Sādhanā Vol. 38, Part 5, October 2013, pp. 945–970. © Indian Academy of Sciences

Core safety of Indian nuclear power plants (NPPs) under extreme conditions

J B JOSHI[1,*], A K NAYAK[2], M SINGHAL[3] and D MUKHOPADHAYA[4]

[1]Homi Bhabha National Institute, Anushaktinagar, Mumbai 400 094, India
[2]Reactor Engineering Division, Bhabha Atomic Research Centre, Trombay, Mumbai 400 085, India
[3]Nuclear Power Corporation of India Limited, Anushaktinagar, Mumbai 400 0094, India
[4]Reactor Safety Division, Bhabha Atomic Research Centre, Trombay, Mumbai 400 085, India
e-mail: jbjoshi@gmail.com

Abstract. Nuclear power is currently the fourth largest source of electricity production in India after thermal, hydro and renewable sources of electricity. Currently, India has 20 nuclear reactors in operation and seven other reactors are under construction. Most of these reactors are indigenously designed and built Heavy Water Reactors. In addition, a 300 MWe Advanced Heavy Water Reactor has already been designed and in the process of deployment in near future for demonstration of power production from Thorium apart from enhanced safety features by passive means. India has ambitious plans to enhance the share of electricity production from nuclear. The recent Fukushima accident has raised concerns of safety of Nuclear Power Plants worldwide. The Fukushima accident was caused by extreme events, i.e., large earthquake followed by gigantic Tsunami which are not expected to hit India's coast considering the geography of India and historical records. Nevertheless, systematic investigations have been conducted by nuclear scientists in India to evaluate the safety of the current Nuclear Power Plants in case of occurrence of such extreme events in any nuclear site. This paper gives a brief outline of the safety features of Indian Heavy Water Reactors for prevention and mitigation of such extreme events. The probabilistic safety analysis revealed that the risk from Indian Heavy Water Reactors are negligibly small.

Keywords. Indian NPPs; PHWR; AHWR; heavy water reactor; core safety; extreme events; thorium.

1. Introduction

Sustainable, reliable and affordable energy supply is a foundation of economic stability and growth for any country. It is more or less well-known that the per capita energy consumption

*For correspondence

and quality of life are strongly related. In view of this, there is strong energy demand around the world, which is growing due to rise in population. From a sustainable energy perspective, there are limited options. Increase in fossil fuel based energy supply inevitably leads to environmental issues. Further, the existing reserves of coal would be inadequate to meet an enhanced rate of energy consumption comparable to today's world average per capita level. Renewable energy sources like solar, wind, etc. are fast emerging as promising alternatives to traditional energy. However the technology for large scale production of energy from renewable resources is in nascent stage and will take long time to make up for the exponential energy demand. Moreover, these energy sources must be deployed to the fullest extent possible to meet the large concentrated energy needs for industries and urban centers. Thus, not only in India, but from a global perspective, nuclear energy has become a viable, sustainable and clean energy source of future.

Today, the world has about 437 nuclear power reactors in operation around the world which generates about 371 GWe (http://www.iaea.org/pris). In the entire history of commercial nuclear power so far, only three major accidents leading to damage of reactor core, have taken place (at Three Mile Island (Tolman *et al* 1988), Chernobyl (The Chernobyl Accident 1992) and recent Fukushima (IAEA mission report 2011)). In the case of the Three Mile Island accident (Tolman *et al* 1988), even though the core had melted, there was no radiation exposure to any plant operator or any member of the public in spite of a series of human errors. This was all because of proper adherence to the defence-in-depth principles in the design of the plant constructed in the early seventies. The Chernobyl nuclear power plant (Sehgal 2011) was one of the Soviet nuclear power stations. The reactor design did not fully conform to stipulated principles of defence-in-depth applied to the reactors of such vintage constructed in the Western world. More specifically, the accident was a consequence of several design deficiencies compounded by a series of human errors. The recent Fukushima accident (Srinivasan & Gopi Rethinaraj 2013) has been a concern for public since it happened especially with regard to safety of nuclear power plants. The accident in Fukushima occurred mainly due to extreme events such as earthquake of magnitude of 9.1 on Richter scale followed by gigantic tsunami of height 14–15 m. These resulted in prolonged station blackout conditions with unprecedented devastation of on- and off-site infrastructures such as destruction of fuel tanks of the diesel generators; flooding of the diesel generator building, etc. which serve as emergency power supply to nuclear reactors. Of course, the accidents led to release of radioactivity due to probable melt down of reactor core and hydrogen explosion in the containment; however, there were no casualties in the accident since the post accident habitation programme was well-managed by Japanese Government. Out of these accidents, the Chernobyl accident was definitely more severe in all its dimensions resulting in causalities.

These accidents have reinforced the necessity for further improvement of safety in the design of nuclear power plants. The lessons from the accidents have led to a higher attention to improvement in man–machine interfaces to minimize operator actions and errors in case of any extreme events and retrofitting additional safety systems to cater to such low probable extreme events for example that happened in Fukushima. Rigorous calculations have been performed for currently operating plants in India to prove that there is no degradation of the health of reactor in case of any postulated extreme events. In addition to deterministic analyses, probabilistic safety assessments have been mandatory for identification of design weakness which is supplemented by providing redundancy and diversity in necessary systems such that coolability of reactor is maintained in low probable extreme events. In fact, the current design and safety standards are rigorous and adequate from the design, operation, accident prevention and mitigation perspective. Regulatory infrastructures all over the world have been substantially augmented over the years with most of the key regulatory philosophies and practices based on internationally agreed

standards. The mechanisms of information exchange across the world have been substantially augmented to learn from each other's experiences. The designs of next generation reactors have considered extremely low probability Beyond Design Basis Accidents as a part of the design.

Considering the need for a much larger scale of deployment of nuclear power in the future, the safety goals for future nuclear power plants are sought to be further enhanced. Under the IAEA's International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) a set of objectives, requirements, and criteria have been accordingly formulated for the new reactors (www.iaea.org/INPRO). Most of the new designs are introducing inherent and passive safety features that do not depend upon external source of power or human actions for their operation and safety. In fact, possibility of core melt down accidents are almost not possible in the new designs; and if happens are managed by severe accident management guidelines such that no activity release beyond the acceptable limit can occur at the plant boundary. In our opinion, with advances in technology and a better understanding of the nuclear power, the possibility of accidents like Three Mile Island, Chernobyl or Fukushima will ever happen again is practically zero. This paper discusses the design safety features of Indian nuclear reactors against such extreme events.

2. Physics of nuclear safety

In a nuclear reactor, electricity is produced by conversion of thermal heat received by the coolant from heat produced by nuclear fission. For fission to occur, a neutron should be absorbed in fissile atomic nucleus such as uranium-235 or plutonium-239. The heavy nucleus splits into two or more lighter nuclei (the fission products), releasing kinetic energy, gamma radiation and free neutrons. A portion of these neutrons may later be absorbed by other fissile atoms and trigger further fission events, which release more neutrons, and so on, known as a nuclear chain reaction. Heat is produced due to conversion of the kinetic energy of fission products to thermal energy when these nuclei collide with nearby atoms. Some of the gamma rays produced during fission are absorbed by the reactor and produce heat; following termination of chain reaction also, the heat gets generated due to interaction of radiation released from radioactive decay of fission products and materials that have been activated by neutron absorption with matter which is called decay heat. A kilogram of uranium-235 releases approximately three million times more energy when undergoes fission than a kilogram of coal burned conventionally (7.2×10^{13} joules per kilogram of uranium-235 versus 2.4×10^{7} joules per kilogram of coal). The heat released due to fission must be removed adequately by a cooling medium; otherwise which would result in heat up of the uranium fuel. This is done by supplying adequate amount of coolant to the core, which continuously removes heat generated due to fission and transports the heat to the turbine for electricity generation. Due to large amount of heat released in the fission process, the nuclear reaction should be controlled so that the heat removal process can be carried out in a stable manner. The power output of the reactor is adjusted by controlling the nuclear fission rate. This is done with the help of control rods which are made of a neutron poison to absorb neutrons. Absorbing more neutrons in a control rod means that there are fewer neutrons available to cause fission, so pushing the control rod deeper into the reactor reduces its power output, and removing the control rod will increase it.

Moreover, operating a nuclear reactor in a safe way requires control of nuclear reaction, removal of heat generated due to fission by using coolant so that the temperature of uranium fuel does not exceed certain limit under any circumstances. When nuclear fuel overheats, the clad of the fuel may get damaged. The function of the clad is to retain the fission products in

the gap between fuel and clad. If the clad is damaged, the fission products (such as cesium-137, krypton-88, iodine-131 which are radioactive) that has accumulated in the gap can reach out into the coolant and finally to the environment if there are breaches in the pipes or vessels holding the coolant and the containment which houses the reactor primary heat removal system. Containment can breach if there is very high pressure of steam in the containment, generated from the high temperature coolant escaping from the pipes or vessel holding the coolant in the reactor primary side and the containment cooling system is unable to cool the steam. Another reason could be hydrogen explosion as happened in Fukushima. Hydrogen generation in the water cooled reactors is the effect of fuel heat up. At high temperature, Zirconium in Zircaloy cladding used in fuel rods oxidizes in reaction with steam as

$$Zr + 2H_2O \rightarrow ZrO_2 + 2H_2 + \text{heat}.$$

When mixed with air, hydrogen is flammable, and hydrogen detonation or deflagration may damage the reactor containment. If the containment is breached, radioactive fission products can reach the public through air, water and soil.

In summary, to prevent radioactive release which is the safety concern for nuclear power plants, coolability of the heat generating fuel pins should be always ensured. This should be done not only during reactor operation but also after the reactor is shut down because of decay heat generated in fuel pins.

3. Designing for safety of Indian nuclear power plants

To ensure safety (i.e., to satisfy the safety goal of meeting allowable radiological consequences during all foreseeable plant conditions), the following fundamental safety functions shall be achieved for all the plant states which include normal operation, anticipated operational transients, design basis events and beyond design basis events (Bajaj 2008):

- control of the reactor power;
- removal of heat from the fuel; and
- confinement of radioactive materials.

For a given plant state, and for each of the above safety functions, success criteria are prescribed to characterize the corresponding predefined safe plant state. Using these criteria, the provisions are defined that are required to maintain or to bring back the plant to a safe state. The accomplishment of these fundamental safety functions is assured by following a defence in depth approach.

One of the objectives of Defence in Depth concept (DiD) is to provide multiple physical barriers to retain radioactivity if released due to failure of previous barrier. The safety functions aimed to protect these barriers and the concept of ALARA (as Low As Reasonable Achievable) with regard to release of radioactivity to the public. The DiD consists in a hierarchical deployment of different levels of provisions (equipment and procedures) in order to maintain the effectiveness of physical barriers placed between radioactive materials and the public or the environment in normal operation, anticipated operational occurrences and in accidents.

3.1 *Provisions for levels of defence-in-depth*

Sl.No.	Levels	Objective	Essential means
1.	Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
2.	Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
3.	Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
4.	Level 4	Control of Severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
5.	Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

According to the DID concept, if the provisions dealing with safety of a given level fail to control the evolution of a sequence of events, the subsequent level will come into play. Therefore, the strategy of the DID is based on the principle of reduction and limitation of consequences of incidents and accidents. The different levels are intended to be independent; the general objective of DID being to ensure that a single failure at one level of defence, and even combinations of failures at more than one level of defence, do not propagate to jeopardize DID at subsequent levels. The DID approach covers both human and equipment failures.

Figure 1 shows a conceptual picture of the DID. As far as the reactor is concerned, the uranium oxide fuel itself is the first barrier which can house the fission products; the fuel claddings serve

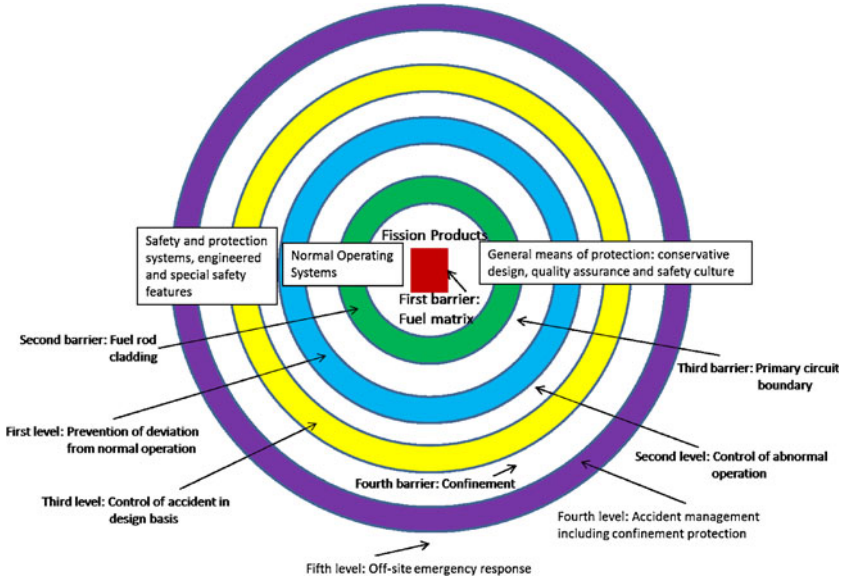

Figure 1. Conceptual picture of defence in-depth.

as the second barrier. The boundary of the primary circuit serves as the third barrier and the containment equipped with its ventilation system serves as the fourth barrier.

The safety of the facility is grounded on technical, human and organizational provisions permitting in all situations to fulfill the main safety functions. The purpose is to protect the physical barriers and the control of reactivity; the heat removal from the core (or fuel cooling); the confinement of radioactive elements and radiation protection of the workers. The purpose of the ALARA principle is to limit as far as possible the radiation dose exposure of the workers of a nuclear power plant and public as adopted in the safety objectives.

The demonstration of the adequacy of the design with the safety objectives is made through the analysis of three kinds of conditions:

3.1a *The design basis conditions*: It must be shown that the consequences of accidents occurring due to all postulated events as considered in the design, are well within the targets in terms of radiological releases and radiation protection. It must be checked that the risk of whole core degradation initiated by the Postulated Initiating Events is very low.

3.1b *Beyond design basis conditions*: The consequences of these accidents are analysed and demonstrated to be lower than the limiting release targets to the environment.

3.1c *Residual risk situations*: The consequences of these situations are not analysed. If these situations are not demonstrated to be physically impossible, prevention measures regarding their occurrence have to be demonstrated to be sufficient to 'practically eliminate' them.

3.2 *Safety Analysis: A safety analysis*

A safety analysis of the plant design is conducted which includes deterministic and probabilistic analysis with the inclusion of uncertainties and sensitivity analysis. On the basis of this analysis, it is demonstrated that all levels of the defence in depth are adequately implemented and that the plant as designed is capable of meeting prescribed limits for radioactive releases under normal operation and acceptable limits for accident condition.

3.2a *Deterministic analysis*: The deterministic analysis proves the design basis of the plant by analysing the plant conditions for normal and abnormal conditions. The applicability of the analytical assumptions, methods and degree of conservatism used are verified. The deterministic analysis uses best estimate methods and realistic sensitivity analysis to verify plant design margins. For new designs, where there may be insufficient data to allow best estimate methods to be used, conservative assumptions are adopted based on engineering judgment. The safety analysis of the plant design is updated with regard to significant changes in plant configuration, operational experience, advances in technical knowledge and understanding of physical phenomena, and is consistent with the current state-of-the-art.

3.2b *Probabilistic analysis*: A probabilistic safety analysis of the plant is carried out in order to provide a fundamental and structured approach to understanding plant behaviour during normal and abnormal conditions. This analysis is used to identify risk dominant accident sequences, safety critical systems, components, and structures, important process and procedural steps

necessary for safety, the timing of safety critical sequences and whether the plant meets the desired safety objectives for public health and safety. Besides, the purpose is to provide a systematic analysis to give confidence that the design will comply with the general safety objectives and 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. In addition, the analysis provides assessments of the probabilities of occurrence of severe plant conditions and assessments of the risks of major off-site releases necessitating a short term off-site response. More importantly, the analysis establishes the required reliability of Systems, Structures and Components.

3.3 *Safety criteria for nuclear power plants*

The designers of NPPs have to meet specified safety criteria as laid out by the regulatory authorities. The safety criteria are derived from the safety objectives and expressed in quantitative terms. The approach follows the principle that plant states that could result in significant radioactive releases are of very low frequency (likelihood) of occurrence, and plant states with significant frequency (likelihood) of occurrence have only minor or no potential radiological consequences.

Once the safety targets are set, the designer systematically determines the inherent features, equipment, and procedures (i.e., design provisions) needed to meet the goals. These provisions are then grouped into the lines of protection required to achieve each level of defence in depth. The provisions and their implementation may, in turn, generate complementary conditions that have to be addressed through an iterative process; their failure has to be considered as a complementary potential challenge. The approach focuses on each level of defence in depth by identifying the safety functions that need to be performed; the objectives to be achieved by that level of defence; the challenges posed by the design to maintain that function; the mechanisms that will lead to the failure of the function; and the provisions that are in place to deal with the failure mechanisms. The method represents the implementation of defence in depth to meet the primary safety criteria (Table 1).

Of course, the plant design ensures that its lines of defence in depth meets the dose limits (primary criteria) as specified above; in reality, the plant designs specify additional safety limits called design margins for all plant states. These margins are expressed in terms of fuel temperatures and called as secondary safety criteria. For example:

– For normal operations and operational transients, the acceptance criteria is expressed in terms of thermal margin such that critical heat flux is far above the operating heat flux in any fuel element.

Table 1. Example of primary safety criteria in NPP Design.

Sl.No.	Consequence	Normal operation/AOO	Accident condition
1.	Doses to the Public (AERB Safety Guide No. AERB/SG/G-8 2001)	< 1 m Sv in a year	< 0.1Sv for the whole body < 0.5Sv for thyroid of children
2.	Doses to the operator (AERB Safety Guide No. AERB/SG/O-5 1998)	a) 30 mSv in any year b) 20 mSv averaged over five consecutive years (on a sliding scale of five years, i.e 100 mSv in the five year period)	

– For infrequent anticipated operation occurrence and transients, the requirements are that the primary coolant pressure should be well within the design overpressure limit of the system and there shall be no fuel damage as demonstrated from prediction of no occurrence of critical heat flux and no fuel centerline melting. Also there should be minimum challenges to protection and safety systems, i.e., most of the corrective actions should take place by actuation of normal regulating and control systems.
– For accident conditions considered in design, fuel failures may occur but the calculated radiological consequences to the environment must be shown to be within prescribed reference dose limits.

3.4 *Design provision ensuring reactor safety*

Nuclear power technology is based on engineering practices that are proven by testing and experience, and which are reflected in approved codes and standards and other appropriately documented statements. Systems and components are conservatively designed, constructed and tested to quality standards commensurate with the safety objectives. Approved codes and standards (AERB/NPP-PHWR/SC/D 2009) are used whose adequacy and applicability have been assessed and which have been supplemented or modified if necessary. If opportunities for advancement or improvement over existing practices are available and seem appropriate, such changes are applied cautiously and subjected to necessary testing.

3.4a *Design feature of Indian PHWR*: PHWR technology as a first phase of three stage programme is well-established in the competitive commercial domain in India. India has a fleet of PHWRs currently under operation. The size of the first sixteen PHWRs was selected as 220 MWe. As the large carrying capacities became available in the grid, the 220 MWe design was scaled up to 540 MWe. Two units of 540 MWe each are successfully operating. The design has been further scaled up to 700 MWe by permitting limited boiling of coolant, using the same core as that of 540 MWe PHWRs. Four units of 700 MWe PHWRs are under construction and many more are planned in future to meet growing energy need of the country.

PHWR system offers certain intrinsic advantages (Narora Atomic Power Station -1&2 2007). The prompt neutron generation time, for a PHWR is about 10^{-3} sec which is one order higher than Light Water Reactor. Thus, for a given reactivity, neutron transients are slow, making the reactor easier to control. The on-power fuelling feature of PHWRs allows the excess reactivity reserve in the core to be kept at a minimum. The reactivity worth invested in regulating system is therefore low, typically $\sim$15 mk. Thus the individual rod worth and the total reactivity change possible due to any malfunction in control system is limited. Further, on power detection and removal of failed fuel and short bundle length limits the consequences in case of single failure.

A heavy water moderated core provides a relatively spacious gap between the fuel channels. This gap is occupied by low-temperature and low-pressure moderator. The reactivity control devices are installed in this low-pressure and low-temperature moderator environment. There is no possibility of fast ejection of any of the control rods. Furthermore, the spacious core lattice allows complete separation between regulating and protective functions. The space is also sufficient to provide two independent fast acting shutdown systems working on diverse principles. During normal plant operation including plant start up and shut down, reactor neutronic power regulation/control is achieved automatically through an independent dedicated system, known as Reactor Regulating System (RRS). This system is designed to achieve fine as well as coarse

control depending on system requirement. During reactor trip, all the devices of reactor regulating system also get driven in/dropped into the core along with shut-off rods of shutdown system no. 1 (SDS#1). The shut down system #1 uses gravity drop of large number of cadmium absorber elements. The design incorporates several features such as facility for on-line testing, improved dashpot arrangement, etc. The shut down system #2 (SDS#2) employs gadolinium nitrate liquid poison, which is injected into moderator through liquid poison injection assemblies. High-pressure helium is used for effecting fast injection. A series-parallel array of fast acting valves is provided to isolate the high-pressure helium. The valves are tested on-line (without system actuation) for ensuring their availability. Design features enhancing passive nature of the system such as floating ball arrangement for preventing high pressure helium entering calandria have been provided. While a negative worth equivalent to SDS-1 is realized in about 2.5 s of system actuation, the total negative worth is much larger when the entire poison is mixed with the moderator (Bhardwaj 2006). These features provide a high degree of assurance that reactor shutdown will occur when required. Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are intentionally taken or whenever a chain reaction might be initiated accidentally.

The initial inherent response of a PHWR to a reactivity increase is prompt and negative reactivity feedback; the increase in the fuel temperature gives a rapid negative reactivity feedback through the Doppler effect. This prompt negative feedback ensures that the reactor is stable in normal operation and allows control by mechanical or hydraulic devices.

Primary Heat transport systems are designed for highly reliable heat removal in normal operation. They would also provide means for the removal of heat from the reactor core during anticipated operational occurrences and during most types of accidents that might occur. When reactor operates at power levels above 2% full power, failure of power to coolant circulation pumps, initiates a reactor trip and coolant circulation is continued by thermosyphon to remove the decay heat generated in the core. Location of steam generator above the core facilitates sufficient thermospyphon without causing clad surface temperature to exceed allowable limits. During power rundown of the reactor, coolant circulation would be supplied by the pumps which remain operating (if any) supplemented by the pumping action provided by the energy in the flywheels of unpowered pumps.

The location of the headers above the core limits the size of any single opening in the primary circuit below the elevation of headers to one feeder or pressure tube (Bajaj & Gore 2006). This arrangement prevents total core draining and make-up by Emergency Core Cooling System can ensure core flooding. Following a loss of coolant accident (LOCA), the loop isolation valves are closed when the PHTS pressure drops below a set value, thus isolating the failed loop from the intact loop. The intact loop removes the decay heat from PHT side through thermosyphoning, on secondary side through SGs by providing water to SGs by auxiliary boiler feed pump.

The emergency core cooling system of 700 MWe comprises of two parts, a passive high-pressure injection, followed by active long-term recirculation phase for removal of decay heat. All headers injection concept has been adopted. The injection is initiated automatically on sensing a fall in reactor inlet header pressure below 40 kg/cm^2 (g) along with the presence of any one conditioning signal i.e., a high calandria level or high pump room pressure. There are two trains of High Pressure Light Water Injection System. Each train consists of a horizontal gas accumulator and two horizontal light water accumulators to inject high pressure water into the core in the event of LOCA. ECC recirculation phase ensures prolonged cooling to remove decay heat from core. There are two trains of long term recirculation phase. Each train consists of two 100% capacity pumps and two 50% plate type heat exchangers. The components of a train are located diametrically opposite to respective components of other train.

Parameters to be monitored in the control room are selected, and their displays are arranged, to ensure that operators have clear and unambiguous indications of the status of plant conditions important for safety, especially for the purpose of identifying and diagnosing the automatic actuation and operation of a safety system or the degradation of defence in depth. The control room is designed to remain habitable under normal operating conditions, anticipated abnormal occurrences and accidents considered in the design. Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control room for circumstances in which the main control room may be inhabitable or damaged.

Standard Indian PHWRs have certain advantages which make accident progression slower, viz.

- The steam generators are located above the core and as such decay heat can be removed passively by thermo siphoning of the primary system and boiling of water in the SG with water available in steam generators. Indian PHWRs have provision for supplying water to depressurized steam generators by diesel engine driven pumps, which do not require station power supplies. Steam discharge valves are provided such that the steam generator can be depressurised even in case of complete loss of power and compressed air.
- Secondly, the core is always surrounded by large quantity of low temperature and low pressure water in calandria and calandria vault. These inventories significantly delay progression of severe accidents and thereby provide time to intervene and take corrective actions. These inherent heat sinks come into picture only when primary heat sink through steam generators or shutdown cooling system becomes unavailable.

Provisions corresponding to level-1 of defence in depth as incorporated in the design ensuring that possibility of such an accident is remote and provisions at level-2 and level-3 ensure that such accidents can be safely mitigated, thereby avoiding their progression into severe accident domain.

3.4b *Severe accident prevention features (National Report to Convention on Nuclear Safety 2012)*: Following modifications after Fukushima are made to strengthen preventive aspect of accident management:

(i) Improving availability of onsite power supply—This is achieved by ensuring availability of onsite emergency diesel generators under external natural events. For this, available margins for onsite power supply with respect to earthquake and external flood are evaluated and necessary upgrading in the following form is contemplated.

  – Providing back up emergency diesel generator at a higher location, where normal emergency diesel generator location is assessed to be vulnerable from the point of view of external natural events.
  – Providing a smaller/mobile diesel generator, which can be utilized to power essential loads and charge station batteries for obtaining plant information and emergency lighting.

(ii) Improving steam generator heat sink—Improved availability of steam generator heat sink for maintaining thermosyphoning mode of decay heat removal is achieved by

  – Indian PHWRs design incorporate provision of supplying water into steam generators by diesel engine driven pumps; which are independent of station power

supplies. These diesel engine pumps are further secured against external flood and seismic conditions.
- In selected units, additional diesel engine operated pumps are installed at locations secured from external flood to transfer deaerator storage tank inventory to steam generators.
- In some units provision exists to transfer deaerator storage tank inventory to steam generators by gravity.
- Provisions are made to provide hook-up connections outside reactor buildings, through which water can be supplied to steam generators and end shields either by mobile pump or fire tenders. These connections would be kept isolated in normal operation through valves and spectacle flanges. The design of these connections is qualified for maximum anticipated earthquake and flood at the site. These provisions will take care of extended loss of power supply scenario.
- The 700 MWe units have a design feature of passively removing decay heat from steam generators by recirculating steam generator inventory through condensers located at elevation higher than steam generators. Water inventory to secondary side of these condensers can be replenished from outside reactor building. With this replenishment of inventory, steam generator heat sink can be maintained for extended duration. In addition, as backup, provision of supplying water to steam generators by diesel engine driven pumps is retained.

(iii) Improving onsite water storage—Standard Indian PHWRs have onsite water storage sufficient for seven days of residual heat removal in case of loss of offsite power supply. This water storage is designed to be available against earthquake and external flood. In case of station blackout, this inventory when used only for replenishing steam generator heat sink can cater decay heat removal for about a month. Following additional provisions are made for improving onsite water storage.

- Based on station specific review, onsite water inventory is augmented wherever strengthening is considered necessary.
- Water sources at or near stations are identified, from where water can be transported with fire tenders.

(iv) Hook up to Primary Heat Transport System/Emergency Core Cooling System (ECCS)—Indian PHWRs have Provisions to supply water into ECCS by fire water system, in case long term recirculation part of the system is not successful or develops some problem during the mission period. This provision is reviewed and necessary strengthening is done.

A provision to inject water into Primary Heat Transport (PHT) system is made to be used in extended station blackout. With this Provision, issue of making up leakages to keep PHT system in solid state gets addressed. This water supply arrangement is from outside reactor building without utilizing station power supplies. i.e., by diesel engine operated pumps/fire tenders.

3.4c *Severe accident mitigation features (National Report to Convention on Nuclear Safety 2012)*: In the unlikely situation of preventing accident progression, there could be potential of core damage. To mitigate accident sequences involving significant core damage, the following safety measures are made.

(i) Injection of water in calandria—Indian PHWRs have a large quantity of low pressure and low temperature heavy water inventory surrounding the core. Under beyond design basis accidents, this inventory acts as a heat sink and provides decay heat removal capability for several hours. Being a low pressure system, simple means can be employed to replenish this inventory thereby increasing autonomy of this heat sink and preventing significant core damage. For this purpose, hook-up connections are made and are brought outside reactor building. From these connections water can be supplied to calandria either by connecting mobile pump or fire tenders. Replenishing water into calandria provides continuous heat rejection from the core and maintain core integrity or keep core materials within calandria depending on the time when action is credited to refill the calandria. The design of this arrangement is qualified for maximum anticipated earthquake and flood at site.

(ii) Injection of water in calandria vault—Surrounding the calandria is another large inventory of water in the calandria vault, which is also available at low pressure and temperature. Thus this inventory provides a back up to water inventory in calandria and provides another retarding barrier in case calandria barrier for limiting accident progression could not be maintained. Provisions are made to supply water into calandria vault by hook-up connections that are brought outside reactor building. This connection is kept normally isolated through valves and spectacle flange. From this Connection, water can be supplied to calandria vault either by connecting mobile pump or fire tenders. By introducing water in calandria vault.

  – External cooling can be maintained for calandria and thus core or core material can be kept confined within calandria.
  – Even in case of calandria breach, core material can be kept cool and molten core concrete interaction can be avoided.

3.4d *Design feature of Indian AHWR*: India has a small reserve of uranium fuel. However, India has nearly a third of the entire world's thorium reserves, which can be bred in a reactor to become fissile. Hence, our strategies for large scale deployment of nuclear energy must be, and are therefore, focused towards utilization of thorium. The importance of nuclear energy, as a sustainable energy resource for our country, was recognized at the very inception of our atomic energy program. A three-stage nuclear power program, based on a closed nuclear fuel cycle, was then chalked out. The first stage of nuclear power programme targets burning of natural uranium as start off an atomic power programme. The plutonium produced by the first stage can be used in a second generation of power stations designed to produce electric power and convert thorium into U-233, or depleted uranium into more plutonium. The second generation of power stations may be regarded as an intermediate step for the breeder power stations of the third generation all of which would produce more U-233 than they burn in the course of producing power. Thus the third stage of the program is aimed at development of advanced nuclear power plants for utilization of thorium.

This has led to the development of the Indian Advanced Heavy Water Reactor (AHWR) (Sinha & Kakodkar 2006) mainly for the purpose of large scale power production from Thorium as a demonstration plant. Another objective of the reactor is to have an inherently safe design so that the reactor can be located close to the population centre. The AHWR is a 300 MWe vertical pressure tube type reactor cooled by boiling light water and moderated by heavy water fuelled by dual MOX consisting of (PU-Th)O2 and (233U-Th)O2 designed for a 100 year lifetime.

The physics design of AHWR has several inherent safety features. The design envisages a negative fuel temperature coefficient of reactivity (Doppler coefficient), negative power coefficient under all plant conditions and negative core-averaged coolant void reactivity coefficient. These have been achieved by suitable fissile contents in a harder thermal spectrum conducive to resonance captures. The equilibrium core design has a very low excess reactivity thereby minimizing the reactivity swings and enhancing the safety. A low power density (compared to other heavy water reactors) of about 4 kW/l ensures higher margins during operational transients. The control rod withdrawal speeds are also lower, which minimizes the effect on control rod related reactivity insertions. Two independent and functionally diverse fast acting shutdown systems provide a significant safety margin. In addition, the reactor regulating system continuously monitors and controls local and global power. Two Group philosophy ensures fulfillment of different safety functions like shutdown capability, decay heart removal, minimizing radioactivity release and monitoring status of plant with reference to previous functions, by avoiding common cause failures. Safety systems have been divided in two independent and diverse groups, where each group can perform all the safety functions even when the other group is unavailable. The classification of various active and passive systems into two independent groups ensures that all the safety functions can be met in AHWR. For example, in case of LOCA, ECCS system of group I and containment isolation system of group II are actuated simultaneously, but independently. Safe shutdown capability is achieved by providing two independent shutdown systems with appropriate trip coverage for all postulated initiating events is another example.

The major design objectives of the reactor include:

- Reduced Core Damage Frequency (CDF) as compared to the existing plants.
- Reduced Large Early Release Frequency (LERF)-to an insignificant level.
- Implementation of emergency measures in public domain is not required.
- Enhance robustness against malevolent acts (insider threats).

To achieve the above safety goals, passive and inherent safety features have been instrumented into the design of the reactor. Apart from the fuel safety features cited before, some of the other safety features of the reactor are: (i) absence of pumps in the main heat transport system; (ii) high pressure and low pressure emergency core cooling system (ECCS) trains; (iii) direct injection of ECCS water into the fuel cluster, (iv) large inventory of water in the main heat transport system to make the system sluggish; (v) large water pool above the core to make full core submergence in case of LOCA; etc. which make the reactor inherently safe. Important passive safety features of the reactor are: (i) core heat removal by natural convection of the coolant during normal operation and in shutdown conditions; (ii) decay heat removal by isolation condensers (ICs) immersed in a large pool of water in a gravity driven water pool (GDWP); (iii) direct injection of ECCS water into the fuel cluster in a passive mode during postulated accident conditions, such as loss of coolant accidents (LOCAs), initially from the accumulators and later from the GDWP; (iv) containment cooling by the passive containment coolers during LOCA; (v) passive containment isolation via formation of a water seal in the ventilation ducts, following a large-break LOCA; (vi) passive shutdown of the reactor by the injection of poison to the moderator, using a high-pressure steam in the case of a low probability event of failure of the wired shut down systems due to any malevolent actions (sensors, signal carriers and actuators) mechanical shutdown system (SDS-1) and the liquid poison injection system (SDS-2); (vii) passive concrete cooling system to protect the concrete structure in a high temperature zone, etc. The availability of a large inventory of water in the GDWP, at higher elevation inside the containment, facilitates

sustainable core decay heat removal, ECCS injection, and containment cooling for several days without invoking any active systems or operator actions.

3.4e *Managing a core melt down accident in AHWR*: The AHWR design practically eliminates a core melt down accident. However, a core catcher has been incorporated in the design to further enhance the defence-in-depth. The core catcher prevents the recriticality, terminates the severe accident progression and quenches the corium in the containment besides providing long term cooling to the corium. It is situated in 7.4 m diameter 2.1 m deep cavity below the calandria and consists of sacrificial concrete layer, high porosity concrete layer, riser tubes, water pool and two downcomers from GDWP supplying water to the water pool. To cater to the loss of all water, fire water hook-up for injection into the downcomer is provided.

There is a need to prevent accumulation of hydrogen in the reactor building during severe accident. Passive Autocatalytic Recombiners (PARCS) are installed in the containment building to manage hydrogen so as to eliminate formation of explosive mixture.

4. Assessment of safety

Safety analysis is performed for assessment of plant response for plant conditions ranging from normal operation/operational transients through anticipated operational occurrences/transients, low-frequency events to limiting design basis events and severe plant conditions.

A comprehensive set of Postulated Initiating Events (PIEs), which affect the process parameters following failure/malfunction of equipment/system, are identified considering entire plant systems and its locations for in-depth evaluation of specific plant design (AERB Safety guide No. AERB/SG/D-5 2000). These PIEs are classified into symptomatic groups depending on the similarity of their consequences. Limiting cases are identified based on detailed analysis and covered in respective plant safety analysis reports (Tarapur Atomic Power Station -3&4 2007). These PIEs range from events of infrequent nature (with frequency of occurrence upto 10^{-2} per year) such as small break Loss-Of-Coolant Accident (LOCA) to limiting design basis events (frequency of occurrence down to 10^{-6} per year) such as large break LOCA and multiple failures, e.g., LOCA coincident with failure of a mitigating safety system, Station Black Out (SBO). For each PIE, consequent event sequence is developed and satisfactory response and thereby adequacy of mitigating safety system is demonstrated. For performing safety analysis of these PIEs, various computer codes are developed having capability to model the physics of the various phenomena involved during the progression of events. Most such codes have been developed in-house by the utility, i.e., NPCIL as well as research institute i.e., BARC. These computer codes are put to rigorous benchmarking and testing and validated against experimental data and comparison with predictions from other validated codes. Experimental facilities have been built to generate large number of data for the validation of these codes. Validation exercise is also performed through plant commissioning tests and operational transients. These computer codes have also been validated against International Collaborative Standard Problem (ICSP) exercise and Coordinated Research Project (CRP) initiated by IAEA-TECDOC-1688 (2012) . These international validation exercises built the confidence in the usage of these codes for safety analysis which are used to verify the overall code predictions applicable for the plant, viz. simulation of loss of coolant accident, station blackout, thermosyphoning, etc. Thus, the safety characteristic of the plant is evaluated utilizing extensively validating computer codes.

4.1 *Safety characteristics of PHWR for extreme events*

Potentially, a severe accident in PHWRs could result from:

- Accident sequence initiated as loss of coolant accident (LOCA), followed by simultaneous or sequential loss of ECCS and moderator heat sink.
- Prolonged loss of offsite and on site power supplies (i.e., extended and unmitigated station black out.

Here prolonged loss of offsite and on site power supplies (i.e. extended and unmitigated station blackout) under extreme condition is covered as a representative case.

4.1a *Severe accident scenario resulting from SBO*: One of the accident sequences considers total loss of power supply to the station, and this accident is called Station Blackout. As there is no power, all running equipment stop and reactor trips. Heat sink through steam generators cannot be provided as water cannot be pumped into steam generators. In the design, such an accident has been considered and stations are provided with pumps having their own diesel engines (fire water pumps) and therefore do not depend on station power supplies. This however, requires a simple action on part of operators i.e., to depressurize steam generators which enables injection of water to steam generators by low head fire water pumps. With fire water injected into SGs, core cooling can be maintained for extended duration (figure 2).

Only if fire water cannot be injected into SGs, a prolonged loss of makeup to SGs would cause dry out of SGs. The SGs dry out time is of the order of 1 hr. Provisions have been made in these reactors where even considering failure of fire water supply to SGs; water can be admitted to SGs through hook up points. Water from hook up points can be introduced by mobile pumps/fire tenders. This activity can be carried out within half an hour and thus SG heat sink can be continued; and cooling to the fuel can continue.

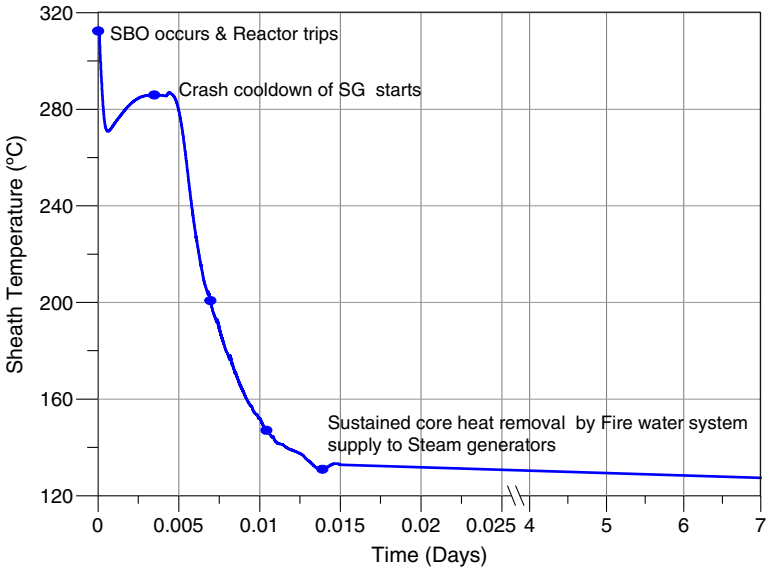

Figure 2. Temperature variation of sheath temperature during extended SBO for TAPS-3&4.

In addition to SGs, PHWRs have large inventory of moderator and calandria vault water surrounding the fuel in channels. In the unlikely event of SGs heat sink becoming unavailable, these water inventories provide decay heat removal capabilities, individually for a minimum of 8 h and 2 days, respectively. Thus these inherent heat sinks in the design provide adequate time to supplement their inventory by hookup arrangements.

4.2 *Safety characteristics of AHWR for extreme events*

In AHWR, extreme events leading to core melt down are eliminated in design by incorporation of several inherent and passive safety features for example, passive mode of core cooling in main heat transport system, passive decay heat removal using Isolation Condensers, passive moderator and passive end shield cooling system, passive containment isolation system and passive poison injection system, etc. The performance of these passive features/systems has been validated extensively by conducting experiments in separate effect test facilities as well as in integral test facilities. In addition to this, a dedicated core catcher has been incorporated in AHWR design to terminate the severe accident progression by quenching the corium and providing long term cooling.

Following examples depict the capability of these passive systems in AHWR in managing extreme events like that of Fukushima, Chernobyl and Three Mile Island by passive means without requiring operators' actions for prolonged period.

The Fukushima accident occurred mainly due to prolonged station blackout conditions and unavailability of safety systems. A situation similar to Fukushima has been considered in AHWR. Due to occurrence of seismic event, the reactor was considered to be tripped on seismic signal and a prolonged station blackout condition prevailed in AHWR. The IC system got valved in by opening of passive valve and active valves upon Main Heat Transport System reaching high pressure due to occurrence of station blackout condition. The passive valve uses steam energy of the Main Heat Transport System to open and the active valve opens due to loss of pneumatic pressure in the system because of occurrence of station blackout condition. Hence, these valve openings are guaranteed in case of station blackout scenario. Once the IC system gets connected to the Main Heat Transport System of AHWR, the steam generated due to decay heat condenses in the large water pool of GDWP tank in which the IC tubes are submerged. After that, the condensate return back into the Main Heat Transport System thus maintaining the system inventory. Our analysis indicated that the decay heat could be removed through ICs into GDWP passively even for more than 110 days without exceeding the allowable the clad surface temperature (figure 3).

Even an extremely low probable Chernobyl type of accident cannot occur in AHWR and can be managed passively without requiring any intervention of operators. The RBMK design had positive void coefficient of reactivity at low power condition which led to significant power excursion and damage of core. On the other hand, AHWR has negative void coefficient of reactivity under all operational states which will never allow the reactor to the scenario of Chernobyl. Nevertheless, an extremely low probable scenario has been postulated for AHWR in the lines of Chernobyl as an academic exercise, and the safety of AHWR has been evaluated. If AHWR happens to operate at low power and enters into an undesirable unstable condition and operator withdraws all the control rods together (similar to what had happened in Chernobyl), the maximum power rise in AHWR is limited due to negative void reactivity coefficient (figure 4) unlike that of Chernobyl. At this condition, the steam flow rate increases leading to MSIV closure causing the Main Heat Transport System pressure to rise. When the pressure reaches the set point

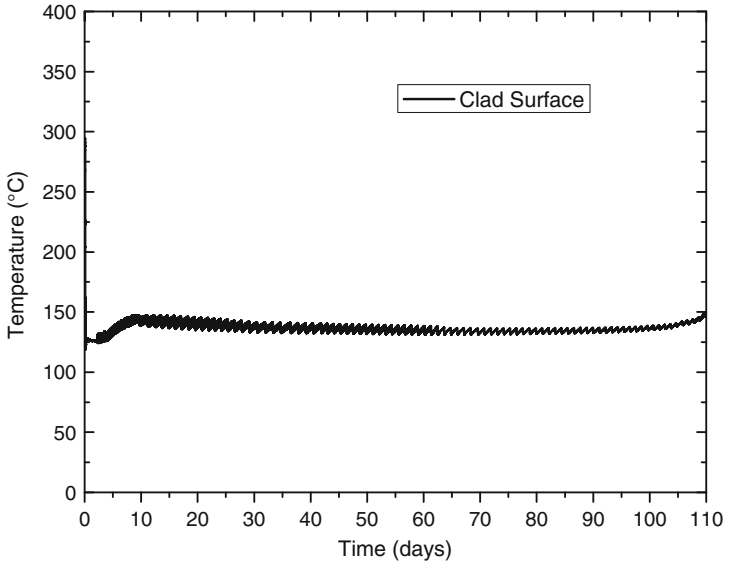

Figure 3. Variation of clad surface temperature in AHWR during a prolonged SBO.

of passive poison injection system, it actuates causing the reactor to be shut down passively. Once the reactor is shut down, decay heat is removed passively by ICs, and the clad surface temperature remains well within the safe limits (figure 5).

On the event line of TMI, an accident scenario of similar type has been postulated for AHWR. It is assumed that the reactor is operating at normal power, when feed water supply becomes unavailable. As a result, turbine gets tripped and Main Heat Transport System (MHT) gets boxed up. Reactor is tripped on high pressure signal. In this case, it is assumed that IC is not available due to some unforeseen reasons with assumption that passive valve does not function, which is

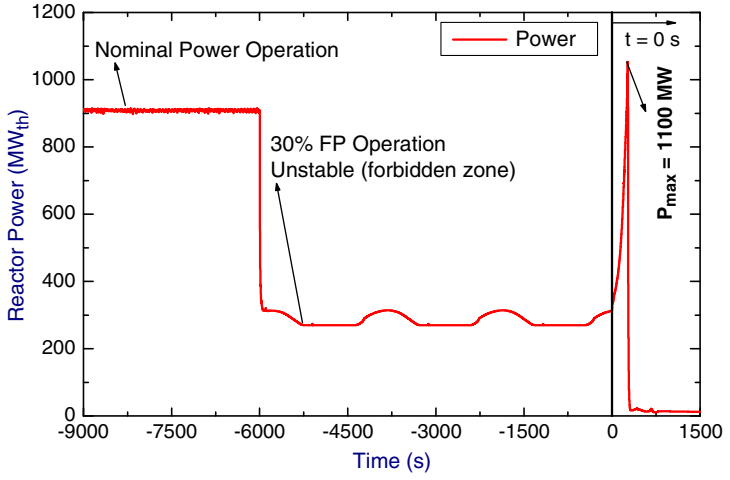

Figure 4. Rise in reactor power in case of Chernobyl type accident in AHWR.

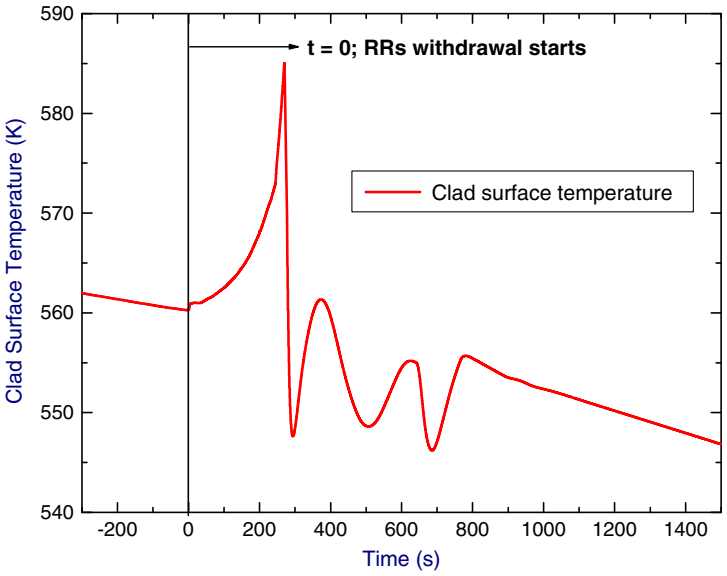

Figure 5. Rise in clad surface temperature in case of Chernobyl type accident in AHWR.

unlikely since it uses fluid energy from the system to open. Nevertheless, an academic exercise has been carried out assuming the IC system does not function. This results in rise of MHT pressure to the set point of Safety Relief Valve (SRV). It is postulated that SRV is stuck open and releases the inventory of Main Heat Transport System into the GDWP. This results in a LOCA condition causing depressurization of Main Heat Transport system. Once the pressure

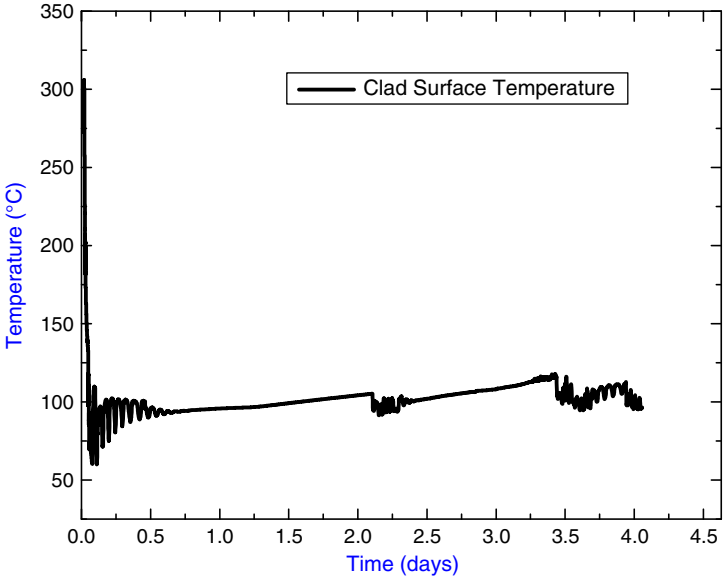

Figure 6. Variation of clad surface temperature in case of TMI accident in AHWR.

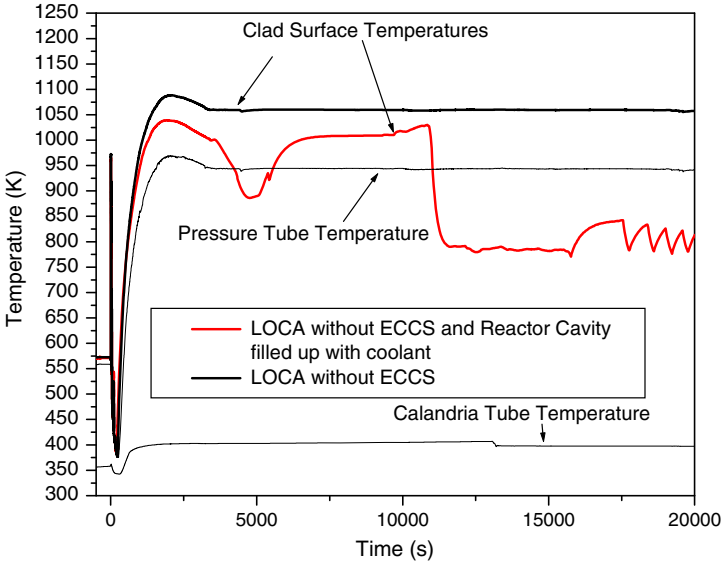

Figure 7. Clad surface temperature for LOCA without ECCS.

falls, injection of water from Accumulator followed by from GDWP continues into the reactor core cooling the fuel pins. The scenario ultimately results a closed circulation system: steam from MHT system to GDWP through SRV-cold water from GDWP to MHT system through ECCS line, thus maintaining system inventory and coolability of fuel pins. Figure 6 shows variation of clad surface temperature during the transient. It is observed that, clad surface temperature remains within the safe limits.

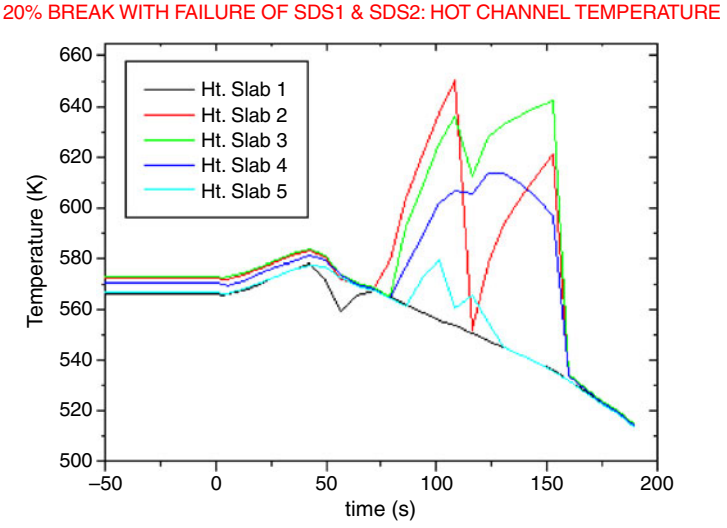

Figure 8. Clad surface temperature for LOCA with failure of wired shutdown system.

Even safety margins for single channel events like 98% flow blockage and stagnation channel break are met by tripping the reactor by providing three independent trip parameters. Clad surface temperatures for LOCA with unavailability of ECCS and LOCA with failure of wired shut down system have been evaluated and are shown in the figures 7 and 8. Even under such conditions, the clad surface temperature remains well within safe limits.

5. Probabilistic safety assessment (PSA)

A key factor in making assessments of safety adequacy is the ability to tie the levels of the defence in depth concept to reliability targets in compliance with the safety goals that are acceptable for nuclear plants. This linkage provides the integration of deterministic defence in depth concepts with probabilistic considerations to satisfy the established safety goal.

5.1 *PSA for PHWR*

5.1a *Level-1 PSA*: A comprehensive Level-1 PSA has been conducted for all Standard Indian PHWRs. Latest methodologies and approaches recommended by IAEA/NUREG guidelines were adopted for conducting this PSA. These studies has been done for internal initiating events during full power operation considering reactor core as the main source of radioactivity.

The major objective of these Level-1 PSA study was to provide an understanding of the possible design vulnerabilities to core damage arising from hardware, human or procedural deficiencies and dependencies.

The major steps followed in performance of these studies are as mentioned below: (a) Collection of information on design and operation of plant, (b) initiating Event Identification and grouping, (c) consequence categorization, (d) event tree development, (e) system modelling. (i) Fault Tree Development as per definition of system failure criteria. (ii) Collection of component failure statistics and parameter estimation. (iii) Common cause failure analysis. (iv) Human reliability analysis (pre and post initiators). (f) Initiating event quantification based on plant outages, Fault tree methodology, reference literature and Chi-squared methodology. (g) Event tree sequence quantification, (h) core damage frequency quantification, (i) uncertainty, importance and sensitivity analysis.

The Level-1 PSA study helps in—

(i) Presenting an integrated picture of the safety of the PHWR which encompasses-design, operational practices, component reliability, dependencies and human reliability.
(ii) Identifying predominant contributors to possible severe core damage in terms of component failures and human actions. Attention then can be devoted to ensuring high reliability of these components and human actions through appropriate design and O&M practices (including surveillance testing, ISI, Allowable Outage Time, Optimisation, Operator Training, Procedures, etc.)
(iii) Identifying any weak-links or imbalances affecting the safety of the plant with reference to components/human actions, which could be improved.
(iv) Evaluating Core Damage Frequency in terms of relative importance of contributors, so as to make comparative assessments.
(v) To provide an assessment of reliabilities of systems having bearing on reactor safety.
(vi) To provide a template for 'living' PSA model to assess the effect of any design and procedural changes, and to provide a tool for plant configuration management.

In addition to the internal events, limited external hazards/events that originate from causes external to the plant and create extreme environment common to several plant systems have been considered in PSA. External hazards are significant since they are ideal candidates for Common Cause Failures. External hazards include earthquakes, floods, high winds, aircraft crashes, cyclones, etc. For Indian PHWR's a typical Flood PSA and Shut Down PSA study have been completed for KAPS 1&2 with internal event Level-1 PSA as base case. Our results indicate that the limiting value for Core Damage Frequency including both Internal and External Initiating Events is 1×10^{-5} / Reactor-yr for new reactors.

5.1b *Level-2 PSA*: The Level-2 PSA deals with frequency and magnitude of releases to environment and consists of probabilistic and deterministic analysis elements. The probabilistic element consists of the development and quantification of containment logic models for each PDS. The deterministic element consists of calculating the release magnitude from the core, physical process of accident progression including containment response and source term analysis of radionuclide releases to the environment for the representative events from each PDS using appropriate codes. The objective of this study was as follows

- To gain insights into the progression of severe accidents and containment performance.
- To identify plant specific vulnerabilities of the containment to severe accidents.
- To identify major containment failure modes and to estimate the corresponding releases of radionuclides.
- To provide a basis for plant specific backfit analysis and evaluation of risk reduction options.
- To provide a basis for the evaluation of off-site emergency planning strategies.
- To provide a basis for the development of plant specific Severe Accident Management Guideline (SAMG).
- To provide a basis for Level-3 PSA.

The following are the stages of the performance of the Level-2 PSA:

(i) Interface with Level-1 PSA, modification to Level-1 event trees, incorporation of Plant Damage States (PDS's) and re-quantification of PDS frequencies. Plant damage state analysis, binning and categorization of Level-1 accident sequences into PDS's and determination of release magnitudes for each PDS i.e., the source terms are identified.
(ii) Assessment of accident progression for severe accidents based on the plant specific deterministic analysis.
(iii) Containment analysis defining the spectrum of containment response and related release states and sequences.
(iv) Development of Containment Event Tree (CET).
(v) Analysis of severe accident management provisions as per SAMG.
(vi) Reliability analysis of containment ESF's by fault tree method.
(vii) CET quantification and incorporation of final release categorization in CET's for estimation of frequencies of various release categories.
(viii) Determination of final release categories by re-grouping event sequences based on the similarity in their release characteristics.
(ix) Quantification of frequencies of various release categories and Large Early Release Frequency (LERF).

The final release categories after merging the preliminary release categories is based on the overall equivalent ground release of iodine and noble gases and dose computation (used only for categorization purpose). Release Category-1 (RC-1) and RC-2 involve the release of more than 5% of total core inventory of iodine activity, thus comprising what is known as large release. IAEA Safety Series 50-P-8 indicates to release of 5–10% of total core inventory of radio iodine as large releases, a value of >5% release of iodine has been considered to constitute the large release in the study. The sequences involving Large Break LOCA with the loss of reactor protection and containment failure constitute the RC-1; and the release is considered to be instantaneous.

The sequences of LOCA initiators with complete loss of decay heat removal (Emergency Core Cooling & Moderator Circulation) and containment failure constitute the RC-2. The release calculations for RC-2 shows that release of iodine and noble gases is maximum during the first 10.4 h after the accident as the Fission Products (FPs) are assumed to be released from the core between 0 and 10.4 h. Although the release calculation is done for 2 months, the amount of FP release is maximum within 10.4 h. LERF is the sum of frequencies of the event sequences leading to release of RC-1 and RC-2.

Limits on LERF are specified 10^{-6}/reactor-year. The predicted results of PHWR studies are well within these limits.

5.2 *PSA for AHWR*

The objective of the study is to determine the consequence of postulated Infrequent Beyond Design Basis Events in AHWR and to estimate the risk. A study towards Level-1, Level-2 and Level-3 PSA has been carried out for AHWR for assessing the system robustness and quantification risk to public (Hari Prasad *et al* 2011).

5.2a *Level -1 PSA*: A level-1 PSA has been performed for AHWR considering only internal IEs, full power operation state with reactor core as the source of radioactivity release. The component failure data have been obtained from references. The various steps involved are:

(i) Identification of Initiating Events (IEs);
(ii) construction of event-tree for each of the identified IE;
(iii) reliability analysis of process and safety systems;
(iv) estimation of core damage frequency;
(v) classification of consequences; and
(vi) uncertainty analysis.

A comprehensive list of the Initiating Events (IEs) applicable to the design of AHWR has been prepared taking into account the list available for PHWRs and PWRs and the design features specific to AHWR. Reliability analysis of process systems like Active Process Water System (APWS), Feed Water system, Non Active Process Water System (NAPWS), Service Water System (SWS), Moderator system, and End Shield Cooling System (ESCS) has been carried out to arrive at the failure frequency of these systems. Also reliability analysis of safety systems like Emergency Core Cooling System, Passive Poison Injection Systems, and Core Decay Heat Removal Systems comprising of Isolation Condensers, Gravity Driven Water Pool Recirculation System have been carried out to evaluate their unavailability.

Core can be either in safe state or in partially damaged state or fully damaged state depending on the severity of the accident. In order to identify the extent of damage that has occurred, plant damage state categorization has been devised based on thermal hydraulics studies. Only thermal criteria are assigned to determine the Plant Damage State (PDS) and damage of channels/channel is not considered for state determination.

As per the thermal criteria, four categories are specified for AHWR as defined below:

(i) **Core damage state:** The core damage state is defined as the accident condition which results in peak clad temperature beyond 1473 K.
(ii) **Core degradation state:** The core degradation state is defined as the accident condition which results in peak clad temperature beyond 1073 K, and within 1473 K.
(iii) **Deviation from safe state:** The deviation from 'safe state' is defined as the accident condition which results in the peak clad temperature beyond 673 K, and below 1073 K, which is the fuel failure criteria.
(iv) **Success state:** The success state is defined as the safe condition, wherein fuel temperature is less than peak clad temperature 673 K.

The accident sequences resulting in Core Damage State has been considered in Core Damage Frequency (CDF) estimation. The Core Damage Frequency (CDF) is calculated and found to be ∼5.46e-8/yr. The frequency for Core Degradation is found to be 2.56e-7/yr. These values are lower than other water cooled reactors.

5.2b *Level-2 PSA*: A Level-2 PSA predicts containment failure modes, as well as the frequency and inventory of radionuclide releases to the environment. While not providing a full risk assessment for AHWR, some insight into risk is provided by the relative frequencies of various release categories.

In Level-2 PSA for AHWR, dominant event sequences leading to 'core damage state' are identified. Deterministic analyses for two enveloping events from the identified events are carried out with a 'multi step and multi physics' methodology to complement the level-2 PSA predictions. The frequency of events are:

- Large LOCA with unavailability of SDS-1 and 2 - 6.3E-10/yr,
- Main Steam Line Break (MSLB) with unavailability of SDS-1 and 2 and Main Steam Isolation Valves (MSIV) - 8.52E-14/yr.

As a part of this study, frequencies are also calculated for unavailability of different containment Engineered Safety Features (ESF) in case of Large LOCA with unavailability of SDS-1 and 2. Fission product generated and released to environment, are estimated for these events. In case of Large LOCA with unavailability of SDS-1 and 2, 94% of I and Cs and 66–70% of Xe and Kr released from core are found to be deposited/remained in MHT piping. Substantial amount of I (50%) and Cs (98%) from the release in containment are found to be deposited in the containment. In case of MSLB with unavailability of SDS-1 and 2 and MSIVs, 99% of released fission product is found to be deposited/remained in MHT pipings.

5.2c *Level-3 PSA*: Level-3 PSA has been carried out to estimate dispersion of released radio nuclides from the containment and related doses (thyroid and bone marrow) at various distances from the plant boundary and at different weather conditions. The two enveloping transients, i.e., (i) Large LOCA with unavailability of SDS-1 and 2 and all containment ESFs and (ii) MSLB

with unavailability of SDS-1 and 2 and MSIVs, result a maximum thyroid dose of 0.4.87–2 Sv and 5.76e-1 Sv at 0.5 km of plant boundary. Frequency of exceedence versus dose has been calculated for thyroid and bone marrow for these two events at different weather conditions. The high frequency scenarios are found to have very low predicted doses as compared to allowable dose limit for public (Hari Prasad *et al* 2011).

6. Conclusions

In this paper, a review of safety features of Indian Heavy Water Reactors against extreme events has been discussed. Deterministic and probabilistic safety analyses have revealed that extreme events can be managed in Indian Heavy Water Reactors with almost zero risk to the public. This is possible because of inherent safety features of heavy water reactors in addition to built-in engineered safety features with several layers of defence-in-depth which not only prevent accident progression and if still happens, can be mitigated. Besides in the new reactor such as AHWR, core meltdown accidents is almost not possible due to the presence of several inherent and passive safety features as demonstrated against accidents like Fukushima, Chernobyl and TMI.

7. Suggestion for future work

The Foregoing sections bring out the current status pertaining to the best design practices. Focus has been given to the reliability of design and utmost safety. In order to maintain these two features, a third consideration of economical design is becoming important in terms of capital (Rs/MW) and operating costs (Rs/kWhr). These three considerations together demand deeper understanding of physics of turbulence, two phase regime maps and hold-up particles, theories of heat transfer and mixing at microscopic level, etc. The overall description of this comprehensive subject has been given by Joshi (2001), Joshi & Ranade (2003). These papers also bring out the need for substantial additional work for evolving economic design. A brief summary is given below.

(i) Appropriate rate of heat removal as against the rate of heat generation is the key feature of design. The accurate prediction of heat transfer coefficient needs the identification and dynamics of turbulent eddies. For single phase flow this subject has been described by Joshi *et al* (2009), Kulkarni *et al* (2001), Deshpande *et al* (2009) and for two phase flow by Joshi *et al* (1980). However, these investigations have been performed for simple geometries. The actual channels and moderators in PHWR and AHWR consist of several internals such as fuel rods, their supports, etc. Therefore, the future studies should include the large eddy and direct numerical simulations of flow in channels. These need to be supplemented with flow visualisations (Laser Doppler anemometry, particle image velocimetry, ultrasound Doppler velocimetry, etc.) and tomographic measurements (γ-ray tomography, electrical capacitance tomography). These measurements need to be supplemented with dynamic pressure measurements at various locations. The techniques need to be developed for mining of the data becoming available from LES and DNS simulations and a variety of experimental measurements. These analyses are expected to give microscopic information on the dynamics of turbulent eddies and hence the rate of heat transfer from first principle.

(ii) The understanding of theory of mixing is very important, for instance, mixing of poison in the moderator. It is known that the mixing strongly depends upon the continued effect of convection, eddy diffusion and molecular diffusion Joshi & Shah (1981); Nere *et al* (2003);

Kumaresan & Joshi (2006). Therefore, the future studies should include the investigation of relationship between the knowledge fluid mechanics obtained in the step (i) above and the mixing. These studies would optimise the usage of poison in the moderator.

(iii) Modelling of multi-dimensional multi-phase flow in rod bundles needs to be carried out in the future studies. This work element is very challenging considering the complexity of internal geometry of channels.

Acknowledgement

Contribution to this paper by the team members from Reactor Safety & Analysis Directorate, NPCIL and Reactor Engineering Division, BARC and Reactor Safety Division, BARC is greatfully acknowledged .

References

AERB Safety guide No. AERB/SG/D-5 2000 Design basis events for pressurized heavy water reactor

AERB Safety Guide No. AERB/SG/O-5 1998 Radiation protection during operation of nuclear power plants

AERB Safety Guide 2001 No. AERB/SG/G-8 2001 Criteria for Regulation of health and Safety of Nuclear Power Plant Personnel, The Public and the Environment Issued in June

AERB/NPP-PHWR/SC/D 2009 Design of Pressurised heavy water reactor based nuclear power plants (Rev. 1)

Bajaj S S 2008 Safety analysis in nuclear power plants. *An Inter. J. Nucl. Power Nupower* 22(2–3): 24–33

Bajaj S S and Gore A R 2006 The Indian PHWR. *Nucl. Eng. Des.* 236: 701–722

Bhardwaj S A 2006 The future 700MWe pressurized heavy water reactor. *Nucl. Eng. Des.* 236: 861–871

Deshpande S S, Mathpati C S, Gulawani S S, Joshi J B, Ravi Kumar V and Kulkarni B D 2009 Effect of flow structures on heat transfer in single and multiphase jet reactors. *Ind. Eng. Chem. Res.* 48: 9428–9440

Hari Prasad M, Gera B, Thangamani I, Rastogi R, Gopika V, Verma V, Mukhopadhyay D, Bhasin V, Chatterjee B, Sanyasi Rao V V S, Lele H G and Ghosh A K 2011 Level-1, -2 and -3 PSA for AHWR. *Nucl. Eng. Des.* 241(8): 3256–3269

IAEA 2011 International fact finding expert mission of the Fukushima Dai-ichi NPP accident following the Great East Japan earthquake and tsunami, IAEA mission report

IAEA-TECDOC-1688 2012 Comparison of Heavy Water Reactor Thermal Hydraulic Code Predictions with Small Break LOCA Experimental Data

Joshi J B 2001 Computational flow modelling and design of bubble column reactors. *Chem. Eng. Sci.* 56: 5893–5933

Joshi J B and Ranade V V 2003 Computational fluid dynamics for designing process equipment: Expectations, current status and path forward. *Ind. Eng. Chem. Res.* 42: 1115–1128

Joshi J B and Shah Y T 1981 Hydrodynamics and mixing models for bubble column reactors. *Chem. Eng. Commun.* 11: 165–199

Joshi J B, Sharma M M, Shah Y T, Singh C P P, Ally M and Klinzing G E 1980 Heat transfer in multiphase contactors. *Chem. Eng. Commun.* 6: 257–271

Joshi J B, Tabib M V, Deshpande S S and Mathpati C S 2009 Dynamics of flow structure and transport phenomena-1: Experimental and numerical techniques for identification and energy content of flow structures. *Ind. Eng. Chem. Res.* 48: 8244–8284

Kulkarni A A, Joshi J B, Ravi Kumar V and Kulkarni B D 2001 Application of multi-resolution analysis for simultaneous measurement of gas and liquid velocities and fractional gas hold-up in bubble column using LDA. *Chem. Eng. Sci.* 56: 5037–5048

Kumaresan T and Joshi J B 2006 Effect of impeller design on the flow pattern and mixing in stirred tanks. *Chem. Eng. J.* 115: 173–193

Narora Atomic Power Station -1&2, 2007 Safety Report Vol. II. Accident Analysis Rev-1

National Report to Convention on Nuclear Safety 2012 (Second Extra Ordinary Meeting on Contracting Parties) Government of India

Nere N K, Patwardhan A W and Joshi J B 2003 Liquid phase mixing in stirred vessel: Turbulent flow regime. *Ind. Engg. Chem. Res.* 42: 2661–2698

Sehgal B R 2012 Nuclear Safety in Light Water Reactors: Severe Accident Phenomenology, Elsevier Publication

Sinha R K and Kakodkar A 2006 Design and development of the AHWR-the Indian thorium fuelled innovative nuclear reactor. *Nucl. Eng. Des.* 236(7–8): 683–700

Srinivasan T N and Gopi Rethinaraj T S 2013 Fukushima and thereafter: Reassessment of risks of nuclear power. *Energy Policy* 52: 726–736

Tarapur Atomic Power Station -3&4, 2007 Safety Report Vol. II. Accident Analysis Rev-3

The Chernobyl Accident 1992 Updating of INSAG-1, IAEA SAFETY SERIES No. 75-INSAG-7

Tolman E L, Kuan P and Broughton J M 1988 TMI-2 accident scenario update. *Nucl. Eng. Des.* 108(1–2): 45–54