BASIC PROFESSIONAL TRAINING COURSE

Module IV

Design of a nuclear reactor

IAEA
International Atomic Energy Agency

International Atomic Energy Agency, May 2015

v1.0

Background

In 1991, the General Conference (GC) in its resolution RES/552 requested the Director General to prepare 'a comprehensive proposal for education and training in both radiation protection and in nuclear safety' for consideration by the following GC in 1992. In 1992, the proposal was made by the Secretariat and after considering this proposal the General Conference requested the Director General to prepare a report on a possible programme of activities on education and training in radiological protection and nuclear safety in its resolution RES1584.

In response to this request and as a first step, the Secretariat prepared a Standard Syllabus for the Post-graduate Educational Course in Radiation Protection. Subsequently, planning of specialised training courses and workshops in different areas of Standard Syllabus were also made. A similar approach was taken to develop basic professional training in nuclear safety. In January 1997, Programme Performance Assessment System (PPAS) recommended the preparation of a standard syllabus for nuclear safety based on Agency Safely Standard Series Documents and any other internationally accepted practices. A draft Standard Syllabus for Basic Professional Training Course in Nuclear Safety (BPTC) was prepared by a group of consultants in November 1997 and the syllabus was finalised in July 1998 in the second consultants meeting.

The Basic Professional Training Course on Nuclear Safety was offered for the first time at the end of 1999, in English, in Saclay, France, in cooperation with Institut National des Sciences et Techniques Nucleaires/Commissariat a l'Energie Atomique (INSTN/CEA). In 2000, the course was offered in Spanish, in Brazil to Latin American countries and, in English, as a national training course in Romania, with six and four weeks duration, respectively. In 2001, the course was offered at Argonne National Laboratory in the USA for participants from Asian countries. In 2001 and 2002, the course was offered in Saclay, France for participants from Europe. Since then the BPTC has been used all over the world and part of it has been translated into various languages. In particular, it is held on a regular basis in Korea for the Asian region and in Argentina for the Latin American region.

In 2015 the Basic Professional Training Course was updated to the current IAEA nuclear safety standards. The update includes a BPTC text book, BPTC e-book and 2 "train the trainers" packages, one package for a three month course and one package is for a one month course. The" train the trainers" packages include transparencies, questions and case studies to complement the BPTC.

This material was prepared by the IAEA and co-funded by the European Union.

Editorial Note

The update and the review of the BPTC was completed with the collaboration of the ICJT Nuclear Training Centre, Jožef Stefan Institute, Slovenia and IAEA technical experts.

CONTENTS

1 TYPES OF NUCLEAR REACTOR

Learning objectives

After completing this chapter, the trainee will be able to:

1. *List the basic components of nuclear reactors.*
2. *List the basic types of nuclear power plant.*
3. *Sketch and describe a Pressurized Water Reactor (PWR).*
4. *Sketch and describe a Boiling Water Reactor (BWR).*
5. *Describe the basic features of PHWR, GCR and LWGR reactors.*
6. *Describe a Fast Breeder Reactor.*
7. *Describe the basic features of small and medium reactors.*

1.1 Basic components of a nuclear reactor

A nuclear power plant can be basically divided into the nuclear part and the conventional part. In the nuclear part the fission energy is converted into heat which is used to produce steam. In the conventional part this steam runs the turbine connected to the generator. The conventional part of a nuclear power plant is very similar to a conventional thermal power plant from the boiler onwards. The nuclear part is also called the *Nuclear Steam Supply System* (NSSS); its main component is the **nuclear reactor** where the nuclear fission chain reaction takes place.

The reactor contains **nuclear fuel**, which consists of uranium (sometimes mixed with plutonium). There are, however, two main kinds of uranium atom, called *isotopes*: the majority (99.3%) of the atoms are uranium-238 or ^{238}U, and a small minority (0.7%) is uranium-235 or ^{235}U. Only ^{235}U can sustain a nuclear fission chain reaction. Nuclear fuel can be made from *natural uranium* (with only 0.7% of ^{235}U) or *enriched uranium* where the share of ^{235}U is artificially increased (usually up to 5 %).

The chain reaction is maintained by subatomic particles called *neutrons*. The neutrons born during fission are very energetic and are called *fast neutrons*. For inducing further fissions, however, the most efficient are slow or *thermal neutrons* which have low kinetic energy (0.025 eV). A reactor must therefore have means to slow down neutrons. This is the role of the **moderator**, a material made of light elements. The most usual moderator is ordinary water, also called light water (H_2O).

If ordinary hydrogen ^{1}H is replaced with its heavy isotope deuterium ^{2}H (denoted also D), its compound with oxygen is called *heavy water* D_2O. Heavy water is a more efficient moderator than light water, because it absorbs almost no neutrons in the process of slowing them down. A reactor with heavy water can use natural uranium as fuel, while a light water reactor requires enriched uranium.

A third possible moderator is graphite which is a form of carbon. Similarly to heavy water, graphite-moderated reactors can also use natural uranium fuel. In fact, the first nuclear reactor, built by Enrico Fermi in 1942, used graphite as the moderator.

Nuclear reactions produce large quantities of heat which must be transferred from the fuel. This is the role of the **reactor coolant**. The coolant must be in liquid or gaseous form and should not absorb neutrons substantially. In many cases the reactor coolant and moderator are the same substance, but this is not necessary. In particular, graphite-moderated reactors are cooled with gas (CO_2, He) or light water.

Each reactor also has a **control system**, which is used to start-up the reactor, to shut it down, and to adjust the reactor power level. The control system contains materials that are strong neutron absorbers (boron, indium, cadmium…).

There are several classes (types) of nuclear power plant. The basic distinction between them is defined by the type of fuel, the moderator and the coolant.

In addition to the production of electricity, nuclear reactors are also used for some other purposes. Besides reactors for the propulsion of ships and submarines, these other reactors are mainly **research reactors**. Their design varies considerably, but nevertheless they have the same main components as any nuclear reactor (fuel, moderator, coolant, and control system).

1.2 PRIS – Power Reactor Information System

The IAEA has developed a comprehensive database of existing nuclear power plants worldwide. This database is called the **Power Reactor Information System** or **PRIS** (http://www.iaea.org/pris) and has been maintained by the IAEA for over four decades. PRIS contains information on power reactors in operation, under construction or those being decommissioned. The database covers:

- Reactor specification data (status, location, operator, owner, suppliers, milestone dates) and technical design characteristics.
- Performance data including energy production and energy loss data, outage and operational event information.

Monthly production and power loss data has been recorded in PRIS since 1970 and is complemented by information on nuclear-power generated energy provided to non-electrical applications such as district heating, process heat supply or desalination. Information relating to the decommissioning process of shutdown units is also available from PRIS.

A set of internationally accepted performance indicators has been developed for calculations with PRIS data. The indicators can be used for benchmarking, international comparison, or for analyses of nuclear power availability and reliability according to reactor type, country or worldwide. The analyses can, in turn, be applied to evaluations of nuclear power's competitiveness compared to other power sources.

Two official Agency publications are produced each year using PRIS data:

- *Nuclear Power Reactors in the World* [1], published since 1981, is one of the IAEA's most popular annual publications. It includes specifications and performance history data of operating reactors, as well as reactors under construction, being planned, or reactors being decommissioned.
- *Operating Experience with Nuclear Power Stations in Member States* [2] has been providing comprehensive information on nuclear power reactor performance in IAEA Member States since 1970. The publication contains information and performance data for all operational power reactors. In addition to annual information, the report contains a historical summary of performance during the lifetime of individual reactors and figures illustrating the worldwide performance of the nuclear industry.

1.3 Pressurized Water Reactor - PWR

A significant majority of nuclear power plants are cooled by ordinary water. The main advantage of water is that it is cheap and that there is extensive experience using it as the working medium in conventional thermal power plants. Usually water is used as the moderator as well. Therefore it must be in in liquid state at least in the surroundings of the fuel, because water vapour is less efficient in moderating neutrons and also in heat transfer. At standard atmospheric pressure water boils at 100 °C, therefore the pressure in the reactor should be higher if a higher temperature is desired (in order to achieve a higher thermodynamic efficiency). Water exists as a liquid only below its critical temperature of 375 °C. Therefore the coolant temperature in Light Water Reactors (LWRs) is always below the critical temperature of water.

The first and still the most common type of light water reactor is the **Pressurized Water Reactor**. Its main feature is that the pressure is so high that the water does not boil in the reactor. This pressure is typically around 15.5 MPa (155 bar), the highest temperature of the so-called *primary* water is around 330 °C. The heat from the primary water is transferred to the *secondary* water in **steam generators**. There, secondary water is converted into steam which drives the turbine. The temperature of the steam of around 280 °C also

determines the thermal efficiency – around 34%.

The reactor vessel or pressure vessel is made of steel and is around 22 cm thick. Its diameter is around 4 m and height around 12 m. The fuel is slightly enriched uranium (3 – 5%), which is in the form of several thousand fuel pins around 1 cm thick and around 4 m long.

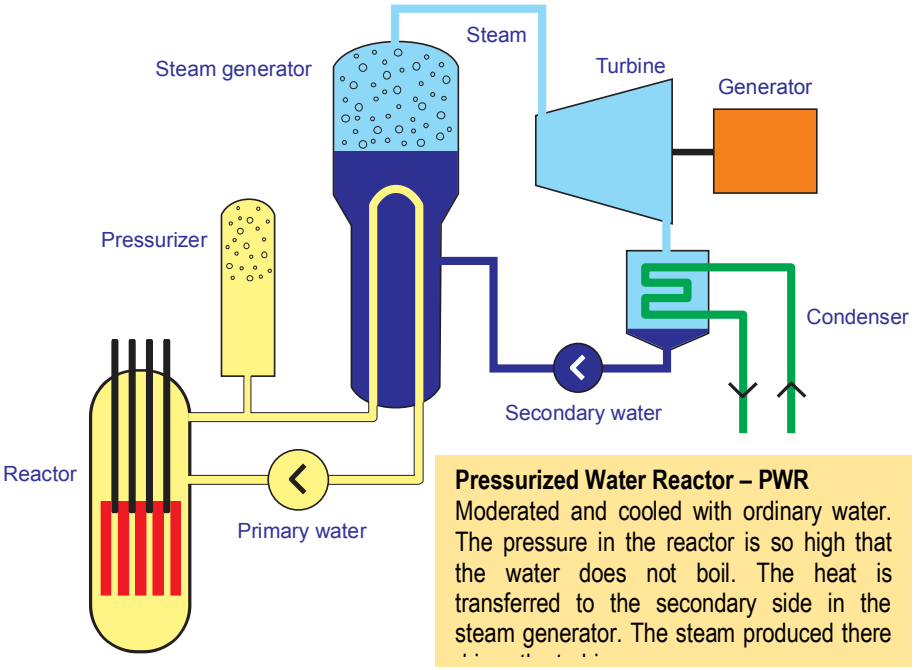


Fig 1.1: Schematics of a Pressurized Water Reactor.

In most cases, the whole *primary system* (reactor vessel, steam generators) is placed inside the **containment**. This is a large steel-concrete building designed, in case of a potential accident, to prevent or minimise the release of radioactive materials in to the environment.

The Russian version of the pressurized water reactor is called **VVER** (Vodo-Vodjanoj Energetičeskij Reaktor – water cooled, water moderated power reactor). The physical principles of a PWR and a VVER reactor are the same, but there several important technical differences. While steam generators in western PWRs are vertical, they are horizontal in VVERs. Older VVERs also don't have a full containment building.

The main advantage of PWRs is that the primary, radioactive coolant is effectively separated from the environment by the intermediate, secondary system. On the other hand, this intermediate system means more components, more possible failures and a higher cost. There have been several problems with steam generator vibrations and leaks in the past.

Nevertheless PWR technology proved to be generally reliable and cost effective. Today around 62 % of all operating NPPs are of this type (53% PWR and 9% VVER).

1.4 Boiling Water Reactor - BWR

The second type of light water reactor is the **Boiling Water Reactor** (BWR). In contrast to a PWR, in a BWR water boils in the reactor itself and the steam produced, with a temperature around 290 °C, is directly led to the turbine. The pressure in the reactor vessel is about half of the pressure in a PWR, so consequently its walls are thinner (around 15 cm). Because the systems for steam separation are inside the reactor vessel, it is larger (diameter around 6 m, height 22 m). The fuel is in several aspects similar to PWR fuel, though not completely the same. Boiling water reactors have containment but its design can vary considerably. Because the turbine is driven by primary steam which becomes radioactive when passing through the reactor core, an additional biological shield is required for the whole steam system.

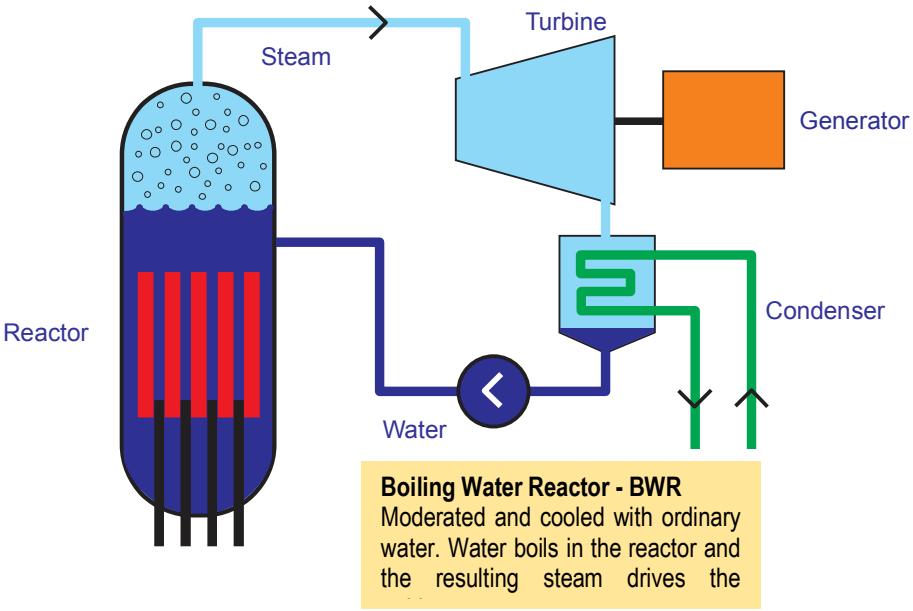


Fig 1.2: Schematics of a boiling water reactor.

The advantage of the boiling water reactor is its relatively simple design; its disadvantage is that the turbine, the condenser and other steam system parts are contaminated with radioactive substances. Despite there being no steam generators, the cost of some other components is higher and the end result is that the total investment and operating costs are very much comparable with those of a PWR. Boiling water reactors are the second most common type of reactor (after PWRs) – around 19 % of reactors in the world are BWRs. The Fukushima Daiichi nuclear power plant had 6 units, all of them BWRs.

1.5 Pressurized Heavy Water Reactor - PHWR

If heavy water is used as moderator, the fuel can be natural uranium. The design of two German-made heavy-water reactors in Argentina has some similarities with light-water PWRs. The Canadians, however, have developed the significantly different concept of the **Pressurized Heavy Water Reactor** (PHWR) which is commonly known under the name **CANDU** (CANada – Deuterium – Uranium). Fuel of natural uranium is contained inside a large number of pressure tubes, through which coolant (heavy water) flows under pressure. A set of these tubes is called a *calandria* and is placed inside a large tank of heavy water which is not pressurized and acts as moderator. The fuel is grouped into so-called '*bundles*', about half a metre long elements, 10 cm in diameter, made of individual fuel pins. This design enables fuel to be replaced on-line, i.e., during operation of the reactor.

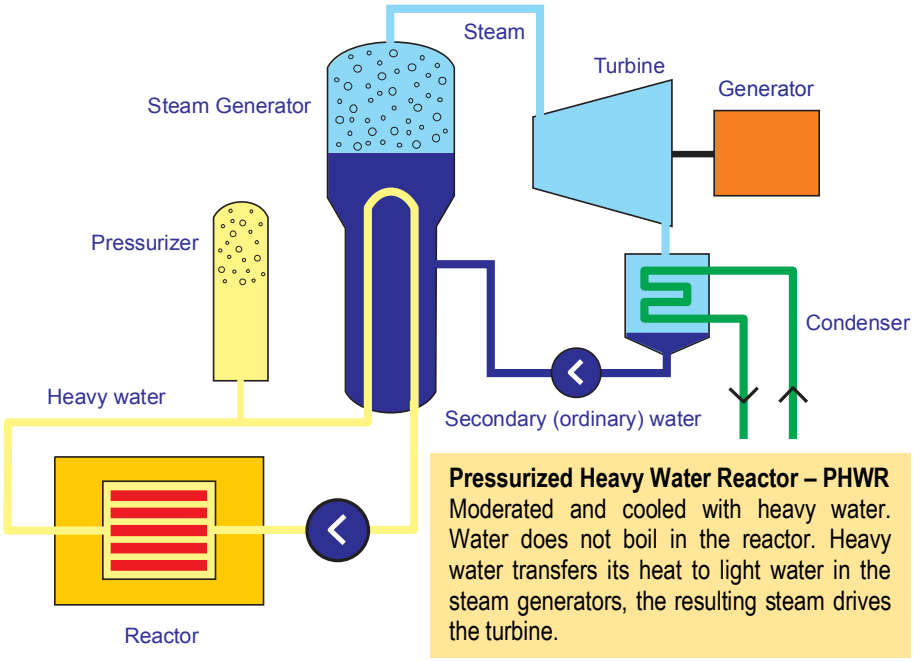


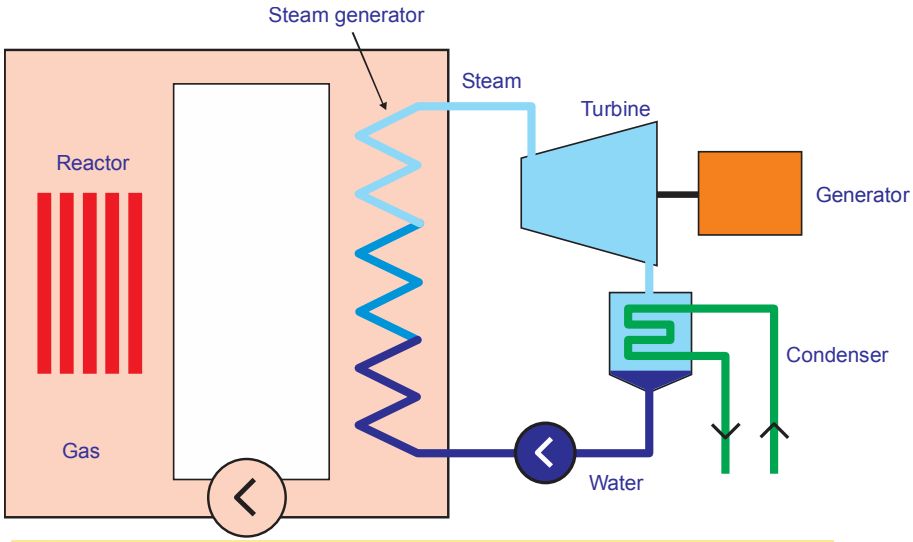
Fig. 1.3: Schematics of the CANDU heavy water reactor.

The main advantage of the CANDU reactor is the possibility to use natural uranium, but with the availability of enriched uranium, it turns out that the most economical operation is achieved by using slightly enriched (around 1%) uranium. The disadvantage of heavy water reactors is the expensive production of heavy water and the replacement of its losses, the relatively complex regulation system and lower thermal efficiency (up to 30% absolute).

Besides Canada, CANDU reactors operate in India, Pakistan, Argentina, South Korea, Romania and China, their share representing 11% of all the reactors in the world.

1.6 Gas Cooled Reactors – GCR, AGR, HTGR

Natural uranium can also be used as fuel in graphite-moderated reactors. Naturally, such reactors require some other medium as the coolant. A type of reactor called the GCR (Gas Cooled Reactor) was developed in the United Kingdom which is cooled with CO_2 at a temperature of around 400 °C. They are also known as Magnox reactors, because their fuel cladding is made of a magnesium alloy. An improved version called the AGR (Advanced Gas-cooled Reactor) uses slightly enriched uranium in stainless steel cladding which allows a CO_2 temperatures up to 650 °C.



Gas Cooled Reactor – GCR, Advanced Gas-cooled Reactor – AGR
The moderator is graphite, the coolant is gas which in the steam generator transfers its heat to water. The resulting steam drives the turbine.

Fig. 1.4: Schematics of gas-cooled reactor.

In the United States two reactors called HTGR (High Temperature Gas-cooled Reactor) were built cooled with helium at a temperature of 750 °C, and the fuel was a mixture of enriched uranium and thorium.

The advantage of gas cooled reactors is their high thermal efficiency, which in principle means that less fuel is consumed for a given production of electricity. Nevertheless other costs, including the investment costs, are higher than for light water reactors. Today gas cooled reactors only operate in the United Kingdom (3 % of all NPPs in the world), but now the British have switched to the PWRs.

1.7 Light Water Graphite Moderated Reactor - LWGR

Graphite moderated reactors can also be cooled with water. In the former Soviet Union such reactors were called RBMKs (Reaktor Bolshoy Moshchnosti Kanalniy – High Power Channel Reactors). Probably for non-proliferation reasons (possibility of plutonium production) such reactors were built exclusively on the territory of the former Soviet Union. In 1986, one of this type of reactors in **Chernobyl** (nowadays in the Ukraine) suffered the worst nuclear accident ever.

In the RBMK reactor, water boils in pressure tubes that encompass the fuel rods. The fuel is uranium enriched to around 2 %. The pressure tubes are distributed in a large graphite structure which acts as the moderator. Steam that is produced in the fuel area is collected in large vessels, the steam separators. The reactor core is quite large and has a complex control system. There is no containment. Refuelling can be done during operation of reactor.

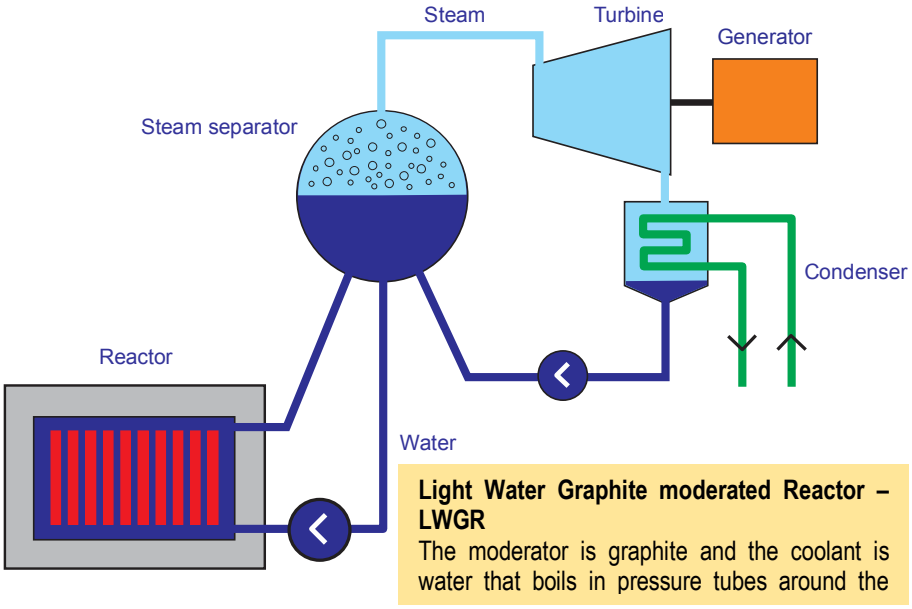


Fig 1.5: Schematics of a light water graphite moderated reactor (RBMK).

An important feature of RBMK reactors is that they are unstable at low power. Besides the lack of safety culture, this was the main cause of the accident that happened in Chernobyl on April 26, 1986.

After the accident, several modifications were made to the remaining RBMK reactors in order to improve their safety but nevertheless new reactors of this type are no longer built. About 3 % of all nuclear power plants today are RBMK reactors and they are all in Russia.

1.8 Fast Breeder Reactor - FBR

In all the reactors described so far the chain reaction is maintained by slow, so-called thermal neutrons. Hence they are also named thermal reactors. But fast neutrons born immediately after fission can sustain a chain reaction, though the underlying technology is more demanding than for a thermal fission chain reaction.

An important feature of fast neutron-induced fission is that a higher number of new neutrons is born compared to thermal neutron-induced fission. To sustain the chain reaction, on average one neutron from

fission is required. Some of the remaining neutrons leak out of the reactor, some are absorbed in various construction materials, but the majority are absorbed in the non-fissile isotope of uranium, ^{238}U. This absorption reaction leads to production of the artificial element **plutonium**, which is fissile and can be used as nuclear fuel. Fast reactors are therefore also often called **breeder reactors**, because in addition to energy they produce more nuclear fuel (plutonium) than they consume. This apparent paradox can be explained by the fact that breeder reactors produce fuel from normally non-fissile ^{238}U which in natural uranium is 140-times more abundant than ^{235}U. In principle, fast breeder reactors could therefore cover world electricity demand for several thousand years.

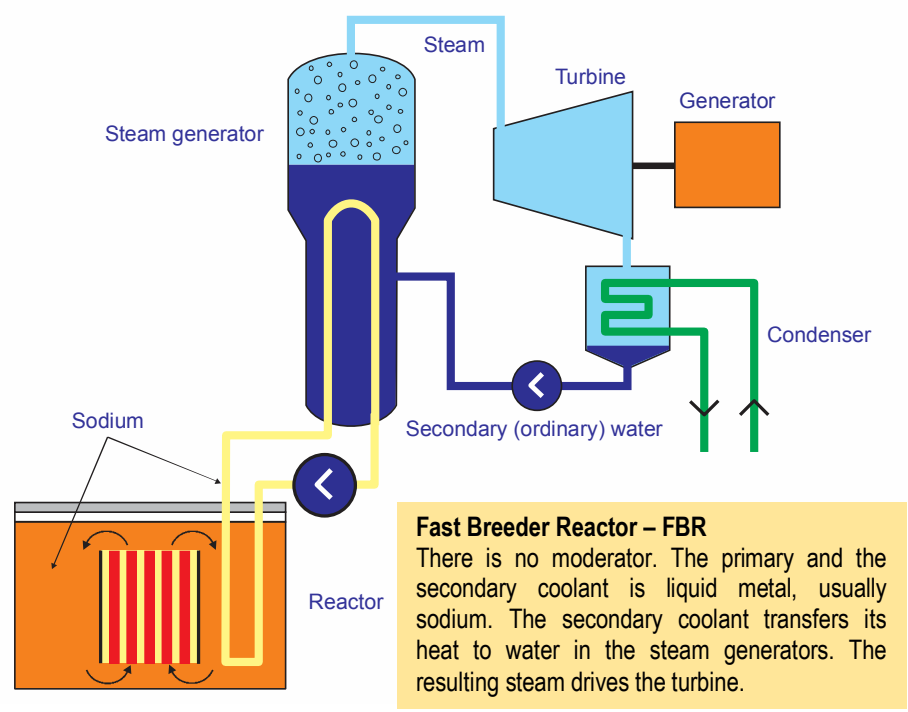


Fig. 1.6: Schematics of a fast breeder reactor.

Plutonium is produced in the nuclear reaction on the non-fissile isotope ^{238}U in all such reactors. Also in thermal reactors substantial quantities of plutonium are produced this way, but on the other hand, significantly less than in breeder reactors.

Fast reactor fuel is 10-30% enriched uranium or is mixed with 10-30% of plutonium. There is no moderator and also the coolant is made of material that does not slow down the neutrons. The majority of fast reactors are cooled with liquid sodium. The boiling point of sodium is quite high, therefore the coolant can be under normal pressure and a pressure vessel is not necessary. Because sodium becomes very radioactive, its heat is transferred to a secondary (non-radioactive) sodium loop which in the steam generator heats water. The resulting steam drives the turbine.

1.9 Small and Medium Reactors – SMR

According to the classification adopted by the IAEA, small reactors are reactors with an equivalent electric power of less than 300 MW(e) and medium sized reactors are reactors with an equivalent electric power of between 300 and 700 MW(e). Worldwide, 131 Small and Medium Reactors (SMR) are in operation in 26 Member States, with a capacity of 59 GWe. As of 2014, 14 SMRs are under construction in 6 countries, namely Argentina, China, India, Pakistan, the Russian Federation and Slovakia. Research is being carried out on approximately 45 advanced SMR concepts for electricity generation, process heat production, desalination, hydrogen generation and other applications in 10 Member States. These include Argentina, Canada, China, France, India, Italy, Japan, Republic of Korea, Russian Federation, South Africa and the United States of America. SMRs are under development for all principal reactor types: light water reactors (LWRs), heavy water reactors (HWRs), gas cooled reactors (GCRs) and liquid metal cooled reactors (LMCRs).

The considerable development work on small to medium sized designs generally aims to provide increased benefits in the areas of safety and security, non-proliferation, waste management, and resource utilization and economy, as well as to offer a variety of energy products and flexibility in design, siting and fuel cycle options. Specifically, SMRs address deployment needs for smaller grids and lower rates of increase in demand. They are designed with modular technology, pursuing economies of series production, factory fabrication and short construction times. The projected timelines of readiness for deployment of SMR designs generally range from the present to 2025–2030. The status and near term prospects of SMRs are described in [3].

1.10 Questions

1. Which subatomic particle sustains the nuclear fission chain reaction?
2. List the four basic components of a nuclear reactor.
3. Which of the uranium isotopes is fissile and what is its abundance in natural uranium?
4. What is the name of the artificial element produced from uranium that is fissile?
5. List two types of reactor that are moderated with ordinary (light) water.
6. Which type of reactor is the most common worldwide?
7. State the moderator for each of the reactors given below:
   a) PWR
   b) CANDU
   c) Chernobyl

d) Fukushima
e) Fast breeder reactor

8. In which types of NPP does the reactor coolant run the turbine?
9. Give two types of nuclear power plant that are moderated with graphite.

2 DESIGN OF RESEARCH REACTORS

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Briefly describe the history and statistics of research reactors.*
2. *List the main types of research reactor.*
3. *Distinguish the main types of research reactor fuel.*
4. *Recognize the importance of research reactors for nuclear safety in power reactors.*

Ever since the first controlled nuclear chain reaction was achieved on 2 December 1942 by a team headed by Enrico Fermi at the University of Chicago, research reactors have played an important role in the development of nuclear science and technology. In contrast to power reactors, whose essential aim is the safe and economical production of energy, usually electricity, research reactors have many and varied goals, leading to many and varied designs and operating modes. Most research reactors are two or more orders of magnitude smaller in power rating than typical power reactors, so the inventory of radioactive materials in their cores is also much smaller, leading to a smaller hazard potential. Nevertheless, safe siting, design and operation are essential to maintain the excellent safety record that research reactors have achieved.

2.1 Research reactor statistics

The IAEA maintains the Research Reactor Database (http://nucleus.iaea.org/RRDB/RR/ReactorSearch.aspx?rf=1) which is periodically updated according to information received from member states. As of May 2014, the following statistical information can be derived from this database:

- During the over 70-year history of research reactors, 747 reactors were built in 69 countries. Of these, 246 reactors in 55 countries are still classified as operational. These reactors range from zero-power critical assemblies to several hundred megawatt experimental power reactors, such as the Phénix reactor in France. The Russian Federation has the largest number of operational research reactors, closely followed by the U.S.A. Twenty-five countries have only a single operational research reactor.
- Of the 55 countries with operational research reactors, 29 of them having 45 operational research reactors do not have an operating power reactor.
- The RRDB lists a total of 501 reactors as either shut down or decommissioned. The database does not distinguish between reactors that are permanently shut down and those that may be in extended shutdown.
- There are 18 reactors listed as either under construction or

planned. However, the viability of several of these projects is uncertain.

One can see that research reactors were and remain very widespread around the world. A significant number of operational research reactors are located in countries that do not have an operating power reactor, and therefore represent a major part of the overall national nuclear programme. In many cases, lack of financial and human resources, ageing of the facility, lack of utilization and inadequate regulatory oversight make continued safe operation of these reactors a significant challenge to the owners, their governments and the international community.

2.2 Research reactor utilization

Research reactors and the neutrons they produce have a very wide variety of uses in nuclear science and technology. These include applications in education and training, biology, agriculture, medicine, analytical and environmental sciences, materials science, geochronology, industry and safety research.

Many research reactors are located at universities and institutes and serve as important tools in education and training. This role may become increasingly important with the increased interest in expansion of nuclear power worldwide, and the need for scientists, engineers and technicians to staff new nuclear power plants and research programmes.

Neutron activation analysis is a widely used technique for determining the concentrations of various trace elements, and is used in biological and agricultural research, forensics, soil assay and similar applications.

The production of radioactive isotopes for use in medical diagnostics and treatment is a major mission of many research reactors. Some of the most important medical isotopes include ^{99}Mo, which decays with a 66 hour half-life, used as a generator of ^{99m}Tc, widely used in blood flow studies and evaluation of the condition of the heart and other internal organs, and ^{131}I, used for thyroid disorders. Another reactor produced isotope, ^{60}Co, has wide applications as a gamma source in medical therapy, food and water sterilization and industrial applications. Some research reactors have been used for boron-neutron capture therapy (BNCT), a technique for treatment of certain cancers.

Research reactors produce neutron beams for use in scattering experiments for determination of material structures and properties. Materials intended for use in nuclear power reactors can be irradiated in a research reactor to evaluate their response, such as embrittlement

or dimensional change, before they are used in a power reactor. Similarly, fuel samples can be tested under steady-state and transient conditions to evaluate performance and safety (see additional discussion below).

Some industrial applications of research reactors include neutron radiography as a complement to X-ray and other non-destructive evaluation techniques, evaluation of residual stresses in machine parts, 'doping' of silicon for use in semi-conductor applications, and irradiation of gemstones to improve their brightness.

Experiments done in research reactors have made significant contributions to the safety of current and future power reactors. More discussion of this aspect of research reactor utilization is found below. Over the years, research reactors have made major contributions to the nuclear industry and to the well-being of humanity. While the need for research reactor services and products remains strong in many areas, there are many challenges to be met in an increasingly economically competitive and safety-conscious environment. One approach to meeting these challenges is consolidation of their functions into modern regional research reactor facilities having the resources to ensure that services are provided at minimum cost and with maximum safety. For example, the European Union is moving towards having a limited number of major research reactor facilities, such as the FRM-II reactor at the Technical University of Munich, primarily for neutron beam research, the Jules Horowitz reactor, under construction at Cadarache, France, primarily for materials testing and in-core irradiations, and possibly the planned PALLAS reactor in the Netherlands.

2.3 Types of research reactor

There are many design variations in research reactors, influenced by the primary purpose of the reactor: materials testing, neutron source, multi-purpose, pulsed, critical experiments, or training. These variations include:

- The cooling system design – pool, tank-in-pool, natural convection air-cooled;
- The moderator – ordinary (light) water, heavy water, graphite, solid hydrogenous compound;
- The reflector – ordinary water, heavy water, beryllium, graphite;
- The fuel – low-enriched uranium, high-enriched uranium, uranium-aluminium alloy, uranium silicide, uranium-zirconium hydride;
- The power level.

Most research reactors of low and medium power (up to the range of one or a few megawatts) are of the open pool, or 'swimming pool', design. These reactors are cooled and moderated by light water and

are generally cooled by natural circulation, although forced circulation cooling may be necessary for operation in the megawatt power range. The water pool is deep enough (several metres) to provide shielding sufficient to make the top of the pool safe for workers. Reflectors of beryllium or tanks of heavy water are commonly used to enhance the core neutron flux. The open pool design is suitable for in-core and in-reflector irradiations, since access to these areas from the top of the pool is relatively unimpeded. Many open pool reactors have beam ports extending radially from the core, providing neutron beams for various experiments, radiography and other uses. Examples of large open pool reactors include OSIRIS (70 MW, Saclay, France) and the Multi-purpose Reactor – G.A. Siwabessy (RAS-GAS, 30 MW, Serpong, Indonesia). The most modern open-pool, multi-purpose reactor is the recently commissioned OPAL (20 MW, Lucas Heights, Australia). Open pool reactors may be suitable for installation of in-core loops to be used for safety testing of fuel elements for power reactors under prototype conditions of pressure and temperature. Examples of such test arrangements include the PHEBUS (38 MW) and CABRI (25 MW) facilities, both at Cadarache, France.

The Training, Research and Isotope Production Reactor of General Atomic (TRIGA) is a widely used example of an open pool reactor. Steady-state power ratings of the TRIGA reactors range from 100 kW to 14 MW. These reactors are unique in that many of them have a pulsing capability. The U-ZrH fuel used provides an inherent, instantaneous negative reactivity feedback when heated in a power pulse, which serves to limit an excursion following a positive reactivity insertion resulting from rapid removal of a transient control rod. A complete tutorial on the TRIGA reactor may be found in the IAEA's safety training material.

Another variation on the open pool design is the so-called 'tank-in pool', in which the reactor core is enclosed in a closed tank through which the coolant is pumped. This design is often used for high power reactors where the coolant loop is slightly pressurized, or in designs using heavy water as a moderator and/or coolant, making it necessary to separate the heavy water from the light water in the tank. Heavy water is used as a moderator when a very high thermal neutron flux is desired for beam port experiments or high-flux irradiations. Examples of this design include FRJ-2 (23 MW, Jülich, Germany), FRM-II (20 MW, Munich, Germany), NRU (130 MW, Chalk River, Canada) and HANARO (30 MW, Daejeon, Korea). The new Jules Horowitz reactor to be built at Cadarache will also be of this design.

A closed tank design is used in cases where a higher power than can be accommodated with a tank-in-pool design is needed. These reactors generally operate at elevated pressure and temperature, and so have some similarities to power reactors. Examples include BR2 (100 MW, Mol, Belgium), HFR (45 MW, Petten, Netherlands), JMTR (50 MW, Oarai, Japan) and HFIR (85 MW, Oak Ridge, USA).

At the other end of the power rating scale, numerous low power reactors used for training, university research, activation analysis and applications requiring only a low neutron flux have been built. These reactors are typically rated at a few tens of kilowatts or less. Noteworthy designs of this type include the Canadian Safe Low Power Critical (K) Experiment (SLOWPOKE), the Chinese Miniature Neutron Source Reactor (MNSR) and Argonne's Nuclear Assembly for University Training (ARGONAUT) from the U.S.A.

2.4 Research reactor fuels

The fuels used in research reactors, like the designs, are very diverse. The most common form is plates or concentric tubes of U-Al alloy or U_3Si_2Al dispersion, clad with aluminium. The U-Al fuels are typically enriched to about 93% ^{235}U, while the silicide fuels are enriched to 19.75% ^{235}U. Many research reactor designed in the Soviet Union now use 36% enriched fuel.

TRIGA reactors use a U-ZrH or U-$ZrH_{1.65}$ alloy fuel in Al or 304 stainless steel cladding. The original TRIGA fuel was 20% enriched, but some reactors converted to the FLIP (Fuel Life Improvement Programme) fuel, which is 70% enriched.

In an effort to remove highly enriched uranium from research reactors worldwide, the IAEA, the U.S.A. and the Russian Federation are cooperating in the Reduced Enrichment Research and Test Reactor (RERTR) programme. The RERTR programme, started in 1978 at the Argonne National Laboratory in the U.S.A., has as its aim conversion of as many research reactors as possible to low-enriched uranium (LEU) fuel (less than 20% ^{235}U) without unacceptable penalties in performance of the reactors. A reduction in the enrichment by a factor of about 5 means an increase in the content of ^{238}U in the fuel, resulting in increased neutron absorption and decreased density of fissile atoms. To compensate, it is necessary to increase the total mass of uranium, which requires a fuel with a higher uranium density. The RERTR programme has developed U_3Si_2 fuel, enriched to 19.75% with a uranium density of 4.8 g/cm^3. Qualification studies carried out by the Argonne Laboratory, in cooperation with CEA and CERCA in France, have shown that the irradiation behaviour of the silicide fuel is satisfactory. It is now also being manufactured in Russia for use in Soviet-designed research reactors. AECL (Atomic Energy of Canada Limited) has also developed and qualified Al-U_3Si dispersion fuel which is used in the NRU and HANARO reactors. LEU fuel development is continuing to produce and qualify a fuel having an even higher density so that the very high power reactors that at present cannot use the silicide fuel successfully can be converted.

2.5 Research reactors and power reactor safety

Experiments conducted in research reactors have been of great importance in developing the safety technology for power reactors and our understanding of the behaviour of materials under irradiation and in accidents.

Steady-state irradiation of sample fuels, cladding and structural material have been carried out in many materials testing reactors. Because these reactors can operate at a much higher power density and neutron flux than is available in power reactors, it is possible to achieve high levels of fuel burn-up and materials neutron fluence in a much shorter time than would be possible in a power reactor. Thus, research and development of new fuels and materials can proceed at a faster rate than would otherwise be possible.

Experiments in research reactors have contributed significantly to safety technology for both water-cooled and sodium-cooled reactors. These experiments generally involve fuel and material samples and are highly instrumented to monitor changes under conditions simulating transient and accident conditions. Measurements of interest include, inter alia, fuel failure energy in transients, fuel relocation following failure, fission product release from failed fuel and fission product transport in the reactor cooling system.

Some of the reactors used and the types of experiments done include:

- The PHEBUS reactor (Cadarache, France): The PHEBUS-FP experiments simulated a severe accident in a PWR involving meltdown of a portion of the core to study the release of fission products and their subsequent behaviour in the primary coolant system and the containment.
- The CABRI reactor (Cadarache, France): This reactor was used for a series of experiments simulating accidents in fast reactors intended to provide data for validation of computer codes that model fuel failure and fuel relocation in such severe accidents. It was later used for measurements of the failure energy of irradiated LWR fuel samples, and is now being refurbished for use in further LWR safety experiments.
- The Transient Reactor Test (TREAT) facility (Argonne National Laboratory – West, now Idaho National Laboratory, U.S.A.): This reactor has been used for many simulations of fast reactor accidents to obtain data on fuel failure and fuel relocation for modelling and code validation.
- The Japan Safety Research Reactor, JSRR (O'arai, Japan): Experiments on failure of LWR fuels have been conducted in this reactor.
- The Impulse Graphite Reactor, IGR (Semipalatinsk, Kazakhstan): This reactor has been used for many transient experiments on LWR fuels and recently on a programme of experiments to investigate fuel relocation in fast reactor

accidents.

- The BR-2 reactor (Mol, Belgium): This reactor hosted a series of experiments simulating fuel failure and meltdown in fast reactor accidents.

2.6 Questions

1. Describe the study areas in which the research reactors are used.
2. List some of the most important medical isotopes that are produced in research reactors.
3. List some of the most important types of research reactor.
4. Briefly describe the open pool TRIGA reactor.
5. What are most common fuels used in research reactors?
6. Explain how the use of research reactors contributes to the development of the safety of power reactors.

3 SAFETY CONCEPTS IN THE DESIGN OF NUCLEAR REACTORS

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe the basic safety objectives in the design of a nuclear installation.*
2. *Define the term "Design Basis Accident (DBA)".*
3. *Define the term "Postulated Initiating Event (PIE)".*
4. *List the levels of defence in the design of a nuclear installation.*
5. *Describe the concept of a series of physical barriers.*

3.1 Basic safety objectives

The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation. [4]

This fundamental safety objective of protecting people (individually and collectively) and the environment has to be achieved without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. To ensure that such facilities are operated and activities conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken:

- To control the radiation exposure of people and the release of radioactive material to the environment;
- To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;
- To mitigate the consequences of such events if they were to occur. [4]

In order to achieve the safety principles in designing a nuclear power plant, a comprehensive safety analysis is carried out to identify all sources of exposure and to evaluate the radiation doses that could be received by workers at the installation and the public, as well as potential effects on the environment. In this context, the following definitions are important:

Design basis accident (DBA) is a postulated accident condition against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits. [4]

Postulated initiating event (PIE) is an event identified during design as capable of leading to anticipated operational occurrences or accident conditions. [4]

In the design of a nuclear power plant, the safety analysis examines all plant states:

- all planned normal operational modes of the plant;
- plant performance in anticipated operational occurrences;
- design basis accidents;
- event sequences that may lead to a severe accident; and
- severe accidents.

On the basis of this analysis, the robustness of the engineering design in withstanding postulated initiating events 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.

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 loss of control of the reactor, there is a non-negligible probability that an accident may happen. Measures are therefore taken to ensure that the radiological consequences are mitigated. Such measures include:

- engineered safety features and systems;
- on-site accident management procedures established by the operating organization;
- possible off-site intervention measures established by the appropriate authorities in order to mitigate radiation exposure if an accident has occurred.

3.2 The concept of defence in depth

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.

First level of defence

Its aim is to prevent deviations from normal operation and the failure of items important to safety. This leads to the requirement that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, it is important to select appropriate design codes and materials, and to pay attention to quality control in the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal

hazards contribute to the prevention of accidents at this level of defence.

Second level of defence

Its aim is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. This recognises 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.

Third level of defence

For this level, it is assumed that, although very unlikely, escalation of certain anticipated operational occurrences or PIEs might not be controlled at a preceding level and that an accident could develop. These unlikely events are anticipated in the design of the plant.

This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures must be capable of preventing damage to the reactor core or significant off-site releases and of returning the plant to a safe state.

Fourth level of defence

Its aim is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. The most important objective of this level is the protection of the confinement function and thus to ensure that radioactive releases are kept as low as reasonably achievable.

Fifth level of defence

This is the final level of defence 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.

A relevant aspect of the implementation of defence in depth is the provision in the design of a **series of physical barriers**, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations. The number of barriers that are necessary depends upon of amount and the radionuclidic composition of the radioactive material, the effectiveness of the individual barriers, the possible internal and external hazards, and the potential consequences of failures.

3.3 Questions

1. What is the fundamental safety objective for a nuclear installation?
2. Which tools are used to ensure that safety objectives are met?
3. Describe the meaning of the abbreviations DBA and PIE.
4. How many levels of defence in depth are there in the design of a nuclear installation?
5. Give an example of a series of physical barriers in a nuclear power plant.
6. Give an example of a series of physical barriers in a radwaste repository.

4 BASIC SAFETY FEATURES OF THE DESIGN

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe the main organizational requirements of the design organization.*
2. *Describe the main design management requirements.*
3. *Describe the main design requirements for defence in depth.*
4. *Define the main fundamental safety functions which must be ensured.*
5. *List and briefly describe the main requirements for plant design.*
6. *List and briefly describe main requirements for the design of plant systems.*

The principal safety requirements for the design of nuclear power plants are given in SSR-2/1, Safety of Nuclear Power Plants: Design, Specific Safety Requirements [5].

4.1 Management of safety

The operating organization has overall responsibility for safety. However, the design organization must ensure that the installation is designed to meet the requirements of the operating organization, including any standardized utility requirements. Thus, the design organization must:

- implement safety policies established by the operating organization;
- have a clear division of responsibilities with corresponding lines of authority and communication;
- ensure that it has sufficient technically qualified and appropriately trained staff at all levels;
- establish clear interfaces between the groups engaged in different parts of the design, and between designers, utilities, suppliers, constructors and contractors as appropriate;
- develop and strictly adhere to sound procedures;
- review, monitor and audit all safety-related design matters on a regular basis; and
- ensure that a safety culture is maintained.

The design management for a nuclear power plant must ensure that:

- all components important to safety have the appropriate characteristics 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,
- the requirements of the operating organization are met,
- due account is given to the capabilities and limitations of the

personnel who will eventually operate the plant,
- adequate safety design information is supplied to ensure safe operation and maintenance of the plant **and to allow subsequent plant modifications** to be made,
- recommended practices for incorporation into the plant administrative and operational procedures are supplied (i.e. operational limits and conditions),
- the results of the deterministic and complementary probabilistic safety analyses are taken into account, so that due consideration has been given to the prevention of accidents and mitigation of their consequences,
- 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.

Wherever possible all components important to safety must be:
- designed according to the latest or currently applicable approved standards,
- of a design proven in previous equivalent applications,
- selected to be consistent with the plant reliability goals necessary for safety.

Where an unproven design or feature is introduced or there is a departure from an established engineering practice, its safety must be demonstrated to be adequate:
- by appropriate supporting research programmes, or
- by examining operational experience from other relevant applications.

The design must take due account of relevant operational experience that has been gained in operating plants and of the results of relevant research programmes.

A comprehensive safety assessment is carried out to confirm that the design as delivered for fabrication, for construction and as built meets the safety requirements set out at the beginning of the design process.

The safety assessment must be part of the design process, with iteration between the design and confirmatory analytical activities, and increasing in scope and level of detail as the design programme progresses.

The operating organization ensures 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.

A quality assurance programme that describes the overall arrangements for the management, performance and assessment of the

plant design must be prepared and implemented. This programme is supported by more detailed plans for each system, structure and component so that the quality of the design is ensured at all times.

The design, including subsequent changes or safety improvements, must be performed in accordance with established procedures that call on appropriate engineering codes and standards, and must incorporate applicable requirements and design bases. Design interfaces are identified and controlled.

The adequacy of the design, including design tools and design inputs and outputs, must be verified or validated by individuals or groups separate from those who originally performed the work. This verification, validation and approval must be completed before implementation of the detailed design.

4.2 Principal technical requirements

Defence in depth is incorporated into the design process. The design therefore:

- provides multiple physical barriers to the uncontrolled release of radioactive materials to the environment;
- is conservative, and the construction must be of high quality, so as to provide confidence that plant failures and deviations from normal operation are minimized and accidents prevented;
- provides for control of the plant behaviour during and following a PIE, using inherent and engineered features, i.e. uncontrolled transients are minimized or excluded by design to the extent possible;
- provides 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;
- provides equipment and procedures to control the course and limit the consequences of accidents as far as practicable;
- provides 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.

To ensure that the overall safety concept of defence in depth is maintained, the design must 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.

The design must 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.

To ensure safety, the following fundamental safety functions must be capable of being performed in operational states, in and following a design basis accident and, to the extent practicable, in and after the occurrence of plant conditions considered to be beyond those of design basis accidents:

- Control of the reactivity;
- Removal of heat from the core;
- Confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

A systematic approach is followed to identify the systems, structures and components that are necessary for fulfilling the safety functions at all times following a PIE.

The plant design is such that its sensitivity to PIEs is minimized. The expected plant response to any PIE must be those of the following that can reasonably be achieved (in order of importance):

- A PIE produces no significant safety-related effect, or produces only a change in the plant towards a safe condition due to its inherent characteristics; or
- Following a PIE, the plant is rendered safe by passive safety features or by the action of safety systems that are continuously operating in a state necessary to control the PIE; or
- 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
- Following a PIE, the plant is rendered safe by specified procedural actions.

In order to achieve the main safety objectives incorporated in the design of a nuclear installation, all actual and potential sources of radiation must be identified and properly considered, and provision is made to ensure that such sources are kept under strict technical and administrative control.

The design must have as an objective the prevention or, if this fails, the mitigation of radiation exposures resulting from design basis accidents and selected severe accidents.

Plant conditions that could potentially result in high radiation doses or radioactive releases are restricted to a very low likelihood of occurrence, and it is further ensured that the potential radiological consequences of conditions with a significant likelihood of occurrence are only minor.

4.3 Requirements for plant design

Safety classification

All items important to safety (components, including software for instrumentation and control, etc.) must be first identified and then classified on the basis of their function and significance with regard to safety. They are designed, constructed and maintained such that their quality and reliability is commensurate with this classification.

The method for classifying the safety significance of items important to safety is primarily 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 frequency with which the item will be called upon to perform a safety function; and
- The time following a PIE at which, or the period for which, the item will be called upon to perform a safety function (operate).

The design ensures 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

For all items important to safety the design basis specifies the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards. The items mentioned above must meet specific acceptance criteria over the lifetime of the nuclear power plant.

If the design basis for each item important to safety is systematically justified and documented, then this documentation could provide information necessary for safe plant operation.

Categories of plant conditions

Plant conditions are identified and grouped into a limited number of categories according to their frequency of occurrence at the NPP. The categories typically cover:

- Normal operation;
- Anticipated operational occurrences which are expected to occur over the operating lifetime of the plant;
- Design basis accidents; and
- Design extension conditions, including accidents with significant degradation of the reactor core (in old terminology: severe accidents).

Postulated initiating events

In designing the plant, it is recognized that challenges to all levels of defence in depth may occur and design measures are 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

An analysis of PIEs is made to establish all those internal events that may affect the safety of the plant. These events may include equipment failures or malfunctions.

Fires and explosions

All components important to safety are 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 the state of the plant is maintained. These requirements are achieved by suitable incorporation of:

- redundant parts,
- diverse systems,
- physical separation, and
- design for fail-safe operation.

Such incorporation achieves the following objectives:

- Prevents fires from starting;
- Detects and extinguishes quickly those fires which do start, thus limiting damage;
- Prevents the spread of those fires that have not been extinguished, thus minimizing their effects on essential plant functions.

A fire hazard analysis of the plant is carried out to determine the necessary rating of the fire barriers, and fire detection and firefighting systems of the necessary capability are then provided.

Other internal hazards

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 site are taken into account in the design of the plant. Appropriate preventive and mitigatory measures are 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 are also considered in the design, where appropriate.

External events

The design basis natural and human induced external events are determined for the proposed combination of site and plant. All those

events with which significant radiological risk may be associated are considered. A combination of deterministic and probabilistic methods are used to select a subset of external events that the plant is designed to withstand, and the design bases are determined.

Natural external events that are considered include those that have been identified in site characterization, such as earthquakes, floods, high winds, tornadoes, tsunami (tidal waves) and extreme meteorological conditions. Human induced external events that are considered include those that have been identified in site characterization and for which design bases have been derived.

Site-related characteristics

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, are taken into account.

Combinations of events

Where combinations of randomly occurring individual events could credibly lead to anticipated operational occurrences or accident conditions, they are considered in the design. Certain events may be the consequences of other events, such as a flood following an earthquake. Such consequential effects are considered to be part of the original PIE.

Design limits

A set of design limits consistent with the key physical parameters for each structure, system or component are specified for operational states and design basis accidents.

Operational states

The plant is 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) are assumed to be available. The design is such that the response of the plant to a wide range of anticipated operational occurrences allows 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. 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, is addressed in the design, and appropriate limitations on the unavailability of safety systems are specified.

Design basis accidents

A set of design basis accidents is derived from the listing of PIEs in order to set the boundary conditions according to which the structures, systems and components important to safety are designed.

Where prompt and reliable action is necessary in response to a PIE, provision is made to initiate the necessary safety system actions 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 is revealed in sufficient time and that adequate procedures (such as administrative, operational and emergency procedures) are defined to ensure the reliability of such actions.

Severe accidents

Certain very low probability plant conditions may jeopardize the integrity of many or all of the barriers to the release of radioactive material. These conditions are beyond design basis accidents which may arise owing to multiple failures of safety systems, leading to significant core degradation. These event sequences are called severe accidents. Consideration is given to these severe accident sequences, using a combination of engineering judgement and probabilistic methods, in order to determine those sequences for which reasonably practicable preventive or mitigatory measures can be identified. Acceptable measures are based upon realistic or best estimate assumptions, methods and analytical criteria do and not necessarily involve application of the conservative engineering practices used in setting and evaluating design basis accidents. On the basis of operational experience, relevant safety analysis and results from safety research, design activities for addressing severe accidents take into account the following:

- Important event sequences that may lead to a severe accident are identified using a combination of probabilistic methods, deterministic methods and sound engineering judgment.
- These event sequences are then reviewed against a set of criteria aimed at determining which severe accidents are addressed in the design.
- Potential design changes or procedural changes that could either reduce the likelihood of these selected events, or mitigate their consequences, are evaluated and implemented if reasonably practicable.
- Consideration is given to the plant's full design capabilities, including the possible use of some systems beyond their originally intended function and anticipated operating conditions, 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 is 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 are established, taking into

account representative and dominant severe accident scenarios.

4.4 Design for reliability of systems and components

All components important to safety are designed to be capable of withstanding all identified PIEs with sufficient reliability.

Common cause failures

The potential for common cause failures of items important to safety is considered to determine where the principles of diversity, redundancy and independence should be applied to achieve the necessary reliability.

Single failure criterion

The single failure criterion is applied to each safety group incorporated in the plant design.

Spurious action is considered as one mode of failure when applying the concept to a safety group or system.

Compliance with the criterion is considered to have been achieved when each safety group has been shown to perform its safety function 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 is exceptional, and must be clearly justified in the safety analysis.

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.

Fail-safe design

The principle of fail-safe design is considered and incorporated into the design of systems and components important to the safety of the plant as appropriate. If a system or component fails, plant systems are designed to pass into a safe state with no necessity for any action to be initiated.

Auxiliary services

Auxiliary services that support equipment that forms part of a system important to safety are considered to be part of that system and are classified accordingly. 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.

In-service testing, maintenance, repair and inspection

All components important to safety are 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 is 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 site personnel to radiation.

Ageing

Appropriate margins are provided in the design for all 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.

Human factors

The design must be operator friendly and aimed at limiting the effects of human error. Attention is 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.

Systematic consideration of human factors and the human-machine interface is included in the design process at an early stage and continues throughout the entire process to ensure an appropriate and clear distinction of functions between operating personnel and the automatic systems provided.

The human-machine interface is designed to provide the operators with comprehensive but easily manageable information, compatible with the necessary decision and action times. Similar provisions are made for the supplementary control room.

The design is aimed at promoting the success of operator actions with due regard to 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 must be kept to a minimum. The design takes into account 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, i.e. that the information necessary for the operator to make such a decision is simply and unambiguously presented. It also must be taken into account that following an event, the physical environment in the control room or in the supplementary

control room, and the access route to that supplementary control room, is acceptable.

4.5 Other design considerations

Sharing of safety systems between multiple units of a nuclear power plant

Safety systems must not be shared between two or more nuclear power plants unless this enhances safety.

In exceptional cases it is permitted that safety system support features and safety related items are shared between two or more units, but it must be demonstrated that this design contributes to safety. If such sharing does not contribute to safety (or even increases the likelihood or the consequences of an accident at any unit of the plant), then this design must not be permitted.

Systems containing fissile or radioactive materials

All systems within a nuclear power plant that may contain fissile or radioactive materials must be designed:

- To prevent the occurrence of events that could lead to an uncontrolled radioactive release to the environment;
- To prevent accidental criticality and overheating;
- To ensure that radioactive releases of material are kept below authorized limits on discharges in normal operation, and below acceptable limits in accident conditions, and are kept as low as reasonably achievable; and
- To facilitate mitigation of the radiological consequences of accidents.

Escape routes from the plant

The nuclear power plant is 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.

Escape routes must meet national and international requirements for radiation zoning and fire protection, and national requirements for industrial safety and plant security.

After an event considered in the design, there must be available at least one escape route from working and other occupied areas.

Communication systems at the plant

Effective means of communication are provided throughout the nuclear power plant to facilitate safe operation in all modes of operation. It is also important that communication is functional after events considered in the design.

Suitable alarm systems and means of communication are provided so that all persons present in the plant and on site can be warned and instructed, even under accident conditions.

Suitable and diverse means of communication necessary for safety within the nuclear power plant, in the immediate vicinity and with off-site agencies is ensured and must be available at all times.

Control of access

The plant is isolated from the surroundings by a suitable layout of the structural elements in such a way that access to it can be permanently controlled. In particular, in the design of the buildings and the layout of the site provision is made for operating personnel and/or equipment, and attention is paid to guarding against the unauthorized entry of persons and goods to the plant.

Unauthorized access to, or interference for any reason with items important to safety (including computer hardware and software) must be prevented.

Prevention of harmful interactions of systems important to safety

If there is a significant probability that systems important to safety will have to operate simultaneously, their possible interaction is evaluated, and the effects of any harmful interactions are prevented. In the analysis, account is taken not only of physical interconnections, but also of the possible effects of one system's operation, malfunction or failure on the physical environment of other essential systems, in order to ensure that such changes in the environment do not affect the reliability of system components in functioning as intended.

Interactions between the electrical power grid and the plant

The design of NPP must be such that the functionality of items important to safety is not compromised by disturbances in the electrical power grid, including loss of supply, anticipated variations in the voltage and frequency of the grid supply.

Decommissioning

At the design stage, special consideration is given to the incorporation of features that facilitate the decommissioning and dismantling of the plant.

4.6 Safety analysis

A safety analysis of the plant design must be conducted in which methods of both deterministic and probabilistic analysis are applied. On the basis of this analysis, the design basis for items important to safety are established and confirmed. It is also demonstrated that the plant as designed is capable of meeting the prescribed and acceptable

limits for potential radiation doses and radioactive releases for each category of plant conditions, and that defence in depth has been achieved.

Deterministic approach

The deterministic safety analysis includes the following:

- Confirmation that operational limits and conditions are in compliance with the assumptions and intent of the design for normal operation of the plant;
- Characterization of the PIEs 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 the automatic response of safety systems in combination with prescribed actions of the operator.

The applicability of the analytical assumptions, methods and degree of conservatism used must be verified. The safety analysis of the plant design is updated with regard to significant changes in plant configuration, operational experience, and advances in technical knowledge and understanding of physical phenomena, and is consistent with the current or ”as built” state.

Probabilistic approach

A probabilistic safety analysis of the plant is carried out so as:

- To provide a systematic analysis to give confidence that the design complies 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”) are 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 the 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.

4.7 Requirements for design of plant systems

Safety recommendations for the design of plant systems are given in several Safety Guides:

- NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants [6]
- NS-G-1.4, Design of Fuel Handling and Storage Systems in Nuclear Power Plants [7]
- NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants [8]
- NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants [9]
- NS-G-1.7, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants [10]
- NS-G-1.8, Design of Emergency Power Systems for Nuclear Power Plants [11]
- NS-G-1.9, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants [12]
- NS-G-1.10, Design of Reactor Containment Systems for Nuclear Power Plants [13]
- NS-G-1.11, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants [14]
- NS-G-1.12, Design of the Reactor Core for Nuclear Power Plants [15]
- NS-G-1.13, Radiation Protection Aspects of Design for Nuclear Power Plants [16]

Reactor core and associated features

General design

The reactor core and associated coolant, control and protection systems must be designed with appropriate margins to ensure that the specified design limits are not exceeded and that radiation safety standards are met in all operational states and in design basis accidents, with account taken of the existing uncertainties.

The maximum degree of positive reactivity and its maximum rate of increase by insertion in operational states and design basis accidents is limited so that no resultant failure of the reactor pressure boundary can occur, cooling capability is maintained and no significant damage occurs to the reactor core.

It must be ensured in the design that the possibility of recriticality or a reactivity excursion following a PIE is minimized.

The reactor core and associated coolant, control and protection systems are designed to enable adequate inspection and testing throughout the service lifetime of the plant.

Fuel elements and assemblies
Fuel elements and assemblies must be designed to withstand satisfactorily the anticipated irradiation and environmental conditions in the reactor core, notwithstanding all processes of deterioration that can occur in normal operation and in anticipated operational occurrences.

Fuel assemblies are designed to permit adequate inspection of their structure and component parts after irradiation. In design basis accidents, the fuel elements remain in position and do 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 are not exceeded.

Control of the reactor core
The provisions for fuel are 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 are provided to ensure that there are no regions of the core in which the provisions for fuel could be breached without being detected.

Provision is 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.

Reactor shutdown
Means are 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 are such that the specified limits are not exceeded. A part of the means of shutdown may be used for the purpose of reactivity control and flux shaping in normal power operation, provided that the shutdown capability is maintained with an adequate margin at all times.

The means for shutting down the reactor consist of at least two different systems to provide diversity.

At least one of the two systems, on its own, must be 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.

At least one of these two systems, on its own, must be 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.

In judging the adequacy of the means of shutdown, consideration is 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.

The means of shutdown are 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 are taken into account.

Instrumentation is provided and tests are specified to ensure that the shutdown means are always in the state stipulated for the given plant condition.

Reactor coolant system

The reactor coolant system, associated auxiliary systems, and the control and protection systems are designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded in operational states. The reactor coolant pressure boundary is equipped with adequate isolation devices to limit any loss of radioactive fluid.

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, are 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 are selected so as to minimize activation of the material.

The reactor pressure vessel and the pressure tubes are designed and constructed to be of the highest quality with respect to materials, design standards, capability of inspection and fabrication.

The design of the components contained inside the reactor coolant pressure boundary, such as pump impellers and valve parts, are 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
The components of the reactor coolant pressure boundary are designed, manufactured and arranged in such a way that it is possible,

throughout the service lifetime of the plant, to carry out adequate inspections and tests of the boundary at appropriate intervals. Provision is made to implement a material surveillance programme for the reactor coolant pressure boundary, particularly in locations subject to 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.

Indicators of the integrity of the reactor coolant pressure boundary (such as leakage) are monitored. The results of such measurements are taken into consideration in the determination of which inspections are necessary for safety.

If the safety analysis of the nuclear power plant indicates that particular failures in the secondary cooling system may result in serious consequences, the ability to inspect the relevant parts of the secondary cooling system must be ensured.

Inventory of reactor coolant
Provision is 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.

Clean-up of the reactor coolant
Adequate facilities are provided for removal of radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel.

Removal of residual heat from the core
Means for removing residual heat are provided. Their safety function is 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.

Interconnections and isolation capabilities and other appropriate design features (such as leak detection) are provided on the assumptions of a single failure and the loss of off-site power, and by the incorporation of suitable redundancy, diversity and independence.

Emergency core cooling
Core cooling is 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 ensures that:

- The limiting parameters for the cladding or fuel integrity (such as temperature) do not exceed the acceptable value for design basis accidents (for the relevant reactor design);
- Possible chemical reactions are limited to an allowable level;

- The alterations in the fuel and internal structural alterations do not significantly reduce the effectiveness of the means of emergency core cooling; and
- Cooling of the core is ensured for a sufficient time.

Design features (such as leak detection, appropriate interconnections and isolation capabilities) and suitable redundancy and diversity in components are provided in order to fulfil these requirements with sufficient reliability for each PIE, on the assumption of a single failure.

Adequate consideration is given to extending the capability to remove heat from the core following a severe accident.

Inspection and testing of the emergency core cooling system
The emergency core cooling system is designed to permit appropriate periodic inspection of important components and to permit appropriate periodic testing to confirm the following:

- The structural integrity and leak tight 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 conditions specified in the design basis, to the extent practicable.

Heat transfer to an ultimate heat sink
Systems are provided to transfer residual heat from all components important to safety to an ultimate heat sink. This function is carried out at very high levels of reliability in operational states and in design basis accidents. The reliability of the systems is achieved by an appropriate choice of measures including the use of proven components, redundancy, diversity, physical separation, interconnection and isolation.

Adequate consideration is 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
A containment system is provided in order to ensure that any release of radioactive materials to the environment in a design-basis accident will be below specified limits. This system may include, depending on design requirements:

- leaktight structures;
- associated systems for the control of pressures and temperatures;
- features for the isolation, management and removal of fission products, hydrogen, oxygen and other substances that could be

released into the containment atmosphere.

Strength of the containment structure
The strength of the containment structure, including access openings and penetrations and isolation valves, is calculated with and constructed to provide 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. Provision for maintaining the integrity of the containment in the event of a severe accident is considered. In particular, the effects of any predicted combustion of flammable gases are taken into account.

Capability for containment pressure tests
The containment structure is 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.

Containment leakage
The reactor containment system is designed so that the prescribed maximum leakage rate is not exceeded in design-basis accidents. The containment structure, equipment and components affecting the leaktightness of the system are 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 must be possible, either at the containment design pressure, or at reduced pressures that permit estimation of the leakage rate at the containment design pressure.

Adequate consideration is given to the capability of controlling any leakage of radioactive materials from the containment in the event of a severe accident.

Containment penetrations
The number of penetrations through the containment is kept to a practical minimum. All penetrations through the containment meet the same design requirements as the containment structure itself. They are protected against reaction forces stemming from pipe movement or accidental loads such as those due to missiles, jet forces and pipe whip. Adequate consideration is given to the capability of penetrations remaining functional in the event of a severe accident.

Containment isolation
Each line that penetrates the containment as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere is 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 are

above acceptable limits. These lines are fitted with at least two adequate containment isolation valves arranged in series (normally with one outside and the other inside the containment), such that each valve is capable of being reliably and independently actuated. 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 has at least one adequate containment isolation valve. This valve is outside the containment and located as close to the containment as practicable. Adequate consideration is given to the capability of isolation devices maintaining their function in the event of a severe accident.

Containment air locks
Access by personnel to the containment is 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.

Internal structures of the containment
The design provides for ample flow routes between separate compartments inside the containment. The cross-sections of openings between compartments are 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. Adequate consideration is given to the capability of the internal structures to withstand the effects of a severe accident.

Removal of heat from the containment
The capability to remove heat from the reactor containment is ensured. The safety function is fulfilled by reducing the pressure and temperature in the containment, and maintaining both 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 has adequate reliability and redundancy to ensure that this can be fulfilled on the assumption of a single failure. Adequate consideration is given to the capability of removing heat from the reactor containment in the event of a severe accident.

Control and clean-up of the containment atmosphere
Systems to control fission products, hydrogen, oxygen and other substances that may be released into the reactor containment are provided. Systems for cleaning up the containment atmosphere have suitable redundancy in components and features to ensure that they can fulfil the necessary safety function, on the assumption of a single failure. Adequate consideration is given to the control of fission products, hydrogen and other substances that may be generated or released in the event of a severe accident.

Instrumentation and control

General requirements for instrumentation and control systems important to safety

Instrumentation is provided to monitor variables and systems over their ranges for normal operation, in anticipated operational occurrences, in design-basis accidents and in severe accidents, as appropriate, to ensure that adequate information is obtained on the status of the plant. Instrumentation is 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 from the plant necessary for its reliable and safe operation. Instrumentation and recording equipment is provided to ensure that essential information is available for monitoring the course of design-basis accidents and the status of essential equipment, as well as for predicting, as far as is necessary for safety, the locations and quantities of radioactive materials that could escape from the locations foreseen in the design. The instrumentation and recording equipment is adequate for providing information, as far as practicable, for determining the status of the plant in a severe accident, and for taking decisions in accident management. Appropriate and reliable controls are provided to maintain the variables within specified operational ranges.

Control room

A control room is 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. Special attention is 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 provides for reasonably practicable measures to minimize the effects of such events. The layout of the instrumentation and the mode of presentation of information provides the operating personnel with an adequate overall picture of the status and performance of the plant. Ergonomics is taken into account in the design of the control room. Devices are provided to give, in an efficient way, visual and if appropriate, also audible indications of operational conditions and processes that have deviated from normal and could affect safety.

Supplementary control room

Sufficient instrumentation and control equipment is available, preferably at a single location (supplementary control room) that is physically and electrically separate from the control room. The reason for that is so that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and the essential plant variables can be monitored when there is a loss of capability to perform these essential safety functions in the control room.

Use of computer-based systems in systems important to safety

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 are established and implemented throughout the life cycle of the system, and in particular, the software development cycle. The entire development is subject to an appropriate quality assurance programme.
The level of reliability necessary is commensurate with the safety importance of the system in question. The necessary level of reliability is 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. The level of reliability assumed in the safety analysis for a computer-based system includes a specified conservatism to compensate for the inherent complexity of the technology and the consequent difficulty of analysis.

Automatic control
Various safety actions are automated so that operator action is not necessary within a justified period of time from the onset of an anticipated operational occurrence or design basis accident. In addition, appropriate information is available to the operator to monitor the effects of the automatic actions.

Functions of the protection system
The protection system is 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 the 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
The protection system is designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed. The redundancy and independence designed into the protection system is sufficient to ensure as a minimum that:

- No single failure results in loss of the protection function; and
- The removal from service of any component or channel does not result in loss of the necessary minimum redundancy.

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 are used to the extent practicable to prevent the loss of a protection function. The protection system is designed, unless its adequate reliability is

ensured by some other means, 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 permits all aspects of functionality from the sensor to the input signal to the final actuator to be tested in operation. The design is 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
Where a computer-based system is intended to be used in a protection system, the following requirements are also taken into account:

- The highest quality of and best practices for hardware and software are used;
- The whole development process, including control, testing and commissioning of the design changes, is systematically documented and reviewable;
- In order to confirm confidence in the reliability of the computer-based systems, their assessment by expert personnel independent of the designers and suppliers is undertaken; and
- Where the necessary integrity of the system cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfilment of the protection functions are provided.

Separation of protection and control systems
Interference between the protection system and the control systems is 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) is ensured and it is demonstrated that all relevant safety requirements are fulfilled.

Emergency control centre

An on-site emergency control centre, separated from the plant control room, is 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 is available there. The room provides means for communication with the control room, the supplementary control room, and other important points in the plant and the emergency organizations. Appropriate measures are taken to protect the occupants for a protracted time against hazards resulting from a severe accident.

Emergency power supply

After some PIEs, various systems and components important to safety need emergency power. It is 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.

Waste treatment and control systems

Adequate systems are provided to treat radioactive liquid and gaseous effluents in order to keep the quantities and concentrations of radioactive discharges within prescribed limits. In addition, the 'as low as reasonably achievable' (ALARA) principle is applied. Adequate systems are provided for the handling of radioactive wastes and for storing these safely on site for a period of time consistent with the availability of the disposal route on site. Transport of solid wastes from the site is executed according to the decisions of the competent authorities.

Control of releases of radioactive liquids to the environment
The plant includes 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.

Control of airborne radioactive material
A ventilation system with an appropriate filtration system is provided for 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 ability to control radioactive releases.

Control of releases of gaseous radioactive material to the environment
A ventilation system with an appropriate filtration system is 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 the prescribed limits.

Fuel handling and storage systems

Handling and storage of non-irradiated fuel
The handling and storage systems for non-irradiated fuel are 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 conditions 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 fuel.

Handling and storage of irradiated fuel
The handling and storage systems for irradiated fuel are designed:
- To prevent criticality by physical means or processes, preferably by use of geometrically safe configurations even under conditions 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 are implemented to prevent any loss of fuel.

Radiation protection

General requirements
Radiation protection is directed to preventing any avoidable radiation exposure and to keeping any unavoidable exposures as low as reasonably achievable. This objective is accomplished in the design by means of the following:
- 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 site personnel;
- Making provision for the treatment of radioactive materials in an appropriate form and condition, for either their disposal, their storage on site or their removal from the site; and
- Making arrangements to reduce the quantity and concentration of radioactive materials produced and spread within the plant or released to the environment.

Design for radiation protection
Suitable provision is made in the design and layout of the plant to minimize exposure and contamination from all sources. Such provision includes adequate design of systems and components in terms of the following: 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. The shielding design is such that radiation levels in operating areas do not exceed the prescribed limits, and facilitates maintenance and inspection so as to minimize the exposure of maintenance personnel. In addition, the ALARA principle is applied.

The plant layout and procedures must provide for control of access to radiation and contamination areas and must also minimize contamination from the movement of radioactive materials and personnel within the plant.

Means of radiation monitoring
Equipment is provided to ensure that there is adequate radiation monitoring in operational states, design-basis accidents and, as practicable, severe accidents.

4.8 Questions

1. What are the requirements for the design organization?
2. What does design management ensure?
3. What must be done in the case of an unproven design or feature?
4. What are the fundamental safety functions that must be performed to ensure safety in all operational states and in the case of the accident?
5. List the factors that are taken into account when classifying the SSC.
6. List the categories of plant condition.
7. Briefly describe the meaning of the terms: *Common cause failure, Single failure criterion, Fail-safe design, Auxiliary service*.
8. Briefly describe the two methods of safety analysis, the deterministic and the probabilistic approach (what do they include).
9. List the requirements for the reactor core and its associated features.
10. List the requirements for the reactor coolant system.
11. List the requirements for the containment system.
12. List the requirements for instrumentation and control.
13. What is the function of the protection system and what is its design purpose?
14. List the requirements for the fuel handling and storage systems.

15. List the requirements for radiation protection.

5 SAFETY GUIDANCE FOR RESEARCH REACTOR DESIGN

Learning objectives

After completing this chapter, the trainee will be able to:

1. *Describe the important points of the contents of IAEA NS-R-4.*
2. *List other IAEA publications relevant to safety in research reactors.*
3. *Describe the main safety issues regarding research reactors.*
4. *Describe serious research reactor incidents and accidents.*

5.1 IAEA Safety Requirements NS-R-4

Safety requirements for research reactors are described in the IAEA document NS-R-4, Safety of Research Reactors [17]. This document is a comprehensive, stand-alone collection of safety requirements in all areas pertinent to research reactor safety. Therefore, it covers design and operation, but also regulatory supervision, management and verification of safety, site evaluation and decommissioning. It also provides brief guidance on applying a graded approach to implementation of the requirements. As is the case for all safety requirements documents, the emphasis is on the requirements that must be satisfied for safety rather than on the ways in which they can be met. Safety Guides, Safety Reports and TECDOCs provide more guidance on ways to meet the requirements.

Factors to be considered in a graded approach

As noted above, research reactors come in a wide variety of sizes and designs and they are used for many varied purposes. Therefore, a graded approach to the application of safety requirements is needed. The requirements in Safety Requirements NS-R-4 are intended to be applied to research reactors having a limited potential for hazard to the public and the environment. Most research reactors have a small potential hazard to the public and the environment, but they may pose a greater hazard to the operators and facility personnel. The scope, extent and detail of the safety analysis for a low power research reactor may be significantly less than that required for a high power reactor because certain accident scenarios may not apply or need only a limited analysis. At the other end of the scale, research reactors having a power level in excess of several tens of megawatts, fast reactors, and reactors in which experimental devices such as high pressure and temperature loops, cold and hot neutron sources and other potentially hazardous in-core apparatus may require extensive analysis, including application of standards for power reactors and/or additional special safety measures.

The need for flexibility in utilization to satisfy the needs of the

facility's users requires a flexible approach to achieving and managing safety. In any case, all of the safety requirements are to be applied unless the waiving of certain requirements can be justified, with account taken of the nature and magnitude of the potential hazards presented by the reactor and the activities conducted. Some of the factors to be considered in developing a graded approach to implementation of the requirements include:

- Reactor power, which establishes the requirements for cooling of the core during operation and after shutdown, and provides the thermal driving force available to cause core damage and potential dispersal of the core radioactive inventory.
- Radiological source term, which reflects the hazard to the public and the environment in case of an accident. The source term is importantly influenced by the reactor power, the operating schedule of the reactor, the fuel design and the cooling system design;
- The amount and enrichment of fissile and fissionable material;
- The presence of spent fuel elements, heating systems, high pressure and temperature systems, or systems containing chemically reactive materials in the reactor, or the presence of flammable materials, which may affect the safety of the reactor;
- The design of the reactor, including the type of fuel elements, the type and mass of moderator, coolant and reflector;
- The potential amount and rate of reactivity addition and the reactivity control mechanisms, inherent feedback mechanisms and other safety features available to counter any reactivity excursion;
- The quality of the containment or confinement structure;
- Utilization factors, including the presence of experimental devices, experiments and tests, and the presence in the facility of external personnel associated with utilization;
- Siting factors, including the proximity of the facility to population centres.

Clearly, many factors must be considered in formulating a graded approach. Many of these factors are established at the design stage, but some may change with changes in utilization of the reactor, its operating mode or site parameters. The managers of the research reactor must be aware of such changes during the lifetime of the facility and make changes in the graded approach as necessary.

Design philosophy

The top-level design philosophy for research reactors does not differ from that for power reactors. A research reactor is designed to satisfy the safety objectives that are discussed in Chapter 3. The defence-in depth concept is applied to provide graded protection against uncontrolled release of radioactive materials. Proven technology and conservative margins are used in the design, a quality assurance programme is implemented, and the design provides for surveillance and inspection throughout the life of the reactor. Physical barriers to

release of radioactive material are provided, although the number and strength of these barriers may be less than those provided in a power reactor. Three basic safety functions must be satisfied:

- Control of reactivity, in particular providing for reactor shutdown and maintaining it in a safe shutdown state for all operational conditions and design basis accidents (DBAs);
- Provision of adequate heat removal after shutdown, in particular from the core, including in DBAs;
- Confinement of radioactive material to prevent or mitigate any unplanned release to the environment.

The safety functions are provided for by incorporating an appropriate combination of inherent and passive safety features, engineered safety systems and applying administrative procedures over the lifetime of the reactor. In the design of the safety systems, the single failure criterion is applied, high reliability is ensured and provisions are made for regular inspection, testing and maintenance.

General design requirements

The IAEA document Safety Requirements NS-R-4 [17] includes design requirements that are summarized here. Note that these are very brief summaries of the requirements and readers should consult the source document for a complete discussion.

Classification of structures, systems and components (SSCs): SSCs important to safety, including software used in instrumentation and control, are specified and classified according to their function and significance to safety, including the consequences of failure to perform their function. This classification may be used to grade the design and quality requirements applied. Codes and standards applicable to SSCs are identified and applied in accordance with their safety classification.

The design considers all challenges that the reactor may be expected to encounter during its lifetime. The demands imposed on the reactor by these challenges and the conditions under which they may be encountered determine the design basis of the research reactor facility. The challenges may arise from normal operations including utilization, site-related characteristics, internal events such as equipment failures, fires and explosions, or natural- or manmade external events. A suitable set of postulated initiating events (PIEs) and DBAs is formulated, and suitable inherent, passive or engineered safety features provided to ensure that safety is maintained in these events.

The design applies the principles of redundancy and the single failure criterion, diversity, independence and fail-safe design, and it provides for ease of inspection, testing and maintenance.

Radiation protection is an important design consideration in research

reactors to ensure protection of the staff and outside users. Design provisions may include shielding, ventilation, filtration, and decay systems (decay tanks) for radioactive materials. In addition, monitoring instruments for radiation and airborne radioactive material, both inside and outside the controlled area, must be provided. The structural materials are chosen to limit doses to personnel during operation, inspection, maintenance and decommissioning. The effects of radionuclides produced by neutron activation in reactor process systems (e.g., ^{16}N, ^{3}H, ^{41}Ar, ^{24}Na and ^{60}Co) are considered in the design for radiation protection.

Special consideration is given to experimental equipment since it can cause hazards directly if it fails, can cause hazards indirectly by affecting safe operation of the reactor, and can increase the hazard from a PIE by its consequent failure and the effects of this on the accident sequence. Every proposed modification to a reactor or experiment that may have major safety significance is designed to standards equivalent to the reactor itself and is fully compatible with the reactor. The radioactive inventory and generation and release of energy is considered in the design of all experimental devices.

Safety analysis and verification of safety

A safety analysis is conducted as part of the design process of a research reactor. This analysis addresses the response of the reactor to a range of PIEs that may lead to anticipated operating occurrences (AOOs) or postulated accidents, some of which may be the DBAs for the design. These analyses are used as the basis for the design of SSCs important to safety and for the selection of operational limits and conditions (OLCs) for the reactor. The scope of the safety analysis includes:

- Characterization of the postulated initiating events (PIEs) that are appropriate;
- Analysis of event sequences and evaluation of the consequences of the PIEs;
- Comparison of the results with radiological acceptance criteria and design limits;
- Demonstration that the AOOs and DBAs can be managed by the automatic safety system response in combination with prescribed operator actions;
- Determination of OLCs for normal operation;
- Analysis of safety systems and the engineered safety features;
- Analysis of the means of confinement;
- Consideration of the safety of experimental devices and their impact on the safety of the reactor.

The safety analysis is usually done using deterministic methods, but probabilistic methods may be used to complement the deterministic analysis. The data derived from the safety analysis is used by the operating organization as the basis for a comprehensive safety assessment to confirm that the reactor meets the safety requirements.

The safety assessment is part of the design process, with iterations between the design work and the analysis activities, and increases in scope and detail as the design progresses. The safety assessment is continued throughout the life of the reactor. The operating organization establishes one or more safety committees, independent of the reactor manager, to advise on relevant safety issues of the design, commissioning, operation and utilization. Safety Report Series, No. 55 [18], provides additional guidance on Safety Analysis for Research Reactors.

Selected postulated initiating events

The starting point for a safety analysis, whether it is deterministic or probabilistic, is a set of postulated initiating events. There are many techniques available for developing a set of PIEs, including such things as failure modes and effects analysis, fault trees, and the like, but operating experience and engineering judgment are important contributors as well. Safety Requirements NS-R-4 provides an appendix that lists many PIEs. They cover the following broad categories:

- Loss of electrical power supplies;
- Insertion of excess reactivity;
- Loss of coolant flow;
- Loss of coolant;
- Erroneous handling or failure of equipment or components;
- Special internal events, such as fires, explosions, flooding, loss of support systems, security incidents, experiment malfunctions and the like;
- External events, including natural phenomena and manmade events;
- Human errors.

Examples of operational aspects of research reactors that require particular attention

Safety Requirements NS-R-4 includes an annex that discusses some operational aspects that require particular attention in research reactors. These aspects highlight some of the essential differences between research reactors and power reactors, as follows.

Core configurations are frequently changed in research reactors, and such changes involve manipulations of fuel assemblies, control rods and experimental devices, many of which have considerable reactivity worth. Care must be exercised to ensure that the relevant subcriticality and reactivity limits for fuel storage and core loading are not exceeded.

Changes in core loading also affect the nuclear and thermal characteristics of the core. These characteristics must be correctly determined and checked to ensure that the nuclear and thermal safety limits are not exceeded before the reactor is put into or returned to operation.

Experimental devices may significantly affect the safety of the reactor. These devices must be adequately assessed for their safety implications and suitable documentation be made available.

Research reactors and experimental devices are often modified to adapt to changing requirements for utilization. Every modification must be properly assessed, documented, reported and, if necessary, given formal approval before restarting the reactor.

In pool-type research reactor in particular, components, experimental devices and materials are frequently manipulated in the vicinity of the reactor core. These manipulations must be done strictly in accordance with procedures and restrictions to prevent any interference with the reactor or its cooling system, avoid any loose parts, and prevent radioactive release or undue radiation exposure.

Guest scientists, trainees, students and others who visit research reactors may have access to the controlled area and may be actively involved in utilization of the reactor. All procedures, restrictions and controls aimed at ensuring safe working conditions for visitors and that their activities do not affect reactor safety must be strictly observed.

5.2 Other safety guidance for research reactors

In addition to the Safety Requirements, additional IAEA safety guidance is available. These safety guides are concerned not only with the design of research reactors, but other aspects of their utilization. They are listed here for the sake of completeness and because of the specific nature of research reactors:

- SSG-20, Safety Assessment for Research Reactors and Preparation of the Safety Analysis Report [19];
- SSG-24, Safety in the Utilization and Modification of Research Reactors [20];
- NS-G-4.1, Commissioning of Research Reactors [21];
- NS-G-4.2, Maintenance, Periodic Testing and Inspection of Research Reactors [22];
- NS-G-4.3, Core Management and Fuel Handling for Research Reactors [23].
- NS-G-4.4, Operational Limits and Conditions and Operating Procedures for Research Reactors [24];
- NS-G-4.5, The Operating Organization and the Recruitment, Training and Qualification of Personnel for Research Reactors [25];
- NS-G-4.6, Radiation Protection and Radioactive Waste Management in the Design and Operation of Research Reactors (2009) [26];
- SSG-10, Ageing Management for Research Reactors [27];

- SSG-22, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors [28];
- WS-G-2.1, Decommissioning of Nuclear Power Plants and Research Reactors [29].

The Code of Conduct on the Safety of Research Reactors [30]

A number of research reactor safety issues have been raised in the last decade, and many of these persist. These include:

- Ageing of research reactors. Since many research reactors worldwide are over 30 years old, issues of ageing of the facilities and staff are especially important in assessing safety. While many facilities have undergone upgrading, modernization and refurbishment during their lifetime, constant attention to the effects of ageing is needed to ensure continued safety.
- Lack of adequate regulatory supervision. A key to safety is an effectively independent regulatory body, with the authority, competence and resources needed to draft regulations and guides, assess the safety of research reactors, issue licences, inspect and enforce regulations and licence conditions.
- Some research reactors are in a status that has come to be called 'extended shutdown', that is, neither operating nor decommissioned. While some reactors may be in this status of extended shutdown for refurbishment and upgrading, the concern is that other such reactors may lack the essential staff and resources to maintain safety and security at an acceptable level with fuel remaining in the reactor or on the site.

Concern over these issues led to development of the Code of Conduct on the Safety of Research Reactors [30], which was recommended by INSAG in 2000. This Code serves as guidance to states for the development and harmonization of policies, laws and regulations on the safety of research reactors.

The scope of this Code is the safety of research reactors at all stages of their lives, but does not apply to the physical protection of research reactors and to research reactors within military or defence programmes.

The objective of this Code is to achieve and maintain a high level of safety in research reactors. The objective can be achieved by proper operating conditions, prevention of accidents, mitigation of the radiological consequences, etc.

Application of this Code is accomplished through national safety regulations, and a summary of the Code is given in the following few lines.

The first topic is the role of the state and this chapter covers:

- How the state establishes and maintains a legislative and

regulatory framework;
- The need for a regulatory body, what are the main obligations of state to the regulatory body, etc.
- A financing system which ensures safe operation of the research reactor.

The next topic covered in this Code is the role of the regulatory body. This part of the Code describes topics similar to those, which could be applicable for an NPP, such as:

- Assessment and verification of safety;
- Financial and human resources;
- Quality assurance;
- Human factors;
- Radiation protection;
- Emergency preparedness;
- Siting;
- Design, construction and commissioning;
- Operation, maintenance, modification and utilization;
- Extended shutdown;
- Decommissioning;

The Code also describes the role of the operating organization. This part is divided into four major areas:

- **General recommendations:** Assessment and verification of safety, financial and human resources, quality assurance, human factors, radiation protection and emergency preparedness.
- **Safety of research reactors:** Siting, design, construction and commissioning, operation, maintenance, modification and utilization.
- **Extended shutdown**
- **Decommissioning**

At the end the Code also describes the role of the IAEA.

5.3 Some serious research reactor incidents and accidents

While the overall safety record of research reactors has been excellent, there have been several serious accidents, some resulting in loss of life. A brief description of these is provided here so that the reader can appreciate the need for strict adherence to safety principles and procedures, and the potential consequences of procedure violation or carelessness.

21 August 1945 - Los Alamos (USA)

A criticality accident occurred when an experimenter was piling reflector blocks around a sub-critical fuel assembly and the last block fell on the fuel assembly. The person carrying out the experiment received a dose equivalent of 5.1 Sv and died 28 days later. The building guard received an equivalent dose of 0.5 Sv.

21 May 1946 - Los Alamos (USA)

Another criticality accident similar to the previous one occurred in the same installation, caused by accidentally bringing a hollow beryllium shell too close to the fuel when demonstrating how to induce a critical state in a fuel assembly. Eight people received equivalent doses of between 0.37 Sv and 2.1 Sv. The person carrying out the experiment died 9 days later.

12 December 1952 - NRX - Chalk River (Canada)

A power excursion occurred due to the regulating rods being inadvertently removed and failure of the safety rods to drop. The excursion resulted in destruction of the core and release of approximately 4000 m3 of reactor coolant water containing about 3.7×10^{14} Bq of activity, which spread into the basement of the reactor building.

29 November 1955 - EBR-1 (USA)

A power excursion occurred during an experiment to measure the reactivity coefficient of the reactor. The reactivity meter was not connected to the safety system. This accident caused the meltdown of around 40% of the core.

15 October 1955 - Vinča (Yugoslavia)

A mistake by an operator led to an inadvertent increase in the level of the heavy water and the uncontrolled criticality of the reactor. Six people received equivalent doses of between 4 Sv and 11 Sv. One person died and the other 5 had bone marrow transplants in Paris and survived.

03 January 1961 - SL1 - Idaho Falls (USA)

Human error during the manual removal of the central regulating rod led to a power excursion and steam explosion. Two operators were killed outright. A third person died two hours later from injuries.

30 December 1965 - Venus - Mol (Belgium)

A power excursion due to human error during the manual removal of a regulating rod resulted in the operator receiving 5 Sv to the chest and 40 Sv to the foot, which led to subsequent amputation of the leg.

07 November 1967 - SiloeE - Grenoble (France)

Partial meltdown of a fuel element during an overpower test resulted in release of about 2×10^{15} Bq of radioactivity into the water of the pool and 7.4×10^{13} Bq through the stack (mainly noble gases).

23 September 1983 - RA-2 - Constituyentes (Argentina)

A power excursion was caused by flouting the safety rules during modification of the core. The doses absorbed by the operator were of the order of 21 Gray as gamma rays and 22 Gray as neutrons. 13 other people were exposed to doses of between 0.006 Gray and 0.25 Gray.

The operator died 48 hours after the accident.

Note:
The International Nuclear Event Scale (INES) was introduced in 1990 as a way to inform the media and the public of the safety significance of a nuclear event on a consistent scale. The INES is a seven-point scale, ranging from an anomaly (e.g. abnormal leak of primary coolant), to a major accident (e.g. Chernobyl, Fukushima). In retrospect, the accidents at VENUS and SILOE could be classed as INES Level 3 (a serious incident, because of the severe spread of contamination and/or acute health effects to a worker). The other accidents mentioned above could be classed as INES Level 4 (an accident without significant off-site risk, because of significant damage to the reactor or radiological barriers and/or fatal exposure of a worker).

6 CASE STUDY: OSIRIS REACTOR

6.1 Background information

The OSIRIS reactor was built at the nuclear studies centre at Saclay in 1964-1966. It is a pool-type reactor having a maximum authorised thermal power level of 70 MW, in which light water is used as the moderator and coolant, and provides biological shielding. It uses U_3Si_2-Al fuel plates which are aluminium clad, enriched in ^{235}U to 19.75%. The water in the primary coolant system passes upwards through the core. The OSIRIS reactor operates in continuous three-weekly cycles with a week's shutdown between them. It is mainly used for:

- Irradiation of structural materials or fuels used in the different types of power reactors;
- Production of artificial radioisotopes and silicon doping; and
- Activation analysis.

A neutron model (critical assembly) is installed in the vicinity of the OSIRIS reactor (ISIS reactor, power 700 kW). The latter is also a pool-type reactor and operates when required during working hours. It is used to test new configurations of the core of the OSIRIS reactor by carrying out reactor physics measurements, such as the reactivity worth of the control rods, power distributions and gamma heating. It is also used for neutron radiography.

The OSIRIS and ISIS reactors are connected by "channels" which are used to transfer spent fuel elements in water. Each reactor has its own control room.

6.2 Reactor core

The core of the reactor is located at the centre of the pool. It is housed in a zirconium alloy tank with an AG3 rack comprising 56 square cells. These cells contain the fuel elements, the control rods, the reflector elements and the experimental devices.

The current configuration of the core includes 38 fuel elements, 6 control rods, 5 cells reserved for experimental irradiation, and 7 positions for the reflector elements and the molybdenum-99 production devices.

The fuel elements consist of parallel fuel plates swaged to two side plates, with a nozzle at the bottom and a hold-down lock at the top. The characteristics of the "silicide" fuel elements are indicated in the table below (Table 6.1).

The 6 control rods of the reactor are identical and consist of a fuel part and an absorber part (hafnium). When the reactor is operating, two safety rods are in the up position, with three shim rods and a regulating rod.

The control rods placed in the core are controlled by mechanisms located in a room under the pool. They are connected by shafts that pass through the bottom of the pool.

The reactor has two operating modes:

- An operating regime with a maximum power level of 1.4 MW in which the core is cooled by natural convection of the water in the pool; and
- A nominal or intermediate power operating regime in which the core is cooled by forced convection using the primary coolant system pumps (three pumps in service and one in reserve).

Table 6.1: Core parameters of the OSIRIS reactor (U_3Si_2).

Core characteristics of the OSIRIS reactor	
^{235}U enrichment	19.75%
Number of core elements	38
Size of the element	82.4 mm x 82.2 mm
Number of plates per element	22
Plate cladding	AG3
Size of a plate (mm): ▪ fissile height ▪ fissile length ▪ total thickness ▪ fissile core thickness ▪ cladding thickness	 630 68.4 1.27 0.51 0.38
^{235}U mass per plate	20.83
^{235}U mass per element (g)	458.26
Thickness of the coolant channel between 2 plates (mm)	2.43
Mass of boron 10 / element (g)	0.4

These two operating regimes are covered in the control system by the low and high power regimes:

1. Low power regime (from the sub-critical state to 1.4 MW):
   Three identical start-up systems (known as low-level systems) with moveable detectors (fission chambers) are used to determine the power of the reactor from the position of the counter and its count rate. In case the thresholds associated with the neutron parameters of the core (thresholds established at 1.1 MW and 1.4 MW) are exceeded, the regulating rods automatically stop rising and the safety rods drop.
2. High power regime (up to rated power +10%)
   Two operating modes are associated with the high power regime:

- Operation at a power level < 1 MW
  The safety actions relating to this operating mode and associated with the neutron parameters of the core are identical to those of the low power regime. As in the case of the low power regime, safety actions are based on signals from the moveable start-up counters.
- Operation at a power level ≥ 1 MW
  When the operating power level of the reactor is 1 MW or greater, the safety actions of the high-level systems are introduced and the safety actions of the start-up systems are prevented from operating. From this point onwards, all the safety actions associated with neutron parameters are established by the high-level systems.

For reactor control, the power signal used is that of the control system, fitted with a non-compensated ionisation chamber. The low-level, high-level systems and the control system are re-calibrated periodically by means of heat balance, carried out on the water in the primary coolant system, and by measuring the activity due to nitrogen-16 in the primary coolant system water.

The instrumentation and control system was renovated in 1993. A programmed protection system is used for the acquisition and processing of neutron and thermal hydraulic measurements, as well as the generation of shutdown commands using logic safety systems (2 out of 3 voting logic). The emergency shutdown commands cut off the power supply to the electromagnets holding the safety rods, causing them to drop by gravity.

6.3 Core structure

The core structure is located at the centre of the bottom of the pool. It consists of a vertical pipe of rectangular cross-section which includes, from bottom to top:

- A water inlet casing;
- The core housing;
- A water outlet casing; and
- A duct.

The core cooling water comes in through the inlet casing, moves upwards through the core and goes out through the output casing. On the one hand, the direction of the core cooling water requires that all the elements contained in the core be secured to prevent them from rising and, on the other hand, a downward current through the duct be established to limit contamination of the surface of the pool by warm, radioactive water coming out of the core.

The fuel elements are secured by attaching the lower end fitting of each element to a tie rod. Furthermore, the upper part of each element

is fitted with a horizontal handling pin equipped with a hold-down lock which is engaged in the walls of the cellular rack of the core.

6.4 Reactor pool

The reactor pool and the water channels are filled with deionised water which is used as biological shielding and, in the case of the pool, to cool the core and in the case of all the water channels, to remove the decay heat released by the stored spent fuel elements.

The reactor pool (volume: 536 m^3) comprises a stainless steel liner mounted on a concrete structure which ensures mechanical strength and provides biological shielding.

The reactor pool mainly contains the pool and core cooling system pipes, the mechanisms and supports of the various neutron-measuring chambers and spent fuel element storage containers.

6.5 Cooling systems

Primary coolant system

When operating normally, the heat released by the reactor core is removed by a flow of 5450 m^3/h (~ 1.5 m^3/s) of deionised light water which enters at the base of the core structure, flows upwards through the core and is then channelled to the decay tank. The primary coolant system pumps (three pumps in service and one in reserve) channel the water into a common header from which it is distributed into the four heat exchangers. At the outlet of these exchangers, the water is carried to the base of the core structure.

The pipe which carries the water to the core has two nozzles, on which natural convection flappers are fitted. Under normal operating conditions, both natural convection flappers are maintained in a closed position by the pressure of the water circulating in the primary coolant pipe. In the event of the pressure in the latter dropping below the threshold which triggers reactor trip, both flappers automatically open under the effect of gravity, the water in the pool is let in directly to the base of the core, which is then cooled by natural convection without changing the direction of the circulation.

Secondary systems

The water in the secondary systems comes from the water supply of the Saclay Research Centre. After the water passes through the heat exchangers of the primary coolant systems (core and pool), it is cooled in an atmospheric cooling system comprising four independent units. The secondary systems have four separate loops, sharing the atmospheric cooling system. The following two main loops can be identified:

- The main system (flow rate of 5600 m^3/h) which supplies the four primary coolant system heat exchangers of the core of the OSIRIS reactor and the two heat exchangers of the primary coolant system of the OSIRIS pool; it is fitted with four pumps.
- The system used to cool the primary coolant system of the channels and of the core of the ISIS reactor (flow rate of 120 m^3/h).

Any leaks in the exchanger pipe of the primary coolant system can be detected by monitoring the water make-up of this system, the beta and gamma activity of the water in the secondary system and the activity of the liquid effluents released into the sewer network.

6.6 Reactor containment and ventilation

The reactor containment of OSIRIS is a cylindrical reinforced concrete building (inside diameter: 32 m, thickness: 30 cm) sealed by a dome-shaped roof also made of reinforced concrete (inner height of the top of the dome from ground level: 21 m). The containment is designed to resist an internal overpressure of 20 mbar.

Leak tightness in relation to the water table is ensured by a multi-layer lining under the base mat with a 2 m up stand at the external part of the containment. Three drains located under this layer lead into three sumps and are used to monitor potential leakage of water from the containment.

The containment is maintained at a negative pressure differential of 0.5 mbar in relation to the outside in order to prevent uncontrolled radioactive release in the event of an internal contamination incident.

The ventilation system common to both the OSIRIS and ISIS reactors includes three induction fans (two in operation and one on standby) and three extraction fans (two in operation and one on standby). High-efficiency filters and iodine traps are installed upstream of these fans. The extracted air is released, after monitoring the radioactivity, through a 45 m high stack.

6.7 Electrical supply

The OSIRIS reactor is supplied from the power distribution sub-station of the Saclay Research Centre by two 15 kV lines (under normal operating conditions, a single 15 kV line is in service). The electrical supply to the reactor is three-phase 380 V via 7 transformers. The installation has two fixed generating sets rated at 1700 kVA which, in the event of the loss of off-site (EdF) power, supply power to all the auxiliary systems necessary for operating the reactor.

A third generating set is used to power the safety systems (the ventilation system, the control system and the radiation monitoring system) in case the two above-mentioned generating sets fail.

In the event of a total loss of power supply (EdF network and generating sets), the reactor will automatically be shut down by the safety rods dropping. Decay heat will be removed without difficulty by natural convection of water in the pool.

6.8 Safety considerations relating to experiments

The experimental devices in the OSIRIS reactor are generally intended for technological irradiation of nuclear fuel or structural materials which are placed in or around the reactor core. The main types of experimental device are:

- Simple non-instrumented devices, mainly used for radioisotope production or silicon doping;
- Instrumented devices which generally have double-wall containment; the coolant fluid may be water, gas or NaK; and
- Fuel irradiation loops for different nuclear reactor types.

The fundamental safety design principle applied to the above irradiation devices is:

- Taking every possible constructional measure to ensure that the total rupture of the experimental device (rupture of its own barriers) does not jeopardise the safety functions of the OSIRIS reactor, particularly reactor shutdown and decay heat removal from the core;
- Not separating the safety analysis of a specific configuration of the core relating to an experimental device from the safety analysis of the device itself.

Before any experimental device may be put into the reactor, it is necessary to study two aspects of the safety of the experiment:

- safety of operating the experimental device and the resulting risks; and,
- safety of the reactor whose characteristics may be modified due to the presence of the experimental device.

All experimental devices which may have consequences for safety or entail a new risk that can modify the conclusions of the safety analysis report are subject to a clearly specified authorisation procedure based on a detailed safety case.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Power Reactors in the World, Reference Data Series No.2, IAEA, Vienna, Austria (published annually).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Operating Experience with Nuclear Power Stations in Member States, IAEA, Vienna, Austria (published annually).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Small and Medium Reactor designs, IAEA, Vienna, Austria (2012).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, Safety Fundamentals No. SF-1, IAEA, Vienna, Austria (2006).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Specific Safety Requirements SSR-2/1, IAEA, Vienna, Austria (2012).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Guide NS-G-1.3, IAEA, Vienna, Austria (2002).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Fuel Handling and Storage Systems in Nuclear Power Plants, Safety Guide NS-G-1.4, IAEA, Vienna, Austria (2003).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Guide NS-G-1.5, IAEA, Vienna, Austria (2003).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Guide NS-G-1.6, IAEA, Vienna, Austria (2003).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, Safety Guide NS-G-1.7, IAEA, Vienna, Austria (2004).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Emergency Power Systems for Nuclear Power Plants, Safety Guide NS-G-1.8, IAEA, Vienna, Austria (2004).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants, Safety Guide NS-G-1.9, IAEA, Vienna, Austria (2004).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment Systems for Nuclear Power Plants, Safety Guide NS-G-1.10, IAEA, Vienna, Austria (2004).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, Safety Guide NS-G-1.11, IAEA, Vienna, Austria (2004).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of

the Reactor Core for Nuclear Power Plants, Safety Guide NS-G-1.12, IAEA, Vienna, Austria (2005).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, Safety Guide NS-G-1.13, IAEA, Vienna, Austria (2005).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, Safety Requirements No. NS-R-4, IAEA, Vienna, Austria (2005).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Analysis for Research Reactors, Safety Report Series No. 55, IAEA, Vienna (2008).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Research Reactors and Preparation of the Safety Analysis Report, Safety Standards Series No. SSG-20, IAEA, Vienna, Austria (2012).
[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety in the Utilization and Modification of Research Reactors, IAEA Safety Standards No. SSG-24, IAEA, Vienna, Austria (2012).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Commissioning of Research Reactors, Safety Guide NS-G-4.1, IAEA, Vienna, Austria (2006).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Periodic Testing and Inspections of Research Reactors, Safety Guide NS-G-4.2, IAEA, Vienna, Austria (2006).
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Management and Fuel Handling for Research Reactors, Safety Guide NS-G-4.3, IAEA, Vienna, Austria (2008).
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Research Reactors, Safety Guide NS-G-4.4, IAEA, Vienna, Austria (2008).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, The Operating Organization and the Recruitment, Training and Qualification of Personnel for Research Reactors, Safety Guide NS-G-4.5, IAEA. Vienna, Austria (2008).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and Radioactive Waste Management in the Design and Operation of Research Reactors, Safety Guide NS-G-4.6, IAEA. Vienna, Austria (2009).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management for Research Reactors, IAEA Safety Standards No. SSG-10, IAEA, Vienna, Austria (2010).
[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards No. SSG-22, IAEA, Vienna, Austria (2012).
[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Decommissioning of Nuclear Power Plants and Research Reactors, Safety Guide WS-G-2.1, IAEA, Vienna, Austria

(1999).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety of Research Reactors, IAEA, Vienna, Austria (2006).

The views expressed in this document do not necessarily reflect the views of the European Commission.