely occupied by personnel and where the levels of airborne activity may on occasion be expected to be such as to necessitate protective measures. These systems shall give an indication in the control room, or other appropriate locations, when a high concentration of radionuclides is detected.	
(3) Stationary equipment and laboratory facilities shall be provided for determining in a timely manner the concentration of selected radionuclides in fluid process systems as appropriate, and in gas and liquid samples taken from plant systems or the environment, in operational states and in accident conditions.	
(4) Stationary equipment shall be provided for monitoring the effluents prior to or during discharge to the environment.	
(5) Instruments shall be provided for measuring radioactive surface contamination.	
(6) Facilities shall be provided for monitoring for individual doses to and contamination of personnel.	
6.106. In addition to the monitoring within the plant, arrangements shall also be made to determine the radiological impact, if any, in the vicinity of the plant, with particular reference to:	
pathways to the human population, including the food-chain;	
the radiological impact, if any, on local ecosystems;	
the possible accumulation of radioactive materials in the physical environment; and	
(4) the possibility of any unauthorized discharge routes.	

SAFETY FUNCTIONS FOR BOILING WATER REACTORS, PRESSURIZED WATER REACTORS AND PRESSURE TUBES REACTORS	All of the safety functions in this Annex are fully applicable to the NHR-10. The comments which follow are applicable for the PBMR.
I-1. This Annex gives an example of a detailed subdivision of the three fundamental safety functions defined in para. 406.	
I-2. These safety functions include those necessary to prevent accident conditions as well as those necessary to mitigate the consequences of accident conditions. They can be accomplished, as appropriate, using systems, components or structures provided for normal operation, those provided to prevent anticipated operational occurrences from leading to accident conditions or those provided to mitigate the consequences of accident conditions.	
I-3. A review of various reactor designs shows that current design safety requirements can be met by having systems, components and structures that perform the following safety functions:	
to prevent unacceptable reactivity transients;	
to maintain the reactor in a safe shutdown condition after all shutdown actions;	
to shut down the reactor as required to prevent anticipated operational occurrences from leading to design basis accidents and to shut down the reactor to mitigate the consequences of design basis accidents;	

to maintain sufficient reactor coolant inventory for core cooling during and after accident conditions not involving the failure of the reactor coolant pressure boundary;	This safety function is applicable for the active management of the accident situation, i.e. decay heat removal. If this active system fails, the passive decay heat removal configuration is initiated. In this configuration an acceptable structural temperature must be maintained.
to maintain sufficient reactor coolant inventory for core cooling during and after all PIEs considered in the design basis;	This function is not applicable.
to remove heat from the core after a failure of the reactor coolant pressure boundary in order to limit fuel damage;	Effective decay heat removal depends on radiation between the outer surface of the RPV and its adjacent structures. A new safety function must be introduced regarding the effectiveness of this heat transfer, for example maintaining the emissivity of these surfaces at an acceptable level.
to remove residual heat (see footnote 8) during appropriate operational states and accident conditions with the reactor coolant pressure boundary intact;	
to transfer heat from other safety systems to the ultimate heat sink;	
to ensure necessary services (e.g. electrical, pneumatic, hydraulic power supplies, lubrication) as a support function for a safety system;	
to maintain acceptable integrity of the cladding of the fuel in the reactor core;	This function can be interpreted as referring to the fuel pebbles.
to maintain the integrity of the reactor coolant pressure boundary;	
to limit the release of radioactive material from the reactor containment during and after accident conditions;	
to limit the radiation exposure of the public and site personnel during and after design basis accidents and selected severe accidents that release radioactive materials from sources outside the reactor containment;	
to limit the discharge or release of radioactive waste and airborne radioactive material below prescribed limits during all operational states;	
to maintain control of environmental conditions within the plant for the operation of safety systems and for personnel habitability necessary to allow performance of operations important to safety;	
to maintain control of radioactive releases from irradiated fuel transported or stored outside the reactor coolant system, but within the site, during all operational states;	
to remove decay heat from irradiated fuel stored outside the reactor coolant system, but within the site;	
to maintain sufficient subcriticality of fuel stored outside the reactor coolant system, but within the site;	
to prevent the failure or limit the consequences of failure of a component or structure whose failure would cause the impairment of a safety function.	
I-4. The list of safety functions given above may be utilized as a basis for determining whether a system, component or structure performs or contributes to one or more safety functions and to provide a basis for assigning an appropriate gradation of importance to safety systems, components and structures that contribute to the various safety functions.	

REFERENCES TO ANNEX I

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

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations, Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Siting, Safety Series No. 50-C-S (Rev. 1), IAEA, Vienna (1988).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL LABOUR ORGANISATION, NUCLEAR ENERGY AGENCY OF THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).

Annex II

POSSIBLE PROCEDURE FOR THE DEFINITION OF TARGET WATER RADIOACTIVITY CONTENT

Below are some preliminary considerations of Radiological Protection to identify possible methods to arrive, in any national contest, to the definition of limits for the radioactivity content for drinking water.

The principle of justification (ICRP) has to be considered automatically satisfied since the need for drinking water (or of space heating) is obviously to be satisfied.

As far as the optimization principle, the primary reference could be the IAEA Basic Safety Standards level of annual effective dose for exempted practice or source (Basic Safety Standard, Schedule 1, I-3) equal to 10 μSv per person.

On the basis of this dose value, of the knowledge of the radionuclides present in the drinking water (well known for water being slightly contaminated by reactor water) and of the amount of water drunk by an individual per year it is possible to calculate the maximum activity allowed in the product water.

The same exercise, with obvious adjustments, can be made for the district heating situation: in this case it is important to calculate the effective dose of an individual exposed to radiation coming from heating devices (radiators and so on) containing the slightly radioactive product water.

Annex III

PREVENTION OF THE RADIOACTIVE CONTAMINATION OF PRODUCT WATER

The influence of the reactor type, of the usage of the end product and of various engineering solutions are discussed in the following.

(a) Characteristics of the reactor type

The potential for radionuclide contamination differs significantly depending upon the reactor type. For example, the steam produced by a boiling water reactor would normally not be suitable for direct process use and one or more isolation loops would be required. Though there are concepts which have been proposed, and a limited experience of sea water desalination was done for a short test period in Japan (Kashiwazaki-Kariwa, Unit 1), in practice BWRs have never been used as a source of steam for desalination or similar purposes.

Pressurized water reactors (PWR) and heavy water reactors (HWR) provide a degree of isolation based upon the use of a separate secondary loops. However, since the primary circuit pressure is higher, leaks at the primary/secondary interface within the steam generator might result in radionuclide contamination of steam. While safety studies do not necessarily preclude the direct use of steam from a PWR or HWR in an off-site process, in practice this has not been done in applications to date. Rather, isolation heat exchangers have in all instances to date been incorporated at the reactor site.

In the case of gas cooled reactors with steam generators (e.g. advanced gas cooled reactors (AGR), steam producing high temperature gas cooled reactors (HTGRs)), the steam pressure in the secondary loop is typically higher than the primary circuit gas pressure. Thus, significant radionuclide contamination of the steam is very unlikely to occur from leaks. Tritium diffusion through the steam generator, however, must be considered.

In current liquid metal reactor (LMR) reactor types, the steam is separated from the primary sodium circuit by two heat exchangers. Further, the steam pressure is well above that of the secondary sodium loop. For this configuration, it is clear that a separate steam isolation loop would not be required on the basis of safety. The liquid metal reactor BN-350 in Kazakhstan has shown a long operating experience for water desalination.

(b) Nature of the end product

The product water may have different usage such as process heat, district heating and desalination. Each of these uses will require different degrees of isolation.

(c) Engineering approach

Various engineering approaches have been utilized to minimize the transfer of contamination to the product water. One approach is the use of transfer loops between the reactor loop and the product loop. Assuming a three loop system (i.e. an intermediate loop between the reactor loop and the product loop), pressure may be adjusted in several way. The best way, which is difficult in practice, is for an arrangement where the reactor loop pressure is lower than the

intermediate loop pressure which in turn is lower than the product loop pressure. In this case, transfer between loops is always in the safe direction.

In practice, systems are usually engineered in two ways:

(1) The reactor loop pressure is higher than the intermediate loop; the product loop pressure is higher than the intermediate loop (H-L-H). In this case a pressure barrier against undesired transfer exists between the product loop and the intermediate loop.

(2) The reactor loop pressure is lower than the intermediate loop pressure; the product loop pressure is lower than the intermediate loop (L-H-L). In this case, a pressure barrier against undesired transfer exists between the reactor loop and the intermediate loop.

The H-L-H approach has been employed in the design of the ACT-500 Russian district heating system. The pressures in the primary (reactor), intermediate and product (heating grid) loops are 1.96, 1.2, and 2.0 MPa respectively. The L-H-L approach has been used in the design of the NHR-200 Chinese district heating system. The pressures are 2.5, 3.0 and 1.0 MPa respectively. Each of these approaches has its own advantages and disadvantages as shown below:

	Advantage	**Disadvantage**
ACT-500 (H-L-H)	* Any leakage in the secondary heat exchanger will be directed to the intermediate loop and not to the final product * The allowed radioactive contamination for the intermediate loop is slightly higher and more easily monitored	* The operating pressure for the heating grid is higher
NHR-200 (L-H-L)	* The radioactivities are enclosed inside of primary loop	* It is difficult to monitor the possible contamination of intermediate loop and to exclude the possibility of a leakage from intermediate loop to final product

In some cases, it is difficult to use the approach of H-L-H concept because the pressure of the product loop is dictated by the process itself and it is not very high.

Among the incidents taken into account in a Safety Analysis, the one corresponding to the accidental depressurization of high-pressure intermediate or final loops has to be considered.

Annex IV

AN ASSESSMENT OF PUBLIC EXPOSURES FROM NORMAL OPERATION OF THE CANDESAL® NUCLEAR DESALINATION FACILITY

1. INTRODUCTION

This Annex presents a summary and the main results of a study carried out for Indonesia aimed at evaluating the public exposure from normal operation of a CANDU 6 plant used for desalination using the reverse osmosis and the waste heat from the nuclear plant. The complete study is presented in to this Annex.

The condenser cooling water outflow of a CANDU 6 station has waste heat that can be used to preheat the feedwater of a desalination facility or, as proposed in this study, the condenser outflow water can be used directly as desalination feedwater. The latter option is more energy efficient and does not require an intermediate heat exchanger.

Since the desalination facility is postulated to be sited close to a CANDU 6 station, and to draw its feedwater either from sea water in close proximity to the outfall or directly from the condenser outflow, this introduces the possibility of radiation exposures to the public i.e., radioactivity in the condenser cooling water discharge can be transferred to the desalination feed, to the outflow, and thence to the potable water supply. Public radiation exposures through the potable water supply will be in addition to exposures from the gaseous emissions of the CANDU 6 power station and exposures from background radiation.

The study presents conservative calculations of radiation doses to the most exposed member of the public from consumption of desalinated potable water. There are no projected airborne pathways from normal operation of the desalination plant.

2. RADIOACTIVE SOURCE TERM

The condenser cooling system of a CANDU reactor is a non-radioactive system. However, the low-level radioactive liquid waste system is discharged to the condenser outflow water making the resulting condenser discharge to be slightly radioactive.

Most of the radioactivity contained in the outflow water is tritiated water. Small quantities of other beta/gamma emitters are also present in the outflow.

Note that in a CANDU reactor the heavy water management systems are designed to minimise the losses of heavy water and tritium. One of these systems is a D_2O recovery system which circulates reactor building air through a bed of desiccant. The heavy water vapour collected is extracted in a regeneration stage by heating the desiccant and collecting the condensate. Operating experience has shown that this condensate is principally light water.

Under extreme circumstances, the concentration of heavy water in the condensate is substantially below 0.5%. At these low concentrations it is not cost effective to pass these low isotopic condensates through the heavy water upgrader to recover the heavy water and the associated tritium. For that reasons there are occasions when the low isotopic condensate with the associated tritium is discharged via the liquid waste management system.

Low isotopic condensates are associated with hot, humid summer months. The reference CANDU 6 design allows for humid air drawn through an inlet desiccant bed into the reactor building by the reactor building ventilation system. Some of the associated light water in the air is collected on the inlet desiccant bed, minimizing this source of light water. Dehumidifying the inlet air will raise the isotopic of the condensates collected in the D_2O recovery system and eliminate the discharge of low isotopic heavy water. Waterborne tritium releases are projected to be reduced by a factor of 3 in the next generation CANDU 6 compared with existing plants.

One may propose that the low-level active liquid waste discharge should be routed to a discharge location downstream of the condenser cooling water inlet. This would mean that radiation exposures to the public would be minimised since the waterborne radioactive discharges would be drawn into the condenser cooling water inlet and transferred to the cooling water discharge only after having been diluted to trace concentrations in the bulk ocean. This is a design option that may be invoked if required. However, for the present study, to maintain as much design flexibility as possible, and to be conservative, it is assumed that the condenser outfall waterborne releases of tritium from the low-level active liquid waste discharge are 3.4E14 $Bq.a^{-1}$. This is roughly 45% higher than the CANDU 6 1988–1994 water-borne tritium release average of 1.83E14 $Bq.a^{-1}$. This higher value is used to allow an additional margin in the predictions of consequences from water-borne releases.

The proposed desalination filtration system is composed of a pre-filter, an ultra-filtration unit and a bank of reverse osmosis (R/O) membranes, all in series. These systems would remove most of the particulate/dissolved activity contained in the condenser-outfall/desalination-feed water. The R/O membranes alone are designed to remove the radioactive elements with an efficiency of 97–99% or better. However, in the calculations presented here, for conservatism, the combined pre-filter, ultrafiltration unit and R/O membranes are credited with a total removal efficiency of only 95%.

Note that neither the R/O membranes nor the ultra-filtration units are designed to remove any of the tritium from the potable stream. Therefore, 3.4E14 $Bq.a^{-1}$ of tritium are assumed to be transferred, unattenuated, to the public potable water supply.

The condenser cooling water discharge rate is typically 27 $m^3.s^{-1}$. This translates into 8.5E11 L of cooling water discharged per annum. Therefore, the average concentration of tritium in the condenser cooling water discharge is (3.4E14/8.5E11) = 400 $Bq.L^{-1}$. It is assumed that the tritium concentration in the condenser cooling water is constant. In reality, the instantaneous concentration can exceed 400 $Bq.L^{-1}$, but under normal operations, the annual average will always be less than 400$Bq.L^{-1}$. Since annual doses are being evaluated, the annual average concentration and not the instantaneous concentration is the important value.

3. CALCULATIONAL METHODOLOGY

The pathways analysis methodology recommended in Ref. 2 has been used to calculate doses to the most exposed member of the public. For design flexibility purposes, limiting doses were calculated. This means that doses from the desalinated potable water were calculated for the most exposed member of the public, rather than for a member of the critical group. The most exposed member of the public was taken to be an adult male or a one-year-old infant (whichever produces higher doses) and it is assumed that all the individual's intake of water is derived directly, or indirectly, from the desalination facility.

The following pathways were considered in the assessment:

(1) Intake of drinking water. All of the drinking water is assumed to originate from the desalination plant (tritium and other β/γ emitters). This assumes that commercial drinks such as sodas and carbonated beverages are made with desalinated water.

(2) Immersion/swimming in a pool containing desalinated water (tritium and β/γ emitters).

(3) All bathing and daily hygiene uses (tritium and β/γ emitters).

(4) Evaporation of water and inhalation of the airborne activity by humans (tritium). It is conservatively assumed that the air has a Relative Humidity of 80% and a temperature of 30^0C. It is also conservatively assumed that the relative humidity is entirely due to evaporation of desalinated water with a concentration of 400 $Bq.L^{-1}$.

(5) Evaporation of water and inhalation of airborne tritiated water by animals (e.g. livestock) which are then consumed by humans (tritium).

(6) Irrigation of crops with water from the desalination facility. These crops are consumed directly by humans and by animals that are subsequently consumed by humans (tritium and β/γ emitters). All food intake by animals is assumed to be from crops irrigated by desalinated water.

(7) Consumption of fish inhabiting waters with activity concentrations corresponding to the average tritium and average particulate activity concentrations (tritium and β/γ emitters).

(8) Exposure from ground-deposited activity on the shoreline or elsewhere (β/γ emitters).

4 CONCLUSIONS

The public dose consequences from normal operation of a combined CANDU 6 and Desalination Facility have been conservatively assessed. The radiological consequences are insignificant compared with background doses and are a small fraction of public dose limit (<3.6% of the 1.0 E-03 $Sv.^{-1}$ limit). The majority of the public exposures (99%) will be from tritium in the form of tritiated water. Future CANDU 6 units would be expected to achieve substantial reductions in tritium emissions in the waterborne releases. Since the desalination facility is very effective at removing of elements with large molecular weights, there is likely to be less dose to a member of the public from all sources with the plant operating than if the plant were not present. This is because any increase in tritium dose from the operation of the plant is more than offset by a reduction in dose from natural radionuclides removed by the plant.

The radiological consequences from potential accidents have not been assessed in this study. These would need to be assessed in the next phase of the feasibility study.

REFERENCES TO ANNEX IV

[1] HUMPHRIES, J.R., DAVIS, K., A Technical and Economic Evaluation of The CANDESAL® Approach in Indonesia using Reverse Osmosis and Waste Heat From the CANDU 6 Nuclear Power Plant, CANDESAL Enterprises Inc., Ottawa (1998).

[2] CANADIAN STANDARDS ASSOCIATION, Guidelines for Calculating Derived Release Limits for Radioactive Material in Airborne and Liquid Effluents for Normal Operation of Nuclear Facility, CAN/CSA N 288.1-M87, Etobicoke, Ontario (1987).

Annex V

SAFETY ASPECTS OF THE DESALINATION OF SEA WATER USING NUCLEAR ENERGY*

A. Carnino, N. Gasparini
Division of Nuclear Installation Safety,
International Atomic Energy Agency, Vienna

Abstract

The nuclear plants for desalination to be built in the future will have to meet the standards of safety required for the best nuclear power plants currently in operation or being designed. Some specific characteristics of desalination plants such as siting and coupling require particular consideration from a safety point of view, and further safety studies will be needed when the type and size of the reactor are determined. The current safety approach, based on the defence in depth strategy, has been shown to be a sound foundation for the safety and protection of public health, and gives the plant the capability of dealing with a large variety of sequences, even beyond the design basis. The Department of Nuclear Safety of the IAEA is involved in many activities, the most important of which are to establish safety standards, and to provide various safety services and technical knowledge in many Technical Co-operation assistance projects. The department is also involved in other safety areas, notably in the field of future reactors. The IAEA is carrying out a project on the safety of new generation reactors, including those used for desalination, with the objective of fostering an exchange of information on safety approaches, promoting harmonization among Member States and contributing towards the development and revision of safety standards and guidelines for nuclear power plant design. The safety, regulatory and environmental concerns in nuclear powered desalination are those related directly to nuclear power plants, with due consideration given to the coupling process. The protection of product water against radioactive contamination must be ensured. An effective infrastructure, including appropriate training, a legal framework and regulatory regime, is a prerequisite to considering use of nuclear power for desalination plants, also in those countries with limited industrial infrastructures and little experience in nuclear technology or safety.

1. INTRODUCTION

Several desalination methods are technically feasible and available. Three are currently used on a large scale (Multi-stage Flash, Multi-effect distillation and reverse osmosis), although they have different production throughputs and require different quantities of thermal and electrical energy. Reverse osmosis requires only electrical power (5-7 kWh/m^3); while the other processes require electrical and thermal energy (4.5-24 kWh/m^3).

Nuclear energy has proved to be a viable energy source for desalination, although the economics of the option need to be further investigated, taking into account the infrastructure necessary for nuclear power activities.

There has been a recent resurgence of interest in nuclear powered desalination in North African countries; indeed, the 1996 IAEA General Conference reaffirmed its importance and indicated further activity was needed in this area. In the light of this, it is important to review recent developments in the safety of nuclear power plants and to address some general safety issues and regulatory aspects, as well as some specific safety issues pertinent to this application.

The general approach to safety of nuclear reactors supplying heat or electrical power to desalination plants is equivalent to the approach used for nuclear power plants producing of

* This paper was published in Nuclear Desalination of Sea Water (Proc. Symp. Taejon, 1997), IAEA, Vienna (1997).

electricity. The nuclear plants for desalination to be built in the future will have to meet the standards of safety required for the best nuclear power plants currently in operation or being designed, and for this reason the safety aspects are common with those related to new generation reactors for which a dedicated programme exists at the IAEA. Most of the general safety considerations reported in this paper have been discussed and analysed during the development of this programme. Some specific characteristics of desalination plants such as siting and coupling which require particular consideration from a safety point of view, and further safety studies will be needed when the type and size of the reactor are determined.

2. GENERAL SAFETY ASPECTS OF NUCLEAR POWER PLANTS

Application of the defence in depth strategy will continue to be the overriding approach for ensuring the safety of workers and the public, and for protecting the environment. This strategy is effective in compensating for human and equipment failures, both potential and actual. The concept is based on several levels of protection, including successive barriers that prevent the release of radioactive material to the environment. However, its efficacy depends on rigorous implementation. This implies a determined effort to make the defence effective at each level, particularly for accident prevention and accident mitigation. There is not a unique way to implement defence in depth, since there are different designs, different safety requirements in different countries, different technical solutions and varying management or cultural approaches. Nevertheless, the strategy represents the best general framework to achieve safety for nuclear power plants and, thus, nuclear powered desalination plants. In general, strong implementation of defence in depth requires a determined and constant effort from the design phase, to construction and operation in order to provide graded protection against a wide variety of transients, abnormal occurrences and accidents, including human error and equipment failures within the plant, and events initiated outside the plant.

2.1. Design basis approach and severe accident treatment

Operating nuclear plants are largely designed according to the design basis accidents approach. This means that the plant is deterministically designed against a set of hypothetical accident situations according to well established design criteria in order to meet the radiological targets. The current design basis approach has been shown to be a sound foundation for the safety and protection of public health, in part because of its broad scope of accident sequence considerations, and because of its many conservative assumptions which have the effect of introducing highly conservative margins into the design that, in reality, give the plant the capability of dealing with a large variety of sequences, even beyond the design basis. Often, probabilistic targets for core damage frequency and for containment performance are established. Experience and analysis have shown, however, that some sequences beyond the design basis (i.e. severe accidents) may need to be considered explicitly in the design, providing it with additional safety features to further prevent and mitigate such severe sequences. In this regard probabilistic safety assessment is recognized as a very efficient tool for identifying those sequences and plant vulnerabilities that require specific design features (elimination by design of the most challenging sequences to the containment). This, together with an effective containment system including good control of potential containment by-pass, ensure minimum radiological impact, with an extremely small chance of any off-site radioactive releases. For a nuclear powered desalination plant, the design basis may need to also include some transients or abnormal occurrences that might originate in the desalination unit itself.

2.2. Human error

The contribution of human error to events in the past has been significant. Human errors are a potential source of impairment of defence in depth because human activity is involved at all levels of defence. Therefore, the objectives are that new designs are simpler, and therefore easier to operate, and that specific design provisions are taken to make these plants more tolerant to human failure, as well as to reduce the potential for human interference initiating abnormal plant conditions.

The potential for a deterioration in defence in depth through human failure can be drastically reduced by introducing the following improvements, proposed for new reactors, to make these plants more operator friendly:

(a) Major system simplification through better design and greater inherent design margins that reduce the need for overly complex control systems and procedures;
(b) A greatly improved man-machine interface, with priority given to clear and unambiguous indications of plant parameters, and simpler and more forgiving controls with direct feedback on the results of actions taken;
(c) Prolonged grace periods by providing of increased time constants for the reactor system, or by a higher degree of automation;
(d) Use of symptom based procedures to complement event based procedures for emergency/accident situations;
(e) Greater automation to prevent human error.

2.3. Shutdown and low power states

Recently, increased emphasis has been placed on consideration of non-power states. INSAG-3 and INSAG-10 state that, during normal power operation, all levels of defence should be available at all times. During other plant conditions, an appropriate number of levels have to be available in order to maintain an adequate level of safety. This is because, during certain shutdown conditions, radiological barriers may be rendered ineffective (e.g. reactor coolant pressure boundary, containment) for maintenance or other reasons. Future plants will ensure that the concept of defence in depth can be implemented appropriately under these specific shutdown conditions. Specifically, new reactor designs have explicitly addressed safety in non-power states, primarily through improved defences that reduce the probability and safety significance of loss of decay heat removal events. This is often a design specific determination.

3. SPECIFIC SAFETY ASPECTS OF DESALINATION PLANTS

Simple energy considerations based on a survey of possible sites in North Africa and for different desalination methods show that the total power (electrical and thermal to supply potable water to a medium sized town) needed varies from a few to several hundred megawatts, and thus any proposed reactor falls into the small or medium sized category. Larger sizes would be required for the combined production of water and electrical power.

The nuclear power plants used for water desalination have several characteristics that are similar to those power plants used for district heating reactors (e.g. siting, power size, possibility of combined production), and the experience gained with these plants should be considered in designing nuclear powered desalination plants.

3.1. Coupling

The overall safety of an integrated complex composed of a nuclear reactor plant coupled to a desalination plant is predominantly dependent on the safety of the nuclear reactor plant and the effect of coupling, or rather the interaction between the desalination plant and the nuclear plant. This interaction should be analysed in various coupling situations to assess its effect on the safety of the reactor and on the overall nuclear desalination system, either in normal operation or in an accident situation.

Coupling will not pose any new safety concern if desalination uses only electrical power.

In thermal processes, the energy to be supplied is mainly low temperature process steam or water. Coupling is accomplished via a heat transfer circuit. Since radioactivity exists in the primary steam or hot water, the risk of contamination of product water exists and must be avoided. This can be done by adding intermediate loops maintained at values of pressure such that any leakage would not produce transfer of contamination to the distributed water. These simple measures, together with appropriate instrumentation and monitoring should be effective in preventing contamination of the distributed water. They do not seem to present any particular technical difficulty.

All the information available from the operating experience accumulated on an existing plant (ABTA, Kazakhstan) and from conventional desalination plants will also provide a valuable source of information for design and operation purposes. Operational transients in a desalination plant would have direct feedback into the reactor system. Such transients could have safety implications and need to be assessed.

3.2. Siting

For obvious reasons, the siting of a nuclear powered desalination plant raises some safety concerns, mainly because of the site selection restraints. The plant has to be built on a coastal site and near to populated areas to limit the cost of potable water distribution. The choice of site raises problems related to oceanography (tides, plant elevation) and very often to seismicity (frequent presence of faults on coasts).

The proximity of the nuclear desalination complex to population centres and its implication on the design and to the emergency planning and water supply should be examined.

If the site is in a remote area an important aspect to consider is the availability of adequate external electric power grid or supply for safe operation of the nuclear plant.

4. LEGAL AND REGULATORY ASPECTS OF NUCLEAR SAFETY

There are certain prerequisites for the safe utilization of nuclear power:

(1) To establish a legislative and statutory framework for the regulation of nuclear facilities;

(2) To establish a regulatory body that is independent of the organizations or bodies charged with the promotion or utilization of nuclear energy;

(3) To insure that this regulatory body has the responsibility for authorization (licensing), assessment, inspection and enforcement, and adequate authority, competence and

resources to discharge its assigned responsibilities; no other responsibility assigned to the regulatory body should jeopardize or conflict with its responsibility for regulating safety;

(4) To ensure that there is a clear delineation and separation of responsibilities between the regulatory body and the operating organization.;

(5) To ensure that adequate provision is made for the safe management of radioactive waste;

(6) To establish governmental emergency response capabilities;

(7) To ensure adequate physical protection arrangements;

(8) To provide the technological infrastructure necessary to support the safety of facilities and the radiation related activities.

These basic requirements need to be established well in advance of constructing any nuclear facility and will need considerable resource commitment from any country currently without a nuclear power plant.

In several cases, nuclear desalination plants may be proposed for countries with very little experience of nuclear technology and in particular of nuclear safety. The necessary creation of the infrastructure requires time, human resources and a great deal of training.

There are a large number of new designs that have been proposed for small or medium sized reactors. Although they are mainly based on existing proven technology, they include innovative solutions and systems that require a careful a safety evaluation, safety review and demonstration of licensability which, in some cases, cannot be done by the operator or the local licensing authority because of lack of experience or capability. Licensing of nuclear power plants involves considerable effort and expertise, and good communication between the nuclear authority, the operator and other national authorities. In the case of nuclear powered desalination this will involve additional responsibilities dealing particularly with water use. Joint effort and co-ordination are envisaged between the designer, the utility and the local authorities.

5. THE ROLE AND ACTIVITIES OF THE IAEA

The Department of Nuclear Safety is involved in many activities, the most important of which are to establish safety standards, and to provide various safety services and technical knowledge in many Technical Co-operation assistance projects. The department is also involved in other safety areas, notably in the field of future reactors. The newly established Convention on Nuclear Safety was developed under the auspices of the IAEA.

The IAEA produces many publications related to nuclear safety, the most important of which are those now to be included in the Safety Standards Series (SSS), formerly the Safety Series, which included the NUSS programme. The SSS will comprise three levels: Fundamentals, Requirements and Guides. They will be produced under the authority of the Advisory Commission for Safety Standards (ACSS) and its four subcommittees. These standards are written primarily for national regulatory bodies, which may wish to impose them upon licensees or other related organizations. They are, however, non-binding unless a Member State is receiving assistance or has an agreement with the IAEA, in which case they are mandatory.

5.1. Safety fundamentals (SFs)

Currently, there are three SF publications, but in the long term aim is to combine these into a single publication. These are the first publications in the hierarchy; they present basic objectives, concepts and principles to ensure safety in the development and application of atomic energy or radioactive material for peaceful purposes. The SF publications constitute the reasons why activities must fulfil certain requirements; they do not state what these requirements are, they are self-sufficient and do not include a list of references. In the SF on Safety of Nuclear Installations (SS-110) there are 25 fundamental principles grouped into four main areas, related to the Legislative and Regulatory Framework, the Management of Safety, the Technical Aspects of Safety and the Verification of Safety.

5.2. Safety Requirements (SRs) and Safety Guides (SGs)

Supporting the SFs are Requirements (formerly termed Codes, Standards or Regulations). In the nuclear safety area there will be four main areas: Siting, Design and Operation of thermal neutron nuclear power plants and the Research Reactor Series which has two SR publications. Previously, also Quality Assurance and Governmental Organization were included in the NUSS programme. These have been removed into a 'general safety' category and will be dealt with by the ACSS. All the existing NUSS codes (except QA, which was published in October 1996) are now subject to a comprehensive revision process, which is being overseen by the Nuclear Safety Standard Safety Committee (NUSSAC). This revision will ensure that all the relevant principles in the SF are systematically addressed, thus enabling a coherent set of publications to be produced. The SRs will set out in more detail what is required of Member States to ensure safety in a particular area, and they are governed by the content of the SFs. SRs do not generally present recommendations on or explanations of how to meet the requirements. This more detailed aspect is covered by the third level in the hierarchy, namely, the Safety Guides. The SGs present recommendations on the basis of international experience, of the measures to be followed to meet the requirements set out in the SR publications.

The category of Safety Practice has now been abandoned and these detailed publications will form part of the new Safety Reports Series.

Safety Series publications also deal with Radiation Safety and Waste Safety; they also need to be used as references for national regulations.

5.3. Experience with existing power plants

Over recent years, the IAEA has carried out many missions to operating nuclear power plants, some of which were to reactors of Eastern European countries often used for combined electrical power generation and district heating. A mission was also conducted on the BN-350 plant at ABTA, which is coupled to a desalination plant.

The BN-350 is a sodium cooled fast reactor used to produce electricity and heat. The plant is operated by the Mangyshlak Power Generation Company and its output supplies a large industrial complex, which is relatively isolated from the rest of the Kazakstan electrical grid.

The plant design output is 1000 MW(th), but the current operation is limited to 520 MW(th). The reactor itself is technically separated from the electricity/desalination/heat plant, which takes the steam output and returns feedwater to the nuclear part of the installation.

Therefore, the nuclear safety aspects discussed during an IAEA mission carried out in March 1995 were limited to the nuclear reactor and its cooling system, and did not involve the desalination plant. The topics discussed included detection and control of sodium fires, component ageing, sodium corrosion, vessel in-service inspection, seismic safety and accident analysis.

With the independence of Kazakstan, a new nuclear regulatory body has been created. However, the Kazakstan Atomic Energy Authority still needs assistance in establishing a regulatory body in accordance with current international practice. The IAEA has approved a technical co-operation project to provide this assistance.

Several nuclear plants in the world provide heat for nearby communities. This is a common procedure in WWER plants (Bohunice, Paks, Kola) and other LWRs in cold regions.

Generally, the heated water (or steam) is generated in a separate heat exchanger using part of the steam extracted between the high pressure and low pressure turbines. The pressure in the hot water (steam) distribution system is high enough to ensure that any leaks in the heat exchanger will be into the plant system and not into the water (steam) distribution system. This provision prevents the transfer of possible contamination from the nuclear plants to the heat distribution network.

The technical decision on the amount of diverted steam for district heating purposes depends on economic factors and on the distances involved between a given plant and the nearby towns and villages. No specific safety concerns related to the district heating aspects have been raised during the safety review missions carried out by the IAEA at these plants.

5.4. Current experience accumulated on research reactors

Nuclear desalination plants have been proposed for various Member States, in particular, those that are located in arid areas of Africa, Asia and elsewhere. Many of these countries have no experience at all with nuclear reactors, while a few have one or more research reactors.

Reviewing the experience gained with research reactors in several developing countries the following points can be made that may be applicable to a desalination project:

(1) Experience with a research reactor facility may be quite useful as it usually means that the country already has: a nucleus of a regulatory authority; some infrastructure in radiation protection and waste effluent control related to nuclear reactors; group of knowledgeable personnel in the areas of reactor operations and maintenance; programmes for the training of personnel; and experience with IAEA sponsored projects.

(2) A research reactor facility (especially a larger reactor) can be used to simulate or experiment with some of the processes associated with a desalination plant, and can also be used as a school for training the new staff needed for the new project.

(3) Developing countries vary greatly in their political stability, economic wealth, technological infrastructure, logistical infrastructure, and general technical and safety related attitudes. The following problems have been observed in various countries:

(a) The lack of ability to obtain fresh fuel or spare parts for the reactor because of political instability;
(b) Negligence of important reactor systems that are out of order (for lack of resources, or a proper attitude, or both, in order to replace or repair them)
(c) Lack of an adequate operating budget;
(d) Failure to make use of IAEA assistance (e.g. the equipment procured lies unused for years);
(e) Inadequate security arrangements around the facility (even in riot prone countries);
(f) The lack of any central inspection (e.g. licensing, radiation protection), which is in conflict with the statement made in the previous section;
(g) Unreliable technical and logistical support (electricity, communications, general equipment and spare parts);
(h) The inability to prepare and implement a priority based operational programme.

While gaining experience with a research reactor is expected, in general, to be useful as a first step before introducing nuclear power (or desalination), this same experience can shed light on the deficiencies that may undermine the prospects for such a project unless, in particularly serious cases, adequate international support can be provided.

5.5. IAEA activities on new generation nuclear power plants

The IAEA activities on the safety of new generation reactors, which were formally initiated after the Conference on the Safety of Nuclear Power: Strategy for the Future held in September 1991, are being carried out under the project Safety Approaches to the New Generation of Nuclear Power Plants, foreseen to continue for the next 2 years. The main objective of this project is to foster an exchange of information on safety approaches to new generation nuclear power plants with a view to promoting harmonization among Member States and contributing to the development and revision of safety standards and guidelines for nuclear power plant design. The revision is already in progress and relevant indications have been provided. If is expected that the new standards will have an impact on the design of all nuclear power plants, including those for desalination, constructed in the coming years.

In June 1995, following INSAG's review and comments, the IAEA published a technical publication, Development of Safety Principles for the Design of Future Nuclear Power Plants (IAEA TECDOC-801). The work tried to incorporate the lessons learned from recent operational experience, research and development, design, testing and analysis, as well as from attempts to reflect current trends in reactor safety design. It provides a basis for the development of safety objectives and principles for new generation nuclear power plants and for the revision of safety standards. The key proposal is that severe accidents beyond the existing design basis will be systematically considered and explicitly addressed during the design process for future reactors. The design features provided to address severe accidents are not expected to meet the same stringent requirements (redundancy, diversity and conservative acceptance criteria) used for the safety features to cope with design basis accidents; however, they will be engineered in such a way as to give reasonable confidence that they are capable of achieving their design intent. The publication also emphasizes the need to further lower the risk of any serious radiological consequences and to ensure that the

potential need for prompt off-site protective actions can be reduced or even eliminated (good neighbour concept).

Other safety areas that are specifically addressed in TECDOC-801, and for which new or modified principles were suggested, are:

(1) In the area of safety prevention
– Clarification of the use of probabilistic safety analysis;
– Consideration of modes of operation other than full power (low power and shut down);
– Spent fuel handling and storage;
– Multiple unit sharing equipment.

(2) *In the area of accident mitigation*
– Confinement to mitigate addressed severe accidents.

(3) *In the area of proven engineering safety practices*
– Classification of the safety systems;
– Standardization;
– Consideration of the passive systems;
– Plant security.

(4) *In the area of human factors*
– Design to be user friendly and to avoid complexity;
– Design to reduce dependence on operator action;
– Consideration of operating and maintenance procedures since the design phase;
– Plant security.

Additional effort has been made to prepare a technical publication on the implementation of defence in depth for new generation Nuclear Power Plants. The work was based on the report on defence in depth prepared by INSAG, and the main objective was to bring together the relevant aspects of existing publications on both defence in depth and future reactor designs, and then to apply recent defence in depth formulations specifically to ongoing developments in future plant designs.

Particular attention has been focused on identifying and addressing those factors that have the potential to affect multiple levels of defence in depth. This provides high confidence that appropriate actions will be taken to ensure the effectiveness of the defence in depth concept against failures that have the potential to impact multiple levels of defence in depth. (Human failure, internal and external hazards, etc.).

The report provides a good general framework for a safety evaluation and also gives some indication as to how the defence of each level could be enhanced.

CONCLUSIONS

Use of the nuclear option as an energy source for the desalination process is feasible. The safety, regulatory and environmental concerns in nuclear powered desalination are those related directly to nuclear power plants, with due consideration given to the coupling process. It is important, however, to maintain a progressive approach and to take advantage of state of the art knowledge and techniques; for this reason it is expected that any reactors used for desalination purposes will be designed, constructed and operated in accordance with internationally recognized safety standards.

IAEA missions to operating nuclear power plants coupled to heat production and desalination plants have not revealed any serious specific safety concerns related to the interaction of the nuclear plant with the heat distribution plant or desalination plant, but they have shown that any safety concerns are related to the reactor itself.

Nuclear safety and environmental considerations in nuclear desalination are those arising from the use of nuclear reactors as energy sources. Nuclear safety and regulatory actions should be based on relevant IAEA safety standards. In addition, as a specific requirement, the design, operation and performance of an integrated nuclear desalination complex must ensure the protection of product water against radioactive contamination.

The most serious concern, as experience with research reactors has shown, arises from the fact that very often countries that need water are developing countries, with limited industrial infrastructures and little experience in nuclear technology or safety. An effective infrastructure including appropriate training, a legal framework and a regulatory regime, is a prerequisite to considering use of nuclear power for desalination plants.

Investing in safety, which includes upgrading the national infrastructure, developing competent staff, strengthening the regulatory regime and establishing a positive safety culture, is an essential requirements.

Another relevant aspect is the social and political instability of some countries where nuclear facilities could be possible targets of external attack; the plant would require comprehensive physical protection arrangements.

With respect to existing international safety standards and guides, they also seem to be appropriate covering desalination plants. There seems to be no need to prepare any specific guidance for the safety of nuclear powered desalination plants.

BIBLIOGRAPHY

INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Design, Safety Series No. 50-C-D (Rev. 1), IAEA, Vienna (1988).

INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Research Reactors: Design, Safety Series No. 35-S1, IAEA, Vienna (1992).

INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Governmental Organization, Safety Series No. 50-C-D (Rev. 1), IAEA, Vienna (1988).

INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants, Operation, Safety Series No. 50-C-O (Rev. 1), IAEA, Vienna (1988).

INTERNATIONAL SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

INTERNATIONAL ATOMIC ENERGY AGENCY, Development of Safety Principles for the Design of Future Nuclear Power Plants, IAEA-TECDOC-801, IAEA, Vienna (1995).

INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Fundamentals: The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).

INTERNATIONAL ATOMIC ENERGY AGENCY, Implementation of Defence in Depth for Next Generation Light Water Reactors, IAEA-TECDOC-986, Vienna (1997).

INTERNATIONAL ATOMIC ENERGY AGENCY, Options Identification Programme for Demonstration of Nuclear Power Plants, IAEA-TECDOC-801, IAEA, Vienna (1995).

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

INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Power: Strategy for the Future Conference Proceedings, Vienna, (1991), IAEA, Vienna (1992).

INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Reactor for Seawater Desalination, IAEA-TECDOC-574, IAEA, Vienna (1990).

INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, Report by the International Nuclear Safety Advisory Group, Safety Series No. 75-INSAG-3, IAEA, Vienna (1988).

CONTRIBUTORS TO DRAFTING AND REVIEW

Fiorini, G.L.	Commissariat à l'Energie Atomique, France
Gasparini, M.	International Atomic Energy Agency
Humphries, J.R.	Candesal, Canada
Petrangeli, G.	Agenzia Nazionale per la Protezione dell'Ambiente, Italy
Xue, D.	Institute of Nuclear Energy Technology, China