ROMANIA

National Progress Report

on the Implementation of the Stress Tests

15th of September 2011

FOREWORD

This report provides information on the progress made by Romania in the implementation of the stress tests required by the European Commission following the Fukushima accident.

The report has been prepared by the National Commission for Nuclear Activities Control, based on the preliminary stress test report for Cernavoda NPP submitted by the National Company Nuclearelectrica and on the preliminary regulatory reviews conducted so far.

The information provided in this report reflects the status of Cernavoda NPP activities relevant for the completion of the stress tests as conducted by the 15th of August 2011 (date of preliminary submission) and will be further detailed and supplemented to meet the specifications developed for the final stress test report due by the end of 2011.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Actions taken post Fukushima

CNCAN requested the licensee to do a preliminary reassessment of the protection against beyond design basis events, including extreme external events and the emergency preparedness and response arrangements.

The licensee also initiated measures in response to WANO SOER 2011-02, including:

- a thorough plant walkdown for verifying protection against seismic, fire and flooding events;
- acquisition and testing of mobile diesel generators
- development of new operating procedures for response to Station Blackout and to total and extended Loss of Spent Fuel Pool Cooling events.

CNCAN requested the licensee to perform a reassessment in compliance with the stress test specifications developed by WENRA and endorsed by ENSREG and the European Commission.

1.2 Progress with the conduct of the stress tests

The licensee submitted a preliminary stress test report by the 15th of August. The licensee will submit their final stress test report by the 31st of October, in compliance with the schedule requested by the European Commission

1.3 Overview of the licensee's preliminary stress test report

The licensee created a dedicated team of plant specialists, supplemented with experts from the plant designers (AECL and ANSALDO Nucleare) in order to perform the safety reassessment in compliance with the ENSREG specifications. In support of the reassessment required by the stress tests, new analyses have been performed where required.

The licensee's preliminary stress test report provides extensive information covering all the aspects outlined by the stress test specifications. Due to security reasons and property rights, the licensee's detailed report cannot be made publicly available. Instead, a summary containing all the information relevant for the public is included in this report. The summary of the licensee's preliminary safety evaluations under the scope of the stress tests are included in Sections 3 and 4 of the present report.

1.4 Preliminary regulatory reviews

Preliminary regulatory reviews and inspections have been performed in the period of 15th of August – 9th of September 2011. The main focus was on performing a completeness check, to ascertain whether the stress test specifications and methodology have been complied with by the licensee. Based on the reviews and inspections performed up to date, CNCAN has confidence that the licensee is able to support all the claims made in the report and that any issues and opportunities for improvement arising from the stress test will be adequately addressed.

2. GENERAL INFORMATION ON CERNAVODA NPP

2.1 General information on the Cernavoda NPP Units

Romania has only one nuclear power plant, Cernavoda NPP, with two units in operation. Cernavoda NPP Units 1 and 2 cover up to 19% of Romania's total energy production. The operating license is held by Societatea Nationala NuclearElectrica (SNN).

The Government has plans to further increase nuclear generating capacity through completion of the project of Units 3 and 4 of the Cernavoda NPP. SNN has started the procedure for analysing the opportunity for resuming construction of these two units and the feasibility studies and investment organisation has been delegated to EnergoNuclear, a joint venture between SNN and other investors.

Due to the fact that the detailed design for Units 3 and 4 is not yet finalised, CNCAN agreed that these units will not be covered under the scope of the current stress tests, but that any potential design changes resulting from the stress tests for the operating units will have to be implemented in Units 3 and 4.

All the units are pressurised heavy water reactors (PHWR), CANDU-6 type.

Table 2.1. **General data on Cernavoda NPP Units**

Reactor	Type	Gross Capacity MW(e)	First Criticality	Operating Status
Cernavoda-1	CANDU-6	706.5	16th of April 1996	in operation
Cemavoda-2	CANDU-6	706.5	6th of May 2007	in operation
Cemavoda-3	CANDU-6	720	-	under preservation, plans for resuming construction
Cemavoda-4	CANDU-6	720	-	under preservation, plans for resuming construction
Cemavoda-5	CANDU-6	-	-	under preservation

Each unit is provided with a dedicated Spent Fuel Bay (SFB) for the spent fuel temporary storage. The SFB is designed to accommodate the fuel discharged during 8 years. After 6-7 years of operation, the spent fuel bundles are transferred to the on-site, naturally air cooled dry storage facility (IDSFS) for the spent fuel long term storage. The IDSFS is designated to provide safe, reliable and retrievable storage for spent fuel produced by the Cernavoda NPP Unit 1 and Unit 2 for a period of time of at least 50 years.

2.2 General information on the Cernavoda site and site evaluations

Cernavoda Nuclear Power Plant (NPP) is located in Constanta county, latitude 44.3˚N and longitude 28.01˚E in the Dobrogea Region (Figure 1.1-1). The nuclear site lies about 2 km southeast of the Cernavoda town boundary, at 4 km southeast of Danube River and at about 1.5 km northeast from the first lock on the Danube-Black Sea Channel (DBSC).

The Cernavoda NPP gets its cooling water from the DBSC. The operational requirements for two units is about 90 m^3/s of cooling water. The cooling water is returned to the Danube River. During winter, a fraction can be released into the intake, so that the warmed cooling water discharge can be used to prevent freezing at the intake. The DBSC (64.2 km long) is a waterway beginning near Cernavoda and ending at Agigea – Constanta, at the Black Sea. It was opened to traffic in 1984. The canal has two locks: Cernavoda (km 60.3), at the Danube end and Agigea (km 1.9), at the Black Sea end.

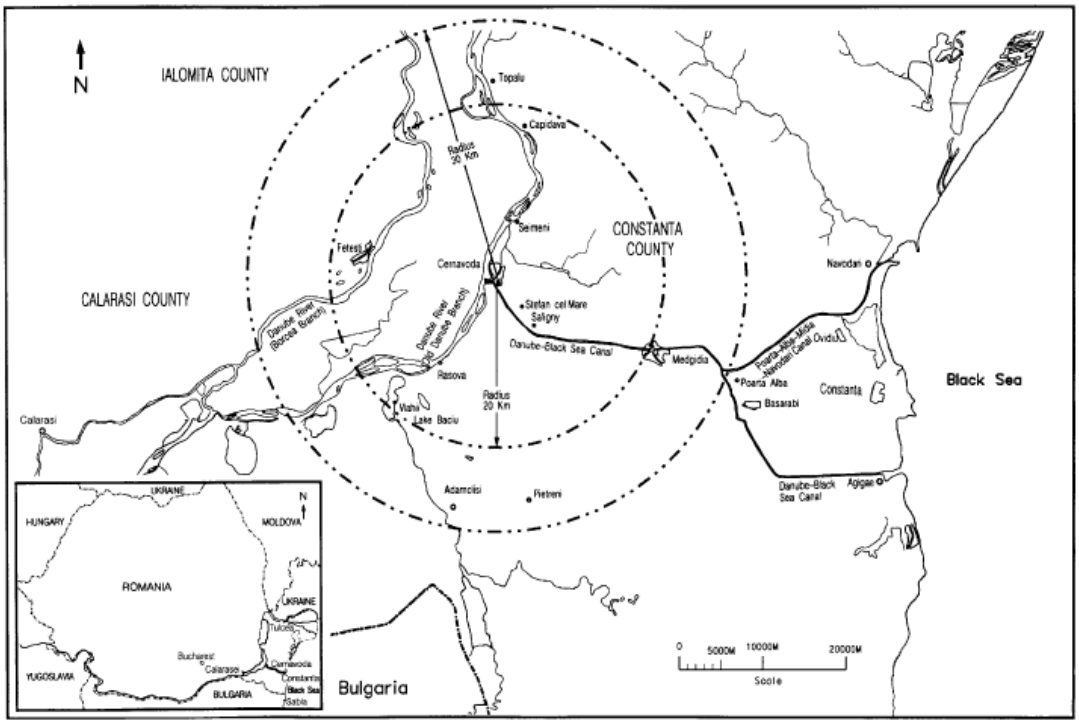

Figure 1.1-1 Cernavoda NPP Site

The Cernavoda site grade level has been established higher than the highest credible flood water level that can theoretically originate from either the Black Sea via DBSC or Danube River.

The site licence for Cernavoda NPP (intended for five units) has been granted in 1979 The safety documentation for demonstrating the fulfilment of regulatory requirements and criteria comprised of the Initial Safety Analysis Report (ISAR) and the supporting technical studies and evaluations.

The factors taken into account in the evaluation of the site from the nuclear safety point of view included both those related to the characteristics of nuclear reactor design and those related to the specific site characteristics. The natural and man-made

hazards analysed for the site include for example: extreme temperatures, snow fall, high winds, flooding, earthquake, low Danube level, explosions, release of toxic and explosive gases, fires, missiles, aircraft crashes.

In accordance with the regulatory requirements, comprehensive safety assessments have been performed to demonstrate that the reactor design ensures a very low probability for accidents resulting in significant radioactive releases and that the site choice and the technical measures taken to mitigate the consequences of the accidents, should these occur, ensure adequate protection of the public and environment. The latest studies of the site-related factors relevant to safety are reflected in the current Final Safety Analysis Reports (FSAR).

2.3 General overview of the CANDU-6 reactor design

Cernavoda NPP is the only nuclear power plant in Europe based on the CANDU (CANada Deuterium-Uranium) technology. Therefore a brief description of the main systems of the CANDU-6 plant is provided in the following.

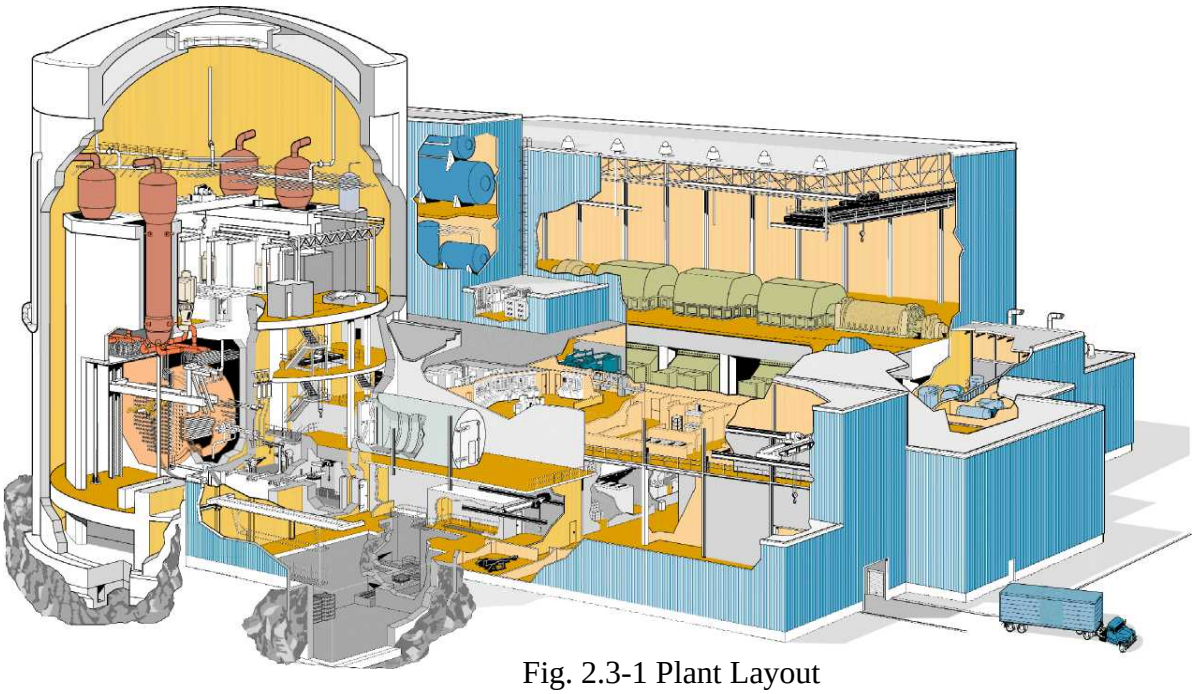

Fig. 2.3-1 Plant Layout

Reactor

The CANDU-6 reactor is fuelled with natural uranium fuel that is distributed among 380 fuel channels. Each six-meter-long fuel channel contains 12 fuel bundles.

The reactor comprises a stainless steel horizontal cylinder, the calandria, closed at each end by end shields, which support the horizontal fuel channels that span the calandria, and provide personnel shielding. The calandria is housed in and supported by a light water-filled, steel lined concrete structure (the reactor vault) which provides thermal shielding. The calandria contains heavy water (D_2O) moderator at low temperature and pressure, reactivity control mechanisms, and 380 fuel channels.

The fuel channels are housed in a horizontal cylindrical tank (called a calandria vessel) that contains cool heavy water (D2O) moderator near atmospheric pressure. Fuelling machines connect to each fuel channel as necessary on both ends of the reactor to provide on-power refueling; this eliminates the need for refuelling outages. The on-power refueling system can also be used to remove a defective fuel bundle in the event that a fuel defect develops. CANDU reactors have systems to identify and locate defective fuel.

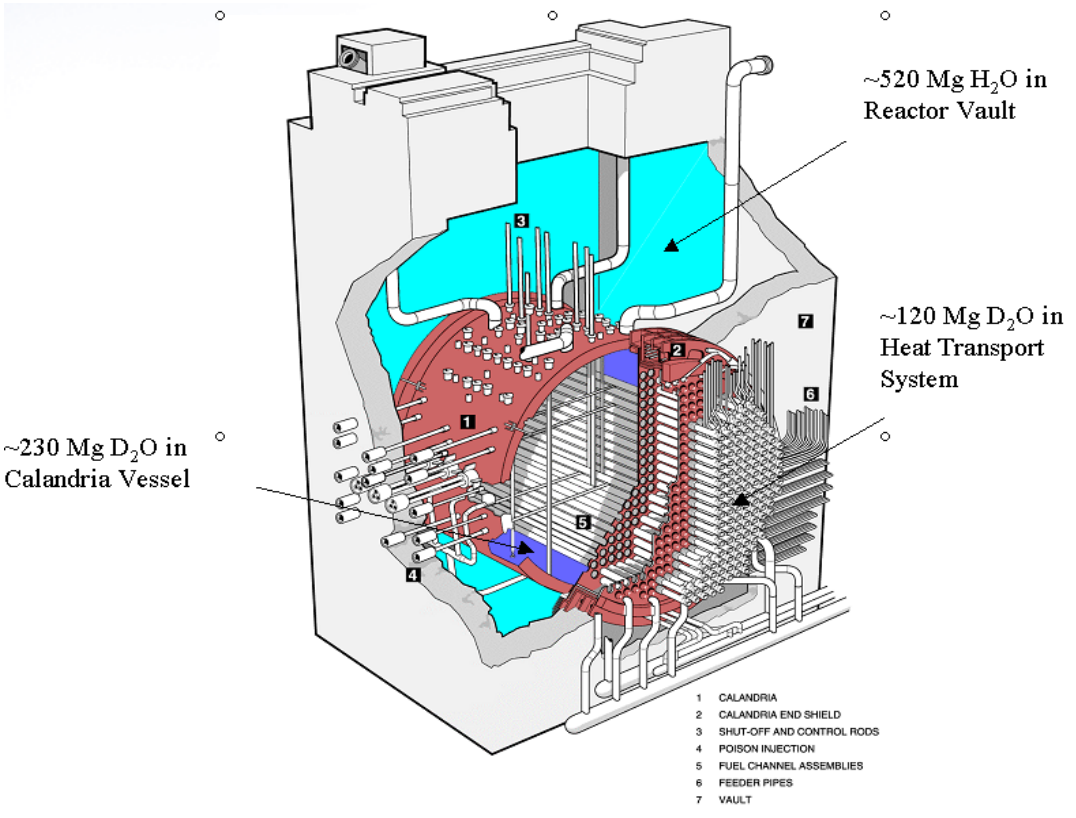

Fig. 2.3-2 Reactor Core Structure and Calandria Vault

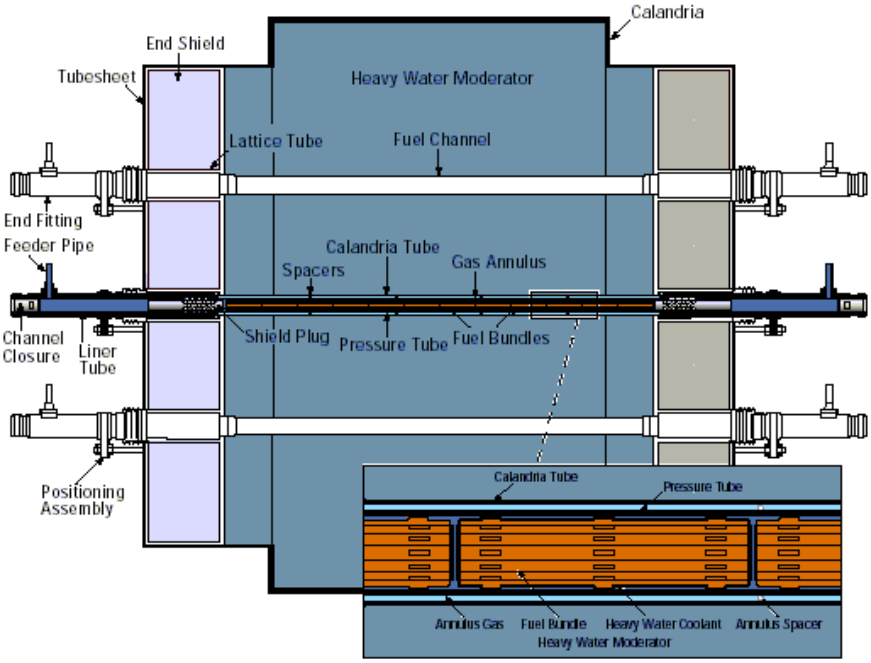

Fig. 2.3-3 Fuel Channels

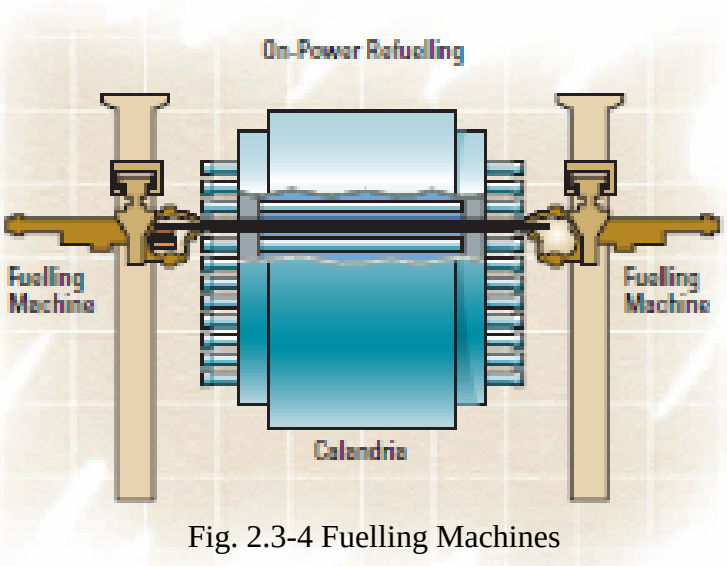

Fig. 2.3-4 Fuelling Machines

Fuel Handling System

The fuel handling system refuels the reactor with new fuel bundles without interruption of normal reactor operation; it is designed to operate at all reactor power levels. The system also provides for the secure handling and temporary storage of new and irradiated fuel.

Heat Transport System

The heat transport system circulates pressurized heavy water coolant (D2O) through the reactor fuel channels to remove heat produced by fission in the uranium fuel. The heat is carried by the reactor coolant to the steam generators, where it is transferred to light water to produce steam. The coolant leaving the steam generators is returned to the inlet of the fuel channels.

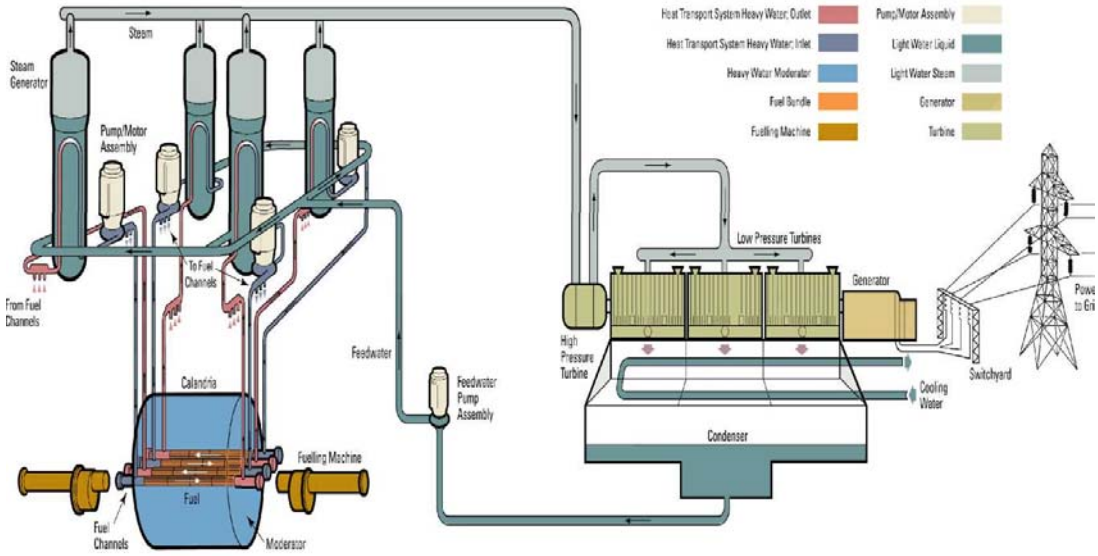

Fig. 2.3-5 Primary Heat Transport System and Balance of Plant

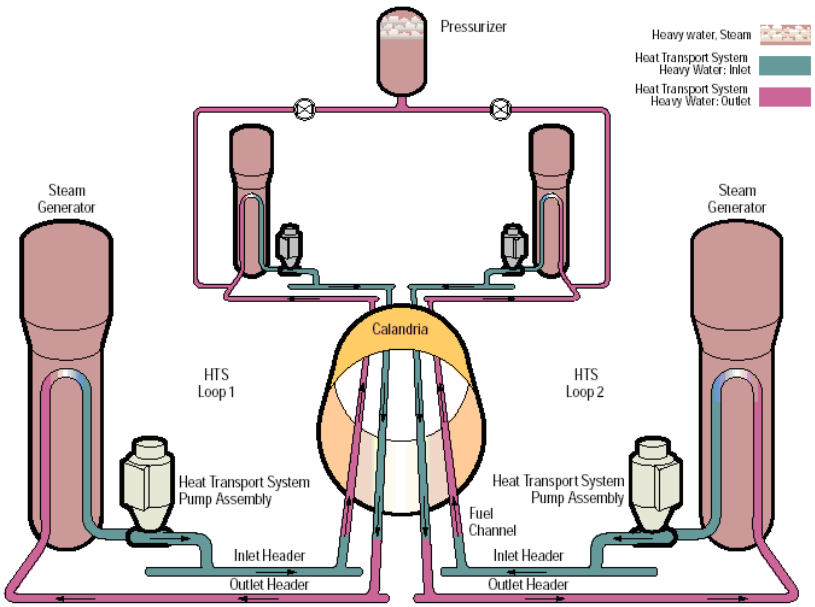

Fig. 2.3-6 Schematic of the Primary Heat Transport System

Moderator System

Neutrons produced by nuclear fission are moderated (slowed) by the D2O in the calandria. The moderator D2O is circulated through systems that cool and purify it, and control the concentrations of soluble neutron absorbers used for adjusting the reactivity.

The heavy water in the calandria functions as a heat sink in the unlikely event of a loss of coolant accident in the heat transport system coincident with a failure of emergency core cooling.

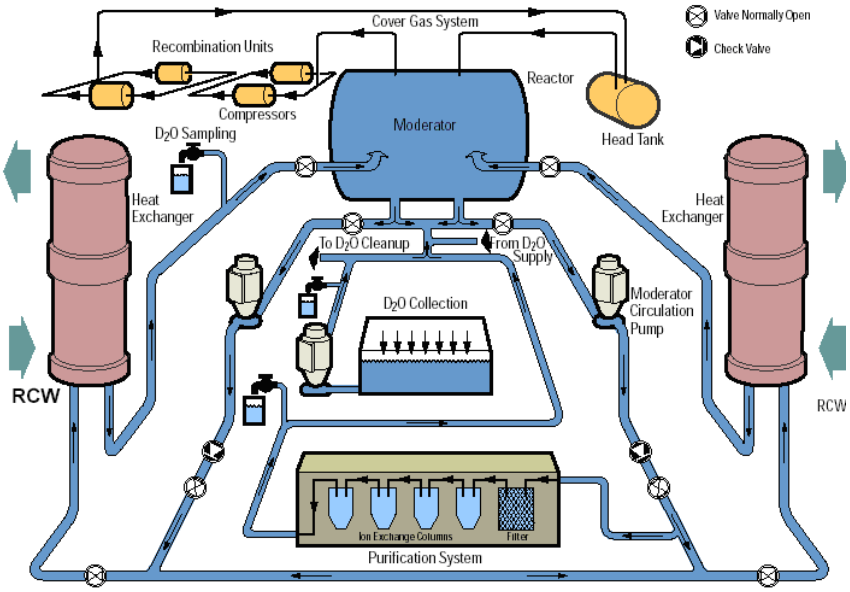

Fig. 2.3-7 Schematic of the Moderator System

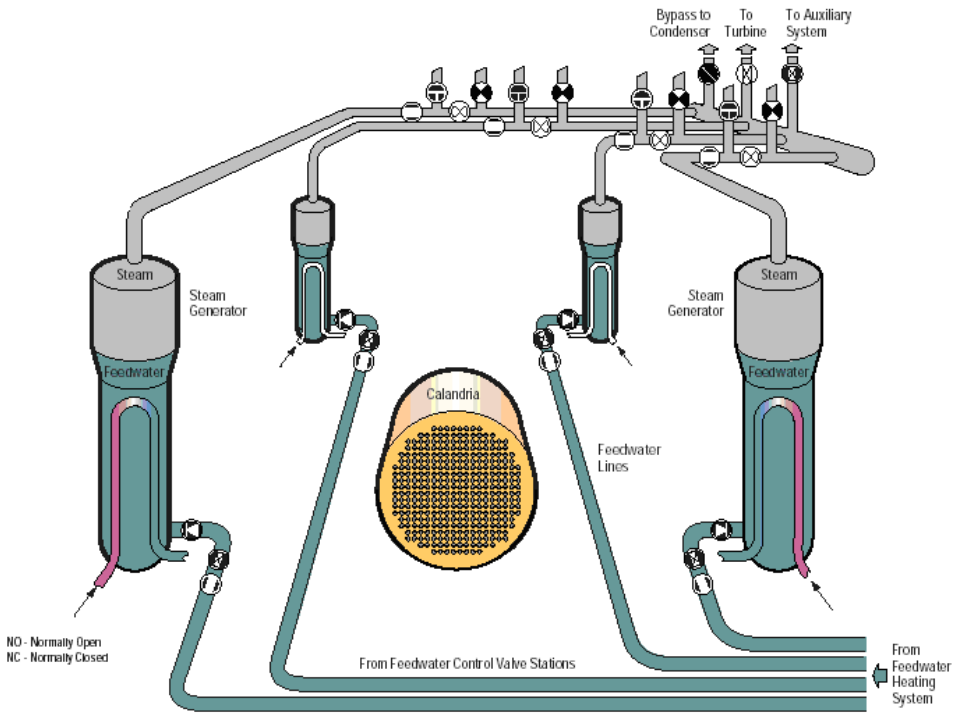

Fig. 2.3-8 Schematic of the Secondary Heat Transport System

Feedwater and Steam Generator System

The steam generators transfer heat from the heavy water reactor coolant to light water (H2O) to form steam, which drives the turbine generator. The low pressure steam exhausted by the low pressure turbine is condensed in the condensers by a flow of condenser cooling water. The feedwater system processes condensed steam from the condensers and returns it to the steam generators via pumps and a series of heaters.

Reactor Regulating System

This system controls reactor power within specific limits and makes sure that station load demands are met via two independent (master / slave) digital control computers (DCC). It also monitors and controls power distribution within the reactor core, to optimize fuel bundle and fuel channel power within their design specifications.

Safety Systems

Four seismically qualified special safety systems (Shutdown System No. One (SDS1), Shutdown System No. Two (SDS2), the Emergency Core Cooling (ECC) System, and the containment system) are provided to minimize and mitigate the impact of any postulated failure in the principal nuclear steam plant systems. Safety support systems provide services as required (electric power, cooling water, and compressed air) to the special safety systems.

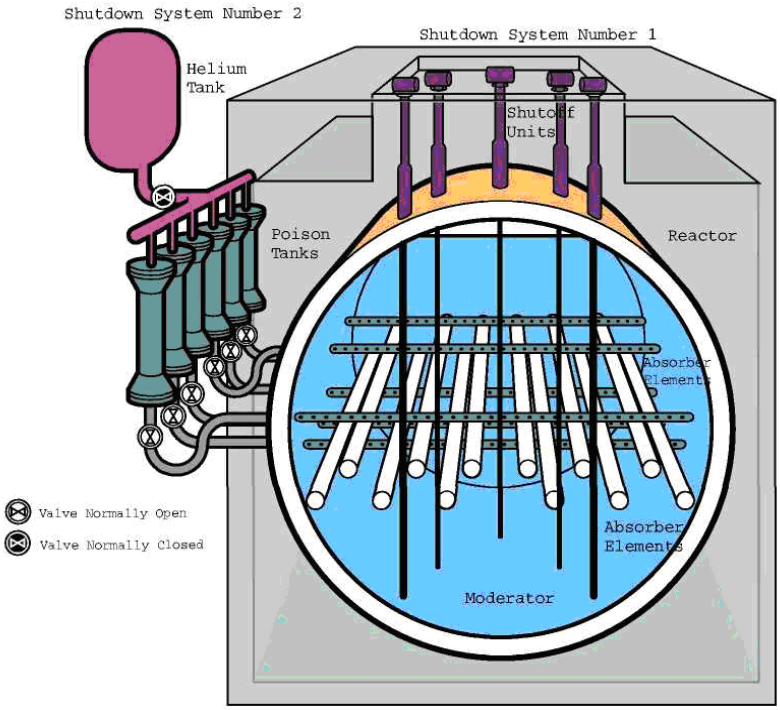

Fig. 2.3-9 Reactor Shutdown Systems

Reactor Shutdown Systems

There are two ‘full capability’ reactor shutdown systems, each able of shutting down the reactor during any postulated accident condition. The two shutdown systems are functionally and physically independent of each other; and from the reactor regulating system. Functional independence is provided by utilizing different shutdown principles: solid shutoff rods for System number 1, direct liquid poison injection into the moderator for System number 2. Physical independence of the shutdown systems is achieved by positioning the shutoff units vertically through the top of the reactor and the poison injection tubes horizontally through the sides of the reactor.

Emergency Core Cooling System

The Emergency Core Cooling (ECC) system is a special safety system, designed to provide make-up and cooling to the PHT for accidents causing a loss of PHT inventory that cannot be made-up by normal process systems to such an extent that fuel cooling by normal means is no longer assured. The ECC performs no normal operating functions, it operates only to mitigate LOCA events.

Emergency coolant injection is provided to the PHT in the event of a LOCA. There are three stages of ECC operation. In the first stage, High Pressure (HP), the water from the ECC accumulator tanks under high pressure is injected into the PHT. In the second stage, Medium Pressure (MP), the water from the dousing tank is pumped into the PHT via the ECC pumps. In the third stage, Low Pressure (LP), the water from the RB basement is pumped into the PHT via the ECC pumps.

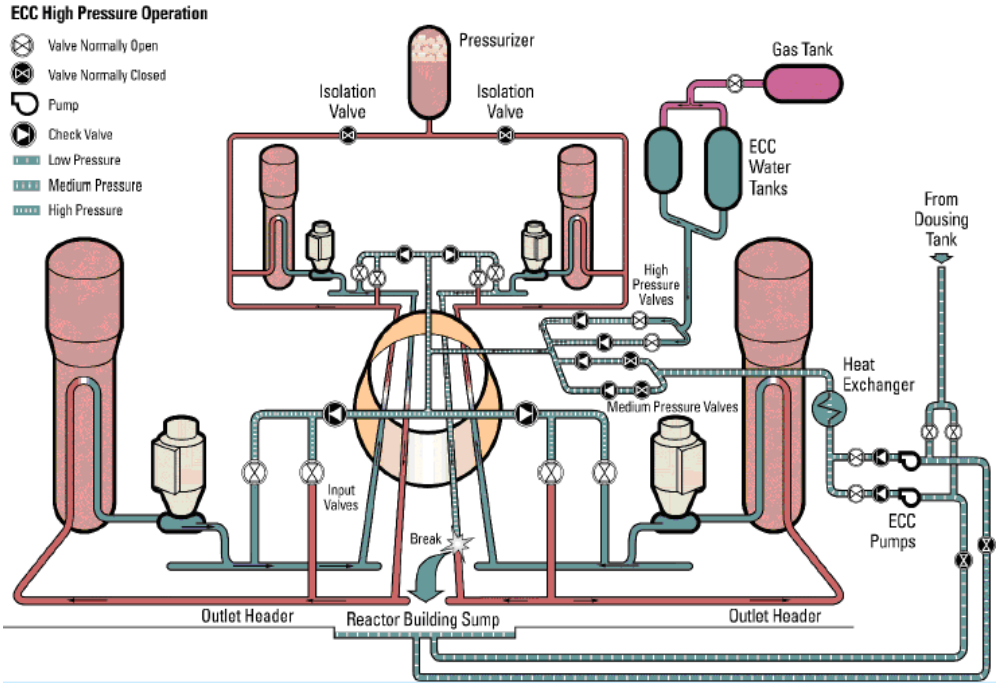

Fig. 2.3-10 Emergency Core Cooling System

Containment System

The containment comprises a number of systems that operate to provide a sealed envelope around the reactor systems if an accidental radioactivity release occurs from these systems. The structures and systems that form containment are:

- a lined, post-tensioned concrete containment structure
- an automatic dousing system
- air coolers
- a filtered air discharge system
- access airlocks
- an automatic containment isolation system.

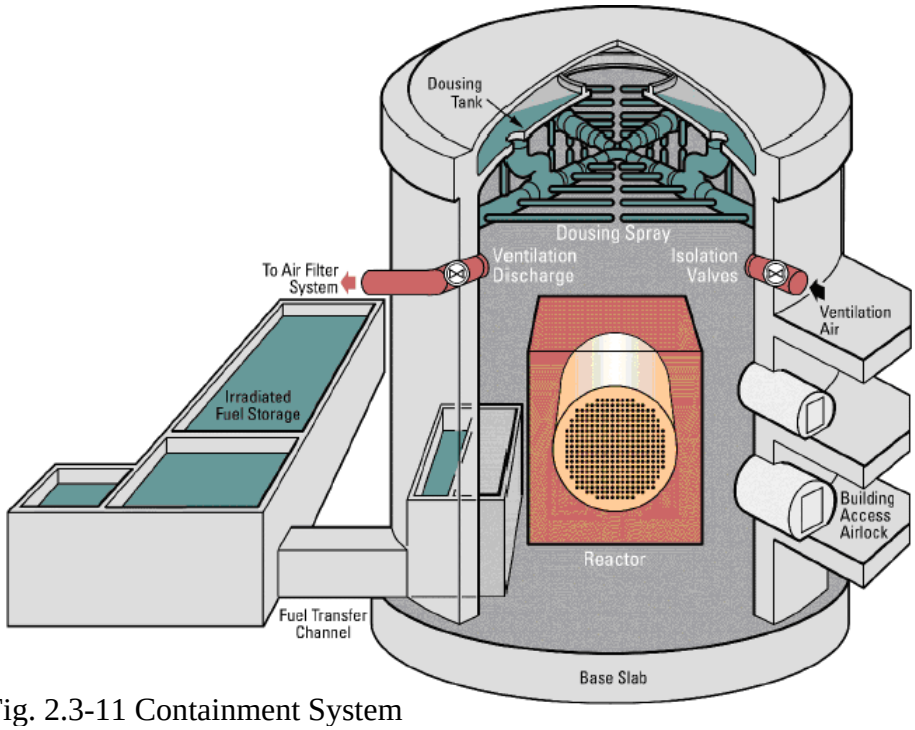

Fig. 2.3-11 Containment System

Spent Fuel Bay

Spent (irradiated) fuel is removed from the reactor channels and is transferred to the Spent Fuel Bays where it is stored under water. The water provides shielding from radiation emitted by the fuel and also provides means to remove decay heat, which is given off by the fuel.

The water in the Spent Fuel Bays is maintained in a clean and pure condition so that the spent fuel can be handled by station personnel with long handled tools working through down below 8 m of water.

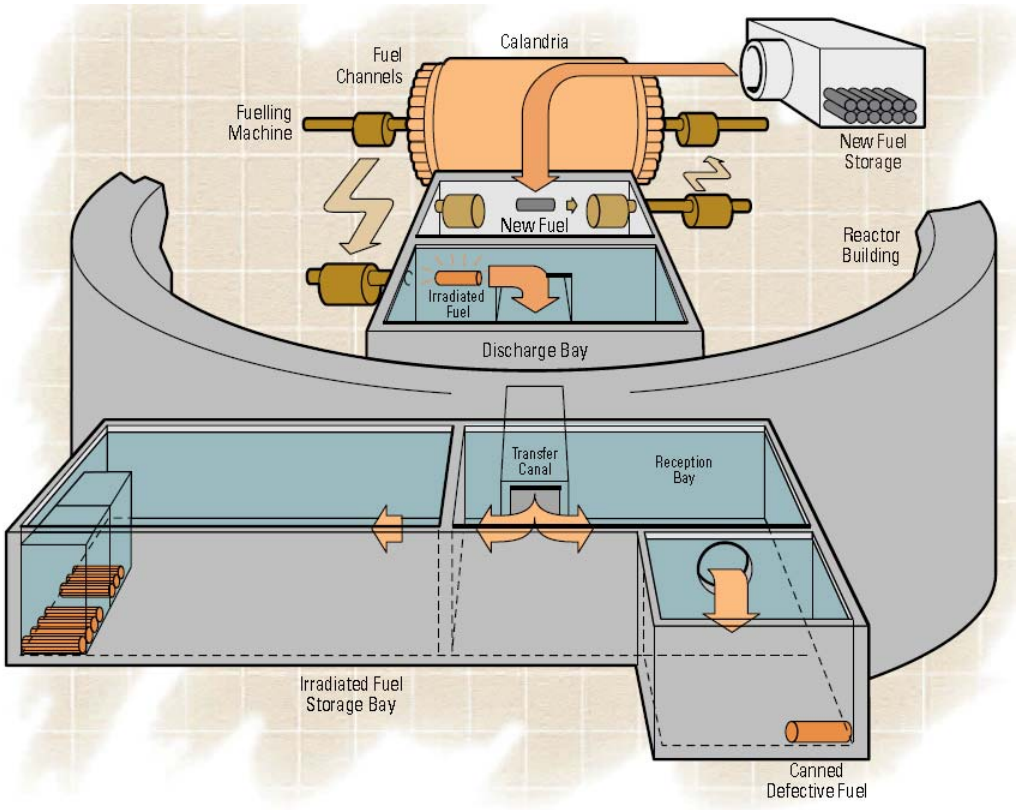

Fig. 2.3-12 Spent Fuel Route

The Spent Fuel Bay Cooling and Purification System are provided to remove the decay heat of the stored fuel and to remove dirt and radioactive particles (fission and corrosion products) from the Storage and the Auxiliary Bays. Although the system is designed to operate a common cooling and purification circuit for all Bays, it is normally operated as two isolated circuits to prevent contaminating the Storage Bay water in case of a failed fuel transfer from the Reactor. Skimmers are provided to clean the water surfaces of the Discharge, Reception, Failed Fuel and Storage Bays. In addition, the operation of a portable Underwater Vacuum Cleaning subsystem is provided.

Fig. 2.3-13 Spent Fuel Bay

Intermediate Dry Spent Fuel Storage Facility

The facility will consist of 27 seismically qualified MACSTOR 200 modules. At present, 4 modules are built and in operation and 3 modules are in construction phase.

Each MACSTOR-200 module is a parallelepiped structure made of reinforced concrete, which embeds 20 metallic Storage Cylinders positioned vertically.

Once filled, the cylinder is covered with a reinforced concrete shield plug and a welded metallic cover plate, both of which are seal-welded to the upper flange of the storage cylinder.

Fig. 2.3-14 Intermediate Dry Spent Fuel Storage

2.4 Safety Philosophy and Defence in Depth

The safety philosophy of CANDU reactors, based upon the principle of defence-in-depth, employs redundancy (using at least two components or systems for a given function), diversity (using two physically or functionally different means for a given function), separation (using barriers and/or distance to separate components or systems for a given function), and protection (seismically and environmentally qualifying all safety systems, equipment, and structures).

An important aspect of implementing defence-in-depth in the NPP design is the provision of a series of physical barriers to confine radioactive material at specified locations. In CANDU design these barriers are the fuel matrix, the fuel sheath (clad), the Heat Transport System (HTS), and the Containment. An additional administrative barrier is the exclusion area boundary.

For design purposes, the safety related systems and structures have been defined as those which, by virtue of failure to perform the safety functions in accordance with

the design intent, could cause the regulatory dose limits for the plant to be exceeded, in the absence of mitigating system action.

The safety related systems and structures of a CANDU NPP can be broadly categorised as follows:

- Preventative: Systems and structures that perform safety functions during the normal operation of the plant, to ensure that radioactive materials remain within their normal boundaries. These are systems and structures whose failure could cause a release exceeding the regulatory dose limits during normal plant operation, in the absence of further mitigating actions, or whose failure as a consequence of an event could impair the safety functions of other safety related systems.
- Protective: systems and structures that perform safety functions to mitigate events caused by failure of the normally operating systems or by naturally occurring phenomena.

Some systems may perform both protective and preventative safety functions, and therefore may have more than one safety category designation.

The protective systems defined above are further identified as:

- Special Safety Systems, which include Shutdown System No. 1, Shutdown System No. 2, Emergency Core Cooling, and Containment.
- Safety Support Systems, which provide essential services needed for proper operation of the Special Safety Systems (e.g., electrical power, cooling water). These systems may have normal process functions as well.

The Special Safety Systems are always in standby during the normal operation of the plant and ready to mitigate the consequences of any serious process failure. They are totally independent from the process systems.

The Special Safety Systems and standby safety related systems have been physically separated by their assignation into two groups (Group 1 and Group 2) in order to provide adequate protection against common cause failures from events such as:

i) Turbine disintegration and resultant missiles;
ii) Fires that can lead to uninhabitable control centre, wide spread system damage, etc.;
iii) Aircraft crash;
iv) Failure of a common process e.g. Electrical Power Systems, Service Water System, etc.;
v) Common adverse environment e.g. extremes of temperature, pressure, humidity, radiation, toxic gases, etc.

In addition, within each group, there is separation between each the Special Safety Systems and between the channels of a system. The separation is achieved by the physical arrangement of equipment and of protective channels.

The essential safety functions that can be performed by either Group 1 or Group 2 are:

- reactor shutdown;

- fuel cooling;
- confinement of radioactivity;
- providing the operators with the alarms and indications required to assess the state of the unit and to take the necessary actions to mitigate the consequences of an accident.

Each group includes one SDS and either the ECCS or the Containment, because the analyses of the most severe cases, as presented in the Safety Report, assume one SDS system is unavailable and that either the ECCS or Containment is unavailable. As it is not possible to suffer more than those unavailabilities, it follows that the safety of the facilities is ensured at all times. Component redundancy is built-in for the Special Safety Systems to ensure that the single failure criterion is satisfied. Special Safety Systems satisfy an unavailability target of 10^{-3} years/year, which effectively requires redundancy of all critical components.

The availability of these systems is verified during operation by regular safety system component tests. Specific requirements are applied to the triplicated instrument cables and the duplicated power and control cables for safety-related systems. The odd and even concept of on-site power distribution is applied to equipment, the raceway system and junction boxes, in order to maintain physical separation between the odd and even systems to achieve maximum reliability under normal and abnormal conditions

To satisfy reliability requirements to meet safety objectives, the Group 1 Electrical Power System is equipped with standby Diesel generators supplied with support services from Group 1 systems. The power distribution system is designed to prevent propagation of electrical faults to the Group 2 Emergency Power Supply System and vice-versa. The portions of the distribution system needed to supply electrical power from the Group 2 Emergency Power Supply System to components required for the earthquake events are seismically qualified.

CANDU-6 is a proven design and sufficient information is publicly available on the general design features and on the CANDU safety philosophy and approach to prevention, mitigation and management of accidents. Therefore, this section only gives some examples of CANDU design features relevant for each of the levels of the defence in depth.

Prevention

- The reactor coolant pressure boundary is designed in accordance with ASME Section III - Class 1 requirements, as supplemented by Canadian Standards in the areas not covered by the ASME Code. The pressure tubes of the PHTS have “leak-before-break” characteristics. The plant is provided with extensive and sensitive leak detection systems. The presence of tritium in the PHTS makes the leak detection very efficient even for very small leaks.
- The on-line tritium in water detection system is used for revealing leaks to heat exchangers and to the S/G tubes.
- PHTS leaks open to Reactor Building atmosphere are revealed by the increasing of D_2O vapours recovery or by balance of heavy water into PHTS.

- The probability of occurrence of a sudden large-size break in a pressure tube is extremely low, in view of the following considerations:
    i) as per design, the tube-wall thickness was selected such that leakage will precede tube rupture ("leak-before-break" concept);
    ii) a leak of a pressure tube can be detected quickly (by means of the surveillance system analysing the gas contained in the annular space between pressure tubes and calandria tubes) thus allowing ample time for corrective action;
    iii) the pressure tubes and their end-fittings can be inspected by means of ultrasonic techniques, thus providing an up-to-date overview of the state of the pressure tubes;
    iv) although the pressure tubes are designed to serve for the entire life time of the plant, they can be replaced with relative ease, thus permitting early elimination of tubes showing any signs of faults.
- On-power refuelling implies that the power distribution reaches an equilibrium in less than a year from initial start-up, and remains virtually unchanged for the reactor's operating life. This greatly simplifies the analysis of core behaviour as a result of postulated accidents.
- On-power refuelling also allows defective fuel to be detected, localised and removed from the core, reducing the contamination of the reactor coolant piping and simplifying maintenance.
- CANDU fuel is very reliable, being composed of natural uranium oxide. Almost no fuel failure happens before the fuel is removed after nominal burn-up.
- There is no criticality hazard in the handling or storage of the UO_2 fresh/spent fuel because it is not enriched and cannot be arranged in a critical array, except for in heavy water.

Control

- CANDU NPPs are provided with extensive instrumentation and control systems, capable of monitoring those variables and systems that can affect the fission process, the integrity of the reactor core, the PHTS pressure boundary and the containment. Most control functions for the reactor and the Balance of Plant, including automatic start-up, are performed by two identical, independent digital computers, each capable of complete station control. The two computers run simultaneously, one acting as instantaneous back-up to the other. Protection functions are, however, not performed by the digital process control computers but by Programmable Digital Controllers (PDCs), there being strict separation between control and protection systems.
- The Reactor Regulation System (RRS) is part of the fully computerised control system. This computerized control system is also responsible for boiler pressure and level control, unit power regulation, primary heat-transport pressure and inventory, and turbine run-up.
- The design philosophy for the RRS is to limit the maximum rate of reactivity additions to a value low enough to achieve safe control in all conditions. The neutronic flux spatial control system is designed to maintain stable control of the power distribution for any of the normal movements of other control

devices such as adjuster rods or liquid zone controllers. The reactivity change due to refuelling is also adequately controlled by liquid zone controllers.

- The low excess reactivity of the CANDU core leads to relatively low reactivity worth of the control devices, limiting the potential severity of postulated loss-of-regulation accidents.
- Apart from the four systems employed by RRS, using control rods, adjuster rods, light water compartments and poison addition into the moderator region, two independent and diverse fast-shutdown systems are provided.
- Furthermore, the relatively open core lattice of the CANDU reactor permits complete separation between control and protection functions also for the neutron poison devices (i.e. the control rods used by RRS are the 4 mechanical control absorbers - MCA, while the SDS #1 uses 28 shutoff rods; poison addition to the moderator is done by RRS through the moderator liquid poison system, while the SDS #2 inserts poison from its own liquid injection shutdown units).
- To insure that localised overrating of the fuel does not occur an array of self-powered flux detectors is provided for application in the regional overpower protective (ROP) system. A separate array of detectors is provided for each of the two shutdown systems.
- The self-protection functions of the RRS (Stepback and Setback) are essential to ensure that station operation is within the boundaries assumed in the analyses. In the majority of event scenarios, the above mentioned self-protection functions can avoid reaching the trip set points of the Shutdown Systems (SDS#1 & SDS#2). The availability of the Reactor Regulating System (RRS) is absolutely required for maintaining the reactor in the critical state. Consequently, on a loss of RRS, the reactor is tripped immediately, with no attempt at re-start.
- Heavy-water neutron kinetics is slower by several orders of magnitude than light-water kinetics, this making the control easier because of the inherent kinetic behaviour of the delayed neutrons.
- Provision of passive heat sink after common mode events like loss of electrical power is ensured by thermosyphoning through the steam generators.
- The plant is provided with two separate control rooms in different locations, each with capability of shutting down and cooling the reactor to cold conditions, and providing continuous monitoring-of-the-plant information to the operating staff; this capability is still maintained in each control room even if total failure of all equipment in the other control room is assumed.

Protection

- The Special Safety Systems are fully automated, although they can be actuated manually if required. Each system is independent of the others, employing its own sensors, logic, and actuators. Each system uses triplicated logic in two out of three logic configuration, (three sensor circuits, with two-out-of-three voting), with the ability to be tested on-line.
- SDS#1 uses solid shutoff rods (stainless steel sheathed cadmium absorbers), dropping by gravity into the core, and is capable of shutting down the reactor

for the entire spectrum of postulated initiating events. SDS#2 uses high-pressure liquid poison (gadolinium nitrate) injected into the (low-pressure) moderator, and is also capable of shutting down the reactor for the entire spectrum of postulated initiating events.

- Each SDS, acting alone, is capable of shutting down the reactor within less than 2 seconds and maintaining it subcritical under cold conditions, for all accident scenarios. In safety analysis, the two most effective of 28 shutoff units for SDS#1 are assumed unavailable. Likewise, one of six liquid poison injection nozzles for SDS#2 is assumed unavailable. Prompt criticality is not reached in accident conditions, as shown by analysis.
- The positive reactivity that would be introduced by loss of coolant accidents is well within the capability of mechanical and hydraulic shutdown systems.
- An important intrinsic safety feature of the CANDU reactor is that all neutron control devices are installed in the low-pressure moderator region, where, in case of a postulated LOCA due to a break in the headers or feeders, they are not subjected to potentially severe hydraulic forces. The moderator also provides a low-pressure environment for the control rods, eliminating the "rod-ejection" scenarios. In addition, the location of neutronics measurement devices in the moderator avoids subjecting this equipment to a hot, pressurised environment.
- Under any operating state, the CANDU 6 has a number of heat sinks. At full power, the main heat sink is provided by the four steam generators. The other heat sinks become more important when in a shutdown state or during abnormal events. This can be either through the Shutdown Cooling System (SDCS), the Emergency Water Supply System (EWS), or the Boiler Make-up water system (BMW).
- The steam generators with the Feed Water System remove reactor heat during normal plant operation. The Auxiliary Feedwater System and/or the Shutdown Cooling System removes the decay heat during plant shutdown. These systems belong to Group 1, they are designed to remove normal and decay heat and are powered by the normal (Class III, II and I) electrical power systems.
- The Shutdown Cooling System (SDCS) is designed for the full nominal operating pressure and temperature of the PHTS, so it can, if needed, be connected to the PHTS immediately following reactor shutdown, precluding the need for depressurisation after a loss of heat sink.
- Following a common mode event that may disable the above means of decay heat removal, a second independent means of decay heat removal is provided by the Emergency Water Supply (EWS) System which is powered independently by the Emergency Power Supply (EPS) System. Accordingly, the EWS and EPS Systems belong to Group 2.
- The EWS system has a function/feature known as the Boiler Makeup Water (BMW). This subsystem automatically feeds water under gravity to the secondary side of the boilers when they become depressurised following a loss of boiler feedwater. The source of BMW system is the water stored in the dousing tank.

- It should be noted that the Group 1 and Group 2 means of removing decay heat have the PHTS and the steam generators in common. Open path to atmosphere is ensured by Group 1 (ASDV) and Group 2 (MSSV) relief devices.
- The ECCS can maintain or re-establish core cooling by supplying coolant to all reactor headers. It consists of three phases: high-pressure water injection (used during the early stages of an event), medium pressure water supply from the containment building's dousing tank (used during the intermediate stages), and low-pressure water supply based on recovery from the building's sump. The ECCS is designed for LLOCA - 100% break of the largest pipe (reactor header). The discharge area is equal to twice the cross-sectional area of the pipe assumed to fail. Sensitivity analysis for the comparison of a 100% longitudinal break and a double ended guillotine break has shown very similar results, so longitudinal breaks have been modelled for all break sizes up to 100%.
- Considerations with regard to the ECCS:
    i) the simple configuration of the individual fuel channels facilitates coolant delivery to all core locations;
    ii) the correct performance of the ECCS does not constitute the final defence against core meltdown in case of LOCA; the accident analyses, supported by experiments, indicate that a LOCA combined with ECCS failure, though resulting in substantial fuel damage (including partial melting of the cladding) and some deformation of the pressure and calandria tubes, does not result in fuel melting; the decay heat can be removed by conduction through the walls of the pressure and the calandria tubes into the moderator, and rejection by the moderator cooling system, which can remove than 4% of the total thermal power, enough to accept decay heat indefinitely.
- The Containment System forms a continuous, pressure-confining envelope around the reactor core and primary heat-transport system. In the CANDU 6 design it consists of a pre-stressed, post-tensioned concrete structure, an automatically-initiated dousing system, building coolers, automatic isolation system and a filtered air discharge system. The containment system prevents releases of radioactivity to the public in the event of failure of the nuclear components of the heat transport system. The design basis event considered is any LOCA event concurrent with dousing failure. This event presents the highest potential in terms of peak pressure. However, the events related to steam systems breaks are also considered in terms of maintaining structural integrity of containment. The containment structure and all other parts of the containment boundary, are pressure and leakage tested before first criticality and leakage tested periodically thereafter. Another inherent safety characteristic of CANDU 6 plants is the low ratio of reactor thermal power to containment volume.

Mitigation

- The large-volume, low-pressure, low-temperature moderator surrounding the fuel channels acts as a heat sink in LLOCA + LOECC scenarios (which for CANDU are included in the design basis), rendering negligible the risk of fuel

meltdown. The pressure tubes will sag and/or strain into contact with the calandria tube where further deformation will be arrested by the cooling of the moderator system.

- In a loss of heat sink or loss of flow event (such as a total station blackout), the reactor coolant will heat up and pressurise which can cause the pressure boundary to fail. In a CANDU reactor experiencing the same initiating event the fuel heat-up in the fuel channels will cause one of the many pressure tubes to rupture, depressurising the system by blowdown into the moderator well before boiler tube might fail and before a high pressure melt ejection can occur. The pressure tubes act like fuses in this instance. Failure of one channel is sufficient to limit widespread channel failures because it results in rapid heat transport system depressurisation and induced blow down cooling. Furthermore, heat transport system depressurisation occurs well before potential formation of molten core conditions, thereby assuring that high pressure melt ejection does not exist as a containment challenge in CANDU reactors.
- A large volume of light water surrounds the calandria vessel in the calandria vault. Thus, the design ensures a passive heat sink capability which, in many event sequences, would provide significant time delays in the progression of the accident. The calandria vault provides the third line of defence (after the ECC and the moderator) in cooling the reactor core during a severe accident. The large volume of water in the calandria vault has adequate thermal capacity to passively prevent calandria vessel failure. Water in the calandria vault can provide continued external cooling of the core debris relocated at the bottom of the calandria. During this process, the significant volume of water inside calandria vault cools the outer calandria vessel wall, maintaining the external cooling of the vessel. As long as calandria vessel is mostly submerged in water and the calandria vault water inventory can be maintained, it is expected that corium will be retained in the calandria vessel and accident progression arrested in-vessel. The externally cooled calandria vessel acts as a “core catcher” containing the core debris. Core disassembly and relocation take place only at low heat transport system (PHT) pressures and that melting of core materials is avoided until after the debris has relocated to the bottom of the calandria vessel.
- Overall, high volumes of water in the Heat Transport System, in the calandria vessel and in the calandria vault, notwithstanding the water volume from the dousing tank, all ensure a CANDU-specific extensive heat sink capability that confers a slow progression of severe accidents
- Since the geometry of the CANDU core is near optimal from a reactivity standpoint, any rearrangement under severe accident conditions ensures shutdown. Therefore, re-criticality under is not a concern for a CANDU reactor.
- The bottom of the large calandria vessel provides a spreading and heat removal area for core debris following a severe core damage accident.

2.5 Deterministic and Probabilistic Safety Assessments for Cernavoda NPP

2.5.1 Background

For the purpose of safety assessment all major systems in CANDU reactors are categorised as “process systems” and “special safety systems”. All special safety systems are independent from all process systems and from each other.

The CANDU safety philosophy is based on the concept of single/dual failures. “Single failure” is a failure of any process system which is required for the normal operation of the plant and “dual failure” represents a combination of the single failure events and a simultaneous failure or impairment of one of the special safety systems. Coincident failure analysis is a systematic assessment of postulated dual failures. Each postulated process failure is systematically coupled with a failure of one of the special safety systems. Loss of the shutdown systems is excluded from required dual failure sequences because the design includes two independent shutdown systems which are each capable of shutting down the reactor.

A distinguishing feature of dual failure assessment is that the analysis of CANDU 6 reactors must show that:

- coolable core geometry is retained, even if the ECCS were to be impaired;
- radioactive releases are adequately prevented, even if the containment system were to be impaired.

2.5.2 Deterministic safety assessments

The deterministic analyses, including the description of initiating events, event sequences, acceptance criteria, methodology, results and interpretation are provided in Chapter 15 of the FSARs. Each of process systems failures (initiating events) considered were analysed for the case in which the ECCS and the containment subsystems are available, and also in combination with various failures/impairments to either ECCS or containment subsystems. Feedwater events and main steam line breaks were also analysed in combination with loss of Class IV power. Large LOCA and small LOCA events are analysed also in combination with loss of off-site power and with impairments to either ECCS or containment system functions.

The licensee updated the deterministic safety analyses originally provided for Unit 1 with the design, based on plant specific models and state-of-the-art computer codes, in order to address the aging effects.

2.5.3 Probabilistic safety assessments

The Level 1 PSA for all operating stages including external (seismic) and internal events show a core damage frequency (CDF) of 3.3E-5 events/year for Unit 1 and 3E-5 events/year for Unit 2. These results are three times less than the internationally accepted target of 1E-4 event/years (IAEA 75-INSAG-3) for operating plants.

In order to support operational decisions with input from probabilistic assessment, Risk Monitor applications are developed based on the plant specific PSA models,

providing on-line / off-line users with friendly interface. The Cernavoda NPP Risk Monitor is based on the Equipment Out Of Service (EOOS) application developed by EPRI, commonly used in nuclear power plants. The use of EOOS for risk-informed decision making was reviewed and approved by CNCAN.

For both Cernavoda Unit 1 and 2 the risk monitoring results show that the medium Annual Cumulative Recorded CDF is lower than the Average PSA Level 1 CDF.

The licensee has started actions to perform a Level 2 PSA for both Cernavoda Units 1 and 2. Meanwhile, fault trees analyses for containment systems have been done that demonstrate it meets the unavailability of 1E-3 years/year, imposed by the design standards. The annually cumulative CDF together with the containment systems performance are monitored and reported quarterly to the Romanian nuclear regulatory authority. The results confirm that the probabilistic safety goals related to core damage and radioactive release frequency are met.

3. SAFETY EVALUATIONS UNDER THE SCOPE OF THE STRESS TEST

The "Stress Test" for Cernavoda NPP U1 and U2, as defined by WENRA, was targeted on the reassessment of safety margins in the light of the events which occurred at Fukushima.

The reassessment considered a set of extreme situations at the plant site brought on by:

i) Earthquake;
ii) Flood; or
iii) A combination of earthquake and flood.

3.1 Earthquake

The present chapter addresses only the earthquake and the earthquake induced flooding (i) and (iii).

3.1.1 Seismic design basis

The first step in the assessment was a systematic review of the original analyses done as part of the Cernavoda NPP siting. The level of earthquake against which the plant is designed and the methodology used to evaluate the DBE has been found adequate as they are in compliance with the international standards. The validity of data in time and the conclusion on the adequacy of the design basis has been confirmed by the most recent studies done as part of Probabilistic Hazard Analyses in 2005, updated in August 2011 and independently confirmed by the Romanian National Institute for Earth Physiscs.

Further on, the provisions to protect the NPP against the DBE provided by the design have been assessed in terms of both key SSCs that are part of the safe shutdown path and operating provisions to prevent reactor core or SFB damage after an eartquake. No gaps have been identified in respect with the design basis and the licensee's process to ensure compliance is considered adequate by CNCAN.

The relevant design and operational provisions to protect the plant against design basis earthquake are summarised as follows.

CANDU reactors are designed for safety with a philosophy to deal with design basis accidents (DBA) and DBE events, in addition to normal reactor operation for power generation, with significant margins. Both diverse and redundant systems are implemented to ensure safe reactor shutdown and fuel integrity with the unique CANDU Two Group and Separation approach as per Safety Design Guides.

The safety-related systems, structures and components (SSCs) are divided into two groups as follows:

- Group 1: PHT, shutdown system one (SDS1), main and auxiliary moderator, steam and feedwater system, emergency core cooling (ECC) system, shutdown cooling (SDC), Local Air Coolers (LACs), Class I, II, III and IV power, and the main control room (MCR).

- Group 2: shutdown system two (SDS2), Containment Structure, Containment Isolation System, Dousing, Air locks, Hydrogen Control, EWS, EPS and the secondary control area (SCA).

DBE is a common mode event, which affects both Group 1 and Group 2. The design approach is to seismically qualify those SSCs (all of Group 2 and some of Group 1 are considered appropriate) necessary to carry out the essential safety functions following a DBE.

The following outlines the reasoning behind seismic qualification of systems that are important to the safety of the plant for DBE:

(1) PHT is seismically qualified so that a LOCA will not be caused by a DBE

(2) SDS1 and SDS2 are seismically qualified so that the shutdown capability is available by two independent means

(3) EPS and EWS systems are seismically qualified so that power and water, respectively, are available to ensure decay heat removal following a DBE

(4) SCA and the indications taken to the SCA are seismically qualified so that adequate monitoring capability is available following a DBE

(5) All subsystems of the Containment System are seismically qualified to ensure that the containment is isolated and secured for radioactive release control

(6) The ECC system is qualified for DBE for PHT inventory make-up and core cooling

(7) The Spent Fuel Bay is seismically qualified to DBE together with the Service Building structure

As per CANDU Safety Design Guides, the separation of Group 1 and Group 2 SSC is implemented in the plant so that failure of any Group 1 Systems Structures and Components (SSCs) would not cause failure to the Group 2 SSCs. As applicable prior to the commissioning the plant, seismic walkdowns in the reactor building, service building and turbine building were performed to ensure that the Group 1 and Group 2 SSCs do not interfere with each other.

The following outlines the justification for the success of the post-DBE operation:

(1) Reactor will be shut down by process parameters trip. Additionally, operator can manually shutdown the reactor from MCR or SCA.

(2) PHT thermosyphoning. PHT thermosyphoning is a proven effective mechanism in transporting the decay heat from the reactor core to the steam generators as demonstrated by analysis and tests of natural circulation and proved through tests during commissioning. Thermosyphoning is ensured by a full PHT with inventory make-up from HPECC water accumulators and/or EWS operation

(3) Steam Generators as heat sink
   - MSSV opening to reject the energy into the environment for decay heat removal is a proven design by station operation

- By design, secondary side water make-up promptly by dousing water inventory in the MSLB scenario and by EWS pump operation using EPS or mobile diesels for the other seismic induced events

(4) The Group 2 SSC, including the seismically qualified fuel design and the Group 1 ECC system, are capable of performing the essential functions required to safely shut down the reactor and cool the fuel following the DBE. The integrity of the fuel is demonstrated by analysis for the DBE or other seismic events. The PHT thermosyphoning using the steam generators as the passive heat sink for the DBE events, is ensured by EWS

(5) The Containment System will perform as designed for containment isolation and contain any radionuclide, for protection of the public from radioactive doses. From design basis events, the LOCA + loss of emergency core cooling (LOECC) event presents the highest potential for fission product release. Safety analysis has shown that, for this limiting event, the public dose limits are not exceeded. The DBE events are significantly less severe transients with fuel failure prevention using the steam generators as the heat sink. The radionuclide release to the public during and after the DBE is well below the public dose limits.

(6) Cernavoda Units 1 and 2 have implemented control panels in the SCA for monitoring of the plant status, and the operators are able to access adequate plant information following the DBE and take appropriate actions to maintain the reactor in the safe shutdown state.

3.1.2 Assessment of the seismic margin

The analyses have been based on the well established methodology and reports elaborated as part of the Seismic PSHA performed in the period 2004-2005 for both Cernavoda NPP Units. The fragility analyses performed as part of these studies, that have been succesfully verified by an IAEA IPSART mission in 2005, have been consequently confirmed and complemented by rigourous plants walkdowns performed in May – July 2011 by a team built-up from plant designer (AECL) engineers and operating organisation engineers. The aim of the walkdowns was to confirm preservation of the original design in term of seismic interaction. The evaluation of seismic margin of Cernavoda NPP was done based on the methodology illustrated in Fig. 3.1.2.

The preliminary seismic margin assessment shows that in comparison with the original design basis eartquake of 0.2g, which has a frequency of 1E-3 events/year, all SSCs which are part of the safe shutdown path after an eartquake would continue to perform their safety function up to 0.4g, which has a frequency of 5E-5events/year. This margin is considered adequate as it complies with the actual safety goals internationally applied for new NPPs.

The potential of Cernavoda NPP units flooding induced by an earthquake exceeding the DBE has been analysed by considering all the failure mechanisms consisting of failure of dams and other hydrological or civil structures collapsing and the tsunamigenic potential of a Black Sea originating earthquake. The results show that the effect of these failure mechanisms has physically no potential for seismically induced flooding of Cernavoda site.

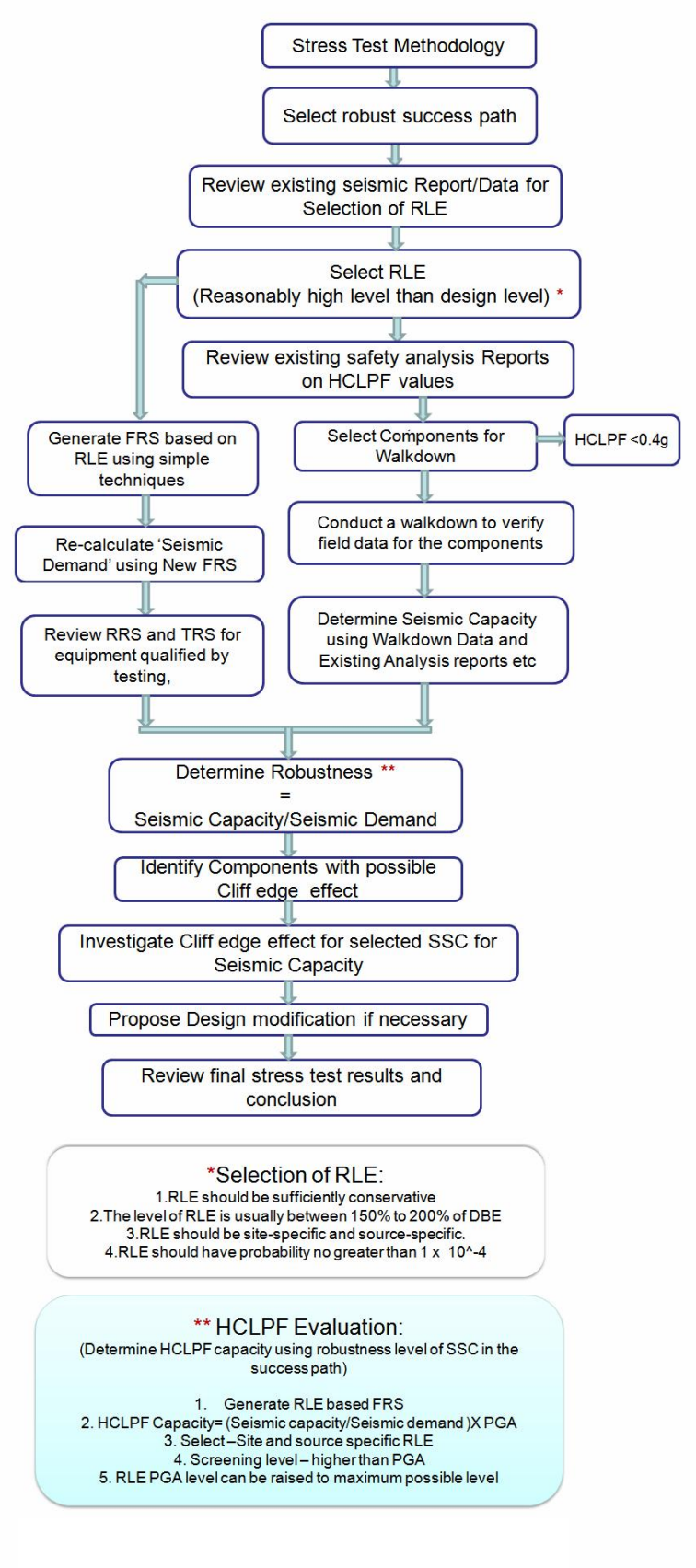

Fig. 3.1.2 Seismic Margin Evaluation Methodology

3.2 Flooding

This section provides the status of Cernavoda NPP design and operation capability to cope with external flooding events as required by the station design.

Cernavoda NPP site is located adjacent to the Danube River that is providing required cooling water flow. The site is 60 km away from the Black Sea coast. The site is bordered on the Northeast by Cismelei Valley and on the Southeast by a bypass channel of Danube-Black Sea Channel (DBSC). Cooling water for the plant is taken from DBSC through a Bypass Channel, Intake Channel and Distribution Basin.

The assessment started with a systematic review of the original analyses done as part of the Cernavoda NPP siting. The sources of flooding have been identified as Danube River, Heavy Rains and combination of these events.

With respect to the Danube river flooding, it has been found that, at the time of the selection of Cernavoda site, it was assumed that two future dams would be built on the Danube River, one upstream of Cernavoda at Calarasi and one downstream at Macin. The supporting studies carried out at that time analysed the different regimes to determine the maximum (flood) water level of the dam accumulation lake, and the extreme case of the upstream dam breaking while the downstream dam holds. The elevation of +16.00 mBSL for Cernavoda NPP site was selected with due consideration of this extreme postulated failure mode.

It was later decided not to build the two dams envisaged at the time Cernavoda NPP site was selected; however the Cernavoda site platform elevation of +16.00 mBSL was not changed.

Based on the original study, since the dams were not built, the maximum design water level for the return period of 1 in 10000 years for Cernavoda NPP is +14.13 mBSL.

In order to confirm the validity of the original design studies in time, a new study has been done in July 2011, using the modern tool of Digital Topographic Model (DTM) to create the external flooding hazard map for Cernavoda NPP site and adjacent area.

The DTM used as input LIDAR scan data of the Cernavoda NPP site and surrounding territory. Subsequently, one specific hydraulic model was developed based on methodology used in the European project “Danube Flood Risk - Stakeholder Oriented Flood Risk Assessment for the Danube Floodplains” within the South East Europe Transnational Cooperation Program (SEE Program).

The results of this study confirmed the validity in time of the original design topographic measurements and concluded that, in comparison with the DBF corresponding to +14.13 mBSL, taking into account also the ground floor elevation for the plant buildings, a margin of +2.17 m exists. The adequacy of this margin is supported by the calculations showing that the Danube flow required to challenge this margin is not physically achievable.

The DTM has been used also as a tool to evaluate the adequacy of the existing plant pluvial system to cope with heavy rain falls. In case of rainfall rate exceeding the

capacity of the drainage system, the runoff is by overland flow to the drainage channel or the DBSC. A calculation for these scenarios demonstrates that the maximum height of water accumulated on the site is less than the ground floor elevation for rainfall rate about 10 times higher than the design maximum rainfall rate; therefore this will not result in flooding the buildings on the site. These results have been verified by plant engineers using local topographic measurements. This margin is considered as being adequate and no additional measures are required to protect the plant against external flooding.

3.3 Station Blackout and Loss of Ultimate Heat Sink

3.3.1 Electrical Power Systems for Cernavoda NPP

The power supply sources for the Cernavoda NPP Units are as follows:

- Redundant offsite sources, which provide electrical power required during startup and shutdown of the unit and can also supply power during normal operating conditions;
- The turbine generator (onsite), which provides electrical power required during normal operation;
- On site standby sources which provide the electrical power required in case of loss of the normal power supply: Class III Standby Diesel Generator (SDG), batteries, Emergency Diesel–generator (EPS, Emergency Power Supply).

The onsite power Distribution system is divided into redundant load groups (EVEN and ODD) so that the loss of any one group does not prevent the minimum safety function from being performed. Furthermore the onsite station service power supplies are classified as four classes that range from uninterruptible power to that which can be interrupted with limited and acceptable consequences, provided as follows:

- **Class I**: Uninterruptible direct current (dc) supplies for essential auxiliaries, control, protection and safety equipment. Batteries provide uninterruptible power for 8 hours.
- **Class II**: Uninterruptible alternating current (ac) supplies for essential auxiliaries, control, protection and safety equipment. Uninterruptible power is provided by batteries, through inverters or by Class III during unavailability of the inverters.
- **Class III**: Power supplies to the safety-related systems. Normal supply of class III distribution system is from service transformers, and it is backed-up by the standby diesel generators with 100% redundancy. Standby electrical diesel can provide power to essential loads to ensure an orderly shutdown. The interruption of power is of a short duration (maximum 180 sec), which is necessary for start-up and loading of the standby diesel generators, in case of loss of normal supply from the turbine-generator and from the grid. Also, class III is the charging source to the class I batteries and back-up supply to Class II loads.
- **Class IV**: Normal alternating current supplies to auxiliaries and equipment, which can tolerate long duration interruptions without affecting nuclear safety, personnel or equipment safety. A complete loss or a loss of either odd or even

division of Class IV power will initiate a reactor shutdown. Loss of offsite power is a design basis event which does not pose any threat for the plant.

EPS: A completely independent, seismically qualified, emergency power supply (EPS) system designed to 100% redundancy and separation requirements is also provided to cope with common mode events, ensuring the safety functions are maintained. This system is intended for back-up supply supporting essential safety functions when all the others electrical supplies are unavailable or when the main control room is uninhabitable.

Mobile diesel generators: Following the Fukushima accident, Cernavoda NPP procured two mobile diesel generators (one for each unit), to provide power if the EPS is not available. The capacity of each mobile diesel generator is of approximately 1 MW, equivalent to that provided by the design non-mobile EPS diesel generators. The mobile diesel generators have autonomy of 6 hours at full load without external support. The available fuels oil on site will ensure more than 3 days of operation without external support, considering only the EPS stored fuel oil.

3.3.2 Heat Sinks for Cernavoda NPP

The heat from the nuclear fuel is transferred to the heavy water in the primary heat transport system. The heat from the heavy water could be transferred to either steam generator using pumps or thermosyphoning or to shutdown cooling (SDC) system using PHTS / system pumps.

- Steam generators produce steam whose energy can be transferred to the turbine, can be dissipated at the condenser, or can be dissipated to the atmosphere via steam safety valves. The steam generators are supplied with light water using feedwater pumps from feedwater system via condensate system during normal operation, or using auxiliary feedwater pump with water from deaerator or condensate storage tank / emergency water tanks for decay heat removal. In case of emergency, steam generators can be supplied gravitationally with water from the dousing tank using boiler make-up water system or can be supplied with water from intake using emergency water supply (EWS) system pumps.
- Shutdown cooling system transfers the heat to recirculating cooling water (RCW) system through its heat exchangers. RCW system transfer the heat to the raw service water (RSW) system through its heat exchangers and the heat is dissipated into the Danube River.

The primary ultimate heat sink is based on decay power heat removal using forced cooldown circulation in PHT system. The heat transfer path consists of the Shut-Down Cooling (SDC), Recirculating Cooling Water (RCW) and Raw Service Water (RSW) systems. The water for RSW system is the Danube River (water taken from the suction bay). After reactor shutdown, the SDC system represents the main system of the primary ultimate heat sink.

The alternate heat sink is used only if the primary heat sink is not available (forced circulation through the core is lost). During the use of the alternate heat sink chains, the difference in fluid density between the steam generator cold leg and hot leg

ensures continuous flow circulation around the PHT circuit. The heat transferred from the SGs primary side will heat up the secondary side cooling water. During the thermosyphoning process, the water in the steam generators secondary side circuits will be at the boiling point (100^{o}C) at atmospheric conditions. The SG's secondary side inventory is transformed to steam, which is released to atmosphere through the ASDVs or MSSVs.

When the alternate heat sink is used, two redundant and different paths can be used to provide cooling water to the steam generators secondary side.

a) Demineralized water provided by "feedwater train" (alternate heat sink)

The first path through which water can be provided to steam generators secondary side is represented by the "feedwater train". The demineralized water is provided by the Water Treatment Plant (WTP). The process in the WTP requires off site electrical power being available. In order to have the WTP supplied with water, the CCW system (class IV electric power) or Back-up Cooling Water system (class III electric power) have to be available. The demineralized water produced in the WTP is transferred to Emergency Water Tanks. The demineralized water from the emergency demineralized water tanks is transferred to Condensate Storage Tank using the class III demineralized-water transfer pumps. The water from the condensate storage tank flows gravitationally to Deaerator tank once the isolation valves are open. Also, the demineralized water can be provided to Deaerator from Condenser hot wells using the Auxiliary Condensate Extraction pump (class III electric power).

The heat from primary side is transferred to SGs secondary side. Finally, part of the water will be transformed to steam in the SGs secondary side. The steam will be released to atmosphere using the ASDVs and MSSVs. In case that CCW system is available (class IV available), the CSDVs and the condenser can be used to condense the steam from the SGs.

The demineralized water from Deaerator is transferred to secondary side of the SGs using the AFW pump (class III power, EVEN bus). The level in the SGs is controlled by level control valves. Separate parallel lines are provided which can be used in case that the main level control valves are not available. The AFW pump cooling is normally provided by RCW system. In case that the AFW pump cooling is lost, the back-up cooling flow can be provided by water inventory from the condensate storage tank. The water is supplied gravitationally to AFW pump from Condensate Storage Tank or from Emergency Water Storage tanks using the demineralized-water class III pumps.

The AFW can provide to SGs a flow larger than the flow required for cooldown purposes after reactor trip, ensuring that a continuous heat sink is available, at least, as long as the AFW pump is running.

b) Water provided by BMW system / EWS system (alternate ultimate heat sink)

The second path can be used to provide water to SGs secondary side is represented by the BMW system (using the demineralized-water inventory from the dousing tank) or by EWS system.

Water supply from BMW (dousing tank inventory)

In case that AFW cannot provide water to SGs secondary side, the alternate source of

demineralized-water that can be provided to SGs secondary side is represented by the water inventory available from the dousing tank. The water will flow gravitationally to the steam generators secondary side once the pneumatic isolating valves are open and the steam generators are depressurized to atmospheric pressure. The BMW pneumatic isolating valves can be operated manually from SCA or manually from field in order to control the SGs level. As long as the flow path will provide water to steam generators, the thermosyphoning process will ensure adequate decay power removal.

Continuous water flow to SGs by EWS

The large dousing tank inventory will ensure, for at least 23 hours, water supply to SGs secondary side. As per plant design, finally the water to SGs secondary side will be directly provided from suction bay. The water is taken from the suction bay by 2 x 100% pumps (for each unit) and is injected in the steam generators secondary side. As long as cooled water will be provided to SGs, the fluid density difference between the hot leg and the cold leg in the SGs will promote the natural circulation (thermosyphoning) through the PHT system. Part of the water provided to SGs secondary side will be released to atmosphere (as steam) through open MSSVs. The electrical power supply for the MSSVs is from class I or from EPS or from mobile diesel generators.

Each EWS pump is powered by any EPS diesel generator (as per design) and the mobile diesels. The intake for the EWS pumps from suction bay is separated from the intake for the RSW pumps: a separate suction pit is provided by design for EWS pumps.

As long as the EWS will provide water to steam generators, the thermosyphoning process will ensure adequate decay power removal.

3.3.3 Accident scenarios involving loss of electrical power and loss of ultimate heat sink

In conformance with the stress test specifications, the licensee has analysed the following scenarios:

- loss of offsite power;
- station blackout (SBO);
- loss of primary heat sink;
- loss of both primary and alternate ultimate heat sinks);
- loss of primary ultimate heat sink with station blackout.

Loss of offsite power is a design basis event which does not pose any threat for the plant. The plant can operate at reduced power levels in the islanding mode. In the case of reactor or turbine generator trip after loss of offsite power, the electrical loads will not be supplied from the plant generator anymore. This event is called loss of Class IV electrical power and is part of the design basis. The plant design ensures reactor shutdown and cooldown under these conditions. The reactor shutdown is ensured by any of the two redundant shutdown systems. The cooldown is ensured by the primary or the alternate ultimate heat sinks (as defined in section 3.3.2).

In the case of SBO, the plant shutdown is ensured automatically either by SDS#1 or SDS#2 on the process trip parameters. Both shutdown systems are designed to fail safe, in such manner that if they are not supplied with electrical power the systems will perform their design function, respectively shutting down the reactor. In this case the cooling of the reactor will be ensured by thermosyphoning in the primary coolant system. The heat will be transferred to steam generators and discharged to atmosphere via steam discharge valves. The necessary water to the steam generators will be gravitationally fed from the dousing tank inventory through the boiler make-up water.

The inventory from the dousing tank ensures cooling of the reactor for at least 23 hours, even under the assumption of no operator action to control dousing tank water supply flow. This time is sufficient to supply electrical power from the mobile diesel generators to the emergency water pumps. The field tests demonstrate that it takes up to 3 hours to connect mobile diesel generators to the emergency water pump motors. These pumps will feed the steam generators with water from the intake for an indefinite period of time.

Containment isolation valves will fail close either on loss of their electrical power supply or loss of instrument air. So containment function considering SBO is not affected.

The monitoring of the critical safety parameters will be ensured using electrical power from batteries. The batteries can continuously supply power for 8 hours, during which time the mobile diesel generators can be connected.

Loss of the primary ultimate heat sink means loss of service water systems which was considered within the design basis of the plant. In this case the shutdown systems can be manually activated from the control room. If they are not manually activated automatic shutdown of the plant is ensured by process parameters as designed (i.e. moderator temperature). The heat sink is ensured in the same way as mentioned in the case of SBO except that the second set of diesel generators (EPS diesels) are available and can continue supplying power to emergency water pumps (the mobile diesel generators are considered as back-up).

Containment and monitoring of critical safety parameters will not be impaired in this event.

Loss of primary ultimate heat sink and loss of alternate ultimate heat sink means loss of service water and emergency water supply systems. In this case the reactor shutdown will be similar to the case of loss of primary ultimate heat sink, either manually or automatically. Reactor cooling, in the first phase will be ensured similar with SBO case or loss of primary ultimate heat sink scenario. The difference is that emergency water supply is unavailable and after the 23 hours when the steam generators are supplied from the dousing tank inventory through boiler make up water system there is the possibility to connect manually the fire water truck to emergency water supply system piping. This will provide water to SGs secondary side from fire water tanks. The fire water tanks can be supplied with water from distribution bay or from the two existing deep ground wells, which are not affected by dry season or low Danube level.

Containment and monitoring of critical safety parameters will not be impaired in this event.

After a loss of the primary ultimate heat sink followed by the SBO, the plant response and event sequence will be similar to the case of station blackout. In this case the reactor will be shutdown manually or automatically by one of the two shutdown system. Heat sink is provided by thermosyphoning in the primary coolant system heating being transfer to steam generators and the steam being release in the atmosphere via steam discharge valves. Water to the steam generators is provided from boiler makeup water system and emergency water supply system. As it was mentioned above boiler makeup water system is using water from the dousing tank to feed gravitationally the steam generators.

Meanwhile, the mobile diesel generators can be started to power emergency water supply pumps that will provide the necessary water to steam generators indefinitely. Containment and monitoring of safety parameters are ensured in the same manner as in the case of SBO.

3.4 Severe Accident Management

3.4.1 Design features and Accident management measures for the prevention and mitigation of core damage

The CANDU-6 reactor has both preventative and mitigating features to ensure a robust design against severe accidents. It has inherent and engineered provisions to prevent core damage, terminate progression of core damage, retain the core within the calandria vessel, localize core debris within the calandria vault, maintain containment integrity, and minimize off site releases.

Progression of accidents in CANDU reactors from those involving little or no fuel damage to significant core damage and possibly core disassembly is strongly influenced by the unique aspects of the reactor design. In particular, the low pressure heavy water moderator in the calandria vessel surrounding the pressure tubes and the large volume of light water in the calandria vault which, in turn, surrounds the calandria vessel, provide a passive heat sink capability which will provide significant time delays in the progression of a severe accident sequence. Such delays are of benefit in that they provide decision and action time for accident mitigation and management measures to be taken.

The preliminary stress test report submitted by Cernavoda NPP distinguishes between two categories of severe accidents:

- Severe accidents within the design basis constitute those accidents in which the core geometry is preserved (fuel remains inside intact pressure tubes) and the core coolability is maintained. CANDU severe accidents, such as “loss of primary coolant with a failure to makeup the coolant with emergency core coolant injection” are analyzed as part of the design basis accidents. In this case, the moderator can remove heat from the reactor preventing fuel melting and maintaining the integrity of the fuel channels. This type of severe accidents within design basis is called “Limited core damage accident (LCDA)”. In LCD accidents, the fuel materials remain within the heat transport system (PHT) boundaries and the core geometry is maintained as long as the moderator system is available. Therefore, a severe core damage accident is possible only with additional assumed

failures - i.e. not only a loss of PHT coolant with a loss of emergency core cooling (ECC) system, but also a loss of moderator as a heat sink. This means that in a CANDU reactor, not all severe accidents may result in severe core damage. In CANDU reactors, there are a number of discrete plant damage states that can result in a limited degree of fuel damage without progressing to severe core damage. Examples are events that affect fuel in a single channel or which rely on moderator cooling for long-term heat removal. Events involving limited fuel damage would not require the use of Severe Accident Management Guidelines, as such events are already anticipated and addressed by the Abnormal Plant Operating Procedures.

- Severe core damage accidents beyond the design basis are those severe accidents in which a large number of fuel channels fail and collapse to the bottom of the calandria. A necessary requirement for severe core damage to occur is that fuel channels not only be voided of coolant due to loss of PHT cooling and failure of ECC system, but they must lose cooling from outside due to loss of moderator (loss of moderator inventory or loss of moderator cooling). This type of severe accidents beyond design basis is called “Severe Core Damage Accident (SCDA)” and the response to SCDAs is based on the Severe Accident Management Guidelines.

A prerequisite for the majority of events to progress to conditions leading to severe core damage is a loss of heat transport system coolant coupled with failure of the emergency core cooling system to inject cold water into the heat transport system (in accident analysis, the sequence is LOCA + LOECC). The loss of coolant may be due either to an initiating pipe break or a consequential induced failure of the heat transport system boundary resulting, for example, from events involving a loss of flow or loss of heat sink.

The LOCA + LOECC sequence is part of the design basis accident analyses for CANDU reactors. These analyses have demonstrated that progression of the event to core disassembly is effectively prevented by the passive rejection of heat from the fuel channels to the moderator fluid. For such scenarios, the heavy water moderator is credited as an effective heat sink.

The CANDU-6 design has inherent design robustness against core damage (i.e., no severe core damage occurs at high pressure, high pressure melt and direct containment heating are precluded, reactivity induced accidents are precluded by the two fast, highly reliable and diverse shutdown systems). The large water inventories surrounding the fuel and the entire core act as a heat sink to remove the decay heat after reactor shutdown, even if all engineered heat removal systems fail, and allow for sufficient time for the implementation of severe accident management actions. Since heat removal is through passive boil off, there is no need for operation of any valves or pumps.

The potential for re-criticality under severe accident conditions was evaluated for the reactor, the spent fuel bay and the fresh fuel storage room and it was concluded that this is not a concern for the CANDU-6 design. Criticality of CANDU fuel bundles in ordinary (light) water is not possible, removing a concern in severe accidents. Injecting light water into the core is part of the severe accident management. In fact, the CANDU core geometry is near the optimum reactivity so that any rearrangement

of the core under severe accident conditions ensures shutdown. The Cernavoda Unit 1 and 2 NPPs spent fuel bays use light water to cool the spent fuel and provide shielding. The 37-element natural-uranium fuel bundles in an infinite array in a light-water medium have been demonstrated to remain subcritical.

As regards the mitigation strategy, based on specific SAMGs developed for this purpose, a severe core damage accident can be arrested by re-filling/cooling the calandria vessel (maintaining in-vessel cooling) or by re-flooding the calandria vault and keeping it flooded thereafter. The core debris would still be contained within the calandria vessel as long as it remains cooled on the outside by the calandria vault water. However, as a next level of defence, ex-vessel phenomena have been considered and design provisions have been reassessed for use in SAMGs aimed at protecting the containment function. The protection of the confinement function is addressed in the following section.

3.4.2 Design features and Accident management measures for the protection of containment integrity

The containment building provides the fundamental barrier protecting the public in the unlikely event of a severe accident by limiting the radioactive releases to the environment. Protection of the confinement function requires limiting the interior temperature and pressure in the containment. The severe accident analyses for a generic CANDU-6 design have been reviewed to identify scenarios that could pose a challenge to the containment integrity. The main conclusions of this review are summarised as follows.

High pressure core melt ejection scenarios do not represent a containment challenge for a CANDU reactor. Primary heat transport system depressurisation (either directly through a break in the system or indirectly via automatic depressurisation of the secondary side by the opening of the main steam safety valves) occurs well before the potential formation of molten corium conditions. Even if the engineered depressurisation mechanisms would fail, fuel overheating will cause a limited number of fuel channels to fail, depressurizing the PHT. Thus, the fuel channels of the CANDU-6 reactor act as ‘pressure relief fuses’ should an accident evolve and produce high PHT pressure and elevated PHT coolant temperature.

Containment bypass through ruptured steam generator tubes is not possible during a severe accident in a CANDU reactor. In CANDU severe accident scenarios, the pressure tube is expected to rupture well before a steam generator tube might fail on PHT overpressure. The PHT relief valves in CANDU-6 will limit the pressures in the heat transport system to below those at which the steam generator tubes would rupture. Thus consequential steam generator tube ruptures leading to containment bypass are precluded.

Steam explosions (energetic fuel-coolant interaction) are considered unlikely during CANDU severe accident progression because of the core geometry that dictates the mode by which the hot debris materials are brought into contact with water.

The main challenges identified are due to hydrogen build-up, containment slow over-pressurisation and molten core – concrete interaction (MCCI).

The hydrogen control strategy employed in Cernavoda Unit 1 relies on the reduction of hydrogen volumetric concentration by inerting the containment atmosphere so that in the longer term the containment integrity is not threatened. Cernavoda 2 is additionally equipped with igniters to deliberately ignite and burn the hydrogen as soon as it reaches flammable concentration, thus avoiding its detonation at higher concentrations. The containment structures are designed to provide natural circulation mixing and the local air coolers' fans, if available, promote forced air circulation for hydrogen mixing to avoid pockets of locally high concentrations. Specific SAMGs have been developed for hydrogen control in severe accident situations, considering situations both with and without containment venting. In addition, installation of passive autocatalytic recombiners will be implemented for both units, to further increase the safety margins and to ensure a hydrogen control feature independent of the availability of electrical power supply.

Slow over-pressurization may occur due to steam generation by decay heating as a result of a loss of the heat sinks. Non-condensable gases, contributing to the containment pressurization, can also be generated by thermal–chemical interactions of hot core materials. Several sources of steam release in the containment during an unmitigated severe accident have been identified and a specific SAMG has been developed to address them, including venting strategies. The existing design features that protect the containment integrity against over-pressurization are the large containment volume and passive condensation on reactor building structures and the local air coolers and dousing spray. In addition to the existing systems and provisions to reduce containment pressure, the installation of an emergency filtered venting system is being contracted for both Cernavoda NPP units.

Prevention of basemat melt-through is based on a SAMG aimed at injecting water into the containment for cooling the core debris and limiting the molten core – concrete interaction. Preferred and alternate strategies have been identified, taking account of the availability of the systems that can be used for water injection and of the expected conditions resulting from various severe accident scenarios. Based on a conservative generic analysis for a CANDU-6 design, if the ex-vessel corium is not submerged in water and cooled, MCCI does not occur until at least two (2) days after the accident initiation, with gross concrete ablation estimated to occur at least four (4) days after accident initiation. This would provide sufficient time for the implementation of mitigation actions to bring the accident into a controlled and stable state. Re-criticality of core debris is not a concern for CANDU reactors.

3.4.3 Accident management measures for coping with loss of cooling to spent fuel pool

Sustained loss of fuel bay cooling represents an unlikely emergency situation, which may be induced by common mode events, like earthquake causing sustained loss of AC power. In the case of a prolonged loss of spent fuel bay cooling, make-up water is required to prevent uncovery of the spent fuel and potential hydrogen generation. Based on calculations performed, there is sufficient time available to establish a source of 1 kg/s water make-up into the spent fuel bay to keep the spent fuel bundles submerged.

Given the large time frame available (15 days until first fuel bundles become uncovered), the loss of Spent Fuel Bay cooling event can be managed successfully following a specific abnormal plant operating procedure (APOP G04).

No adverse consequence is expected as a result of the loss of Spent Fuel Bay cooling. No damage to the spent fuel is expected to occur. Hydrogen production in the area of spent fuel is not credible. The fuel will remain adequately cooled and no personnel radiation doses exceeding administrative limits are expected to occur. There is no possibility of re-criticality of the CANDU spent fuel whether in air or in light water.

3.4.4 General description of the accident prevention and management strategy and procedures

Specific station procedures are in place at Cernavoda NPP Units, that have been designed to mitigate the effects of initiating events and direct the operator to bring the plant to a safe state that usually is defined as cold shut down state. The response to anticipated operational occurrences and to accidents is controlled through a hierarchical system of station procedures as follows:

- Operating Manuals and Alarm Response Manuals – include procedures used by the plant operation staff during routine operation of the nuclear power plant and its auxiliaries and also information regarding abnormal operation and the alarm functions associated with the plant systems (set points, probable cause, operator response, etc.);
- Impairment Manual - includes actions to be taken by the operator in case that operation is close to or getting outside the specified limits of the safe operating envelope;
- Abnormal Plant Operating Procedures (also known as Emergency Operating Procedures (EOPs)) - which direct the operator during accident conditions (for design basis and design extension conditions) and are designed to restore the plant to a safe condition and ensure protection of the health and safety of the plant personnel and of the general public;
- Severe Accident Management Guidelines – which direct the operators and technical support gropus during severe accident conditions and are designed to minimize the severe accident consequences and to bring the plant in a stable end state.
- Emergency Response Operating Manual - includes operator's actions in case of radiological, medical and chemical incidents, fire events, extreme weather conditions, spent fuel transfer/ transport incidents, spent fuel bays and spent fuel dry storage facility incidents, loss of Main Control Room; this manual provide the necessary criteria to classify the emergency and easy access to each of the sections containing the necessary measures to be taken for the different types of emergencies, with the overall process being governed by the on-site Emergency Plan.

Administrative procedures are in place to describe responsibilities for the operating crews when dealing with plant transients and accidents, aiming to obtain consistency

in crew performance. These documents instruct the licensed operating personnel to recognise any abnormal event and mitigate its consequences.

Abnormal Plant Operating Procedures (APOPs), provided for response to design basis accidents and design extension conditions, include event-based type of procedures, as well as symptom based procedures. Two new APOPs, for responding to Station Blackout and Abnormal Spent Fuel Bays Cooling Conditions, have been issued as part of the response to lessons learned from the Fukushima Daiichi accident.

In addition, Cernavoda NPP has implemented a set of Severe Accident Management Guidelines (SAMGs), to cope with situations in which the response based on APOPs is ineffective and the accident conditions progress to severe core damage. The objectives of the SAMGs are:

- to terminate core damage progression;
- to maintain the capability of containment as long as possible;
- to minimize on-site and off-site releases.

The SAMGs for Cernavoda NPP have been developed based on the generic CANDU Owners Group (COG) SAMGs for a CANDU-6 type of plant. In developing the generic SAMGs, COG adopted the Westinghouse Owners Group (WOG) approach, with the necessary technical modifications suitable for implementation in CANDU plants, based on extensive CANDU specific severe accident analysis and research.

Preparation of plant-specific SAMGs was done by customisation of the generic COG documentation package for Cernavoda NPP, removing extraneous information not applicable to the station, incorporating station-specific details and information and making any other adjustments required to address unique aspects of the plant design and/or operation. A total number of 48 documents were prepared (SAG's, SCG's, CA's, SACRG's, SAEG's, DCF, SCST and their associated background documents). Also, another 40 Enabling Instructions were prepared in order to support the line-ups for each strategy presented in the above mentioned documents.

The interface between APOPs and SAMGs was established by introducing the severe accident entry conditions into the APOPs. The interface with the Emergency Plans was provided by making revisions to the existing EPP documentation, to reflect the new responsibilities and requirements arising from the implementation of the SAMGs. Also, all categories of plant personnel involved in the emergency response organisation were trained for SAMG use, and drills are currently being incorporated in the overall Emergency Response Training Program.

The SAMGs have been developed based on the existing systems and equipment capabilities. A limited and focused set of information requirements was defined to support SAMG diagnostics and evaluations. The primary source is from plant instrumentation, supplemented by additional measurements and data expected to be available through emergency response procedures and Computational Aids where appropriate. It is recognised that the design requirements for most plant instrumentation are based on normal operation or accident conditions less severe than expected when a SAMG is entered. The preliminary stress test report presents the availability and suitability of instrumentation to support SAMGs implementation.

The potential for cliff-edge effects has been reviewed based on the severe accident analysis for a generic CANDU-6 design. The preliminary stress test report submitted by the licensee provides information on the cliff-edge effects identified and on the existing safety margins. The SAMGs take account of the time periods available before a cliff-edge effect would occur in an unmitigated accident scenario and include measures for the prevention of cliff-edge effects.

The SAMGs cover also the supply of electrical power and compressed air to equipment credited for prevention and mitigation of core damage, for protecting containment integrity in severe accidents and for the prevention and mitigation of loss of cooling to spent fuel pool.

4. GENERAL INFORMATION ON THE ORGANISATION OF EMERGENCY RESPONSE

4.1 Organisation of the on-site emergency response

The preliminary stress test report submitted by the licensee provided extensive information on the organisation of the response to emergencies, covering all the aspects outlined in the stress test specifications.

An On-Site Emergency Plan is in place to adequately respond to any emergency, ranging from the lowest incident classification ("Alert" level) to the highest classification ("General Emergency") that requires the evacuation of all non-essential personnel on-site. Off-site emergency response is under the responsibility of the local, county and national authorities.

The human resources appointed for emergency response activities has been assessed and identified. 412 persons were specifically trained for the emergency response procedures:

- operation personnel;
- emergency management and technical support personnel;
- assembly area responsible persons;
- medical personnel;
- professional civil fire fighters.

The licensee has included in the preliminary stress test report a conservative evaluation of the on-site vital areas habitability and accessibility, based on selected severe accident scenarios. The estimation of the doses to the operating staff was performed for a period of 7 days, assuming normal 12h shifts. The projected doses to the workers are below the values considered acceptable at international level for justifying emergency actions that reduce the risk for public exposure. For the Main Control Room personnel, the alternative operating area is the Secondary Control Area (SCA), able to control and command all the safety systems. The SCA is seismically qualified and is continuously monitored by a qualified person trained to safe shut down the unit, keep the heat sinks available, alarm the on-site personnel, activate the emergency organization and notify public authorities.

A comprehensive emergency response program and provisions for responding to emergencies, including severe accidents, are in place, covering:

- Organizations and human resources;
- Emergency procedures, training and drills;
- Emergency facilities and equipment;
- Fuel supplies for diesel generators;
- Emergency monitoring and sampling;
- Dose calculations, personnel protection and evacuation;
- Communication provisions and equipment;
- Notifications to public authorities for off-site response.

All the provisions of the emergency program, including the associated documentation, have been approved by station management and the regulatory body and are subjected to periodic testing through emergency exercises.

Emergency response personnel are provided with all necessary provisions to respond to the emergencies, from the initial response phase to post-accident recovery phase. Plant staff will make use of existing equipment, including innovative uses of plant systems and equipment. Where necessary, provisions have been made to bring on site mobile equipment such portable pumps, fire trucks, etc., to allow mitigation of the accident when existing equipment are not available. Two mobile diesel generators have been provided in a secure location on-site for hook-up to provide power for the unlikely situations where all the other electrical power supplies for the plant are lost.

The On-Site Emergency Control Centre is the headquarters for emergency response personnel to deal with the emergencies. It is appropriately equipped with the required instrumentation to assess plant status, and has filtered ventilation system, diesel power generator, food and water provisions to ensure availability for long term operation periods.

The public authorities will assist with any other needs, such as clearing roads, providing fuel, transportation of key emergency response personnel, food and other necessities, etc. A review of the national (off-site) emergency response strategy is currently being performed, with the aim of incorporating lessons learned from the Fukushima accident.

4.2 Organisation of the off-site emergency response

According to the Romanian legislation, the National System for the Management of Emergencies is composed of three types of structures:

- the decisional structure – the committees for emergencies;
- the executive structure – the inspectorates for emergencies;
- the operational structure – the operative centres for emergencies.

All the decisional, executive and operational structures are established on three levels: national, county and local.

The National Committee for Emergency Situations (CNSU) represents the decisional structure at national level. The CNSU is set-up under the co-ordination of the Prime Minister and managed by the Minister of Interior and Administrative Reform (MIRA). All the ministerial, county and local committees are subordinated to CNSU. The County/Local Committees for Emergencies are directed by the county Prefect / local mayor.

The General Inspectorate for Emergency Situations (IGSU), a specialised organisation of MIRA, is established as an executive structure at national level. IGSU has the responsibility of permanent co-ordination of the prevention and management of emergency situations, at national level. At county level, there are established County Inspectorates for Emergencies, acting as public professional emergency services.

Inside each Inspectorate for Emergency Situations an Operative Centre for Emergencies is set-up, with permanent activity, ready to activate the emergency

organisation in case of an accidental event. These Operative Centres for Emergencies are receiving notifications for all types of emergencies, including radiation events.

Also, the responsible organisations at national level are operating such Operative Centres for Emergencies, in accordance with the legal provisions in their field of activity. The National Operative Centre of IGSU represents the operational structure, at national level.

In order to fulfil the legal responsibilities in case of a nuclear accident or radiological emergency, CNCAN has its own Emergency Response Centre (ERC), as part of the National System for the Management of Emergencies. CNCAN – ERC is the national contact point in relation to any type of radiation emergency. As part of the National System, CNCAN-ERC is communicating with IGSU Operative Centre and with other operative centres of public authorities.

By law, the Ministry of Interior and Administrative Reform (MIRA) is responsible for the management of nuclear and radiological emergencies, IGSU and CNCAN being the national competent authorities in case of nuclear accident or radiological emergency. At local level, the intervention is coordinated by the Local Committees for Emergencies and performed by the Local Response Forces. When the emergency situation cannot be solved by the local authorities, the national level (CNSU and IGSU) is activated, in order to support the local intervention. Written agreements and protocols are in place between the responsible organizations, at local and central level, for common activities and exchange of information in emergency situations.

The response organisations have the following responsibilities:

- to elaborate and revise to date an adequate emergency plan;
- to assure by means of laws, Governmental Ordinance, decrees, the legal basis for protection of the population, environment and property, medical care, financial compensations, etc. in emergency situations;
- to establish and maintain a proper structure of the intervention sources able to: advice on nuclear safety and radiation protection, sample and analyse samples, keep in contact with police, army and fire fighting forces, keep contact and receive advice from water management bodies, agriculture produce control bodies, medical services, meteorological forecast facilities.
- to organise and maintain an emergency co-ordination centre equipped with technical means for the expertise of the emergency and sufficient communication means;
- to organise exercises and drills, to maintain the level of personnel training and equipment availability for emergency situations;
- to establish levels for the triggering of the emergency in case of transboundary emergencies.

5. CONCLUSIONS

The licensee has performed a safety review that adequately follows the stress test methodology and has covered in their preliminary report all the aspects required for consideration in the stress test specifications.

The preliminary stress test report submitted by the licensee have provided analyses of all the events and combinations of events required by the stress test specifications, including an assessment of the potential for cliff edge effects and the time available for operator actions.

Specific emergency operating procedures have been developed and implemented to cope with Station Blackout and Loss of Spent Fuel Pool Cooling events. Mobile diesel generators have been procured, are available on site and have been tested to enhance protection against SBO scenarios. Station response to a loss of Primary Ultimate Heat Sink and SBO - combined event does not rely on any off-site equipment for the primary response, all the necessary equipment and resources being available on site and sufficient for coping with a prolonged SBO. For the longer term recovery phase, efforts from the "Transelectrica" National Power-Transport Company will combine with SNN efforts in order to restore off-site power supply.

The preliminary stress test report submitted by the licensee for Cernavoda NPP provided comprehensive information on the inherent design features and engineered systems credited in the prevention and mitigation of severe accident scenarios, on the availability and performance of the heat transfer paths and on the various severe accident management strategies employed. The information provided in the report covered both the analysis of unmitigated severe accident scenarios and the mitigation strategies addressed by the plant specific SAMGs. The claims made in the report are supported by a vast set of references, most of them relating to severe accident analyses and accident management guidelines developed by COG based on more than 30 years of research.

After the Fukushima accident, corrective actions have been developed and implemented to consider the lessons learned from this event. The Emergency Plan and Procedures, Conventions, Protocols and Contracts in place have been reassessed and revised to better accommodate emergency response to severe accidents coincident with natural disasters. Special attention has been paid to the communication systems where actions have been taken, together with National Special Communication Services, to supplement and improve the actual communication systems in place.

A review of the national (off-site) emergency response strategy is currently being performed, with the aim of incorporating lessons learned from the Fukushima accident.

The preliminary regulatory reviews performed to date have focused on verification of the completeness and quality of the stress test report and of the supporting analyses.

In addition, a set of preliminary inspections have been performed by CNCAN staff in support of the review of the licensee's stress test report, aimed at verifying the quality of the process implemented by the licensee in the development of plant specific

SAMGs, training records from training in the implementation of the SAMGs, the currency and availability of emergency operation procedures at the points of use, the procedures for connecting the mobile diesel generators and the related test reports, the procedures for injecting fire water into EWS, etc.

CNCAN noted that a significant effort has been made by the licensee to respond to the lessons learned from the Fukushima accident in a timely manner. Confirmatory assessments have been conducted in response to both WANO SOER and the stress tests. Potential design improvements have been identified and are considered for implementation to further enhance the existing safety margins and reduce the risk from severe accidents.

CNCAN requested the licensees to provide further information on the survivability of key instrumentation in beyond design basis accident conditions and a list of proposed design improvements along with the final stress test report.

No concerns have been raised from the preliminary regulatory review. CNCAN is confident that all the clarifications required will be adequately addressed in the final stress test report submitted by the licensee. Further in-depth reviews and inspections will be performed by CNCAN throughout the development and after the submission of the final stress test report.

The conclusion of the preliminary review conducted by CNCAN is that the risk to the public from beyond design basis accidents at Cernavoda NPPs is low and is kept under control.

LIST OF ACRONYMS

AFW	Auxiliary Feed-Water (system)
APOP	Abnormal Plant Operating Procedure
ASDV	Atmospheric Steam Discharge Valve
BCW	Back-up Cooling Water (system)
BDBA	Beyond Design Basis Accident
BDBE	Beyond Design Basis Earthquake
BMW	Boiler Make-up Water (system)
CA	Computational Aid
CANDU	Canadian Deuterium Uranium
CL I / II/ III / IV	Class I / II / III /IV electrical power
CNCAN	National Committee for Nuclear Activities Control
COG	CANDU Owners Group
CSDV	Condenser Steam Discharge Valve
CSP	Critical Safety Parameter
CV	Calandria Vault
D_2O	Heavy Water
DBA	Design Basis Accidents
DBE	Design Basis Earthquake
DBF	Design Basis Flood
DBSC	Danube-Black Sea Channel
DCC	Digital Control Computer
DG	Diesel Generator
DICA	Dry Spent Fuel Storage
ECC	Emergency Core Cooling (system)
EPS	Emergency Power Supply
EQ	Environmental Qualification
EWS	Emergency Water Supply
FRS	Floor Response Spectra
FSAR	Final Safety Analysis Report
HPECC	High Pressure Emergency Core Cooling
HCLPF	High Confidence Low Probability of Failure
IAEA	International Atomic Energy Agency
LAC	(Reactor Building) Local Air Coolers
LCDA	Limited Core Damage Accident
LOCA	Loss of Cooling Accident
LOECC	Loss of Emergency Core Cooling
LRV	Liquid Relief Valve
LZC	Liquid Zone Control system
mBSL	meters Baltic Sea Level
MCR	Main Control Room
MSSVs	Main Steam Safety Valves
MV	Motorized Valve
NSP	Nuclear Steam Plant
OEP	On-Site Emergency Plan
OM	Operating Manual
OP&P	Operating Polices and Principles
PHT	Primary Heat Transport (system)

PHWR	Pressurized Heavy Water Reactor
PSHA	Probabilistic Seismic Hazard Assessment
R/B	Reactor Building
RCW	Recirculating Cooling Water (system)
RLE	Review Level Earthquake
ROH	Reactor Outlet Header
RRS	Reactor Regulating System
RSW	Raw Service Water (system)
SACRG	Severe Accident Control Room Guideline
SAEG	Severe Accident Exit Guideline
SAG	Severe Accident Guideline
SAM	Severe Accident Management
SAMG	Severe Accident Management Guidance
SB	Service Building
SBO	Station Blackout
SCA	Secondary Control Area
SCDA	Severe Core Damage Accident
SCG	Severe Challenge Guideline
SCS	Shield Cooling System
SCST	Severe Challenge Status Tree
SDC	Shut-Down Cooling (system)
SDE	Site Design Earthquake
SDG	Stand-by Diesel Generator
SDS	Shut Down System
SDS1	Shutdown System No. 1
SDS2	Shutdown System No. 2
SFB	Spent Fuel Bay
SG	Steam Generator (boiler)
SSCs	Structures, Systems and Components
WANO	World Association of Nuclear Operators