S. N. Nuclearelectrica S.A.
CNE Cernavoda

NUCLEARELECTRICA

CERNAVODA NPP UNITS 1 & 2, ROMANIA

SAFETY FEATURES OF CANDU 6 DESIGN AND STRESS TEST SUMMARY REPORT

Table of Contents

0.0 Background & Introduction

On March 11, 2011, an earthquake measuring 9.0 on the Richter scale, followed by a devastating tsunami, combined to cause one of the worst nuclear accidents in recent years at the Fukushima Daiichi nuclear power plant in Japan. Considering the accident at Fukushima, the European Council of March 24th and 25th declared that safety of the EU nuclear power plants be reviewed based on a comprehensive and transparent risk assessment process called "Stress Tests". To achieve this objective, the European Nuclear Safety Regulatory Group (ENSREG) in conjunction with the Western European Nuclear Regulators Association (WENRA) developed and issued a specification called EU "Stress tests" Specification to European countries for assessing and reporting safety of their nuclear power plants. In response to this requirement, Societatea Nationala Nuclearelectrica (SNN S.A.) developed a detailed and comprehensive assessment report for Cernavoda NPP Units 1 & 2 in conjunction with the plant designers (AECL/Candu Energy Inc. and ANSALDO) and submitted to the National Committee for Nuclear Activities (CNCAN) on October 31st, 2011.

The objective of this Stress Test Summary Report is to document SNN's evaluations contained in the comprehensive report as required by the EU "Stress tests" specifications in a concise manner for submission to CNCAN for general public information. This summary report documents the original design basis of Cernavoda NPP Units 1 & 2 followed by an assessment of each of the major issues for Beyond Design Basis Conditions along with conclusions in accordance with the Stress Tests Specification.

1.0 Site and Plant Main Characteristics

1.1 General Information

1.1.1 Site Location

Cernavoda Nuclear Power Plant (NPP) is located in Constanta county, latitude 44.3˚N and longitude 28.01˚E in the Dobrogea Region (Figures 1.1-1, 1.1-2). 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 site is located between the Danube River and the DBSC (Figure 1.1-3).

The Cernavoda NPP gets its cooling water from a branch of the Danube River. The cooling water is also returned to the Danube River after it has provided the cooling function to the non-nuclear systems/components of the plant.

The site was selected after detailed assessment of all characteristics consisting of soil, population, cooling water, industry, transportation routes, including natural events (such as earthquake, extreme temperatures, snow fall, high winds, flooding, etc.) and man induced events (such as explosions, toxic gases, explosive gases fires, etc.), in accordance with the Romanian Nuclear Safety Norms, similar to US NRC requirements.

Figure 1.1-1 Cernavoda NPP site location

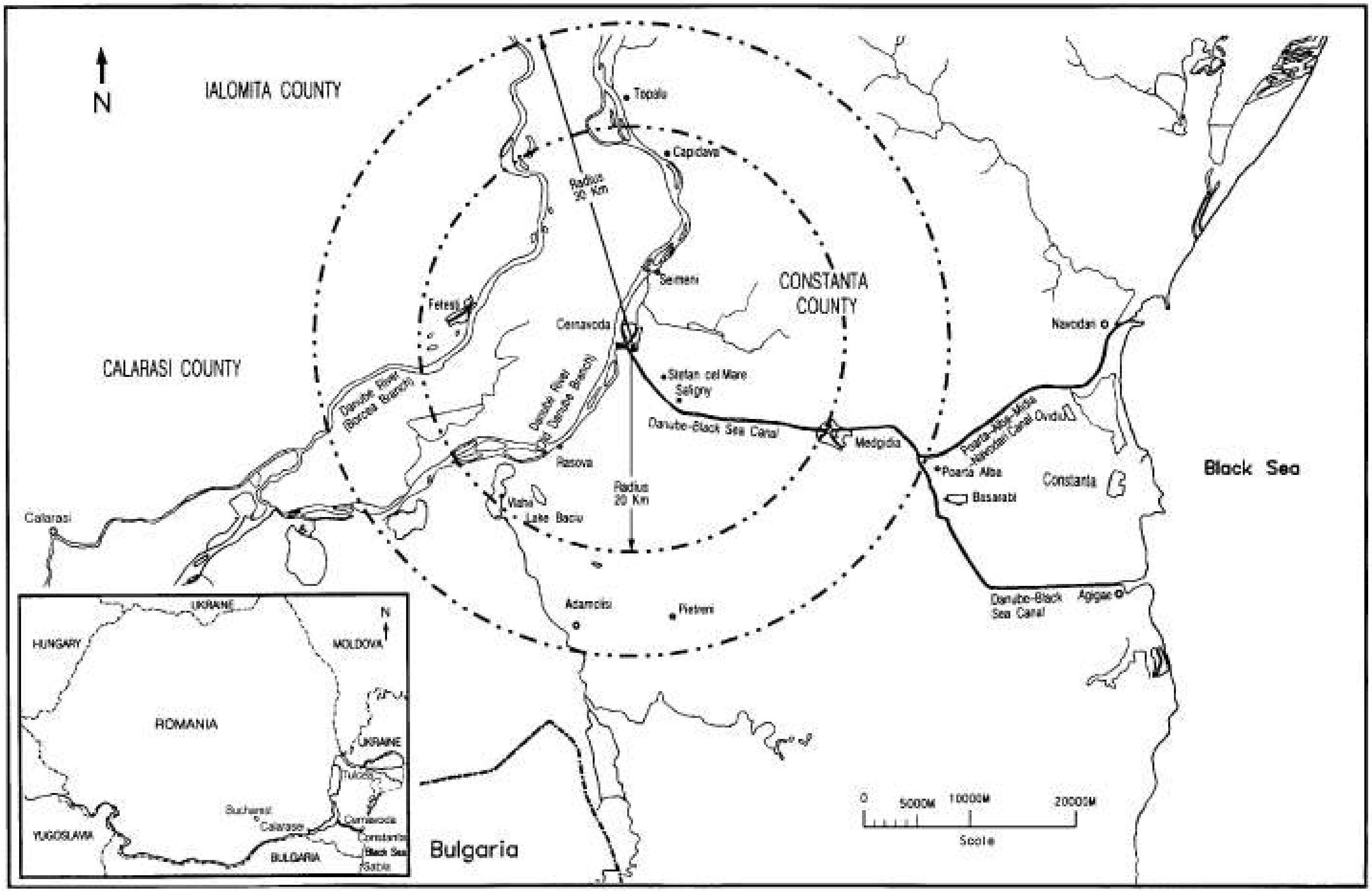

Figure 1.1-2 Cernavoda NPP Site Territory

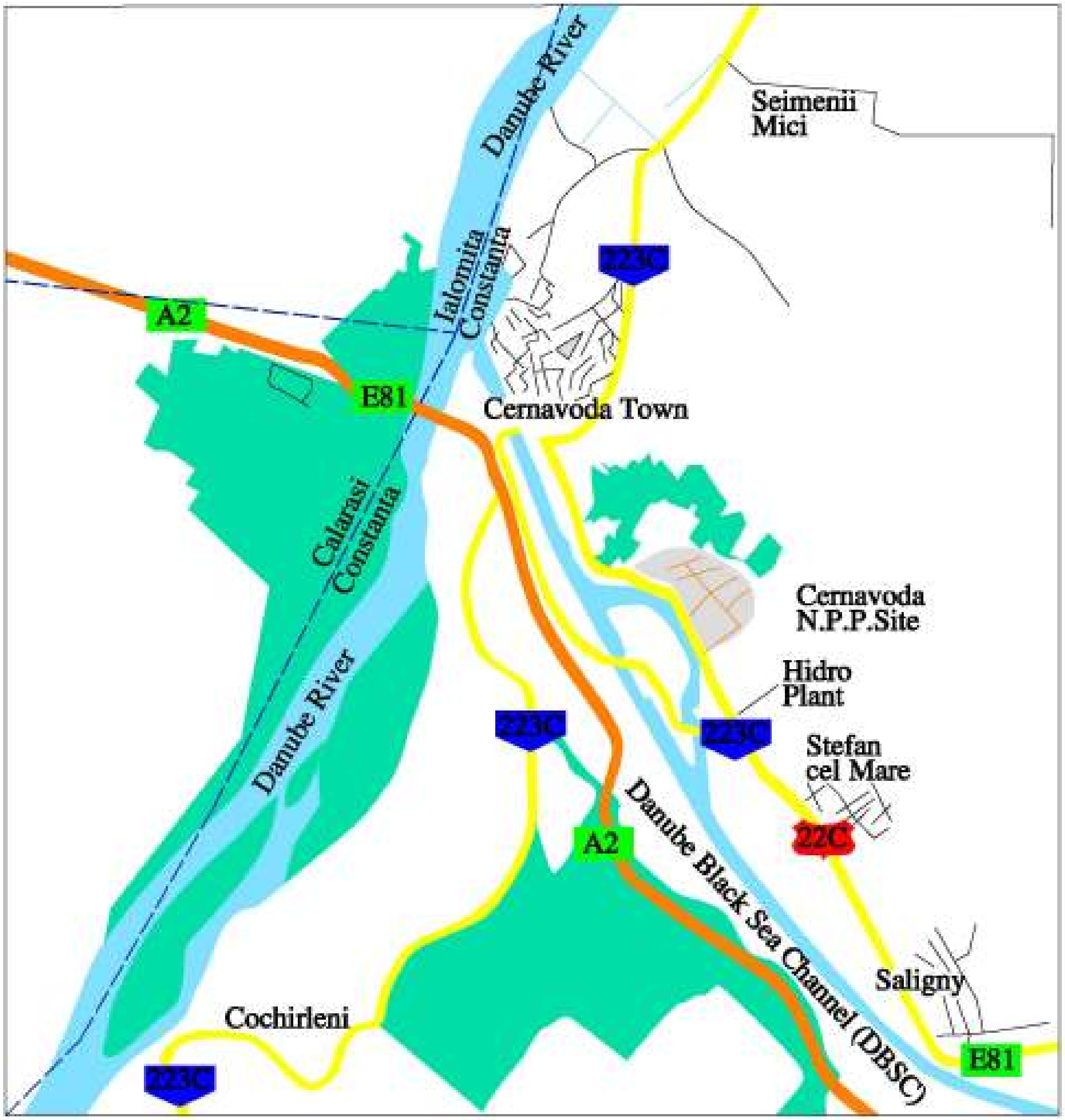

Figure 1.1-3 Cernavoda NPP Cooling Water Source

1.1.2 Number of Units

There are two CANDU 6 units in operation at Cernavoda site (Units 1 & 2). Two more similar units (3 and 4) are held-up in an intermediate construction stage pending authorization for construction. SNN, with its partners, has started the process to analyze restarting construction of Units 3 & 4. The feasibility studies and investment organization has been delegated to EnergoNuclear (EN), a joint venture between SNN and other investors.

1.1.3 License Holder

Societatea Nationala Nuclearelectrica (SNN), the Romanian state owned company, is the owner, operator and license holder for both Units 1 & 2 at Cernavoda.

1.1.4 Type and Power of Reactors

Each of the two operating Cernavoda Units is a Canadian-designed power reactor of the PHWR type (Pressurized Heavy Water Reactor) called CANDU, which stands for **CAN**ada **D**euterium **U**ranium. They use heavy water (deuterium oxide) for moderator and coolant and natural uranium for fuel.

The summary data required by the EU Stress test technical specification is provided in the tables below:

Reactor	Type	Gross Capacity MW (e)	Thermal Power MW (t)
Cernavoda-1	CANDU-6	706.5	2062 / 2071
Cemavoda-2	CANDU-6	706.5	2062 / 2071

1.1.5 Criticality & Commissioning Dates

The commissioning and in-service dates for both Cernavoda units are as follows:

Reactor	First Criticality	In-Service Date Criticality	Operating Status
Cernavoda-1	April 16th, 1996	December 12th, 1996	In operation
Cemavoda-2	May 6th, 2007	October 5th, 2007	In operation

1.1.6 Characteristics of Spent Fuel Storage Bay (Pools)

Each unit is provided with a dedicated, below grade level, seismically qualified Spent Fuel Bay (SFB) in another building outside containment for temporary storage of spent fuel under water (Figure 1.1-4). Spent (irradiated) fuel is removed from the reactor fuel channels and is transferred to the Spent Fuel Bay where it is stored under water. The water provides the necessary shielding from radiation emitted by the spent fuel and also provides means to remove its decay heat. The water in the Spent Fuel Bays is maintained in a clean and pure condition by a cooling and purification system 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. This allows the spent fuel to be handled by station personnel with long handled tools working through down below 8 m of water.

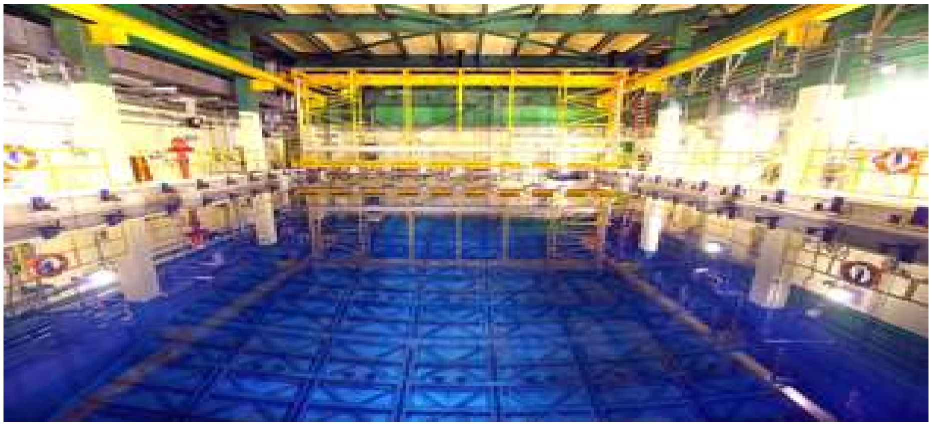

Figure 1.1-4 Spent Fuel Bay Storage

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, natural air-cooled dry storage facility (IDSFS) for the spent fuel long-term storage.

1.2 Major Design Features of Cernavoda CANDU 6 Units

1.2.1 Basic Description of the CANDU 6 Reactor Units

A CANDU reactor utilizes controlled fission in the reactor core as a heat source to supply steam and electrical power. However, unlike other reactors, the CANDU is fuelled with natural uranium fuel that is distributed among 380 fuel channels. Each six-meter-long fuel channel contains 12 fuel bundles.

The fuel channels are housed in a horizontal cylindrical tank (called a calandria) 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.

The CANDU reactor heat transport system is shown schematically in Figure 1.2-1. Pressurized heavy water (D2O) coolant is circulated through the fuel channels and steam generators primary side. The coolant carries the heat to steam generators, where it is transferred to light water to produce steam. The steam is used to drive the turbine generator to produce electricity.

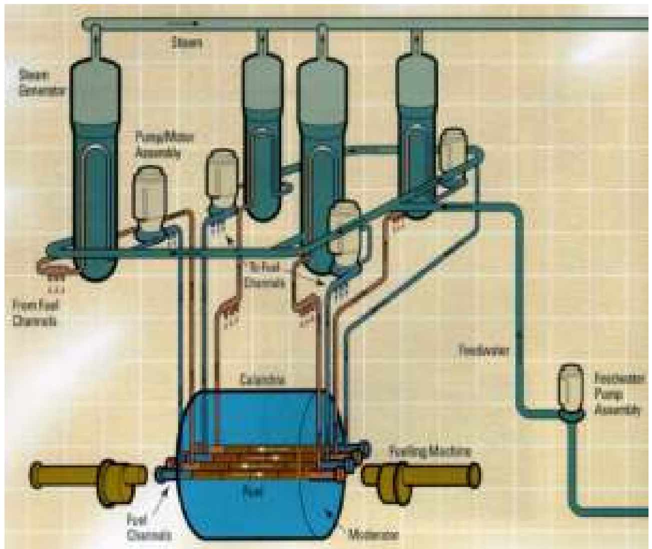

Figure 1.2-1 CANDU Reactor Heat Transport System

REACTOR

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.

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.

PRIMARY HEAT TRANSPORT SYSTEM

The primary heat transport system (PHT) 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.

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.

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.

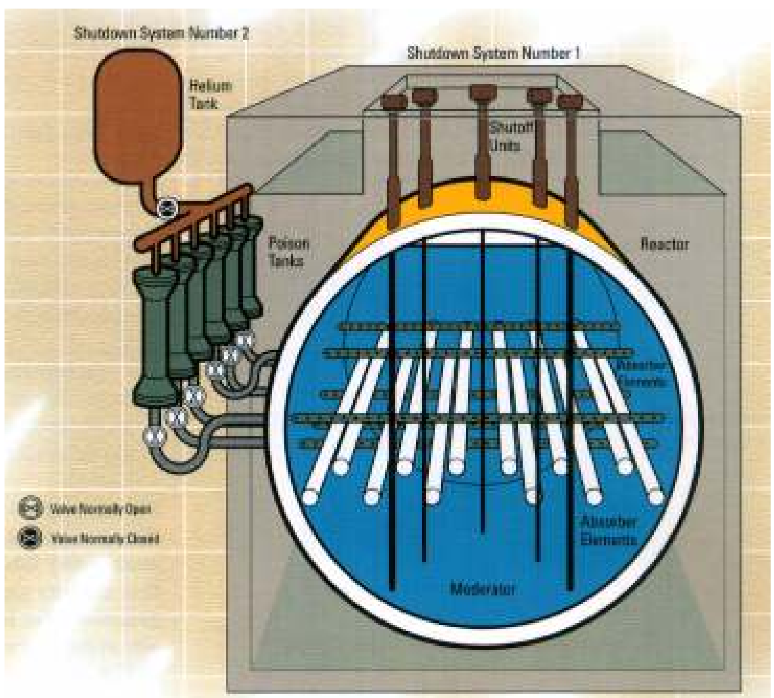

Figure 1.2-2 CANDU Two Shutdown Systems

The two shutdown systems are shown schematically in Figure 1.2-2 SDS1 uses shutoff rods while SDS2 uses poison injection.

REACTOR ASSEMBLY

The CANDU reactor assembly, shown in Figure 1.2-3, includes 380 channels contained in and supported by a horizontal cylindrical tank known as the calandria. Figure 1.2-4 shows the reactor face during construction. The calandria is closed and supported by end shields at each end. Each end shield comprises an inner and an outer tubesheet joined by lattice tubes at each fuel channel location and a peripheral shell. The inner space of the end shields is filled with steel balls and water, and is water cooled. The fuel channels, supported by the end shields, are located on a square lattice pitch. The calandria is filled with heavy water moderator at low temperature and pressure. The calandria is located in a light water filled shield tank. In the case of CANDU 6, this comprises a steel lined, water filled concrete vault.

Horizontal and vertical reactivity measurement and control devices are located between rows and columns of fuel channels, and are perpendicular to the fuel channels.

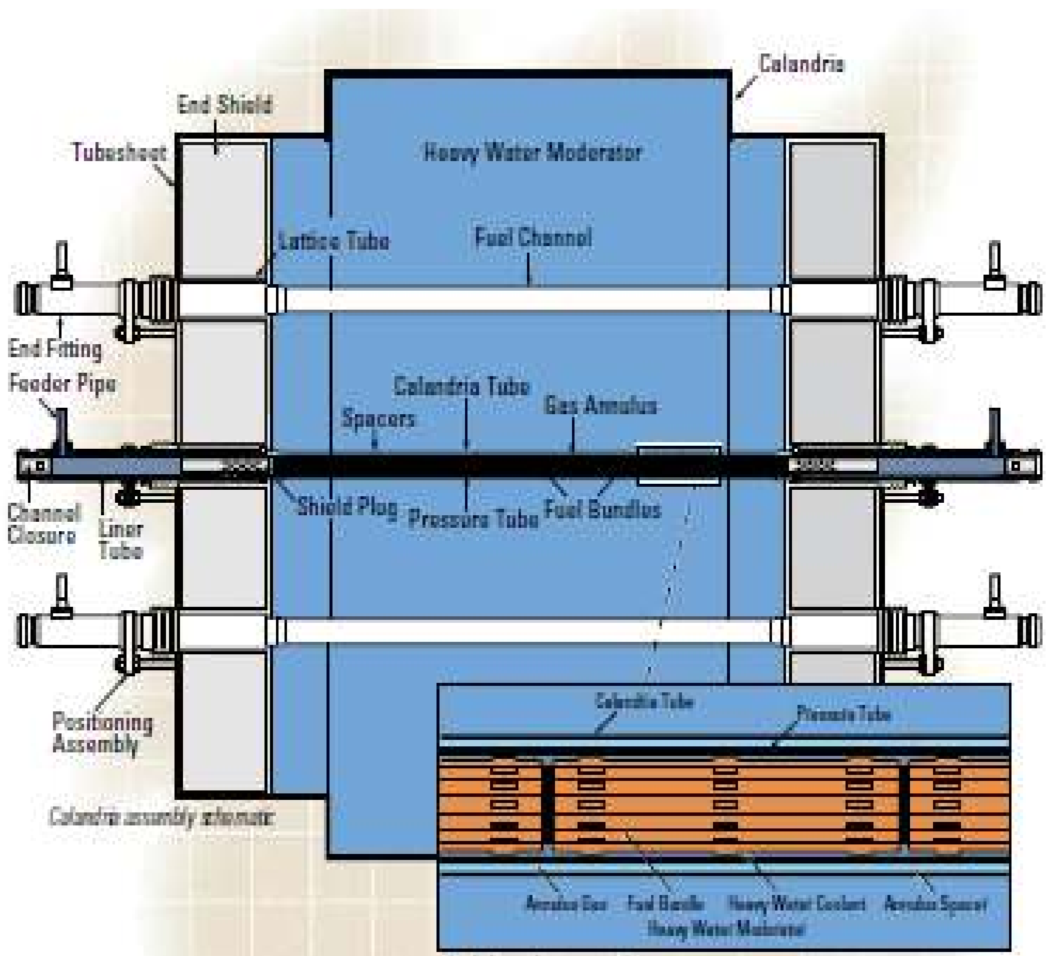

Figure 1.2-3 CANDU Reactor Assembly

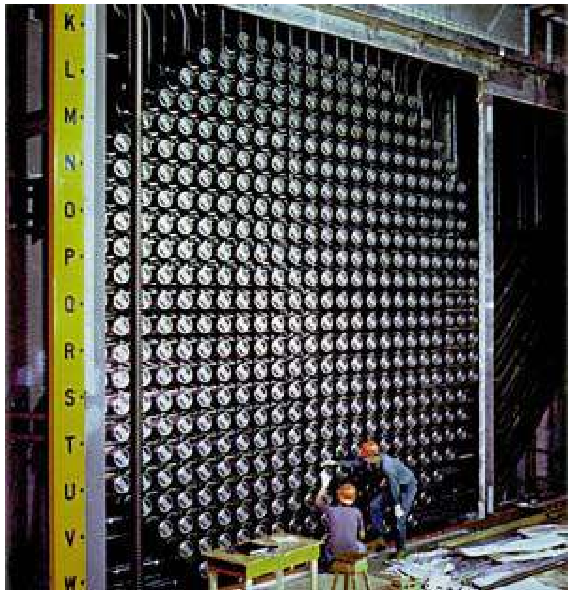

Figure 1.2-4 Reactor Face (during construction)

The fuel channels are also shown in Figure 1.2-3, with additional detail provided in the accompanying figure. Each fuel channel locates and supports 12 bundles in the reactor core. The fuel channel assembly includes:

- a zirconium-niobium alloy pressure tube;
- a zirconium calandria tube;
- stainless steel end fittings at each end;
- four spacers which maintain separation of the pressure tube and calandria tube.

Each pressure tube is thermally insulated from the cool, low pressure moderator, by the CO2 filled gas annulus formed between the pressure tube and the concentric calandria tube. Each end fitting incorporates a feeder connection through which heavy water coolant enters/leaves the fuel channel. Pressurized heavy water coolant flows around and through the fuel bundles in the fuel channel and removes the heat generated in the fuel by nuclear fission. Coolant flow through adjacent channels in the reactor is in opposite directions. During on-power refueling, the fuelling machines gain access to the fuel channel by removing the closure plug and shield plug from both end fittings of the channel to be refueled.

FUEL

The CANDU fuel bundle consists of 37 elements, arranged in circular rings as shown in Figure 1.2-5. Each element consists of natural uranium in the form of cylindrical pellets of sintered uranium dioxide contained in a zircaloy-4 sheath closed at each end by an end cap.

The 37 elements are held together by end plates at each end to form the fuel bundle. The required separation of the fuel elements is maintained by spacers brazed to the fuel elements at the transverse mid-plane. The outer fuel elements have bearing pads brazed to the outer surface to support the fuel bundle in the pressure tube.

Figure 1.2-5 Fuel Bundle

FUEL HANDLING / CHANGING SYSTEM:

- provides facilities for the storage and handling of new fuel;
- refuels the reactor remotely while it is operating at any level of power;
- transfers the irradiated fuel remotely from the reactor to the storage bay.

The fuel changing operation is based on the combined use of two remotely controlled seismically qualified fuelling machines, one operating on each end of a fuel channel. This is shown in the schematic of Figure 1.2-6 New fuel bundles, from one fuelling machine, are inserted into a fuel channel and the displaced irradiated fuel bundles are received into the second fuelling machine at the other end of the fuel channel. Typically, eight fuel bundles in a fuel channel are exchanged during a refueling operation. For a CANDU 6 size reactor (380 fuel channels), about 14 fuel channels per week are refueled.

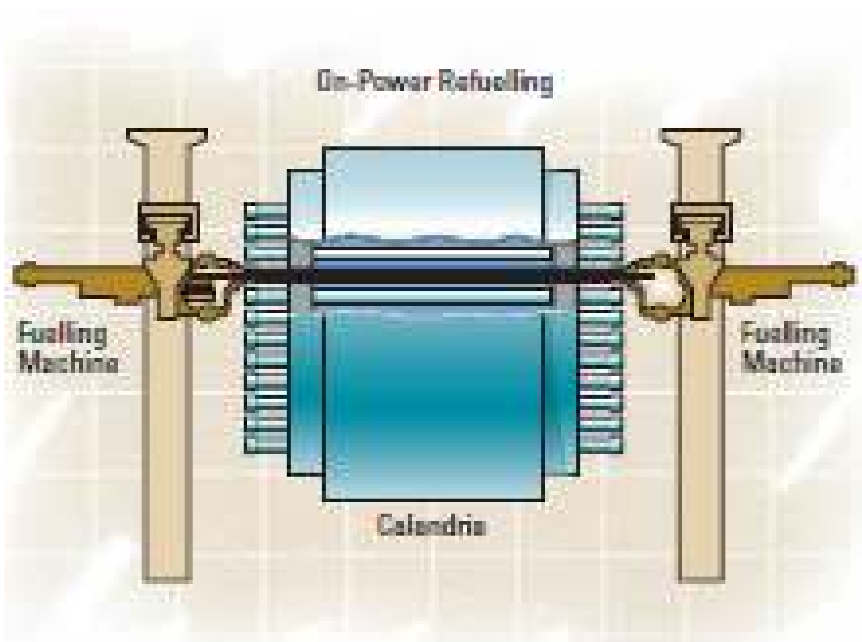

Figure 1.2-6 CANDU On-power Fuelling

Either machine can load or receive fuel. The direction of loading depends upon the direction of coolant flow in the fuel channel being fuelled, which alternates from channel to channel.

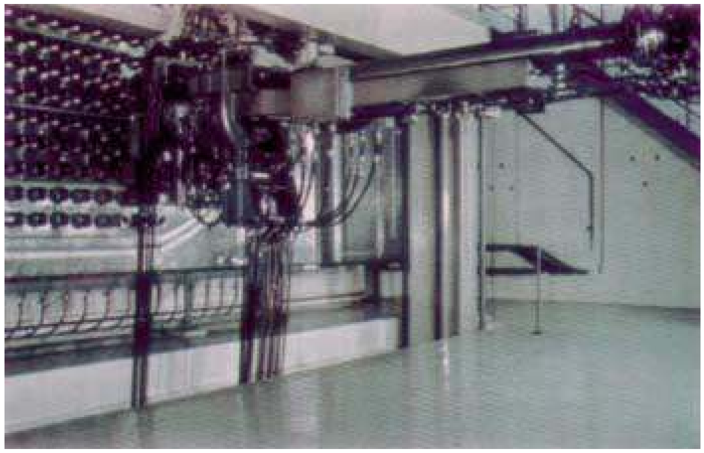

Figure 1.2-7 Fuelling Machine in Operating Position at Face of Reactor

The fuelling machines receive new fuel while they are connected to the new fuel port and discharge irradiated fuel while connected to the discharge port. The cooling of the spent fuel inside the fuelling machine is ensured by a dedicated heavy water cooling system.
The fuelling machine is shown in Figure 1.2-7.

The entire operation is directed from the control room through a preprogrammed computerized system. The control system provides a printed log of all operations and permits manual intervention by the operator using specific approved procedures.

INTERMEDIATE DRY SPENT FUEL STORAGE (IDSFS) FACILITY

As stated in Section 1.1.6, the Spent Fuel Bay is designed to accommodate the fuel discharged from each reactor during 8 years. After 6-7 years of operation, the spend fuel bundles are transferred to the on-site, naturally air-cooled dry storage facility (IDSFS) facility for the spent fuel long-term storage. The IDSFS facility is designed to provide safe, reliable and retrievable storage for spent fuel produced by both Cernavoda Units for a period of at least 50 years. The facility will eventually consist of 27 seismically qualified structures called MACSTOR 200 modules (Figure 1.2-8). At present, 4 modules are built and are in operation and 3 modules are in construction phase.

Each MACSTOR-200 module is a parallel-piped structure made of reinforced concrete, which embeds 20 metallic Storage Cylinders positioned vertically. Each Storage Cylinder is designed to store 10 spent fuel basket each of which can handle 60 spent fuel bundles.

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. Each module has the capacity of storing 10 x 20 x 60 = 12,000 spent fuel bundles.

Figure 1.2-8 Intermediate Dry Spent Fuel Storage Facility

1.2.2 CANDU 6 Inherent Safety Features

There are a number of inherent safety features of the CANDU6 design that are summarized below:

- Reactivity devices work in the near atmospheric pressure moderator environment, and therefore are not subject to pressure-assisted ejection.
- Criticality of CANDU bundles in ordinary (light) water is not possible, removing a concern in severe accidents. Injecting light water into the core is one option that is included into the severe accident management. In fact, the CANDU core geometry is near the optimum reactivity so that severe core damage accidents that could rearrange the core structure will tend to make sure it remains in the shutdown state.
- Because of on-power fuelling, the in-core power distribution reaches equilibrium in less than a year and then remains virtually unchanged for the remainder of the reactor's operating life. Therefore analysis of the reactor core behavior as a result of the postulated accidents is relatively simple.
- The pressure tube concept is used in identifying the location of fuel defects and on-power fuelling permits removal of defective fuel from the core as soon as it is identified or whenever convenient. This helps to keep the heat transport system essentially free from fission product activity. A clean heat transport system allows maintenance work to be done with relatively little exposure of personnel to radiation.
- The effect of changes in operating parameters on reactor power is slow in CANDU reactors because of long neutron lifetime. This characteristic allows the use of slow-acting control devices. These regulating devices, acting alone, are capable of controlling reactor operation over the entire operating range.
- The use of natural uranium fuel and heavy water leads to a design characterized by good neutron economy and low excess reactivity. There is little reactivity worth in the control devices because the burn-up compensation is done by on-power refueling. This limits the potential severity of accidents due to a loss of reactivity control. The largest positive reactivity insertion is from a large Loss-of-Coolant Accident (LOCA) and is well within the capability of mechanical and hydraulic shutdown systems. The

reactivity feedback from steam line breaks, cold or light water injection, or sudden turbine stop valve closure is negative.

- Low temperature and low pressure moderator provides an ideal location for neutronic measurements.
- The cold, low pressure heavy water moderator, about 1 cm away from the fuel in the channels, acts as an emergency heat sink following a loss-of-coolant even if the ECC fails to inject water. The heat removal occurs from the fuel through the pressure tube and calandria tube to the moderator. The moderator can remove more than 4% of the total thermal power, enough to accept decay heat indefinitely.
- The pressure tubes are relatively small in size (10 cm diameter). In a severe accident, such as a LOCA combined with a loss of emergency core coolant injection, 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. Should channel failure occur (for example, due to a further equipment unavailability resulting in a loss of moderator heat removal), then such failures will be spread out in time “softening” the load on containment. Direct containment heating or containment damage due to massive failure of a reactor vessel at high pressure, is precluded.
- The bottom of the large calandria vessel provides a spreading and heat removal area for core debris following a severe core damage accident.
- The calandria vessel is surrounded by a shield tank containing light water for biological and thermal shielding. In severe core damage accidents, this tank also absorbs decay heat either from the moderator liquid or from direct conduction from debris inside the calandria vessel.

In addition to these inherent safety characteristics, CANDU 6 includes engineered systems to enhance reactor safety. They include the following systems:

Two redundant, independent, diverse, separated shutdown systems, testable during operation to demonstrate an unavailability of less than 10^{-3} years/year. They share no devices with the control system or with each other. This triple layer of defence removes the need during reactor design to consider the consequences of accidents without shutdown.

- Likewise they are not a significant risk contributor in Probabilistic Safety Assessment (PSA) terms.
- A shutdown cooling system, which removes decay heat at full temperature and pressure conditions, precluding the need for depressurization after a loss of heat sink.
- In addition to the standby diesel generators in Group 1 safety systems, there are also two independent, separately-located, seismically qualified emergency diesel generators in Group 2 so that a loss of all alternating current (AC) power is of low frequency.
- Two control rooms, the Main Control Room (MCR) and the seismically qualified Secondary Control Area (SCA), each of which can independently perform the safety functions of shutting down the reactor, removing decay heat, and monitoring the status of the plant.

Performance of these systems is evaluated as part of regulatory-required safety analysis included in Safety Report and Probabilistic Safety Assessment documents.

1.2.3 CANDU 6 Heat Sink Philosophy

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 SDC system pumps.

- Steam generators produce steam whose energy can be transferred to the turbine or 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.

It should be mentioned that auxiliary feedwater pump motor, SDC and RCW and RSW pump motors can use as an alternate supply electrical power from standby diesel generators. EWS is seismically qualified and the pump motors are supplied from a second set of diesel generators which are also seismically qualified.

In the case of loss-of-coolant accident the two loops are isolated automatically. In the broken loop the heat is removed using emergency core cooling (ECC) system, which is seismically qualified. In the unbroken loop the heat is removed as described above.

1.2.4 Safety Assessment Summary Results

In addition to the deterministic approach, a level 1 probabilistic safety analysis (PSA) has been performed for both Units at Cernavoda NPP. The PSA developed for Cernavoda NPP covers the following objectives:

- Assess the level of plant safety and identify the most effective areas for improvements;
- Assess the level of safety and compare it with explicit and implicit standards;
- Assess the level of safety to assist day-by-day safe plant operation using the Risk Monitor.

1.2.4.1 Level 1 PSA Results

A Level 1 PSA was performed to identify the sequence of events that can lead to core damage, estimate the Core Damage Frequency (CDF), and provide insights into the strengths and weaknesses of the safety systems and procedures provided to prevent core damage. The events considered in the Level 1 PSA include internal events, failures that originate from plant systems, as well as events such as internal fire, internal flood, and seismic events. As per IAEA 75-INSAG-3, the target severe core damage frequency for existing nuclear power plants is 1E-04 events/yr.

Unit 1 Level 1 Results

The overall CDF per calendar year for CNE Cernavoda Unit 1 operation for all Plant Operating States (POSs) was calculated to be 3.3E-05 events per calendar year.

Unit 2 Level 1 Results

The overall CDF per calendar year for CNE Cernavoda Unit 2 operation for all POSs was calculated to be 3E-05 events per calendar year.

The following main conclusions can be drawn based on the overall PSA Level 1 results for both units:

- The overall calculated core damage frequency for both units, covers radioactivity sources, initiating events and plant operational modes as considered in this study. For both units it is below, and in compliance with the target frequency of 1.0E-04 events/year proposed by IAEA 75-INSAG-3 for operating plants;
- From the qualitative point of view the plant design satisfies the single failure criterion for process equipment and components;
- There are no major design vulnerabilities that may disable the plant heat sinks.

The Level 1 PSA for both Cernavoda NPP Unit 1 & 2 is in compliance with the Romanian regulations and has been confirmed by the National Regulatory Authority, CNCAN.

PSA Applications

Safety, Licensing and Performance Monitoring Department internal procedures were developed for periodic updating and configuration control of PSA / EOOS (Equipment Out-Of Service) model and specific reliability data collection.

During 66 months of use at **Cernavoda Unit 1**, risk monitoring results show that medium of Annual Cumulative Recorded CDF of 2.81E-05, calculated based on the calendar year CDF, is lower than the Average PSA Level 1 CDF, which is 3.0E-05.

During 33 months of use at **Cernavoda Unit 2**, risk monitoring results show that medium of Annual Cumulative Recorded CDF of 1.61E-05, calculated based on the calendar year CDF, is lower than the Average PSA Level 1 CDF, which is 1.77E-05.

1.2.4.2 Level 2 PSA

A Level 2 PSA is performed by the nuclear industry to identify ways in which radioactive releases from the plant can occur and estimate their magnitude and frequency. This analysis provides additional insights into the relative importance of accident prevention and mitigation measures. As per IAEA 75-INSAG-3, the target large early release frequency is one order of magnitude lower than that of severe core damage frequency, namely 1E-05/ events/ year.

Cernavoda Units 1 and 2 have started actions to perform a Level 2 PSA. 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.

1.3 Design Differences between Cernavoda CANDU 6 & Fukushima Type Boiling Water Reactors (BWRs)

1.3.1 Type of Reactors

The reactors similar to the one at Fukushima are Boiling Water Reactors (BWR). The figure 1.3-1 is an illustration of a typical BWR nuclear power station. The light water (normal demineralized) is boiled in the reactor using highly enriched uranium fuel. The steam so produced is radioactive and is used to drive the turbine to generate electricity. The turbine exhaust steam is cooled in a condenser and returned to the reactor in a direct cycle.

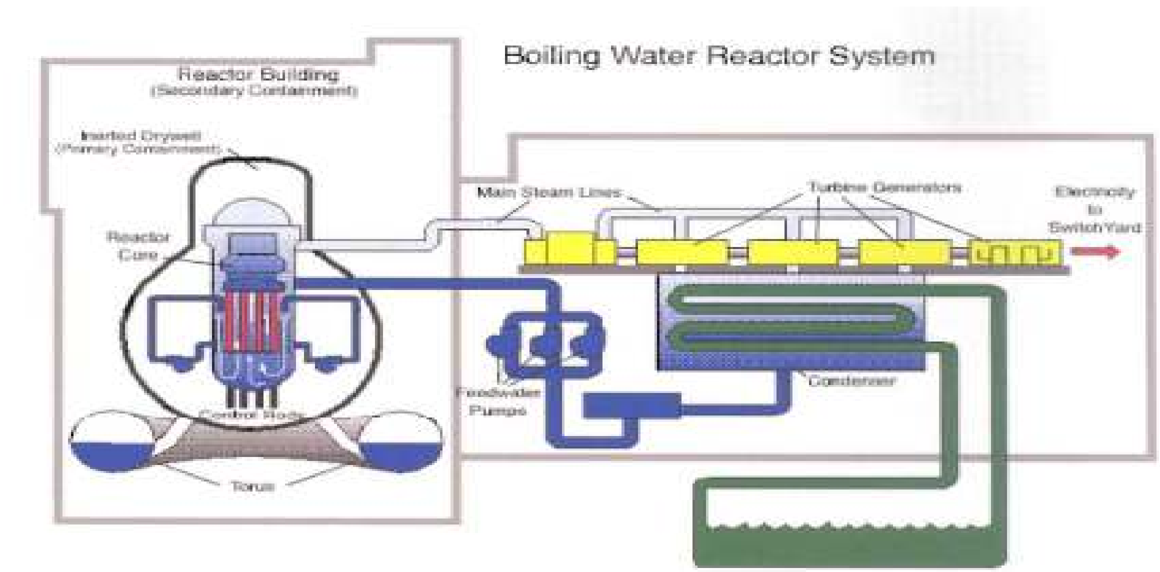

Figure 1.3-1 Boiling Water Reactor System

On the other hand CANDU reactors, similar to the two at Cernavoda, are Pressurized Heavy Water Reactors (PHWR). The figure 1.3.-2 is an illustration of a typical CANDU nuclear power station. The heavy water used to circulate around the fuel in a CANDU reactor picks-up heat from the natural uranium fuel (without boiling). The circulating hot/pressurized heavy water transfers its heat through special alloy material tubes in steam generators to the light water on the outside of the tubes (without coming in direct contact with the light water). The circulating heavy water, after it has transferred its heat to the light water, returns to the reactor. The light water, thus heated on the outside of the alloy tubes of the steam generators, produces steam, which is non-radioactive. This steam is used to drive the turbine to generate electricity. The turbine exhaust is cooled in a condenser and returned to the steam generators and as such the objective is achieved in an indirect cycle.

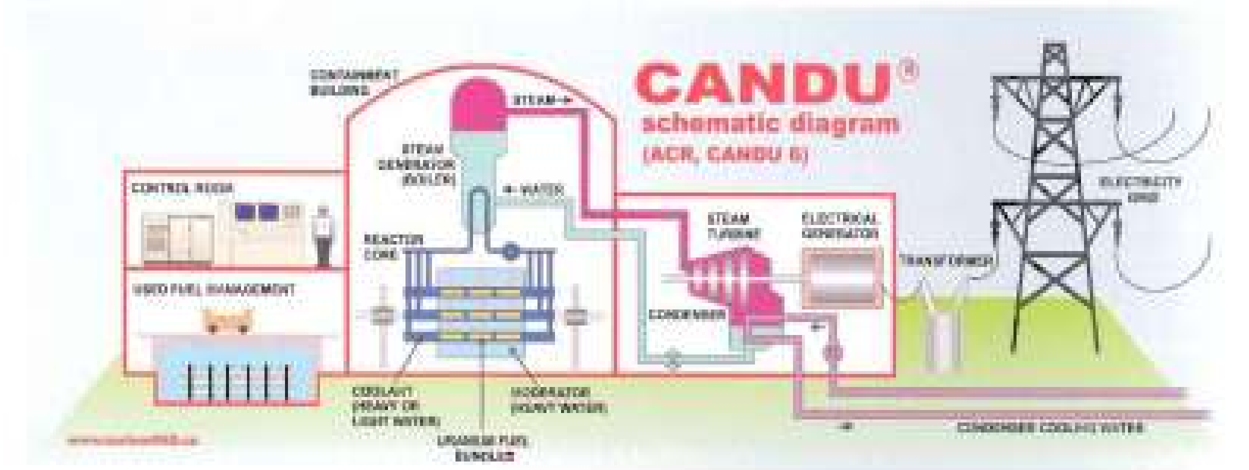

Figure 1.3-2 CANDU Schematic Diagram

1.3.2 Reactor Control, Cooling & Shutdown Systems

This section will briefly explain the differences in how some key safety principles to Control the nuclear reaction, Cool the fuel and Contain radioactivity are achieved in these two types of reactors.

Control: Both types of reactors achieve this principle by two independent systems: shut-off rods insertion and poison (chemical) injection into the reactor core.

In a CANDU reactor, shut-off rods are dropped into the core from the top of the reactor by gravity and for poison injection; a chemical solution called gadolinium nitrate is injected into the moderator (which is a low temperature calandria vessel).

In a BWR plant, because of the geometry and integral components near the top of the reactor pressure vessel, the shut-off rods are pushed up into the core from the bottom of the reactor. For poison injection, a chemical solution called boron is injected into the fuel coolant (which is also the moderator) inside the reactor pressure vessel.

Cool: In a CANDU reactor the heavy water coolant transports heat from the fuel to the steam generators with the aid of circulating pumps. The steam generators provide the heat sink for the reactor fuel. The reactor heat sink is maintained by the plant secondary side, where steam drives the turbine and is then cooled by the condenser and then returned to the steam generators by feedwater pumps powered by the grid. If the grid, supplying power to these pumps, fails (loss of Class IV power), then the reactor shuts down, the turbine trips, and auxiliary pumps, powered by diesel generators (class III power), are used. The steam generators continue to function as heat sinks while the primary side flow providing cooling function for the fuel is achieved by natural circulation (thermosyphoning). Thermosyphoning is effective because the steam generators, providing the heat sink, are located at higher elevation than the reactor. Because the turbine is tripped, steam from the steam generators is bypassed to the condenser where it continues to be condensed to be used again on the secondary side of the plant. If both class IV and class III power is lost, the steam from the secondary side of steam generators is rejected to the atmosphere through relief valves and the reactor continues to be cooled by natural circulation. The make-up water required is added to the steam generators secondary side from the stored inventory or from a system powered by another set of diesel generators, and in the longer term by firewater connections. DC battery power is used to operate control vales and monitor reactor safety critical parameters as required.

In a BWR, light water removes heat from the fuel by boiling inside the reactor pressure vessel. The steam thus formed in the reactor vessel is used to drive a turbine. The steam from the turbine exhaust is cooled by the turbine condenser and returned to the reactor vessel with feed pumps. If power from the grid fails, the reactor and the turbine/generator trip and the steam line to the turbine is isolated. The turbine condenser is at a lower elevation than the reactor vessel and hence natural circulation to use that heat sink is not possible. Standby generators provide power to run the residual heat removal systems. If both the grid and the standby generators are lost, then another cooling system is used that does not use AC power.

The BWR plants have a reactor core isolation cooling (RCIC) system. During such transients, steam from the reactor drives a turbine with its exhaust steam cooled in a suppression chamber called "torus" shaped water filled "wet well" in the primary containment. This turbine drives a pump to inject cold water into the reactor from either a storage tank or from the wet well. When the suppression chamber (wet well) reaches its boiling point, the RCIC is no longer effective. Diesel driven pumps are used to inject water by sprays in the reactor pressure vessel and the suppression chamber/wet well space of the primary containment vessel. If sprays are not effective the reactor pressure will increase causing safety relief valves to be opened either automatically or manually to relieve steam into the primary containment vessel suppression chamber. As the primary containment pressure increases, its pressure is relieved by venting to atmosphere through the standby gas treatment system.

Containment: In both a CANDU and BWR, radioactive fission products are contained in the fuel encased in a metallic sheath made of zirconium. The fuel assemblies are contained in fuel channels as in CANDU plants or the reactor pressure vessel as in BWR plants.

A CANDU reactor is contained in robust concrete containment structure. The BWR reactor is contained in a primary containment vessel (PCV) which is filled with nitrogen. The PCV is steel-lined and surrounded by concrete. The PCV is then surrounded by a secondary containment system structure.

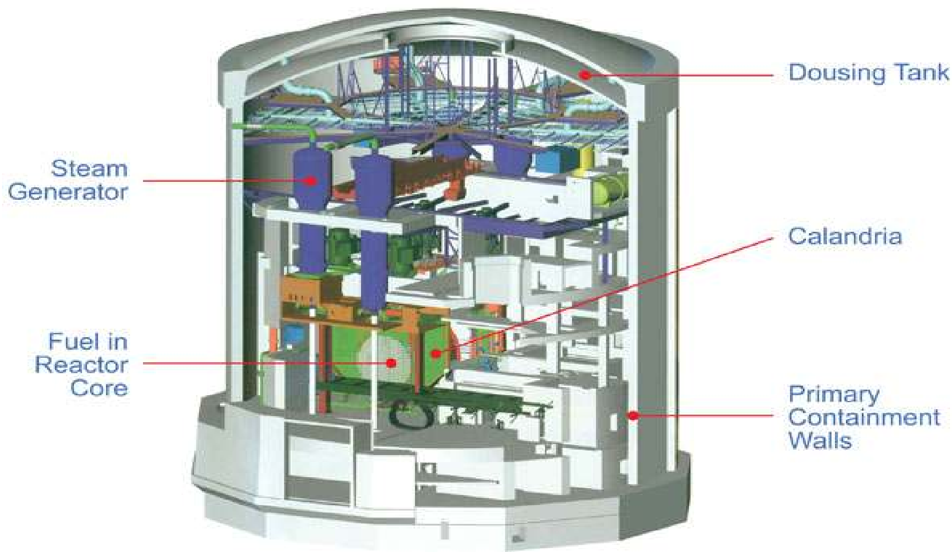

Figure 1.3-3 CANDU Reactor

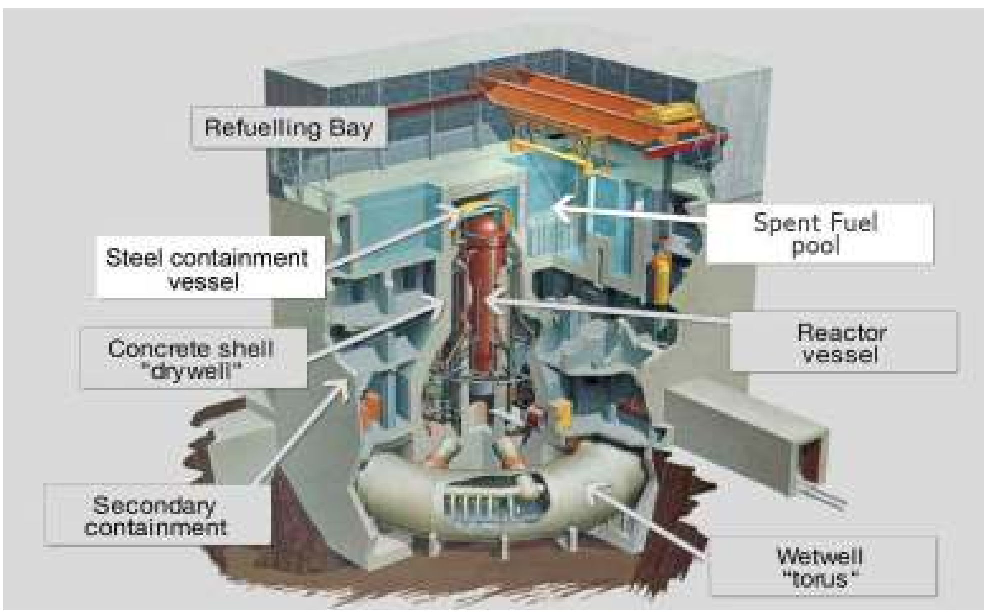

Figure 1.3-4 Boiling Water Reactor

1.3.3 Type of Fuel Used

and regularly while operating to support their full power operation. They are designed to have just enough excess positive reactivity to sustain full power operation only for few days without fuelling. BWRs on the other hand require highly enriched uranium and contain enough fuel (Figure 1.3-6) and excess positive reactivity to be able to operate at full power in between two consecutive outage (typically one to two years apart).

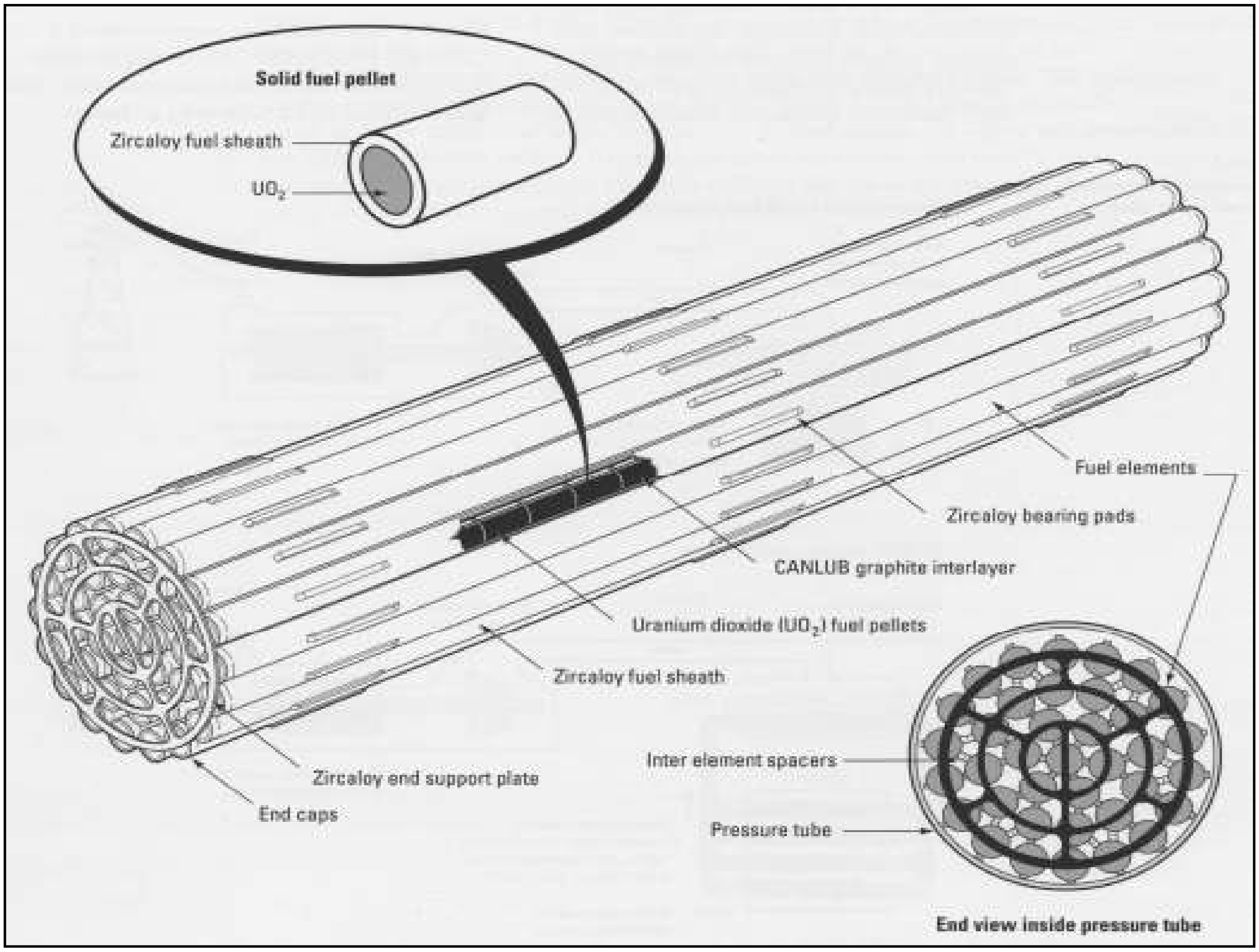

Figure 1.3-5 CANDU Fuel Bundle

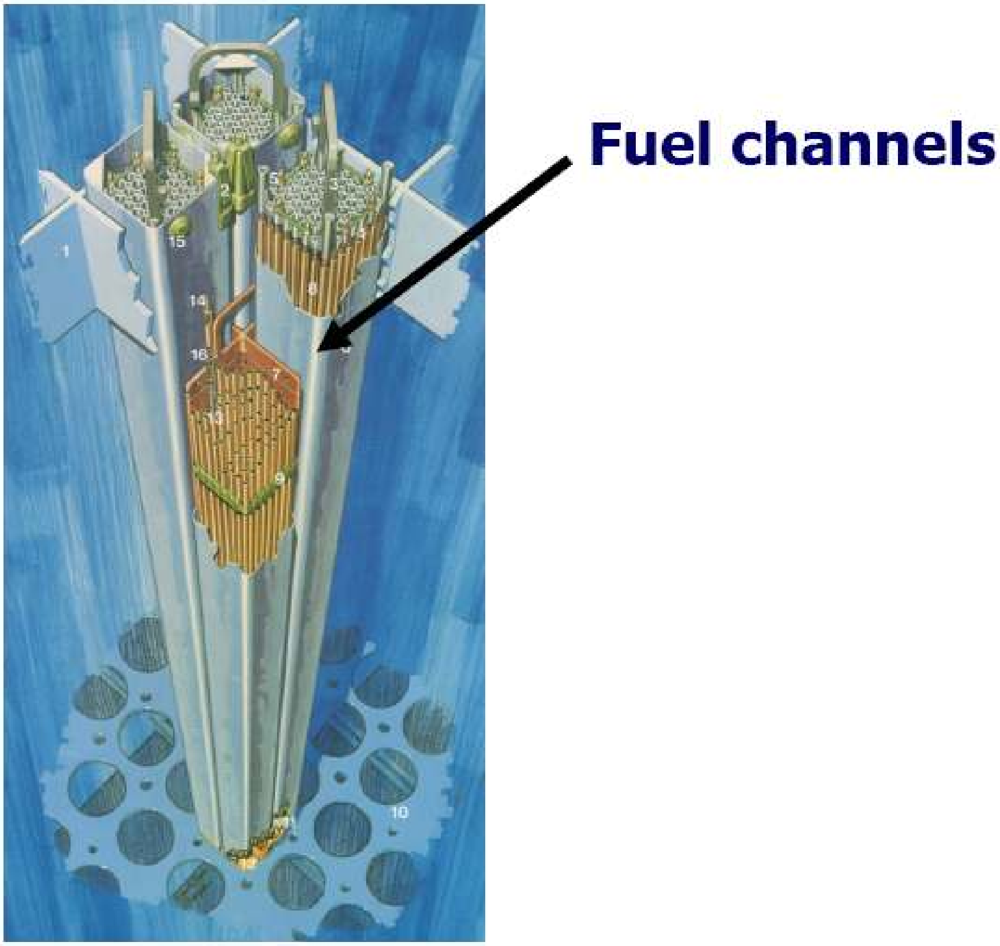

Figure 1.3-6 BWR Fuel Bundle

1.3.4 Spent Fuel Storage Provisions

In both a CANDU and BWR, used fuel is stored in a cooling pool. The pool is cooled by heat exchangers, but if all AC power is lost there is no immediate concern because the massive volume of water would take several days to heat-up to saturation (boiling), after which make-up water can be added from various sources including fire water systems using diesel driven pumps. In a CANDU nuclear plant the spent fuel pool is located below grade level in a separate seismically qualified building (with confinement and filtered exhaust), whereas in a BWR plant it is located inside the secondary containment of the reactor building above the elevation of the reactor.

2.0 WENRA/ENSREG Stress Tests Specification Requirements

The European Council of March 24/25, 2011 stressed that the safety of all EU nuclear power plants be reviewed based on a set of comprehensive and transparent risk and safety assessments (called stress tests). To achieve this Western European Nuclear Regulators Association (WENRA) and the European Nuclear Safety Regulators' Group (ENSREG) developed specific requirements for all EU nuclear power plants to follow for assessment of safety margins. The assessment document is required to address design basis provisions, robustness of the plant for conditions beyond design basis and potential further safety improvements. These stress tests requirements are described below:

2.1 Initiating Events

- Earthquake
- Flooding

In addition to earthquake and tsunami (flooding), the ENSREG specification also requires other initiating events considered e.g. Bad Weather.

2.2 Consequences of Loss of Safety Functions from any Initiating Event at the Plant Site

- Loss of electrical power, including station black-out (SBO)
- Loss of the ultimate heat sink (UHS)
- Combination of both

2.3 Severe Accident Management Issues

- Means to protect from and to manage loss of core cooling function
- Means to protect from and to manage loss of cooling function in the fuel storage pool
- Means to protect from and to manage loss of containment integrity

3.0 Cernavoda Stress Tests Results and Evaluation of Margins

The following sections deal with each of the initiating events and issues required by WENRA/ENSREG stress tests specification. They cover the plant design basis provisions, how the plant complies with its licensing basis while addressing these issues and evaluation of the available safety margins against these events.

3.1 Earthquake

3.1.1 Site Selection and Design Basis Considerations

3.1.1.1 Site Selection Considerations

The National Research - Development Institute for Earth Physics (INCDFP) determined the seismologic data of the Cernavoda Nuclear Power Plant (NPP) site area and of the NPP site as authorized by CNCAN. The site selection was done based on research of data of more than 100 important earthquakes that occurred between 984 and 1980. The seismic analyses considered the NPP site area on a radius of up to 300 km.

Based on the geologic, tectonic and seismological data for the NPP site area, the specialized Institute for Earth Physics (INCDFP) performed analysis and defined the maximum possible earthquakes in terms of magnitude and intensity, their location in relation to the site and characterization of the faults.

Using the data gathered in 340 years and included in the National Oceanic and Atmospheric Administration (NOAA) Colorado, USA and the International Seismological Center (ISC), Berkshire, UK catalogues; D'Appolonia elaborated a map illustrating a division of the earthquakes having 287 recorded epicenters. This assessment points out the existence of three seismic tectonic provinces:

- Vrancea province – the seismic zone formed in the "Avanfosa";
- Balkanic province – Sabla-Dulovo zone in Bulgaria influenced by the orogenetic pressure of the Alps chain;
- Dobrogean province – characterized by some macro-seismic epicenters within a stable platform.

Cernavoda NPP site seismicity is determined by the seismic activity of Vrancea and Sabla-Dulovo seismo-tectonic provinces and by the seismic activity in the area of Galati-Tulcea-Sf. Gheorghe fault and is assessed to relatively stable.

3.1.1.2 Design Basis Considerations

Considering the seismic movement attenuation with epicenter distance for each seismo-tectonic province, the seismic intensity in Cernavoda area was determined for the maximum observed and for the maximum possible earthquake given by each seismo-tectonic province.

The results of the analyses on these data show that, conservatively for Cernavoda area, the maximum observed earthquake may have the intensity I = VII degrees MSK-64, and the maximum potential earthquake I = VIII degrees MSK-64, the ground peak acceleration being a = 0.2 g. The ground peak acceleration at a site generally represents intensity of the ground motion at that location due to a seismic event.

According to the seismic qualification principles adopted for CANDU 6 NPPs, the design considers two seismic activity levels, both levels being imposed by the NPP nuclear safety requirements, namely:

- Design Basis Earthquake (DBE) Level is the engineering presentation of earthquakes generating the most possible severe effects, applicable to the NPP site and having a sufficiently low probability of being exceeded during plant lifetime. The DBE effects on the NPP site are expressed by the ground response spectra (GRS). The DBE effects on the on-site structures are described by the floor response spectra (FRS) or the acceleration time-history that is developed for each area within the structure compatible with FRS.
- Site Design Earthquake (SDE) Level represents the seismic activity with the period of response on the NPP site ≥ 100 years. This is the seismic design level for the plant systems that must remain operational for a long period of time after a loss of coolant accident (LOCA).

Based on the values for intensities and accelerations, the two design earthquake levels are defined as below:

- SDE level - I = VII degrees MSK-64, a = 0.1 g;
- DBE level - I = VIII degrees MSK-64, a = 0.2 g.

Note: I = intensity of the earthquake

The ground spectra of the design of the Cernavoda NPP are shown in Figure 3.1-1.

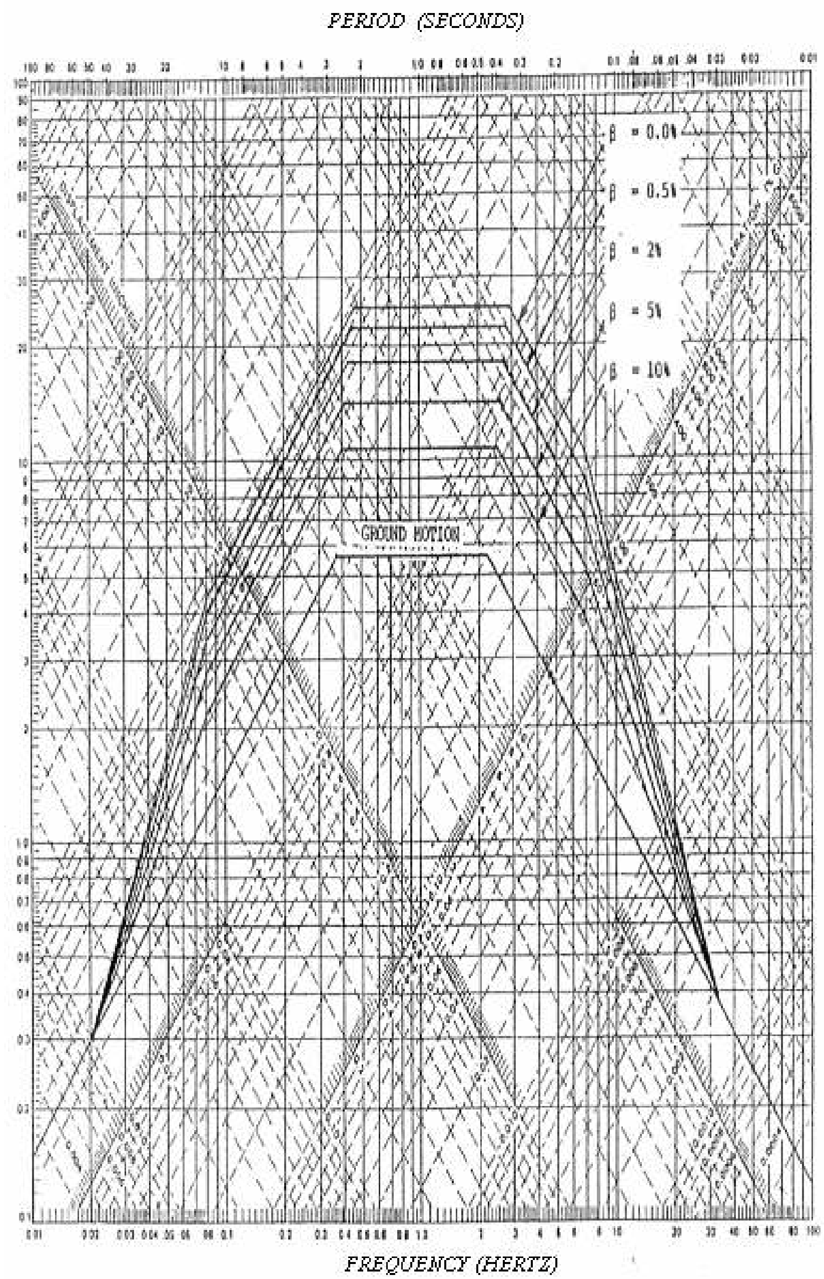

Figure 3.1-1 – Design Basis Earthquake Response Spectra

3.1.1.3 Validity of Data in Time & Conclusion on the Adequacy of the Design Basis

In 2004 a probabilistic seismic hazard analysis (PSHA) was carried out for the existing reactors at Cernavoda, Romania. The PSHA was carried out by a Romanian team under the technical supervision of Paul C. Rizzo Associates, Inc. (RIZZO). Staff from the University of Bucharest (UB) developed the seismo-tectonic and seismic source models, staff from the Technical University of Civil Engineering, Bucharest (UTCB) developed the ground motion models, and Stevenson and Associates-Bucharest (SAB) performed the probabilistic hazard computations.

The main conclusions from this study are:

- The Vrancea sub-crustal seismic source dominates the seismic hazard at the Cernavoda NPP.
- For the maximum historical recorded event, with a magnitude M = 7.5 the corresponding Peak Ground Acceleration (PGA) at the NPP rock surface is 0.11g.
- For the maximum estimated event with a magnitude M = 7.80, the PGA at the NPP rock surface is 0.18g.

Compared with the DBE PGA value of 0.2g, the above results confirm the adequacy of the design basis. As a confirmation of design basis for earthquake, the mean seismic hazard curve calculated as part of PSHA shows the value of PGA for a probability of 10^{-3} as being 0.2g, exactly the value from the design data input for CNE Cernavoda NPPs for a return period of 1000 years.

3.1.1.4 Regulatory Requirements

CANDU 6 NPPs are designed considering the following DBE requirements:

- Canadian Nuclear Safety Commission (CNSC) R-7: “Requirements for Containment Systems for CANDU Nuclear Power Plants”
- CNSC R-8: “Requirements for Shutdown Systems for CANDU Nuclear Power Plants”. Specifically, all CANDU nuclear power reactors shall be equipped with two independent and diverse shutdown systems.
  The SDS1 shall be an independent system from the SDS2 to provide diverse shutdown systems in line with the requirements in CNSC Regulatory Document R-8, Section 3.1.
- CNSC R-10: “The Use of Two Shutdown Systems in Reactors”
  Both R-8 and R-10 require that the shutdown systems prevent systematic fuel failure.
- CNSC R-77: “Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems”.
  R-77 requires that appropriate American Society of Mechanical Engineers (ASME) service limits are met and whether the first or second shutdown system is assumed to act for overpressure protection of the PHT.
- CNSC (AECB) C-6: “Requirements for the Safety Analysis of CANDU Nuclear Power Plants”.

The CANDU 6 reactor core design meets the Romanian regulatory requirements set for normal and abnormal (accident) conditions. A summary of compliance with the fundamental design criteria for reactor systems is documented in the Cernavoda U1 & U2 final safety analysis reports (FSAR) and fundamental safety objectives compliance with NRSN.

The Cernavoda design has been assessed to strictly meet the NRSN requirements and to meet the fundamental safety objectives of all the Law 111 /1998 requirements.

3.1.1.5 Seismic Design Requirements

The design of Cernavoda Units 1 & 2 reactors has been qualified for a DBE with a peak horizontal ground acceleration of 0.2 g using the standard ground response spectra of the Canadian Standards Association CSA-N289.3.

Two categories, (A) and (B), are defined to establish the extent to which components must remain operational during and/or after the DBE:

Category (A) Components are those components which must retain their pressure boundary integrity or structural integrity or passive function and are not required to change state during and/or following an earthquake.

Category (B) Components are those components that must retain their pressure boundary integrity or structural integrity and remain operable during and/or following DBE.

3.1.1.6 Reactor Shutdown Requirements

In accordance with CNSC R-8, for specified events requiring prompt shutdown action, each shutdown system (SDS) shall act alone, to ensure that the reactor is rendered subcritical and is maintained subcritical and the reference dose limits are not exceeded.

In accordance with CNSC R-77, the shutdown system action is required for overpressure protection of the Primary Heat Transport systems (PHT).

Each of the two shutdown systems is designed to independently provide sufficient negative reactivity margin under all reactor conditions, including the condition of maximum excess reactivity. The speed of detection of the onset of postulated design basis accidents and the speed of negative reactivity insertion by each of the two SDS is such that the power transient is terminated and the reactor is brought to a shutdown state and maintains the reactor in a shutdown state indefinitely following the DBE event.

3.1.1.7 Containment Requirements

The containment structure including the containment isolation system shall be seismically qualified to ensure that the dose limits in the event of DBE are satisfied.

3.1.2 CANDU 6 Design Philosophy

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 (SDGs).

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

Group 1: Primary Heat Transport (PHT), Shutdown System one (SDS1), Main and Auxiliary Moderator, Steam and Feed-water, Emergency Core Cooling (ECC), 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, Dousing, Air locks, Hydrogen Control, Emergency Water Supply (EWS), Emergency Power Supply (EPS) and the Secondary Control Area (SCA).

As per the Safety Design Guides governing the design requirements for CANDU nuclear stations, the separation of Group 1 and Group 2 SSC is implemented so that failure of any Group 1 SSC would not cause failure to the Group 2 SSCs.

Should the occurrence of a DBE render the MCR uninhabitable, the Group 2 Secondary Control Area (SCA) is used to operate Group 2 safety related systems, control and monitor the reactor in a safe shutdown state. The design approach is to seismically qualify all of Group 2 and some of Group 1 systems (considered appropriate) to carry out the essential safety functions following a DBE.

The design basis for the CANDU nuclear plants is to shut down the reactor only if an earthquake causes a failure requiring a shutdown, e.g., on low flow trip as a result of loss of Class IV power to the pumps in the PHT system. The CANDU plant has two shutdown systems: SDS1 and SDS2. SDS2 is fully seismically qualified. SDS1 is seismically qualified to permit the shutoff rods to drop into the core on loss of electrical power to their clutch assemblies.

The required CANDU NPP SSCs are designed to sustain the effects of earthquakes expected at the NPP site. The Cernavoda 1 & 2 DBE-qualified SSCs support the following safety functions:

- Safely shutdown the reactor
- Remove the heat from the fuel channels, and
- Control the radioactive release for the events of DBE

3.1.2.1 CANDU Seismic Design Robustness for Seismic Interaction Effects

CANDU nuclear plants have been seismically qualified since the early 1960s based on dynamic analysis utilizing the most stringent seismic requirements. A sufficient selection of SSCs is DBE qualified for assurance of nuclear safety as discussed before. In addition all structures and equipment in the plant are designed to meet the seismic requirements of the Romanian standards. This typically involves using conservative static analysis methods and subjecting the building or the equipment to conservative lateral loads, which represents a percentage of the weight. The complete elimination of seismic interaction effects is achieved by the following:

- The safety related systems are divided in two groups, Group 1 and Group 2. During the plant layout phase special care is taken to provide physical separation between Group 1 and Group 2 systems. A special safety design guide (SDG) is devoted to covering this unique CANDU two group separation philosophy. This is also discussed in Section covering Design Philosophy as mentioned before.
- Special care is taken to prevent interaction between DBE seismically qualified (SQ) SCC and those which are not DBE seismically qualified (NSQ or building code qualified). The interaction effects are taken care of by several methods as follows:
    - Locating the NSQ SSC at lower level than the SQ SSC
    - Locating the NSQ SSC away from SQ SSC
    - Restraining the NSQ SSC or by designing their supports if the NSQ SSC is close to or above the SQ SSC
    - Providing a barrier between the SQ and the NSQ SSC
    - Conducting pre-operational seismic walkdowns to ensure freedom of any seismic interaction.
- Equipment and portions of buildings that have the potential to affect the SQ safety related SSCs are upgraded to meet more stringent safety and seismic requirements. Typically its anchorage is enhanced to accommodate the DBE level with no toppling or dislodging.
- Pre-commissioning walk downs (surveys) are performed after the plant construction is substantially complete by a multi-disciplinary team to look for any possible interactions and to correct them prior to start-up. A seismic survey is not intended to replace the design or any of the established quality assurance activities. Rather, it serves as an additional verification process involving mainly visual inspection to ensure the plant is seismically robust. Any observations originating from such walkdowns are dispositioned and implemented as required prior to start-up of the unit.

3.1.2.2 Spent Fuel Integrity after DBE

The spent fuel bay (SFB) is seismically qualified. The cooling water supply to the SFB may be lost due to loss of electrical power to the cooling water pump. The decay heat from the spent fuel will be transferred to the SFB pool water by natural convection, as long as the fuel is submerged. The evaporation of water from the bays to the atmosphere will carry away some of the decay heat from the spent fuel slowly. The bay water temperature will gradually rise, despite emergency water make-up supplied to maintain normal water level in the bay.

Calculations show that it would take 11 hours for the bay water temperature to reach 49^{o}C and about 3 days before the bay water starts boiling. Given the sufficient time (days), prompt operator action should be successful in recovering the SFB pump operation to prevent boiling of the bay water. Therefore, the scenario of spent fuel dryout and damage is improbable.

3.1.3 Plant Compliance with its Current Licensing Basis

The plant was designed, constructed and licensed to operate taking into account the requirements of nuclear codes and standards, as well as best practice procedures applicable to the seismic qualification of safety related SSCs.

S. N. Nuclearelectrica S.A.
CNE Cernavoda

The goal of Cernavoda NPP is to preserve the original qualification and to provide evidence that all the qualified SSE meet the seismic qualification requirements for the entire station life.

Processes to ensure compliance with the plant-licensing basis have been implemented in the plant. This is an ongoing process, from the plant design to the end of service life, and plant ageing, modifications, repairs and refurbishment, equipment failures and replacements, and abnormal conditions are taken into account.

These processes ensure that all the plant activities that could impact safety, design or licensing basis (including those that could have an impact on the seismic qualification of SSCs are reviewed and/or assessed, the necessary actions are taken, and all documents affected are or will be updated:

- Assessment of the impact of the plant modifications (permanent or temporary) on the seismic qualification requirements of SSCs. This activity is managed through the Configuration Control Program and its package procedures;
- Ensuring that the SSC performance has been preserved by ongoing application of measures such as scheduled maintenance, testing and calibration and has been clearly documented through Maintenance Procedures and Seismic House Keeping Programs;
- Seismic Monitoring & Inspections to confirm the actual condition of seismic qualified SSC and its operability through Seismic Monitoring Program and Monitoring of Plant Buildings Behavior for site and structures;
- Surveillance of seismic qualified SSC and the analysis of the results to ensure that the SSCs are not affected by ageing process through Surveillance Program, Plant Life Management (PLiM);
- The assessment of the SSC failures and their impact on the seismic qualifications, including the necessary corrective actions/ improvements to preserve the seismic qualification through the Operating Experience (OPEX) Program;
- New regulatory requirements that could have an impact on seismic qualification of SSC are managed through the station process called “Register of Licensing Documentation and Tracking of CNCAN Action Items”. This process ensures that all license conditions and other CNCAN specific requirements (including those that could have an impact on seismic qualification) are identified, analyzed, translated into specific plant procedures and tracked for their status until implementation.

Besides these activities carried out in the plant that ensure the compliance with the current licensing basis, CNE Cernavoda performs a Periodical Safety Review (PSR) at regular intervals, typically of ten years, as per CNCAN norms, and International Atomic Energy Agency (IAEA) guidelines. PSR, as it is a comprehensive safety review of all important aspects of safety, includes also a review of the seismic qualification. CNE Cernavoda is currently conducting the first PSR for Unit 1. The interim results show that activities and procedures addressing equipment maintenance as per the design basis conditions are in agreement with the international best practices.

S. N. Nuclearelectrica S.A.
CNE Cernavoda

Specific compliance check already initiated by the licensee following Fukushima NPP Accident - WANO SOER 2011-02 Recommendation 4:

In order to meet the intention of World Association of Nuclear Operators (WANO) Significant Operating Experience Report (SOER) 2011-02 Requirements, the following preliminary steps have been performed:

- Reviewing the design requirements for Fire Protection against the effects of an earthquake;
- Identification of the vulnerable areas to earthquake induced fires;
- Identification of the key areas important to safety and, for this locations, assess the fire fighting capability of permanent and temporary equipment to extinguish fires after an earthquake;
- Identification of the mitigating actions or long-term strategies to ensure that post Safe Shutdown Earthquake fires can be extinguished.

The inspections results confirm the design robustness and a good material condition regarding the fire barrier preservation in the vital areas. No gaps have been found. The strategy and mitigation actions for fire suppression in the vital areas have been confirmed. The use of portable fire extinguisher located in the vicinity of seismically qualified equipment is efficient and can be used even by operating crew if a fire will occur anytime after a safe shutdown. As far as the combustible materials found is concerned, it is quite limited as per the design intent and that fire barriers are appropriate. The firefighting plans have also been validated. Minor follow-up actions are being implemented.

The following observations have been made specifically related to seismic induced flooding:

- For seismic induced flooding or concurrent flooding and seismic events the essential safety functions of reactor shutdown, containment isolation, reactor cooling and monitoring of critical safety parameters are ensured from the Secondary Control Area (SCA) that is seismically qualified and physically separated from internal flooding sources.

- Consequential to a DBE event the pumps representing the main hazard for internal flooding will stop as they, and their power supply sources are not seismically qualified and the plant control is transferred to SCA. Therefore, potential for seismic induced flooding propagation and impact is localized and has no impact on the vital areas/systems hosting the equipment qualified to perform the essential safety functions after an earthquake.

- Regarding the potential for external flooding the areas of interest regarding a flood induced by earthquake is represented by the potential tsunami waves. There has been historical evidence that earthquakes occurred in the Black Sea and generated tsunami waves propagated in the vicinity of the Black Sea side. However, Cernavoda NPP is located 60 km far from the seaside. Based on IAEA Safety Guide DS417, no specific further investigations and studies need to be performed to analyze the tsunami hazard for the plant site provided that the site is located in an area that shows no evidence of past occurrences of tsunamis affecting the site, and that the plant is located:

    - More than 10 km from the sea or ocean shoreline, or more than 1 km from a lake or fjord shoreline, as appropriate; or
    - More than 50 m elevation from the mean water level.

Considering the above there was no further area for inspection other than those performed as part of WANO SOER 2011-02.

3.1.4 Evaluation of Seismic Margins

Stress Test, as defined by WENRA, is "*a targeted reassessment of safety margins for an existing plant in the light of the events which occurred at Fukushima.*" The stress tests need not be applied to the entire plant but only to those SSCs, which are required to support the fundamental safety functions of the plant during a seismic event or anther accident condition. Such a category of SSCs is classified as those belonging to the Success Path since these SSCs are required for safe shutdown, fuel cooling, containment and monitoring of the reactor core. For seismic design, the concern is the safety margin of the plant over and above the design basis conditions called Beyond Design Basis Earthquake (BDBE) conditions. For the stress tests, a reasonably high level of earthquake beyond the design basis earthquake level will be selected to challenge the plant. All SSCs in the Success Path will be evaluated to withstand this reasonably high value of the earthquake level with an acceptable margin. Such a level of earthquake is called the Review Level Earthquake (RLE).

3.1.4.1 Seismic Margin Evaluation Methodology & Success Path

The seismic Stress Tests margin evaluation contains the following procedures:

1. Selection of a Review Level Earthquake (RLE)

Cernavoda Unit 1 and Unit 2 are qualified to a 0.2g CSA DBE GRS. The 0.2g PGA has a return period of 1000 years. Several comprehensive geological investigations of the Cernavoda site have concluded that:

- The site is geologically stable.
- The site is free of any faults.

Based on the recommendations in the NUREG CR-0098, a Ground Motion Response Spectrum (GMRS) with a PGA of 0.33g is selected as the Review Level Earthquake (RLE) Response Spectra as shown in Fig. 3.1-2 is used to evaluate the seismic margins of the required SSCs. At a frequency of occurrence not higher than once in 10,000 years, the PGA is 165 % of the design level corresponding to the RLE.

2. Selection of a Success Path

A *robust* Success Path was selected for careful review. The SSCs in the path were evaluated against the RLE, making use of the existing High Confidence Low Probability of Failure (HCLPF) values from the referenced documents or performing additional calculations where these values are not available or applicable. A Success Path is expected to have a collective capacity to resist an earthquake with ground acceleration sufficiently higher than the RLE at 0.33 g.

3. Plant Walkdowns

Plant walkdowns were conducted to verify robustness of the components and to verify against any adverse effects of seismic interactions including seismic initiated internal flood. Data gathered from the walkdowns for each component in the Success Path were reviewed and used in the determination of the seismic capacity of the component. Existing data, past analyses, engineering judgment, etc, were also be used as much as possible to substantiate the robustness.

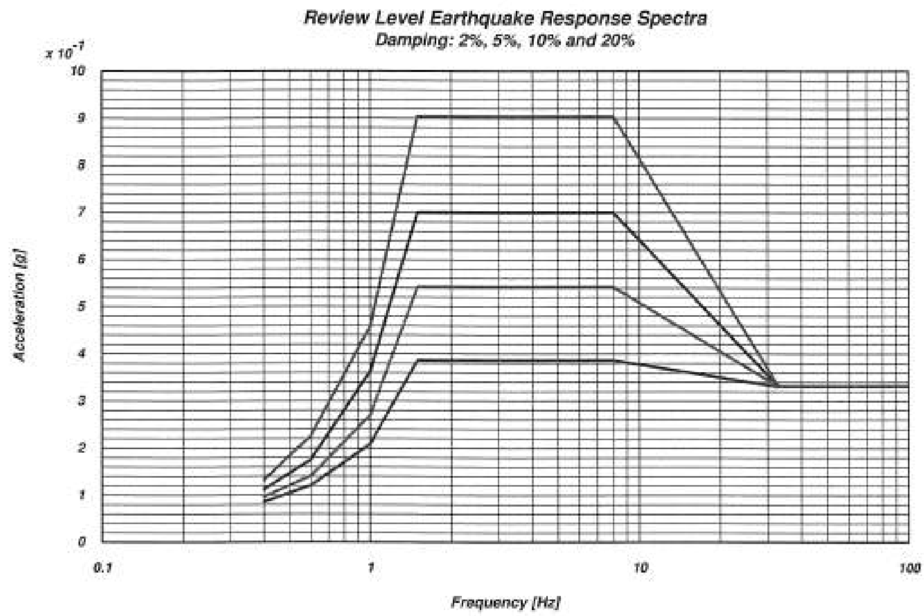

Figure 3.1-2

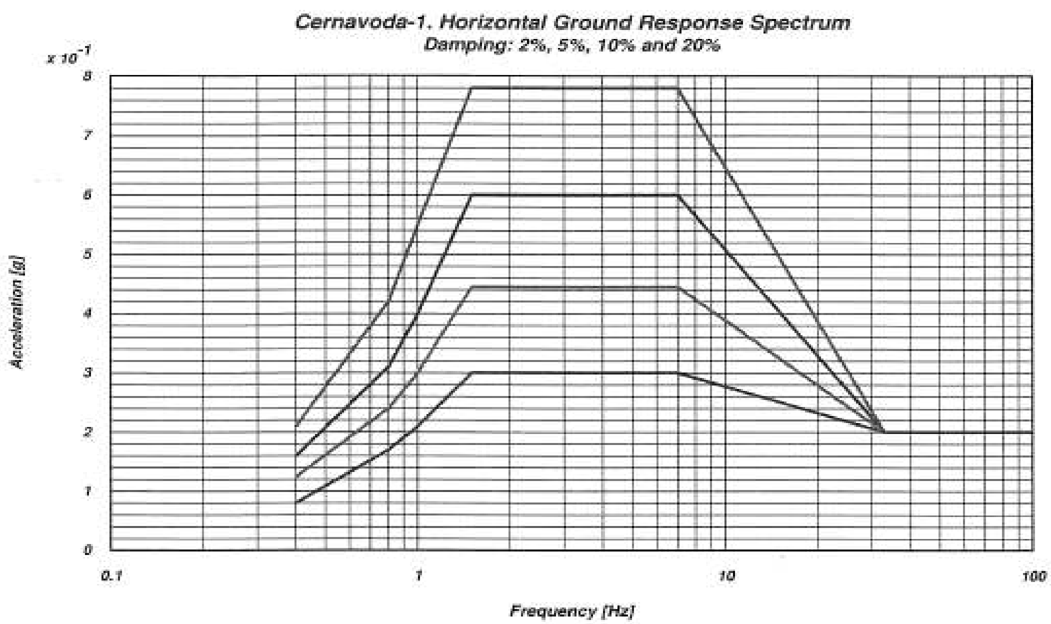

Figure 3.1-3

4. Re-assessment of Seismic Capacity

The High Confidence Low Probability of Failure (HCLPF) capacities were used to screen out robust SSCs based on high HCLPF capacities. The targeted level of 0.4g PGA was used to screen out SSCs, thus giving an additional margin above the RLE of 0.33 g.

The RLE was used to calculate the seismic demand for those SSCs that had not been screened-out. Seismic capacity of the 'screened-in SSCs' was calculated based on 'fitness-for service' considerations. The ability to resist seismic acceleration was calculated as Robustness Capacity in terms of PGA.

Ratio of the seismic capacity to the seismic demand gives a measure of robustness:

$$Robustness\ Capacity = \frac{Seismic\ Capacity}{(Seismic\ Demand)_{RLE}} \times PGA_{RLE}$$

Here Seismic Capacity implies net seismic load that the component can sustain in addition to operational loads, which could be present during an earthquake.

5. Generation of RLE Floor Response Spectra

Floor Response Spectra (FRS) were generated using the RLE as required.

6. Investigation of Seismic Cliff-Edge Effect

A cliff-edge effect, referred to as an abrupt catastrophic collapse of a structure without warning, was assessed for applicable SSCs.

7. Capacity of Equipment Qualified by Test

For equipment in the Success Path qualified by test, the Required Response Spectrum (RRS) and the Test Response Spectrum (TRS) were reviewed. If necessary, a more realistic RRS was regenerated.

8. Design Modifications

Design modifications (potential safety improvements), if applicable, were identified to add robustness to the Success Path and/or to remove any adverse effects observed during the walkdowns.

9. Procedure

The above seismic margin evaluation procedure is illustrated in the attached flowchart (Figure 3.1-4).

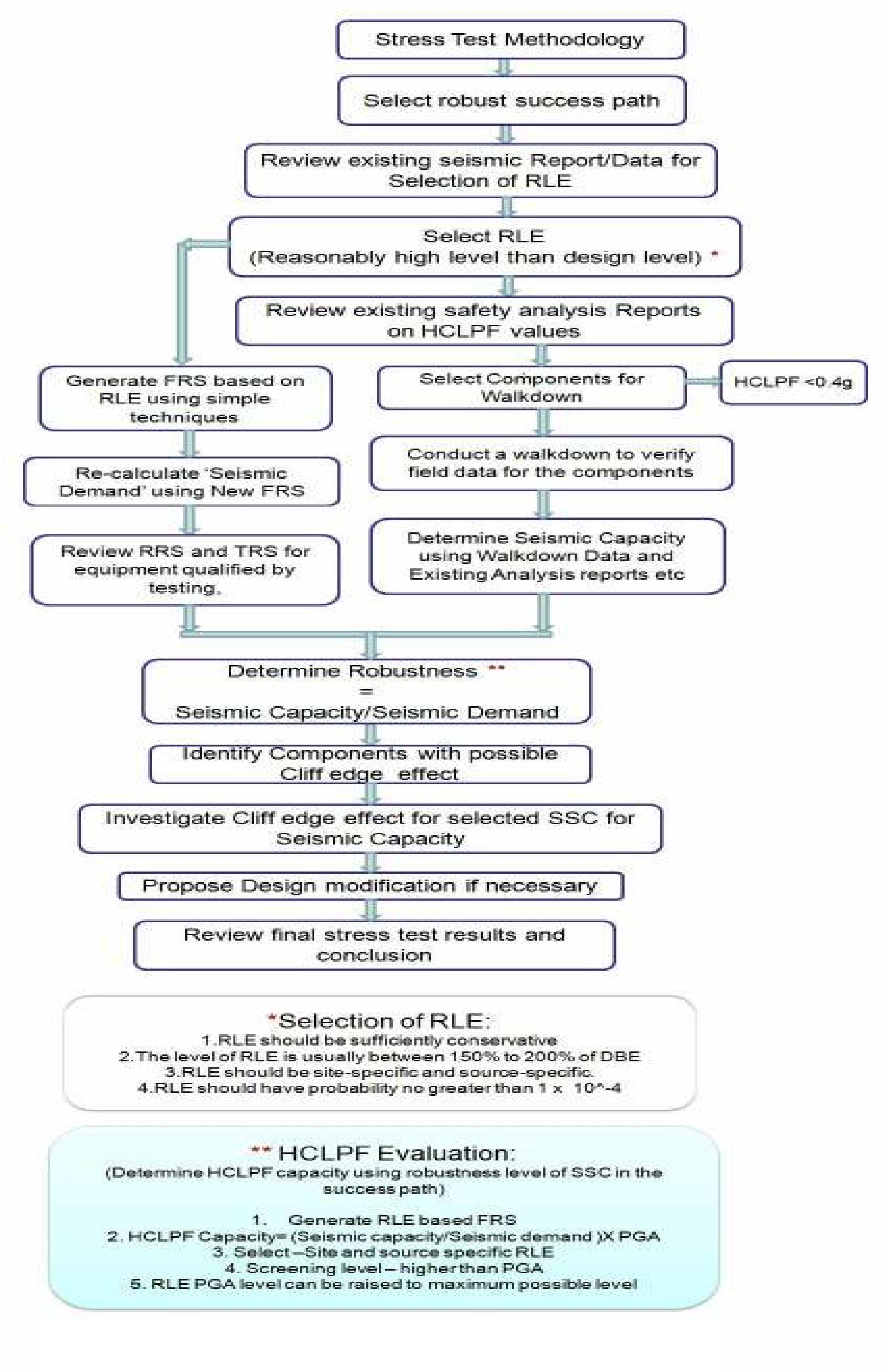
Stress Test Methodology
Select robust success path
Review existing seismic Report/Data for Selection of RLE
Select RLE (Reasonably high level than design level) *
Review existing safety analysis Reports on HCLPF values
Generate FRS based on RLE using simple techniques
Select Components for Walkdown
HCLPF <0.4g
Re-calculate 'Seismic Demand' using New FRS
Conduct a walkdown to verify field data for the components
Review RRS and TRS for equipment qualified by testing.
Determine Seismic Capacity using Walkdown Data and Existing Analysis reports etc
Determine Robustness ** = Seismic Capacity/Seismic Demand
Identify Components with possible Cliff edge effect
Investigate Cliff edge effect for selected SSC for Seismic Capacity
Propose Design modification if necessary
Review final stress test results and conclusion
*Selection of RLE:
1.RLE should be sufficiently conservative
2.The level of RLE is usually between 150% to 200% of DBE
3.RLE should be site-specific and source-specific.
4.RLE should have probability no greater than 1 x 10^-4
** HCLPF Evaluation:
(Determine HCLPF capacity using robustness level of SSC in the success path)
1. Generate RLE based FRS
2. HCLPF Capacity= (Seismic capacity/Seismic demand)X PGA
3. Select – Site and source specific RLE
4. Screening level – higher than PGA
5. RLE PGA level can be raised to maximum possible level

Figure 3.1-4

3.1.4.2 Selection of Success Path

The success path considered for evaluation of seismic margins of SSCs was selected based on the following requirements for the Success path for seismic induced Station Blackout (SBO) and maintaining heat sink:

- The ability to shut the reactor down and maintain it in a safe shutdown condition.
- The ability to maintain a barrier to limit the release of radioactive material.
- The ability to remove decay heat.
- The ability to perform essential safety-related control and monitoring functions.

Evaluation of SSCs

The SSCs in the defined success path were evaluated against the selected RLE. Field walkdowns were done as necessary for SSCs requiring further screening to assess actual conditions. Based on the review of existing calculations and walkdown observations, the evaluations showed that all SSCs in the success path satisfy the established criteria of 0.4g which is 200% DBE for the plant (0.2g).

3.1.5 Flooding due to Earthquakes Exceeding Design Basis

Based on a systematic overview of the Cernavoda NPP Site and Plant, the following potential sources of seismic induced flood have been considered:

- Falling of Santa Maria bridge
- Black Sea Tsunami
- Danube dam (close to Drobeta Turnu Severin)
- Internal Plant Flooding

3.1.5.1 Evaluation of potential flooding event due to Santa Maria bridge fall following severe earthquake

Evaluation of potential event affecting NPP site, due to fall of bridge, shows possibility for an area in front of the Screen House to be flooded by about 30 cm thickness water path. Flooded area does not impact on NPP safety functions.

This evaluation is very conservative. Actually, followings considerations are to be made:

- Total length of bridge is 170 m. Evaluation of potential energy due to its fall takes into account the whole mass, but effective portion of bridge upon channel level is 80 m length;
- Water energy loss exists, due to presence on channel of bends, branches and due to impact of bridge on water;
- The amount of basin water postulated to be considered for the flooding is assumed concentrated at the reference elevation of 16.35 mBSL. A more realistic assumption should consider a water distribution along the elevation axis; the portion of water between the intake nominal level and the reference value of 16.35 mBSL would not be credited so that the effective available mass for flooding would half.

By above considerations, fall of bridge does not represent potential flooding risk for the NPP.

3.1.5.2 Evaluation of potential flooding event due to Black Sea tsunami following earthquake

Distance between Cernavoda NPP site and Black Sea coast is about 60km. Evaluation of potential flooding affecting NPP site, due to water path as consequence of Black Sea Tsunami event, gives possibility (as extreme conservative way) to occur for about 168 m Run-up wave at the Black Sea coast. The evaluation was carried out according to the work of Jack G. Hills and Charles L. Mader [Livermore Workshop 1995]

The historical Run-up waves registered, following earthquake events are of 31 meters. But additional consideration is that Cernavoda site is located in an area showing no evidence of past occurrences of tsunami.

By above considerations, a Black Sea tsunami event will not flood the NPP site. This result is in accordance with IAEA Safety Guide DS 417 which screens out tsunami induced flood for a plant located at more than 10 km from the costal shoreline or more than 1 km from a lake or fjord shoreline or 50 m above a sea, lake or fjord.

3.1.5.3 Danube Dam (close to Drobeta Turnu Severin)

Evaluation of maximum water level has been performed by overlapping the severe failure of the Portile de Fier hydro-electrical plant located 600 km upstream of Cernavoda, to a Danube high water level. The results have concluded that the impact on Cernavoda site is negligible and within the normal fluctuations of the Danube level.

3.1.5.4 Internal Flooding: Beyond Design Earthquake Effect on the NPP Internal Structure and Following Potential Flooding Event

Areas of the plant considered for assessment are listed below:

- Reactor Building;
  (Note that reactor building did not need to be included in this assessment since all systems and components used in the success path necessary for safe shutdown, cooldown and monitoring functions are already designed and qualified to handle these scenarios.)
- Emergency Power Supply (EPS)/Secondary Control Area (SCA);
- Emergency Water System (EWS)

No relevant internal water source exist by design in the SCA /EPS/ EWS buildings. Normally only some fire water systems pipes are present in this area. After a beyond design DBE, the fire water system pumps will stop and if the fire water pipe line break occurs, only a small amount of water will flow inside EPS/SCA, which will not affect the Group 2 system operation.

3.1.6 Conclusions

Based on the assessments completed as mentioned in the previous sections, it is concluded that all components in the Success Path satisfy the established seismic criteria of 0.4g which is 200% DBE for the plant design basis (0.2g) and hence have sufficient margins to meet challenges due to Beyond Design Basis Earthquakes.

The possibility of external flooding induced by a severe earthquake was analyzed and it was concluded it is not a credible event. A severe earthquake cannot induce flooding either by tsunami waves or by dam structure failure. Therefore, the seismic induced flood is not a concern for Cernavoda site.

Since the selected success path remains unaffected because of the SSCs capability to withstand higher than the design basis earthquake, the ability of the plant to continue providing the designed safety functions, per the original design philosophy, is not affected as a result of either a Beyond Design Basis Earthquake or flooding resulting from such an initiating event.

3.2 Flooding

3.2.1 Design Basis Considerations and Provisions

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.

A bypass channel of Danube-Black Sea Channel (DBSC) borders the site on the Southeast and Cismelei Valley on the Northeast. Cooling water for the plant is taken from a branch of Danube River, Intake Channel and Distribution Basin.

Figure 3.2-1 shows the site layout elevations, the relative locations of the 5 units of Cernavoda NPP (Units 1 and 2 already operating, and the on-hold partially completed Units 3-5), Cismelei Valley, Danube River, the Danube-Black Sea Channel, Intake Channel and Distribution Basin.

Water levels of various sources of water around Cernavoda NPP site are as shown in the Table 3.2-1:

Table 3.2-1 Significant elevations for Cernavoda NPP site

Significant Locations	Elevation [mBSL]
Cismelei Valley bottom (at discharge)	+9.00
Danube – Black Sea Channel water average level (in-between Cernavoda and Agigea water lockers)	+7.50
Cernavoda Water Lock top elevation	+13.50
Black Sea level	- 0.50
EWS pumps suction pipe axis	+0.50

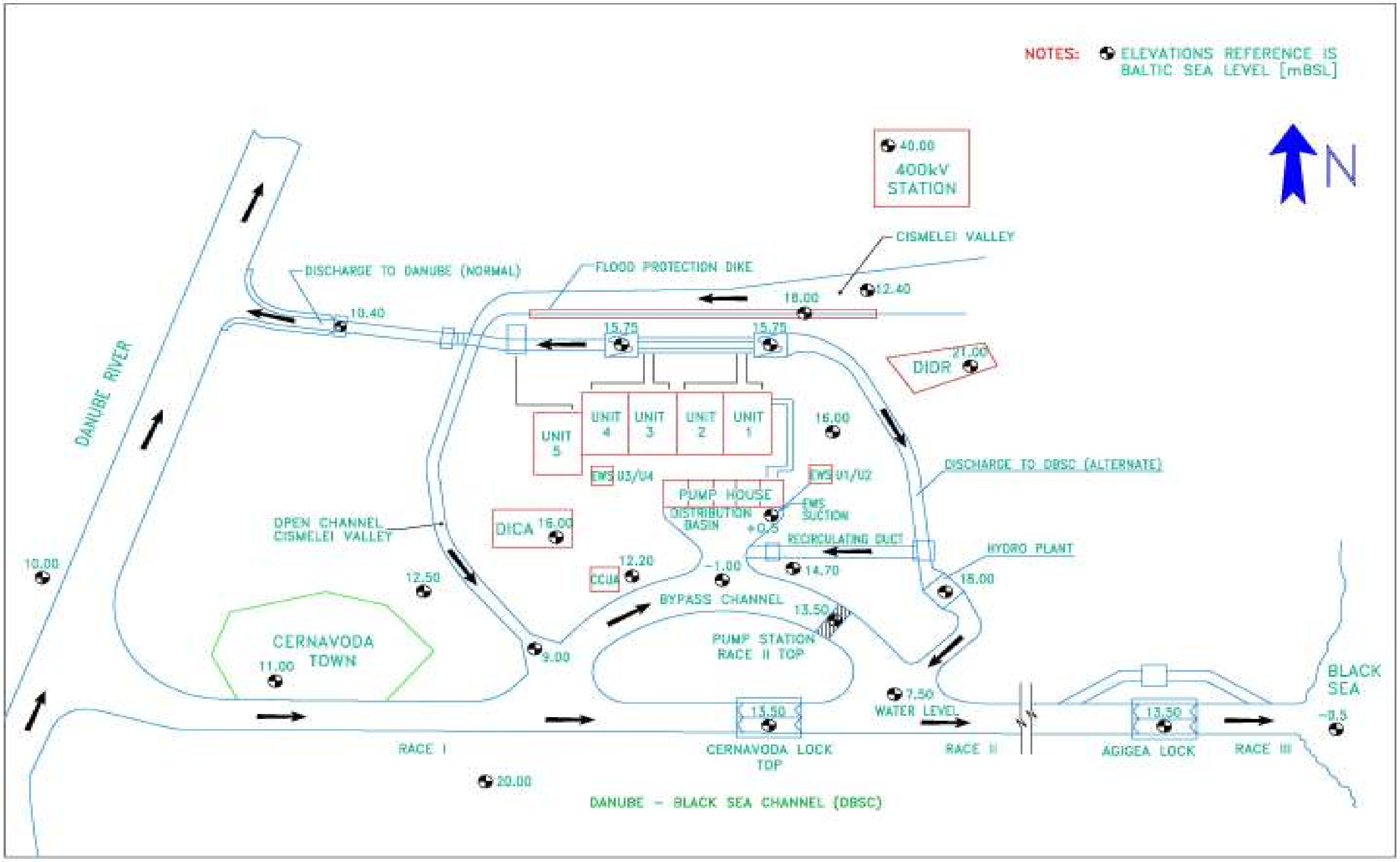
NOTES: ELEVATIONS REFERENCE IS BALTIC SEA LEVEL [mBSL]
N
40.00
400kV STATION
CISMELEI VALLEY
DISCHARGE TO DANUBE (NORMAL)
FLOOD PROTECTION DIKE
12.40
18.00
10.40
15.75
15.75
DIDR
21.00
DANUBE RIVER
UNIT 4
UNIT 3
UNIT 2
UNIT 1
UNIT 5
16.00
EWS U3/U4
EWS U1/U2
DISCHARGE TO DBSC (ALTERNATE)
PUMP HOUSE
DISTRIBUTION BASIN
EWS SUCTION
+0.5
OPEN CHANNEL CISMELEI VALLEY
DICA
16.00
RECIRCULATING DUCT
HYDRO PLANT
10.00
12.50
CCUA
12.20
-1.00
14.70
18.00
BYPASS CHANNEL
13.50
PUMP STATION RACE II TOP
CERNAVODA TOWN
11.00
9.00
7.50
WATER LEVEL
BLACK SEA
13.50
13.50
-0.5
RACE I
CERNAVODA LOCK TOP
RACE II
AGIGEA LOCK
RACE III
20.00
DANUBE - BLACK SEA CHANNEL (DBSC)

Figure 3.2-1

Various elevations (referenced to the meters Baltic Sea Level – mBSL) comprising the design basis related to the plant and main watercourses near Cernavoda NPP are summarized in the Table 3.2 -2.

3.2.1.1 Level of the Design Basis Flood (DBF)

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 analyzed 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 maximum design water level of **+15.90 mBSL** was obtained by adding the maximum theoretical water level with confidence level 0.01%. The general 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 hydro-technical structures at Calarasi nor Macin 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 return period of 1 in 10000 years for Cernavoda NPP is evaluated to be **+14.13 mBSL.** This was later confirmed by actual results..

Therefore, the Design Basis Flood level for Cernavoda NPP established as:

DBF = +14.13 mBSL

This DBF value is supported by the recent studies which update historical data and the most recent analyses. The top elevation +13.50 mBSL of Cernavoda water lock is below DBF level +14.13 mBSL and well below Cernavoda platform +16.00 mBSL elevation. This means that the top elevation **+13.50 mBSL** of Cernavoda water lock is below DBF level **+14.13 mBSL** and well below the Cernavoda NPP platform **+16.00 mBSL** elevation. This also shows that there is an unobstructed path for water to flow towards the surrounding Cernavoda territory lowlands, which are at **+10.00 mBSL** elevation and eventually towards the Black Sea.

Table 3.2.2 Cernavoda NPP Elevation Relative to Water Levels

Significant Locations	Elevation [mBSL]
Cernavoda NPP platform	+16.00
Cernavoda NPP buildings ground floor	+16.30
Cismelei Valley bottom (at discharge)	+9.00
Danube – Black Sea Channel water average level (in-between Cernavoda and Agigea water lockers)	+7.50
Cernavoda Water Lock top elevation	+13.50
Black Sea level	- 0.50
EWS pumps suction pipe axis	+0.50

3.2.1.2 Assessment of adequacy of design basis Flood Levels

Assessment of adequacy of design basis flood levels

Hydro-plant dam failure

Evaluation of the maximum water level also considered the severe failure of the Portile de Fier hydro-electrical plant located 600 km upstream of Cernavoda, resulting in a high-flood wave. The results concluded that the impact on the Cernavoda site would be negligible and within the normal fluctuation of the Danube River level.

Tsunami induced flooding

The Cernavoda NPP site is located at 60 km from the Black Sea coast and adjacent to the Danube River, at +16.50 m above the Black Sea level (compared to the Baltic Sea, Black Sea level is at -0.5 mBSL).

Based on the IAEA safety guidelines, no specific further investigations and studies need to be performed to analyze the tsunami hazard for the plant site (seismic induced external flooding), since that the site is located in an area that shows no evidence of past occurrences of tsunamis, and is located:

- At more than 10 km from the sea or ocean shoreline, or more than 1 km from a lake or fjord shoreline, as appropriate; or
- At more than 50 m elevation from the mean water level.

The conclusion that a tsunami at Cernavoda site is not credible is reached by engineering judgment based on relevant IAEA guidelines.

Even though the guidelines allow this event to be screened out, the potential for generation of tsunami in the Black Sea was evaluated and results show that extreme waves which could be generated are lower than 10 m high. The evaluation showed that the wave would not propagate past the Agigea lock, which is +13.5 mBSL high.

3.2.1.3 Danube Maximum Flood levels

Table 3.2-3 presents below the calculated Danube River maximum annual level at Cernavoda:

Table 3.2-3 Cernavoda maximum Danube water level

Probability of occurrence (%)	**1**	**0.1**	**0.01**
Annual Max. level [mBSL]	12.10	13.03	13.75

The DBF was calculated by adding a correction factor to the level corresponding to 0.01% probability of occurrence. The DBF is calculated to be +14.13 mBSL.

The DBF calculation is confirmed by more recent data and studies as described below.

Figure 3.2-2-presents recorded data from 1961 – 2011 for Danube water flow at Cernavoda, the historical maximum flow of **7000 m^3/s** corresponding to elevation **11.72 mBSL** as recorded in year 2006 year.

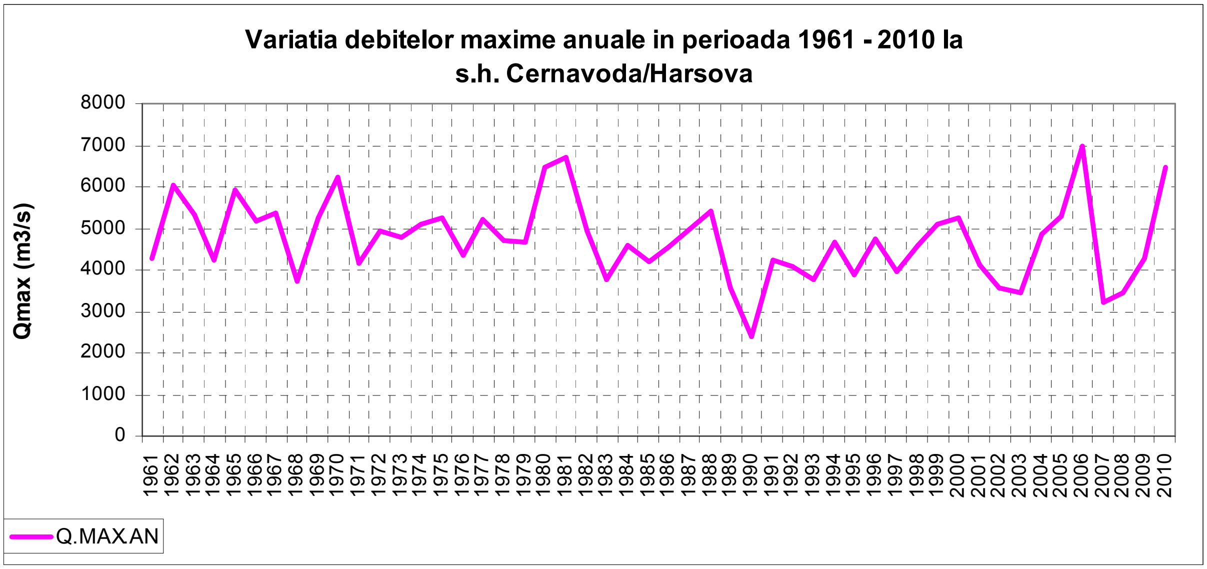

Figure 3.2-2 Yearly maximum flow variation between 1961 - 2010 at Cernavoda/Harsova hydrostation

The modern tool of Digital Topographic Model (DTM) was used 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 the methodology used in European project "Danube Flood Risk" SEE EoI/A/077/2.1/X,2008-2012 Stakeholder oriented flood risk assessment for the Danube flood plains, South-East Europe Transnational Cooperation Program.

3.2.1.4 Flooding due to rainfall on catchments area

One natural valley (Cismelei Valley) captures rainfall over an area of 22.2 km^2 around the Northeast plant territory and discharges the water into the bypass channel.

The discharge capacity of the valley is sized for coincident **DBF = +14.13 mBSL** and intense rainfall resulting in maximum flow **Q= 458 m^3/s**.

3.2.1.5 Flooding due to rainfall on the Cernavoda site platform

The effect of rainfall inside the Cernavoda site perimeter was calculated according to the national regulations for the frequencies, intensities and duration for the maximum rainfall. The values obtained from the records of neighboring Meteorological Station Fetesti (1943 - 1985) and Medgidia (1946 - 1986) were statistically processed and extrapolated till 1901 to determine the extreme meteorological data. The site main drainage header includes drains from 5 units and was sized using the regional rainfall maps and correspond to an hourly maximum rainfall of 97.2 l/m^2

Calculations were performed using the Digital Topographic Model (DTM) of Cernavoda NPP platform.

Even in case of rainfall one order of magnitude greater than the design rainfall, the maximum water height of 20 cm is accumulated on site mainly on pathways.

To compare the design against actual measurements of rainfall it has to be mentioned that the **hourly** maximum quantity of rainfall **recorded at Cernavoda was 47.3 l/m^2** (July 2010). This shows that the site drainage system capacity (97.2 l/m^2) is more than double the greatest **hourly** recorded rainfall at Cernavoda during 1986-2010.

For reference, **the maximum rainfall recorded in Cernavoda in 24 hours was 120.5 l/m^2** (July 2010); the maximum rainfalls recorded in 24 hours in Romania were **262 l/m^2**(July 1934 in Deva) and **224 l/m^2**, (July 1999 in Drobeta Turnu Severin).

The historical maximum rainfall at the nearest meteorological stations to Cernavoda, **hourly** recorded are **97.2 l/m^2** (Fetesti 1994), **70.9 l/m^2** (Medgidia 1974) and **44.2 l/m^2** (Harsova 1971).

3.2.2 Provisions to Protect the Plant against Flooding

3.2.2.1 Key SSC's required for achieving safe shutdown state

According to Section 3.2.1 the DBF level has been determined as +14.13 mBSL. Since the plant platform is located at +16.00 mBSL elevation and as supported by the historic recorded data, it is concluded that all SSCs will survive a DBF level generated by external flood.

The SSCs required to support various configurations of the plant are described in Table 3.2-4 below:

Table 3.2-4 Safety Related Systems Separation into Two Groups

REQUIRED CAPABILITY	Normal Shutdown	GROUP 1	GROUP 2
(a) Shutdown Capability	- RRS - Class IV Power - Instrument Air (Normal Distribution)	- SDS#1 - Class III, II, I Power - Instrument Air (Normal Distribution)	- SDS#2
(b) Decay Heat removal Capability	- Steam to Condenser (CSDV) - Class IV Power - Main Feedwater System and Service Water System (RSW & RCW) - SDCS - Instrument Air (Normal Distribution)	- Steam Reject to Atmosphere (ASDV, MSSV) - Class III, II, I Power - Auxiliary Feedwater System and Service Water System (RSW & RCW) - ECCS - SDCS - Instrument Air (Normal Distribution)	- Steam Reject to Atmosphere (MSSV) - Emergency Power Supply System - BMW / Emergency Water Supply System - Instrument Air (Local Air Reservoirs)
(c) Capability to Limit Release	Containment	Containment (LACs)	Containment (Isolation valves, Airlocks, Dousing)
(d) Monitoring Capability	- Main Control Room - Class II, I Power	- Main Control Room - Class II, I Power	- Secondary Control Area - Emergency Power Supply System

Note:	**Symbols:**
BMW:	Boiler Make-up Water
CSDV:	Condenser Steam Discharge Valves
ECCS:	Emergency Core Cooling System
MSSVs:	Main Steam Safety Valves
RCW:	Recirculating Cooling Water
RRS:	Reactor Regulating System
RSW:	Raw Service Water
SDCS:	Shutdown Cooling System

3.2.2.2 Grouping and Separation based on Safety Functions

According to the Safety Design Guide requirements for safety systems and structures location and separation, the required safety functions are carried out by the following safety related systems:

- **Special safety systems**. (SDS#1, SDS#2, ECCS, Containment);
- **Safety support systems**. These systems provide services to the special safety systems and may also perform a process function in addition to their safety function.
- **Safety related process systems**. The primary function of these systems is to maintain the power production capability of the plant. In addition, a number of process systems perform each of the safety functions during normal operation of the plant and are designated as being safety related.

Separation is required such that sufficient equipment and systems remain available to perform the safety functions following each postulated event, i.e., loss of a safety function in a group must not affect the ability of the other group to perform the same safety function.

According to grouping and separation requirements stated by the Safety Design Guides, the buildings are also divided into Group 1 and Group 2 as follows:

- Group 1 consists of the following buildings:

    - Turbine Building which protects the Service Building's safety related systems against the consequences of possible failures in the Turbine Building and protects the Turbine Building's safety related systems against external events as well as against the effects of events that could occur inside the building (steam line break or fire).
    - Service Building including the Main Control Room, which protects the main control room operators against the effects of external events and environmental conditions.
    - Standby Generators structure, which protects the safety related systems against the effects of external events.
    - High Pressure ECCS structure which protects the system against the effects of external events and environmental conditions.

- Group 2 consists of the following buildings:

    - Secondary control area structure, which protects the safety related systems that provide station control and monitoring in case of Group 1 system unavailability or in case of main control room impairment.
    - The structures dedicated to emergency water supply and emergency power supply, which protect the systems against the effects of external events and environmental conditions.

3.2.2.3 Main Design Provisions to Protect the Site against External Flooding

The elevation of the site was designed to accommodate flooding level that could be reached in the extreme case of the upstream dam failure; however, the plans to build the two dams were not implemented (This minimizes the likelihood of flooding even further). Therefore the elevation of +16.00 mBSL for the Cernavoda NPP platform provides additional margin to the calculated maximum flooding level.

Since the DBF of +14.13 mBSL is more than 2 m below the measured buildings minimum elevation of +16.24 mBSL, no specific provisions are required for flood protection, in addition to the regular site drainage system and the dike with upper elevation +18.00 mBSL raised on Cismelei Valley.

The roads and the general ground elevation of the plant are designed to accommodate drainage of the maximum rainfalls and from concrete platform washing towards the discharge openings of the collecting channels. These channels as well as the remainder of the on-site drainage systems are sized for the maximum design flows.

Electrical power cables that are located in trenches outside buildings, potentially exposed to flooding from rainfalls, are made of one segment and resistant for water submergence since they are insulated.

3.2.2.4 Main operating provisions

<u>Hydro-technical Structures Monitoring</u>

The follow-up of the behavior of the Cismelei Valley channel covering status of channel flowing section, bank slopes and the dam, is performed monthly by visual inspection. Periodic maintenance activities and repair of the observed deficiencies are performed as required.

Topographical measurements are performed twice per year, using the reference (fixed) points defined in the design stage, in order to identify potential horizontal and vertical movements of the structures and buildings.

According to the monitoring results there are no developing movements which confirm stability of the plant structures and buildings.

Internal inspection of the site drainage system is periodically performed as part of Plant Preventive Maintenance Program.

<u>Flood Alerting System</u>

As a preventive measure to protect against potential external flooding events there is in place a national forecast and warning system.

This system provides daily forecasts and warnings, making use of water level thresholds that are developed for specific locations along important rivers in Romania.

For Cernavoda the relevant information related to warning code thresholds, recorded historical level and estimated return period in relation with Danube water level / elevation, is presented in Table 3.2-5.

Table 3.2-5 Danube River high level and warning code thresholds for Cernavoda

Description	Elevation [mBSL]
ATENTION code CP	+9.36
FLOODING code CF	+10.36
DANGER code CA	+10.86
Historical maximum	+11.72
1%	+11.83
0.1%	+12.73
0.01%	+13.53

It should be mentioned that these warning thresholds are established by the state authorities in order to protect the Cernavoda local community and are not related to Cernavoda NPP operation, but they provide early warnings compared to DBF.

Based on the recorded Danube water level at Cernavoda, it has been concluded that it has exceeded the danger code limit of +10.86 mBSL four times in 40 years, the maximum recorded value is +11.72 mBSL. The danger code level is more than 3 m below the DBF level of +14.13 mBSL for Cernavoda NPP.

3.2.3 Plant Compliance with its Current Licensing Basis

The Cernavoda NPP site has been selected and plant has been designed, constructed and licensed to operate taking into account the requirements of nuclear codes and standards, as well as best practice procedures applicable to cope with all the possible flooding hazards.

One of the Cernavoda NPP safety goals is to maintain the most suitable protection against flooding and to provide evidence that all required SSCs will preserve their safety function for the entire station life with due consideration being paid to aging and obsolescence issues of SSCs.

Arrangements to ensure compliance with the licensing basis that involves generating, documenting and maintaining evidence that SSCs (including those that are required to cope with a flooding hazard) can accomplish their safety function during their installed service life have been implemented in the plant. This is an ongoing process, from the plant design to the end of service life, and plant ageing, modifications, repairs and refurbishment, equipment failures and replacements, and abnormal conditions are taken into account.

These arrangements ensure that all the plant activities that could impact safety, design or licensing basis, including the impact from the flooding hazard point of view, are reviewed/ assessed, the necessary actions are taken, and all documents affected are or will be updated:

- As per the Configuration Control Program, the assessment of the plant modifications (permanent or temporary) take the flooding hazard into account in order to ensure the capability of the SSCs to maintain their safety function.
- Ensuring that the SSCs performance has been preserved by ongoing application of measures such as scheduled maintenance, testing and calibration and has been clearly documented (Maintenance Program, Testing Program);
- Inspections to confirm the actual condition of SSCs (Inspection Program, Monitoring Program for site and structures). Specifically for structures and buildings, a monitoring program is

performed twice per year with support from specialized contractors and includes performance of visual inspections, topographic measurements and bathymetric measurements.

- Surveillance of the SSCs (including those that are required to cope with a flooding hazard) and the analysis of the results to ensure that the SSCs are not affected by ageing process (Surveillance Program, PLiM);
- The assessment of the SSCs failures and their impact on the capability to maintain their function to cope with a flooding hazard, including the necessary corrective actions/ improvements to preserve their safety function (OPEX Program);
- New regulatory requirements, including those that could be related to a flooding hazard are managed through the station process called "Register of Licensing Documentation and Tracking of CNCAN Action Items".

Besides these activities performs ensure compliance with the current licensing basis, Cernavoda NPP a Periodical Safety Review (PSR) at regular intervals, typically of ten years as per CNCAN Norms and IAEA guidelines. PSR, as it is a comprehensive safety review of all important aspects of safety, include also a review of External Hazards including flooding. Cernavoda NPP is currently conducting the first PSR for Unit 1.

3.2.3.1 Cernavoda NPP process to ensure that off-site mobile equipment / supplies considered in emergency procedures are available and remain fit for duty

The administrative aspects related to crew response preparedness, including measures taken to support availability of essential equipment are addressed in Section 3.7.

3.2.3.2 Cernavoda NPP specific compliance check already initiated by the licensee following Fukushima accident

In view of Institute of Nuclear Plant Operators INPO ER 11-1 and WANO SOER 2011-2 Recommendation #3 requirements, walk down and inspections were performed at both Unit 1 and Unit 2 by teams from technical, operations, safety and licensing departments using general arrangement drawings and other plant information resources, including Flood Equipment Lists (safety related equipment location / flood areas) developed in support to internal flood and High Energy Live Break (HELB) events PSA.

The locations inspected included the Secondary Control Area and EPS Building, HP/ECCS Building, EWS House, Screen House, Pump House (P/H), Integrated Building (T/B), K-L Gap, Service Building (S/B), Chiller Building, Class III Standby Diesel Generators Building and the on-site drainage system used for mitigation of potential external flooding induced by local intense precipitations. There were no deviations from the design basis found. This conclusion is confirmed by an independent review performed by Ansaldo in support of the present stress test report.

3.2.4 EVALUATION OF FLOODING MARGINS

The Cernavoda plant can withstand credible external floods without compromising fuel cooling. This is achieved by:

1. Designing the platform at a high elevation (+16.00 mBSL) compared with the highest Danube River level;
2. Protecting the site from flooding from the Cismelei Valley using a dike elevated at +18.00 mBSL;
3. Designing the buildings ground elevation at +16.24 mBSL, 24 cm higher than the site platform with ground sloping away from the buildings;

4. Designing the site pluvial drainage system for maximum rainfall rate and with sufficient margin;
5. Designing multiple independent heat sinks and power supplies to provide defence-in-depth against system failures Ref.: Sections 3.4, 3.5, 3.6 and 3.7.

On the basis of the flooding assessments reported in Section 3.2.1 & 3.2.2, the plant buildings will not flood since the water level can't reach +16.24 mBSL elevation due to any flooding scenario.

The following Table 3.2-6 summarizes the safety margins on the design basis parameter values considering the source of external flooding hazard identified.

Table 3.2-6 External Flooding Margin Summary

Source	**Design Basis**	**Protection Level based on the design provisions**	**Margin**
Danube River high level	+14.13 mBSL	+16.24 mBSL	+2.11 m
Heavy rainfall around the plant site coincident with Danube River high level	+17.5 mBSL in Cismelei Valley drainage channel	+18.00 mBSL (dike elevation protection against discharge from Cismelei Valley)	+0.5 m
Heavy rainfall on the plant site	97.2 $l/m^2/h$ (Drainage system design basis – this magnitude of rainfall can be removed by the drainage system without causing any accumulation of water level)	> 10 times design basis (972 $l/m^2/h$) (The maximum increase in water height on platform is about 20cm, less than 24 cm which represent the minimum height above buildings ground floor)	> 10 times design basis (972 $l/m^2/h$) (The maximum increase in water height on platform is about 20cm, less than 24 cm which represent the minimum height above buildings ground floor)
Dam failure (Portile de Fier)	Screened out based on the analysis		
Tsunami	Not Credible due to the long distance from the Black Sea		

These results show that there is significant margin to flooding of the plant buildings by external events. If these margins are exceeded, fuel cooling is assured because there are passive means to keep the fuel cool that do not rely on equipment at low elevations nor electrical power. This is gravity feed from the dousing tank to the boilers via the BMW system, with PHT flow driven by thermosyphoning. Section 3.7 of this report describes this heat sink and shows that there will be at least 23 hours of passive cooling available. In reality, the time available will be longer if the plant was shut down and cooled while electrical power (Class III or EPS) was still available, as would be the case for a slowly-evolving event with early warning of the risk of flooding.

Additional Protective Measures Based on Timing and Predictability

There is sufficient time interval between the warning of the flooding event and flooding itself which allows taking some protective measures.

Furthermore external flooding hazards due to Danube River and Extreme local rainfalls are characterized by a slow time evolution and predictability. This allows preventively initiating a plant trip and reaching the cold shutdown conditions (with shutdown cooling system in operation). If flood levels threaten Class III Power or EPS, this is addressed by aligning an alternate means of cooling the fuel that does not rely on above power supply or by providing temporary protection from flooding for the required systems, as supported by the Operational Decision Making process at the station.

3.2.5 Conclusions

Based on the analysis results obtained by making use of the latest deterministic tools and complemented by probabilistic approach, it is concluded that Cernavoda NPP design intent in relation with flooding hazards is met with sufficient margin.

The design approach for protection of the site from external sources was to construct the plant structures at an elevation higher than the design basis flood and to construct protective structures (dike), where necessary. These features provide adequate protection of all plant structures, systems and components against external flooding.

The Design Basis Flood level for Cernavoda NPP is DBF = +14.13 mBSL (meters referenced to Baltic Sea Level) and the minimum buildings floor elevation is +16.24 mBSL as confirmed by the local topografic measurement results. Therefore, a significant margin of 2.11 m exists between the DBF and the lowest buildings floor elevation.

Flooding level caused by failure of the Portile de Fier dam (closest existing dam to the Cernavoda site), located on the Danube River, 600 km upstream of Cernavoda, was considered and determined to have negligible impact on the levels at the location of Cernavoda. Tsunami originating in the Black Sea was also considered and determined to be screened out because of the physical distance from the Black Sea (60 km away).

Flooding because of extreme rainfall in the catchments area surrounding the site was also considered. The combination of DBF level and extreme rainfall was found to result in level of 17.50 mBSL upstream of the valley; therefore a dike with maximum height of 18.00 mBSL was raised for plant protection. Therefore a margin of 0.5 m exists between the calculated maximum level and the top of the dike.

Even in the worst case scenario considered for dike failure, coincident with Danube River at Cernavoda DBF level +14.13 mBSL and extreme rainfall on catchments area resulting in maximum water 458 m^3/s flow rate, that might impair Class IV power and Class III power safety related systems, there is not a major threat on plant operation as long as a line of defense capable to ensure all the safety functions, remain available.

The design maximum rainfall rate calculated using Romanian national standard is 97.2$l/hr/m^2$. By comparison, the maximum recorded hourly rainfall at Cernavoda site is 47.3$l/hr/m^2$ as recorded in July 2010. This shows that there is sufficient margin in the design basis of the drainage system above the maximum recorded rainfall rate.

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 depth of water on the site is less than 20 cm for rainfall rate about 10 times the design maximum rainfall rate. The ground floor of buildings on site is at least 24 cm above the ground elevation; therefore this will not result in flooding the buildings on the site.

Additional margin also exists in the fact that the credible flooding scenarios, high Danube level or extreme rainfall, are characterized by slow time evolution and predictability. This means that operators have time to protect necessary structures using temporary barriers or put the reactor in a safe state and prepare backup equipment to deal with the situation.

3.3 Other Initiating Events – Severe Weather

As described in Section 1.1.1, due consideration has been given to evaluate all possible meteorological conditions, natural events (such as extreme temperatures, snow-fall, high winds, earthquake flooding etc) and man-induced events (such as explosions, toxic gases, explosive gases, fires etc.) as part of the Cernavoda site selection process.

In view of the WENRA/ENSREG Stress tests specification requirements, SNN undertook additional steps to examine the impact of severe weather (as part of other initiating events) on Cernavoda NPP Units 1 & 2 operations. This assessment work completed in accordance with the IAEA guides (NS-G-3.4, 3.5), and other international regulatory practices such as those in Canada (CNSC C-6 rev 1) and the USA, (NRC NUREG/CR-2300) consisted of screening of possible events and bounding analysis for Cernavoda units.

3.3.1 Methodology for Assessment and Successive Screening Approach

The methodology used to assess and screen potential external events was based on the following approach/process:

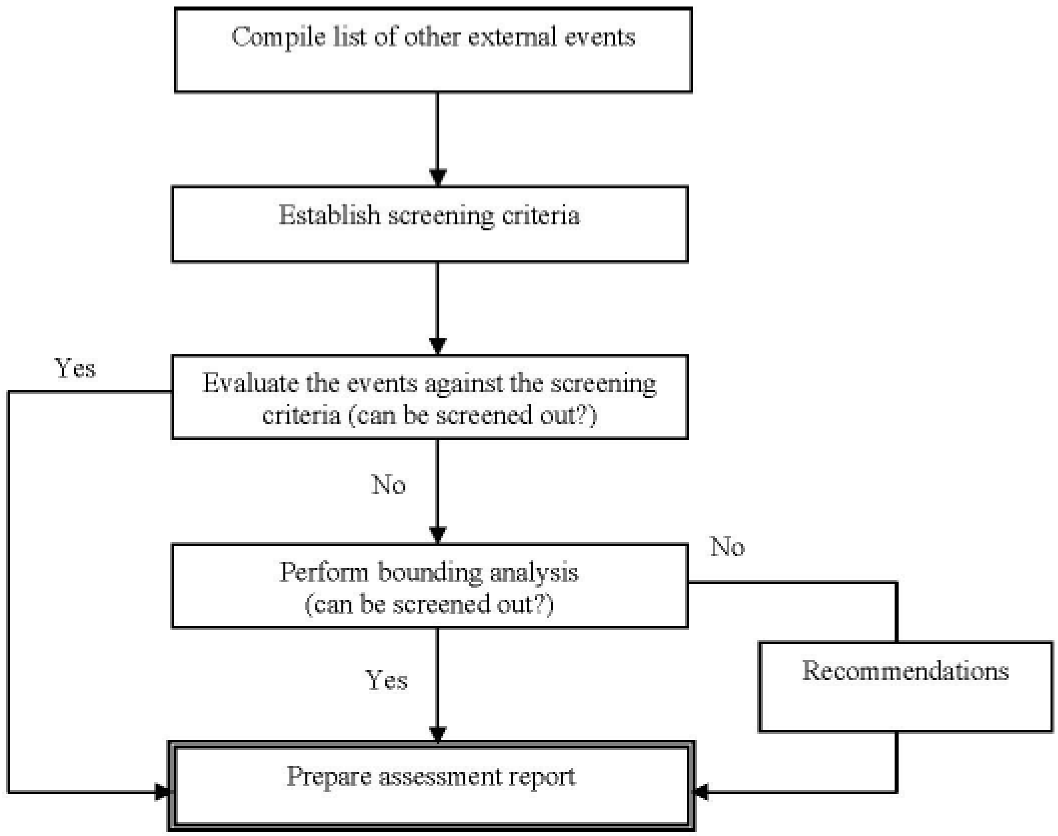

Figure 3.3-1 Severe Weather Event Analysis Flow Diagram

3.3.2 List of External Events

The list of external events assessed for Cernavoda NPP units covered the following:

Table 3.3-1 List of External Events Assessed for Cernavoda Units 1 & 2

Event	Description
Avalanche	A sudden rapid flow of snow down a slope as a result of natural triggers escalating from snow pack.
Coastal erosion	The wearing away of soil and rock by waves and tidal action. Fissures, sinkholes, underground streams and caverns caused by erosion are applicable to coastal erosion.
Drought	A meteorological phenomenon mainly characterized by a strong lack of precipitation. Causes that may lead to draught are various: atmospheric, hydrological, pedological, etc.
Forest fire	Fires originating from forest, grass or scrub outside the NPP buildings.
External flooding	Inundation of the NPP site with water from high river level, precipitation or site run-off, and effects from other sources of flooding such as storm surges from high wind, and tsunami.
Extreme winds and tornadoes	This category includes wind forces from straight wind, hurricanes and tornadoes and secondary effects such as missiles generated by wind..
Fog	Ground level clouds reducing visibility.
Frost/Ice	Includes icing of waterways used as the heat sink, ice accumulation due to frost, snow, freezing rain etc. on plant structures.
Hail	Hail occurs in the warm season as precipitation in the form of ice pellets larger than 5 mm in diameter.
High summer temperature	As per the name of the event.
High river level	As per the name of the event.
Hurricane	Enormous spiralling storms containing raging winds (greater than 120 km/h) and great decks of storm clouds that produce the heaviest rains on earth.
Intense local precipitation	Includes intense rainfall over a period of time.
Landslide	Includes a wide range of ground movement such as falling rock, deep failure of slopes and shallow debris flow.
Lightning	As per the name of the event.
Low river level	As per the name of the event.
Low winter temperature	As per the name of the event.
Sandstorm	Consists of the dust and sand raising from the land surface to the atmospheric due to the wind. The dust and sand remain in suspension for a time, function of the dust or sand grain size and the wind speed.
Seiche	A seiche is a standing wave that occurs in an enclosed or semi-enclosed water body and is usually caused by strong winds and/or changes in atmospheric pressure, landslides into water, underwater volcanic eruptions or earthquakes.
Snow	As per the name of the event.
Soil shrink/swell	Shrink-swell capacity of clay indicates the extent to which it expands when wet and retract when dry. Soil with high capacity is shrink-swell soil.
Storm surge	A storm surge is the onshore pileup of ocean or lake water caused by a combination of low pressure and wind.
Tornadoes	Tornadoes are violently rotating air columns appearing as funnel clouds beneath dark thunderstorm clouds.
Tsunami	A train of water waves generated by impulsive disturbances of the water surface due to non-meteorological but geophysical phenomena such as submarine earthquakes, volcanic eruptions, submarine slumps and landslides or ice fall into a body of water [IAEA Safety Guide “Flood Hazard for Nuclear Power Plants on Coastal and River Sites”, NS-G-3.5.].
Waves	Waves impacting the shoreline of the NPP site due to winds, vessel movement or other sources.

3.3.3 Events Screening

After application of the screening process, the following severe weather related events were considered for the bounding analysis:

- External Fires
- External Flooding
- Extreme winds and tornadoes

All other events were screened out based on the established methodology.

3.3.4 Bounding Analysis Assessment:

3.3.4.1 External Fires:

External fires could result from lightning strikes igniting local ground cover and the situation is exasperated during hot weather and or drought conditions accompanying the lightning strike. The assessment confirmed that the fire truck and fire brigade available on-site all the times along with posting of site security at different points all around the site perimeter are sufficient to address any external fir events.

3.3.4.2 External Flooding:

This initiating event is already discussed in detail in Sections 3.1 and 3.2 of this report.

3.3.4.3 Extreme Winds and Tornadoes

Extreme Winds: Direct wind statistics are documented in the NPP Final Safety Report. The maximum wind speed recorded by the Cernavoda meteorological station during 1986 – 1999 was 65 km/h (18 m/s) on December 10th, 1991 at 1 pm. The absolute maximum wind speed recorded by the 3 meteorological stations at Cernavoda, Fetesti and Medgidia are 126 km/h (35 m/s), 122 km/h (34 m/s) and 101 km/h (28 m/s) respectively.

Statistical data was used to derive a correlation between the maximum wind speed and the velocity of wind gusts. The 1000 year return direct wind speed on the basis of the data at the Fetesti and Medgidia stations are 184 km/h (51 m/s) and 148 km/h (41 m/s), respectively, while the maximum gust speed with the same return period is 220 km/h (61 m/s) and 173 km/h (48 m/s), respectively.

Cernavoda NPP structures are designed and constructed to Romanian Standard STAS 10101/20-78 as a minimum, corresponding to a loading figure of 140 kgf/m^2 (1.37 kPa) that translates to a wind speed of 166 km/h (46 m/s). Therefore, the Cernavoda NPP structures at a minimum would withstand all maximum wind speeds historically recorded (126 km/h).The 1000 year return period extrapolated statistics indicate that wind and/or wind gusts may exceed the minimum 166 km/h design value. However, it is expected that normally there are margins in the design to enable the structures to withstand higher wind speeds.

Further, as per the Safety Report stipulations it is implied that based on seismic design requirements (SDE and DBE), the structures would be more robust than the requirements for wind loading alone.

Tornadoes: Several confirmed tornado events have occurred since 2002 in Romania. On August 12, 2002 a tornado was confirmed (and recorded for the first time in Romania) in Facaieni in southern Romania. On May 7, 2005 a squall line with an embedded bow echo formed over southern Romania producing 3 tornadoes. One tornado occurred in Buftea and another in Ciobanu village and both were classified as category F0 on the Fujita scale. The third tornado occurred at Movilita village and was classified as an F1.

There is lack of information to establish a credible estimate of an annual frequency of tornadoes per unit area in order to derive a Cernavoda specific frequency for a tornado direct hit on the plant. However, it is recognized that damage from a tornado is limited to the direct hit area.

In two separate applications of the bounding analysis for two different Canadian CANDU 6 plants very similar to Cernavoda, the tornado hazard was screened out by demonstrating that the frequency of occurrence was less than 10^{-6} per year

Assuming that a tornado could damage the Emergency Power Supply building and the Emergency Water Supply building and that the equipment therein were unavailable, corresponds to a loss of alternate ultimate heat sink. This scenario has already been addressed in Section 3.5 of this report.

For a lesser damage scenario, such as availability of the EWS building, the onsite mobile diesel (stored in a robust structure) may be used to connect directly to the EWS distribution panel to enable makeup water to the steam generators for decay heat removal. Due to the large spatial separation between the EWS building and the onsite mobile diesel generator storage site, it is unlikely that both the EPS building and the mobile diesels will be hit by the same tornado (if one was to directly hit the Cernavoda NPP). It is therefore judged that a tornado cannot directly cause core damage.

3.3.5 Conclusions

The assessment results show that the severe weather conditions do not generate conditions and scenarios worse than those that have been analyzed in Sections 3.4, 3.5 and 3.6 of this report. In conclusion, none of the external events related to severe weather considered here were found to pose a credible hazard for the Cernavoda plant and hence no further analysis is required for these events.

3.4 Loss of Electrical Power

3.4.1 Cernavoda Electrical Power Supply & Distribution Design Basis

3.4.1.1 General overview

Unit 1 and Unit 2 internal power supply/distribution systems are organized on 4 classes of power:

- Class IV: normal electrical power supply that ensures all safety and production functions;
- Class III: standby diesel generators electrical power supply, that ensures all the nuclear safety functions;
- Class II: Alternating current (AC) uninterruptible power supply (UPS) 380 VAC and 220 VAC;
- Class I: Direct current (DC) uninterruptible power supply (UPS) 380 VDC, 220 VDC, 48 VDC.

The 4 Classes of power are linked in a "cascade", such as:

- if Class IV power is available, this will imply that Classes III, II, I are also available;
- if Class III is available, Class II and I are also credited;
- Class I available implies also Class II available.

In addition, emergency power supply (EPS) generation provides the only design basis earthquake (DBE) seismically qualified power supply, which ensures a back-up for all the main nuclear safety functions: control, cool, contain and monitoring, with operation from the Secondary Control Area. EPS provides back-up for class III, II and I seismically qualified equipment.

Apart from Unit 1 and Unit 2, Unit 0 provides the following support functions:

- System service supply: 110 kV switchyard operation for Unit 1/Unit 2 back-up and Unit 0 internal services;
- Water treatment plant (clarified/demineralized water production);
- Fire water supply;
- Auxiliary steam plant (light oil fuel);
- Domestic water supply;
- Non-essential buildings and structures power distribution.

Unit 0 has its own DC power (UPS).

3.4.1.2 Class IV and Class III power supply

To provide a redundancy of power sources and load groups for process systems, the design of the on-site electrical power system incorporates an "odd" and "even" dual bus concept. In this concept, the odd and even buses each supply part of the electrical power to necessary plant services. Through a judicious selection of load between the two buses, the overall effect on the plant of a partial loss of Class IV power, i.e., a loss of power to one 10.0 kV Class IV bus, is minimized.

Each of Unit 1 and Unit 2 internal services supply is organized in four classes of power. Class IV and Class III are each organized in a separated ODD – EVEN layout. The power is supplied to the following main buses:

- Two 10kV Class IV buses
- Four 6kV Class IV buses
- Two 6kV Class III buses

All the odd and even numbered 10.0 kV and 6.0 kV Class IV buses are normally supplied from the unit service transformers, which in turn are fed from the output of the generator. The back-up supply is provided by the station service transformers that are fed from the 110 kV switchyard. Each transformer can supply the total station service load required to safely shutdown and cool down the reactor in the event of failure of the other supply. An automatic transfer scheme is designed to keep the buses energized in case of failure of one supply, by transferring the load to the other supply.

During normal plant operation, electrical power to the station service is supplied from the unit service transformer. A sudden loss of power from the main supply would not normally lead to a loss of unit Class IV power, since automatic transfer to the system service transformers would occur.

The loss of Class IV power is defined as a total loss of capability to supply power from any service transformer SST's and UST’s to all Class IV 6 kV buses. This is caused by transformer faults, bus faults, grid failure or any combination thereof.

A complete loss of Class IV power could be caused by a combination of failures affecting the grid supply and the station-generated supply. This could happen due to:

- a total station disconnection from external electrical power supply coincident with turbine trip;
- a loss of station-generated power, due to a turbine or reactor trip, with a subsequent collapse of the grid;
- loss of existing supplies during a period of degraded electrical redundancy (bus, breaker, or transformer maintenance).

Upon total loss of Class IV power, there will be a simultaneous temporary total loss of Class III power (for up to 3 minutes). This unavailability of Class III power results in a loss of power to process and service systems. Selected equipment is started automatically in a predetermined sequence following the start of Standby Diesel Generators (SDGs) and restoration of power to the relevant Class III bus via the Reloading Sequencer.

Only two out of the four SDG’s in Unit 1 are required to ensure the supply of all the necessary nuclear safety functions after a loss of Class IV; for Unit 2 only 1 out of the 2 SDG’s is required to provide the similar coverage.

3.4.1.3 Uninterruptible Power Supply (UPS)

The station UPS systems consist of rectifiers, batteries, inverters and supply/distribution network. Each unit has its own independent UPS systems, including also Unit 0. The Unit 1 and Unit 2 UPS refer to two sub-systems: Class I (DC power UPS – battery powered) and Class II (AC power UPS – battery powered via inverters). According to the current evaluation, the batteries can provide power supply for eight hours. Each of the electrical power distribution system has a qualification (seismically, environmental, etc.) similar to its source of power (i.e. EPS diesels including all support systems and EPS distribution is seismically qualified to DBE, Category 'B').

The main purpose of Unit 1 and Unit 2 Class I and Class II Systems is to ensure continuous power supply to all the control and logic functions (48VDC), breakers control voltage (220VDC) and instrumentation loops of the unit (220VAC - 40VDC power sources), and to ensure operation of nuclear safety equipment such as: Shut-off Rods and Control Rods drive, PHT loop isolation and ECC injection motorized valves, Auxiliary (pony) Moderator pump motors, Main Control Room lighting, station emergency lighting.

3.4.1.4 Emergency Power Supply (EPS)

Each of Unit 1 and Unit 2 is equipped with separate emergency power supply (EPS) systems. The purpose of the EPS is to provide an alternate power source to equipment essential to the safe shutdown and cooldown of the reactor, following loss of the normal and standby station supplies as a consequence of a seismic event or other common mode events.

Under SBO conditions, EPS continuous operation is ensured for 6.3 days at Unit 2, respectively 8.6 days at Unit 1. The EPS DGs are 100% redundant, DBE seismically qualified to Category 'B' (maintain integrity and functionality). Also, the entire buildings, support systems including fuel storage and fuel transfer, structures, equipment are DBE seismically qualified to Category 'B'.

The loads of EPS System provide the main nuclear safety functions for the reactor:

- control of reactor power (via SDS1 or SDS2 equipment for Unit 2, SDS2 equipment for Unit 1);
- fuel cooling (ECC pumps, ECC high pressure/ low pressure motorized valves (MV's), EWS pumps / make-up control);
- containment functions (includes some of the local air coolers for Unit 2 only);
- monitoring of the key parameters: reactor power, PHT pressure/temperature, boiler levels, containment pressure, etc.)

The EPS distribution has the same separated ODD / EVEN layout as the other station power supplies. The normal supply for SCA services (DG control panels, motor and building heaters, lighting, starting battery chargers, etc.) is provided from 380VAC Class III, with back-ups (via transfer switches) from EPS ODD or EVEN. In addition, the SCA 220VAC and 48VDC Class II and Class I power distribution panels (PL's) for operation of Group II support systems (control, logic, indication loops) can also be powered from either EPS ODD or EVEN.

Each section of the EPS distribution (ODD/EVEN) consists of:

- one 6 kV bus – powered directly from the EPS DG;
- one 0.4 kV bus – powered from the 6 kV EPS bus via one 6/0.4kV transformer.

The ODD and EVEN buses can be tied together via tiebreakers for flexibility. There are also several local EPS services panels powered from either Class III ODD/EVEN or EPS ODD/EVEN. Only one

EPS DG is required to be operational at any time, the other one act as a back-up. The time available for operator action to start EPS and to provide power supply to loads is about 30 minutes. Based on the regular mandatory testing; the time to perform bus tie transfer is less than 5 minutes.

3.4.2 Loss of Site Power (LOOP)

3.4.2.1 Loss of Off-site Power (Class IV available)

Loss of site power with Class IV available (Islanded operation) is an abnormal operating mode defined as the separation of a part of the 400 kV transmission network from the rest of the grid. The separation could be the result of remote transmission lines breaker trips. The main breaker of the plant generator remains connected to the internal services and plant output transformers.

The loss of line event represents the sudden unit disconnection from the 400 kV output switchyard caused by a protective trip of the 400 kV grid interconnection breakers (two breakers for each unit at Cernavoda NPP), with the unit remaining at high power - isolated on their own internal services supply.

Depending on the initiating event and the resulting 400 kV switchyard configuration, only one or both units of Cernavoda NPP could be affected. If the loss of line event is caused by a progressive or sudden transmission grid failure (rather than a local / single unit output system malfunction), and if the regional 110 kV distribution grid - that provides the back-up for internal services supply - also fails, the units will experience a loss of off-site power event. The difference between a single unit loss of line and the whole station being affected by a loss of off-site power is the operation of equipment in Unit 0, which provides services (demineralized water, etc) to both Unit 1 and Unit 2.

The loss of line event is covered by provisions in the station design. Due to no impact on the station safety related systems, a specific abnormal plant operating procedure for this mode of operation is not required. The dedicated Overall Unit Operating Manual describes the necessary actions to stabilize the plant and to return to the normal operating configuration.

Safety Functions

There are no automatic safety system actions associated with a simple loss of line event, if the station services remain supplied from either the back-up 110 kV external supply system (via the System Service Transformers – SST's) or from the main generator (via the Unit Service Transformers – UST's). There are no automatic safety systems actions associated with a loss of off-site power event, unless the main generator fails to supply power to internal services.

Reactor Shutdown

There are large demineralized-water inventories in the "feedwater train" that ensure unit operation. In the long term, the orderly shutdown has to be considered if the inventory is reduced.

Containment functions are provided as per normal operation state.

Heat Sink

The heat sink is ensured by normal full power operation heat sink. The steam produced in the SG secondary side is condensed in the condenser hot wells. The condensate is recirculated through the "feedwater train" components back to the SGs. Even there are large demineralized water inventories, due to normal operating leaks; the demineralized water inventory is reduced in time (if the WTP demineralized water production was not restored).

In the long-term (if demineralized water production cannot be restored), the heat sink is ensured by the shutdown cooling (SDC) system with heat removal through the recirculation Cooling Water (RCW) and RSW systems to the river.

3.4.2.2 Loss of Off-site Power (Loss of Class IV)

In case of failure of islanded operation and also loss of off-site power events, the station experiences a total loss of class IV event (both ODD and EVEN electrical distribution sections are affected).

If only one electrical distribution division (ODD or EVEN) is lost, a partial loss of class IV event is to be considered. The following safety functions will happen as a result of this event:

Safety Functions

<u>Reactor trip</u>

Immediately following a partial or total loss of Class IV event, a reactor trip will be generated by a process trip parameter. It is expected that both shutdown systems will act and the actual trip parameter initiating the shutdown will vary since the actuating trip signals from the different parameters all act within the same time frame.

<u>Containment</u>

Manual containment isolation is required due to loss of R/B vapor recovery air flow (as per "Impairment manual" requirements).

<u>Heat sink</u>

Since Class IV power is not available, the main PHT system pumps cannot be used for forced circulation decay power heat removal, the thermosyphoning is used for PHT system cooldown to 177^{o}C. Subsequent cooling is ensured by SDC system (heat removal through the RCW / RSW systems to the Danube River).

Alternatively (but not preferred), the SDC system (Class III powered) can be used in emergency conditions using SDC pumps starting from 260^{o}C.

3.4.2.3 Provisions to Prolong Available Time for On-site Power

Following a severe event that would prevent normal supply of goods and services to the station, provisions have been made to ensure continuity of the major safety functions: maintain the reactor in subcritical state, fuel cooling, containment function and monitoring of key plant parameters (CSP's).

There is enough diesel fuel oil on site to provide Diesel generators operation for more than 72 hours. The normal procurement is covered by a long term commercial contract with external specialized firms. The fuel oil arrives on-site 2 to 5 days from notice; there are also provisions for urgent supply from the market in case the normal process is late. For supply of fuel oil in abnormal external conditions, provisions are made as presented in Section 3.7 of this report.

3.4.2.4 Provision to Increase Robustness of Plant

There are four additional levels of defence-in- depth for electrical power supply:

- the class III electrical power supplied from first set of diesel generators with 100% redundancy built-in;
- the class I / II electrical power supplied from batteries for 8 hours;
- the emergency electrical power supplied from the second set of diesel generators (seismically qualified) known as emergency power supply (EPS) designed to 100% redundancy and separation requirements;
- the mobile diesel generators.

Except for the class I / II batteries, the other electrical power sources ensure at least 3 days of continuous power supply without any external support. All of them ensure the safe shutdown. The class I / II batteries ensure the cooling function (basically actuating valves) for a limited time but sufficient to allow the operator to secure another heat sink.

Based on this it can be concluded that additional design changes or operational changes are not required.

3.4.3 Loss of Off-Site Power (LOOP) and of On-Site Back-up Power (Station Blackout- SBO)

In order to analyze the Cernavoda NPP capability to respond to a station blackout (SBO) event, two main scenarios have to be considered:

a) The Station Design Basis Case: The capability of the station to respond to a loss of all Class IV (External Grid and Class IV Distribution Buses) and Class III (Standby Diesel Generators) power sources. This case will consider that the batteries are available.

b) The Beyond Design Basis Case: The capability of the station to respond to a total loss of AC power supply (External Grid, Standby Diesel Generators, Emergency Diesel Generators). This case will consider that the batteries are available.

In both scenarios, nuclear safety functions to place the plant in a safe shutdown state have to be assured by:

- Shutting down the reactor and maintain in a safe shutdown condition;
- Containment integrity;
- Providing a heat sink for fuel cooling;
- Critical safety parameter monitoring

3.4.3.1 LOOP + Loss of Ordinary back-up source (class III SDGs)

The sudden loss of Class IV electrical power could cause the turbine to trip immediately and causing atmospheric steam discharge valves (ASDVs) and main steam safety valves (MSSVs) to lift discharging steam to atmosphere.

Safety Functions Performance

As described below, safety functions are assured as follows:

Reactor Trip will be generated by a process trip parameter. It is expected that both shutdown systems will act and the actual trip parameter initiating the shutdown will vary since the actuating trip signals from the different parameters all act within the same time frame. The associated trip parameters following the event for SDS1 are: Low PHT gross flow or High heat transport system pressure while for SDS2 the parameters are Low core differential pressure and High heat transport system pressure.

Containment functions

Containment Isolation – in case of no automatic actuation, manual box-up will be performed from Main Control Room (using electrical power provided by Class I batteries) or Secondary Control Room (using electrical power provided by Class I batteries if available or Emergency Diesel Generators). Even if Class I batteries are not available, containment valves will fail in a close position to assure containment box-up.

Dousing System ensure containment pressure suppression. However, this system is not required to function for this event.

The LACs are lost since the RCW and RSW are lost following loss of Class III. For Unit 2, some of the LACs are also powered from the EPS to provide air circulation inside containment.

Airlocks are available as long as the seals pressure is maintained by back-up air tanks (which are adequate for 24 hours). After depletion of the back-up air tanks, connection to the nitrogen bottles can be established.

Heat Sink is assured by thermosyphoning process since forced circulation cannot be ensured due to loss of Class IV and Class III power. The operator is directed to initiate high pressure (HP) ECC injection on the PHT primary side to increase the subcooling margin and to depressurize the SGs secondary side by using the MSSVs. Dousing tank inventory (through the Boiler Make-up Water system) will be used for water supply to all SGs secondary side. In the long-term, the operator will use EWS with water supply from the Danube River.

In case EPS is not available, the class I / II batteries could ensure about 8 hours of power supply to essential loads. This provides sufficient time for operator actions to try to recover the EPS or start the mobile diesel generators.

If none of them is available, the fire water trucks will be used to provide water directly to the SGs through the EW pipes.

3.4.3.2 LOOP + Loss of the Ordinary Back-up Source (Class III) Standby Diesel Generators and Loss of EPS (SBO)

Major process parameters evolutions for the first part of the initiating event is similar to Section 3.4.3.1 except that for this scenario the main focus is to maintain the thermosyphoning process.

Safety Functions Performance

For this scenario, safety functions are assured as follows:

Reactor Trip will be generated by a process trip parameter. It is expected that both shutdown systems will act and the actual trip parameter initiating the shutdown will vary since the actuating trip signals from the different parameters all act within the same time frame. The associated trip parameters following the event for SDS1 are: Low PHT gross flow or High heat transport system pressure while for SDS2 the parameters are Low core differential pressure and High heat transport system pressure.

Containment Isolation – The containment valves are fail closed and will be closed after the SBO event. The operator is required to check if the all valves are closed and in case that was no automatic closure, manual box-up will be performed from Main Control Room or Secondary Control Room (using electrical power provided by Class I batteries) if the SBO is seismically induced.

Dousing System ensure containment pressure suppression. However, the system is not required.

The local air coolers are lost (because the RCW and RSW are unavailable following loss of class III. EPS is unavailable for Unit 2 LAC's power supply).

Airlocks are available as long as the seals pressure is maintained by back-up air tanks or the nitrogen bottles.

Heat Sink is provided by thermosyphoning process. On the primary side, the operator is directed to initiate HP ECC injection to PHT system and to open the MSSVs (at least 4). These actions are conditioned by class I electrical power supply. In case that class I / II batteries are not available, the operator will have to open the MSSVs manually and block four out of them open.

Since there could be just a limited amount of water transferred from PHT system during the initial phase of the event, the HP ECC tanks (> 170 m^3) ensure enough water to provide make-up and to pressurize the PHT system.

On the secondary side of the steam generators, the water will be supplied initially from the dousing tank inventory (once the SGs were depressurized to atmospheric pressure and the BMW pneumatic isolation valves were open). The inventory from the dousing tank will ensure a continuously flow for at least 13 hours (assuming that there is no SGs level control). During this time interval, the PHT system will be maintained at (120^{o}C - 130^{o}C) while the fuel sheath temperature will face similar values. At the end of this interval, the SGs will be full of water because the required flow for decay power heat removal is lower than the flow provided. The remaining inventory in the SGs will ensure at least another 10 hours for decay power heat removal, ensuring at least 23 hours in total. Onset of significant void in PHT due to PHT reaching saturation and start boil off is expected after 27 hours from the start of the event.

If the water inventory from the dousing tank is exhausted, the EWS pumps powered by mobile diesels generators will be used to ensure water supply to the SGs secondary side.

If any of these measures failed to provide water to SGs, the fire water trucks connected directly to EWS pipes through the special connections (available to be installed if required) can be used to provide water to SGs secondary side. Once the PHT inventory is maintained by HP ECC make-up, the thermosyphoning will ensure fuel cooling.

3.4.4 Provisions to prevent loss of off-site and on-site electrical power

3.4.4.1 Provisions to prevent loss of off-site power and loss of ordinary back-up sources (Class III - Standby Diesel Generators)

There are three additional levels of defence in depth for electrical power supply:

- the class I / II electrical power supplied from batteries;
- the emergency electrical power supplied from the second set of diesel generators (seismically qualified) known as emergency power supply (EPS) designed to 100% redundancy and separation requirements;
- the mobile diesel generators.

Class I batteries are credited for up to 8 hours for this event.

The EPS system is comprised of two duplicated seismically qualified and functionally independent trains of equipments (ODD and EVEN).

The EPS Diesel fuel oil is stored on-site in 2 x 22.73 m^3 fuel tanks in Unit 1 and 2 similar tanks in Unit 2. The Fuel Supply System consists of 2 separate sub-systems, one dedicated to each of the 2 DGs. The EPS Diesel tanks are installed completely underground, and they are DBE category B qualified.

In the event of Loss of Off-site power and Loss of Class III, EPS will be loaded with one emergency water supply pump, Class I and II panels back-up supplied from SCA, diesel generator auxiliary services and SCA services. The EPS fuel oil storage will assure operation for more than 8 days for Unit 1 and more than 6 days for Unit 2.

In addition, storage fuel oil from Class III standby diesel generators (same qualitative type) can be considered, if necessary.

The mobile diesel generators have autonomy of 6 hours at full load without external support. The available fuel oil on site will ensure more than 3 days of operation without external support, considering only the EPS stored fuel oil.

Except for the class I / II batteries, the other electrical power sources ensure at least 3 days of continuous power supply without any external support. All of them ensure the safe shutdown. The class I / II batteries ensure the cooling function for a limited time but sufficient to allow the operator to secure another heat sink.

Based on that it can be concluded that additional design changes or operational changes are not required.

3.4.4.2 Provisions to Prevent Loss of Off-Site and On-Site Power (SBO)

There are two additional levels of defence in depth for electrical power supply:

- the class I / II electrical power supplied from batteries;
- the mobile diesel generators.

As described in Section 3.4.4.1 the fuel oil available on-site ensures continuous operation of the mobile diesel generators for more than 3 days.

Class I / II batteries are available for a limited time (about 8 hours). The class I / II batteries ensure the cooling function for a limited time but sufficient to allow the operator to secure another heat sink.

The mobile diesel generators have autonomy of 6 hours at full load without external support. The available fuel oil on site will ensure more than 3 days of operation without external support, considering only the EPS stored fuel oil.

If the mobile diesel generators are not available, the on-site fire water trucks will be connected directly to the EWS pipes in order to provide water directly to the SGs. The operator can try to recover either EPS or the mobile diesel generators during this time.

Based on that it can be concluded that additional design changes are not required.

3.4.5 Conclusions

In this chapter the behavior of the plant and the remaining levels of defence in depth for the following initiating events are analyzed:

- loss of off-site power;
- station blackout (SBO);
- loss of primary ultimate heat sink (including loss of alternate ultimate heat sink);
- loss of primary ultimate heat sink with station blackout.

Loss of off site power event alone does not pose any threat for the plant.

There are five levels of defence for electrical power supply at the station:
- the class IV electrical power
- the class III electrical power supplied from first set of diesel generators with 100% redundancy built-in;
- the class I / II electrical power supplied from batteries for 8 hours;
- the emergency electrical power supplied from the second set of diesel generators (seismically qualified) known as emergency power supply (EPS) designed to 100% redundancy and separation requirements;
- the mobile diesel generators.

The plant can operate at reduced power levels in the islanding mode. The operation is limited in time based on administrative considerations if power is not restored. Then the plant is manually shut down and cooled down according to operating procedures and there are no issues related to the heat sink.

Loss of class IV power event alone does not pose any threat for the plant. This event 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 (thermosyphoning in primary coolant system / steam generators / auxiliary feedwater system or boiler make-up water system or emergency water supply system/ steam discharge valves, or shutdown cooling system / service water systems).

There are four levels of defence for electrical power supply:

- the class III electrical power supplied from first set of diesel generators with 100% redundancy built-in;
- the class I / II electrical power supplied from batteries for 8 hours;
- the emergency electrical power supplied from the second set of diesel generators (seismically qualified) known as emergency power supply (EPS) designed to 100% redundancy and separation requirements;
- the mobile diesel generators.

For the loss of Class IV and Class III electrical power supply, the reactor will be shutdown by either SDS1 or SDS2. The long term heat sink will be ensured by BMW or EWS systems powered by EPS.

From the electrical point of view, there are three additional levels of defence:

- the class I / II batteries for 8 hours;
- the EPS diesels designed to redundancy and separation requirements;
- the mobile diesel generators.

The plant cooling is ensured by any of the three electrical supplies as described in Section 3.4.2.

For the Station Black-Out (including loss of EPS), there are two levels of defence in depth:

- the class I / II batteries for 8 hours;
- the mobile diesel generators.

The plant shutdown is ensured by SDS1 or SDS2 that are failing safe. The containment isolation is failing close. The plant cooling is ensured by either of the two electrical supplies as described in Section 3.4.3.

As for all the cases, the plant is safely shutdown and cooled for more than 3 days without external support.

3.5 Loss of Ultimate Heat Sink

3.5.1 General Description of Plant Heat Sinks

For the Cernavoda CANDU 6 reactor, the fuel bundles are located in 380 horizontal channels that are split in two separated symmetrical loops. Each loop consists of two passes. All the channels in the same pass are connected to one reactor inlet header (RIH) and to one reactor outlet header (ROH) through individual vertical feeders. The water is circulated through these horizontal channels and vertical feeders (from the inlet headers to the outlet headers) and through the primary side of the steam generator, forced by one Primary Heat Transport (PHT) pump in each pass. At nominal power conditions, the RIH temperature is around 263^{o}C while the ROH temperature could increase up to

311^{0}C. The PHT system pressure and inventory control is ensured by Pressure and Inventory Control (PIC) system.

Steam Generators (SGs) secondary side is cooled by the flow provided by main Feedwater (FW) system pumps. The steam produced in the steam generators is transferred to the turbine and then is discharged to the condenser. The condenser is cooled using the Condenser Cooling Water (CCW) system. The CCW system water intake is taken from suction bay and is discharged to the Danube River or to the Danube - Black Sea Channel. The CCW pumps can be operated as long as the water level in the suction bay is above 1.59 mBSL. The frequency to have a Danube River water level below this level is less than 10^{-4}/year. The normal water level in the suction bay is 7 mBSL.

In case the reactor power is reduced or if a reactor trip occurs, the steam flow to the turbine will be reduced. The overall plant control will close the governor valves (GV) that provide steam admission to the turbine. Consequently, the steam will be diverted to the condenser through the Condenser Steam Discharge Valves (CSDVs) or to the atmosphere through the Atmospheric Steam Discharge Valves (ASDVs) or Main Steam Safety Valves (MSSVs). The demineralized water inventory to the steam generators is ensured by the feedwater train in the same manner as presented above.

3.5.1.1 General Descriptions of the Primary Ultimate Heat Sink

The primary ultimate heat sink is based on decay power heat removal using forced cooldown circulation in PHT system. The control is performed from Main Control Room (MCR). It 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. Each SDC pump forces the flow through associated SDC heat exchanger.

The secondary side heat removal from SDC heat exchangers is provided by the flow provided by class III power RCW pumps. The heat is transferred through the one of the four RCW/RSW heat exchangers to the RSW system. The same electrical power separation is ensured for the RCW system: 2 pumps are connected to ODD class III electrical power bus while the other 2 are connected to EVEN class III electrical power EVEN bus. The heat transferred through the RCW/RSW heat exchangers is removed by the RSW cooling flow. The RSW system operates in an open loop manner. There are 4 x 100% pumps (shutdown conditions) available for RSW system: 2 pumps are connected to class III electrical power ODD bus while the other 2 are connected to class III power electrical EVEN bus. The water is taken from suction bay (Danube – Black Sea channel) and is discharged in a common header. After leaving each of these loads, the warmed water is collected and discharged into the CCW system discharge channel. Through the channel, the water is transferred to the Danube River at a downstream location relative to the Danube - Black Sea channel intake or to the Danube - Black Sea channel. The RSW pumps will trip if the water level in the suction bay is reduced below 1.45 mBSL.

In case that one of the components of the primary ultimate heat sink became unavailable, the heat removal from the core will be released through the alternate heat sink.

3.5.1.2 General Description of the Alternate Ultimate Heat Sink

The alternate ultimate heat sink described in (a) and (b) respectively below is used when one of those components of the primary ultimate heat sink is unavailable. Depending on the class of electrical power available, the control is performed from MCR if at least class I and / or class II are available. If class III is not available, the EPS has to be started and preparations have to be made for transfer of control to SCA.

The decay heat produced in the core heats up the primary heat transport circuit inventory. The warmer inventory goes to the steam generators where it is cooled down by the cooling water from the steam generator secondary side. 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 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. The SGs secondary side water flow requirement for PHT system decay power heat removal is about 30 l/s at about 3 minutes after reactor shutdown and is reduced to about 5 l/s at about 12 hours. 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. Finally, the SG's secondary side inventory is transformed to steam. The steam is released to atmosphere through the open paths ASDVs or MSSVs. The maximum temperature in the primary circuit will be about 120^{o}C - 130^{o}C. The PHT system pressure and inventory control will be ensured by the Pressure & Inventory Control (PIC) system if class IV or class III is available. In case that PIC system becomes unavailable, the ECC injection (class II) can be used to increase the PHT pressure and to ensure the subcooling margin and boiling prevention. In an ultimate case, as per design, the EWS system (EPS electrical supply or mobile DGs) can be used to provide water supply to PHT system if the rupture disks were broken by HPECC injection.

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 water can be provided to steam generators secondary side is represented by the "feedwater train".

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.

Since the AFW can provide to SGs a flow (42.2 l/s) larger than the flow required for cooldown purposes after reactor trip, 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 that can be used to provide water to SGs secondary side is represented by the Boiler Make-up Water (BMW) system (using the demineralized-water inventory from the dousing tank) or by EWS system.

Water supply from BMW (dousing tank inventory)

In case the Auxiliary Feedwater (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 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. The minimum available demineralized water inventory from the dousing tank is about 2000 m3. The gravitational water flow to all steam generators is about 43 l/s, considering the maximum water level in the dousing tank.

Considering the demineralized-water volume inventory and the maximum gravitational flow rate to SGs, there will be a continuous flow for at least 13 hours. At the end of this interval, the SGs will be full of water because the required flow for decay power heat removal is lower than the flow provided. The remaining inventory in the SGs will ensure at least another 10 hours for decay power heat removal, ensuring at least 23 hours in total.

Continuous water flow to SGs by EWS

The dousing tank inventory will ensure for a limited time interval water supply to SGs secondary side. As per plant design, finally the water to SGs secondary side will be directly provided from suction bay by 2 x 100% pumps (for each unit). As long as cooled water will be provided to SGs, the difference between the hot leg and the cold leg in the SGs will promote the natural circulation (thermosyphoning) through the PHT system. The electrical power supply for the MSSVs is from class I or from EPS or from mobile diesel generators.

3.5.2 Plant Response to Loss of Heat Sinks

3.5.2.1 Safety functions following loss of the primary UHS

Loss of the primary ultimate heat sink can be caused by:
- Earthquake, which is covered in Section 3.1 of the present report.
- Severe water level reduction in the suction basin due to very low level in the distribution bay / intake channel blockage or severe blockage of the filtering chains.

For the loss of primary ultimate heat sink caused by any other event, except for earthquake, Class IV off site electrical power is assumed available. In addition, the Class III, Class II and Class I are assumed available because they are supplied from Class IV power busses.

In case one of the components of the primary ultimate heat sink became unavailable, the heat removal from the core will be achieved through the alternate heat sink. The alternate heat sink relies on thermosyphoning process as described above. Relevant operating procedures to address these situations exist at the station and operating staff is trained to take care of such situations.

3.5.2.2 Safety functions following loss of-the primary and alternate UHS

Loss of the primary and alternate ultimate heat sinks can be caused by:
- Extreme earthquake: The evaluation has been already performed per Section 3.1 of this report.
- Loss the alternate UHS after a loss of the primary UHS (due to alternate UHS systems/components failure).
- Severe water level reduction in the suction basin (EWS unavailable) due to very low level in the distribution bay/intake channel blockage or severe blockage of the filtering chains and EWS suction line.

For the last two scenarios, Class IV off-site electrical power is assumed available. In addition, the Class III, Class II and Class I are assumed available as long as they are powered from Class IV power buses.

Relevant abnormal plant operating procedures exist at the station and the operating staff is trained to manage such situations.

3.5.3 Provisions to Prevent loss of Ultimate Heat Sinks

3.5.3.1 Provisions to Prevent the Loss of Primary UHS

General design provisions

- For RSW pumps, the minimum suctions intake water level in the suction bay is 1.45mBSL. The frequency of reaching this Danube River water low level is < 10^{-4}/year.
- There are two independent flow paths available to discharge the water used for cooling purposes for each unit. The first path is to the Danube River downstream the Danube – Black Sea channel. The second path is to the Danube – Black Sea channel, opposite to the Danube River discharge location.
- The discharge channel for each unit is designed for normal full power cooling flow.
- The flow discharged through the discharge channel, during shutdown conditions is ≈ 10 times smaller than the required cooling flow during full power operation.

Analysis provisions

- Loss of Feedwater is analyzed as part of the plant design (separate section in the Safety Analysis Report – Loss of Feedwater event).
- Loss of SDC cooling is analyzed as part of the plant design.
- Loss of RCW is analyzed as part of the plant design.

Primary UHS systems provisions

- The systems that are part of the primary ultimate heat sink are designed considering redundancy aspects [shutdown conditions: 4 x 100% RCW and 4 x 100% RSW pumps; 2 x 100% SDC pumps (6 hours after plant shutdown)].
- Independent class III power supply (2 RCW/2 RSW pumps are powered from ODD class III electrical bus / 2 RCW/2 RSW pumps are powered from EVEN class III electrical bus. One SDC pump is powered from ODD class III electrical bus while the second one is from EVEN class III electrical bus). Following loss of Class IV power, one pump per bus starts automatically after the class III electrical power is established by the SDG.
- For RCW system, during normal operations, two of the pumps are selected “ON” and one “Stand-by”. The pump selected as “Stand-by” starts automatically, if the breaker of one of the “ON” pump is detected as not being closed.
- For RCW system, valves are provided to automatically isolate the RCW supply to non-essential loads under loss of class IV power conditions.
- For RSW system, two or three of the pumps are selected “ON” and one “Stand-by”. The pump selected as “Stand-by” starts automatically, if the breaker of one of the “ON” pump is detected as not being closed.
- Although the RSW pumps could trip automatically on low bearing cooling water pressure (due to loss of normal clarified water supply), a separate line from pump discharge equipped with filters is provided for cooling the thrust bearing.
- A set of 2 filtering lines (trash rack and traveling water screens) are provided at the intake of the RSW pumps (segregated from the CCW pumps intake). The power supply to these equipments is from class III. The screens are started automatically on detection of a high

differential level. The high-level monitoring circuits are dependent on a common instrument air supply without which the screens would operate only in response to the master timer or local operator control. However, loss of this air supply is alarmed.

- The SDC system can be used for cooldown purposed starting from high PHT temperatures (149^{0}C). During emergency conditions, the system can be brought in operation starting from a PHT system temperature of 260^{0}C using the PHT system pumps or SDC system pumps.
- Relevant Appropriate Plant Abnormal Operating Procedures (APOPs) have been developed to follow during abnormal plant operating conditions.

3.5.3.2 Provisions to Prevent Loss of the Primary UHS and Alternate UHS

General analysis and design provisions

- Loss of PHT system heat sink following an earthquake is analyzed as part of the plant design basis.
- For EWS pumps, the minimum intake water level in the suction bay is 1.21mBSL. The frequency of reaching this Danube River water low level is less than 10^{-4}/year.
- For the "alternate ultimate heat sink" there are water inventory provisions (the dousing tank water inventory is more than 2000 m^3). This inventory ensures at least 7 days of continuous cooling decay power heat removal by the steam generators (operator control the flow to SGs). In case that the water flow cannot be manually controlled, the time this inventory is available for at least 23 hours.
- There are two independent paths available to discharge steam to the atmosphere (ASDVs and MSSVs).
- The MSSVs can be blocked open, by using specific mechanical devices.

Alternate UHS system provisions

- The systems that are part of the primary ultimate heat sink are designed considering redundancy aspects such as Emergency cooling water systems (EWS) is designed with two 2 x 100% pumps, one powered from ODD EPS bus while the other is powered from EVEN EPS bus. The valves and associated controls are also powered from EPS system considering redundancy aspects.
- The systems (EWS and EPS systems and SCA) are seismically qualified for DBE category B (the systems maintain their integrity and functionality after a DBE).
- The MSSVs are DBE category B qualified. They will maintain the integrity and functionality after an earthquake.
- In case of an earthquake, the systems are designed to fail-safe. The PHT system integrity is preserved.
- The steam line will not fail inside reactor building since the pipes are DBE category B qualified.
- The steam line is expected to fail at the designed weakest point outside reactor building. (These pipes are designed according to ASME code requirements but not qualified for DBE category B).

The valves in BMW system fail open on loss of instrument air, while the control can be ensured by local air tanks.

3.5.4 Conclusions

Following loss of the primary ultimate heat sink (SDC + RCW + RSW), the shutdown systems are manually activated from the MCR. Automatic trip acts as back-up. If the MCR is unavailable, they can be manually activated from the SCA. The SCA is qualified for DBE category B. The heat sink is ensured by the alternate ultimate heat sink, seismically qualified for DBE category B with significant margins available. The plant cooldown will be ensured for an unlimited time interval by EWS providing water to SGs secondary side.

Plant response following loss of primary ultimate heat sink and loss of alternate ultimate heat sink (EPS + EWS) will be similar to the case of loss of primary ultimate heat sink. For this case, there are two levels of defence in depth:

- The BMW from the dousing tank. The water inventory in the dousing tank that ensure a continuous heat sink for up to 7 days. Even in the case that the water flow is not controlled (the pneumatic isolating valves fail open), the same inventory ensures at least 23 hours of continuous heat sink. Onset of significant void in PHT due to PHT reaching saturation and start boil off is expected after 27 hours from the start of the event.
- The fire water truck connected manually to EWS system piping will provide water to SGs secondary side from firewater trucks. The firewater truck can be supplied with water from firewater system supplied with water from the two existing deep ground wells that are not affected by dry season or low Danube level. In case that the firewater system is not available, the firewater trucks will be supplied with water from the distribution bay using the motor driven diesel pump.

3.6 Loss of Primary Ultimate Heat Sink with Station Blackout (SBO)

3.6.1 General Description

The primary UHS was described in Section 3.5. Loss of primary UHS could be caused by the loss of RCW or RSW systems - single process failures.

Loss of RSW pumps can also be caused by a common mode event such as the Distribution Bay level decrease below 1.45 mBSL, which is a slow-evolving event. At reduced Danube levels both units will be orderly shutdown (sequentially at 24 hours time interval) and placed under Guaranteed Shutdown State (GSS) well before Distribution Bay reaching the level that poses a threat to the primary UHS operation (at least 3 - 4 days in advance before RSW pump tripping level is expected). This will ensure low decay heat production levels in both reactors before the RSW system will be lost due to reduced water levels in the Distribution Bay.

SBO occurrence will incapacitate both RCW and RSW systems (pumps are powered by class III electrical power supply).

The effect of a SBO event alone, (regardless of the intake water level), will result in a sudden loss of the equipments that are providing / using the primary UHS (main water intake pump station – CCW / RSW / BCW / Fire Water Make-up systems). According to the SBO definition, all the class IV and class III systems and the EPS system will be lost. As a consequence, the AFW pump will be lost and no demineralized-water supply from the “feedwater train” will be available to SGs secondary side. Since the SBO includes loss of EPS (and consequently loss of EWS pumps), the only source of water to SGs (as per plant design) will be water from the dousing tank.

Heat sink

If the SBO occurs coincident with loss of primary UHS, the major process parameters evolution for the first part of the event evolution will be similar with other scenario from which they derive. Since loss of class IV power produces a faster PHT system response, the PHT inventory may swell, the Liquid Relief Valves (LRVs) open and stepback, SDS1 and SDS2 trip occurs on similar parameters as for loss of class IV power event alone. The pressure and inventory control will be ensured by the HP ECC injection. In order to ensure the HP ECC injection (and the SGs secondary side depressurization), the operator is instructed to open and mechanically block open 4 MSSVs. The MSSVs can be opened since class I electrical power is available. Until the SGs manual depressurization is done, the pressure in the SGs secondary side will be maintained at high values. The MSSVs will respond to pressure increase by staggered opening and pressure release. For Unit 1, the ECC injection will be done manually by the operator once the MSSVs were open.

Due to SBO, the only method for decay power heat removal will be the natural circulation. The core cooling will be provided by the heat transfer to SGs secondary side with heat removal to the atmosphere through the open MSSVs. Also, because class IV power is lost, the demineralized-water inventory is limited (no more demineralized water can be produced in the plant). Loss of class III power does not even permit the use of demineralized-water available from the “feedwater train”. Due to assumed loss of EPS, EWS cannot provide water to steam generators. The only reserve of demineralized-water for this sequence in the short term will be the water available in the dousing tank.
The water from the dousing tank can be provided to SGs through the BMW system following opening of the pneumatic isolation valves. The operator can control these valves from MCR or from SCA or manually from the field. The entire dousing tank inventory ensures at least 7 days for decay heat removal.

Even for the conservative case when the flow from the dousing tank cannot be controlled at all (these pneumatic valves fail open), the water could ensure a heat sink for at least 27 hours. However, this is an unlikely situation since BMW pneumatic isolating valves can be manually operated from the field.

Following Fukushima event development, the Cernavoda NPP procured two mobile diesel generators (DGs). The time to install these mobile DGs is within 2.5 up to 3 hours. The minimum time provided by the water available from the dousing tank will ensure enough time for the operators to install the mobile DG’s. The mobile DG’s will be used to power the EWS pump (they will be directly connected to EWS pumps since the EPS power supply is lost). Once the EWS pumps become available, the EWS can provide water to SGs secondary side. The thermosyphoning process will ensure decay power heat removal with steam release to atmosphere through open MSSVs.

3.6.2 Assessment of the Event and Response Capability of the Plant

The response strategy does not differentiate between the loss of RCW and the loss of RSW, because there are only minor specific differences in the set of actions required, depending of the particular system failure. They are generated by different speeds of evolution of certain important parameters (e.g. Moderator temperature) depending on the nature of the system lost (loss of RCW is a faster developing event and requires tripping the reactor sooner).

Station UPS batteries will last for 8 hours based on performance tests completed and engineering evaluation. However, the operator actions to enable the heat sinks can be performed within 45 minutes. All the actions that involve operating remote equipment (motorized and pneumatic valves, etc) should be completed in this time interval, in order to ensure the correct line-up for the alternate UHS operation: opening the required number of MSSVs, controlled opened of EWS make-up and ECC injection in pneumatic valves (fail-open), opening of ECC injection motorized valves.

The case when the SBO occurs later after the loss of primary UHS event is covered in more details in the Section 3.5, which deals with the event occurrence at low power.

Reactor Power Control (Reactor trip)

Manual tripping of SDS1 is an immediate requirement in case a loss of service water has occurred at high power. Automatic setback and trip of SDS1 on high moderator temperature provide a second line of defense, as the operator is expected to recognize and follow the loss of service water event procedure.

In the event of a RSW system failure, the most sensitive system at high power is the turbine lube oil (RSW cooled). Due to loss of cooling, the first alarms will appear on turbine lube oil temperature and will be followed by increased bearing vibrations due to the loss of lubrication properties of the oil. This could lead to increased vibrations and subsequent turbine trip, causing also the automatic reactor power reduction to about 35% by step-back. The subsequent impact on the RCW temperature will be slower, due to the thermal inertia of the high volume of water of the RCW system.

The automatic process trips of SDS1 and SDS2 caused by the loss of class IV power alone have been presented in Sections 3.3. If the “SBO” occurs at the same time with loss of primary ultimate heat sink, the plant response to this event is faster and the shutdown systems are expected to be tripped by the parameters already identified in the corresponding sections.

All the indications and logic of SDS1 and SDS2 are supplied from class I and II electrical power. Both shutdown systems are designed “fail safe”, and thus effectively performing their function in case of class I and / or class II power failure. None of SDS1 or SDS2 performances is affected by a loss of heat-sink, since these systems do not use cooling water.

3.6.3 Actions to Prevent Fuel Degradation following the Event

To ensure the availability of the equipment required for response, the decision was taken that all of the equipment will be stored on-site.

For the purpose of the SBO event response, two 1300 kW, 0.4/6 kV mobile diesel generators (one for each of Unit 1 and Unit 2) have been procured and tested by powering the 380 VAC EPS buses and the EWS pumps. The capacity of each mobile diesel generator is equivalent to that provided by the design non-mobile EPS diesel generators.

The station response at the loss of primary UHS event coincident with – or generated by – a SBO, is based on the EWS system, being powered from the mobile DG’s. For the unavailability of the EWS system (loss of Alternate – UHS), the response has been presented in Section 3.5 and consists of firewater trucks connected directly to EWS pipes through special connections. These connections are installed only if there is no other heat sink available. The firewater trucks will use the water from the fire water tanks, from the domestic water system or from the distribution bay using motor driven diesel pump. The water pumped in the EWS lines will reach the SGs secondary side and will promote thermosyphoning process or IBIF core cooling.

Time necessary to have these systems operating

The time required for electrical power restoration from the mobile diesel generators is within 2.5 up to 3 hours. This time consist of the time required to place in the operating position the mobile diesel generators, to install the power cables and to have them connected to the EPS buses / EWS pumps by shift staff. The installation of the mobile DG has been practiced in each unit.

3.6.4 Conclusions

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 loss of primary ultimate heat sink. For this case, there are three levels of defence in depth:

- the EWS from the dousing tank to the SGs. The water inventory in the dousing tank that ensure a continuous heat sink for up to 7 days. Even in the case that the water flow is not controlled (the pneumatic isolating valves fail open), the same inventory ensures at least 23 hours of continuous heat sink. Onset of significant void in PHT due to PHT reaching saturation and start boil off is expected after 27 hours from the start of the event.
- the fire water truck connected manually to EWS system piping will provide water to SGs secondary side.
- EWS pumps powered by the mobile diesel generators.

As for all the cases where the ultimate heat sinks are lost, there are at least two levels of defence, and it is concluded that no additional design changes are required.

3.7 Severe Accident Management

3.7.1 Introduction: Defence – in – Depth Approach

The CANDU 6 design approach for severe accidents is based on the defence-in-depth principle and includes both prevention and mitigation design features to cope with such events. The defence-in-depth concept considers the plant to contain multiple levels of defence, including the process system, the protective system and the containment system. These systems are designed to act independently of each other to ensure that safety targets are met. CANDU 6 has multiple, highly reliable, passive and active, post-accident heat sinks which provide ample time for plant operators to diagnose the accident, establish means of arresting core degradation in the calandria vessel and preventing further accident progression. The severe accidents progression can be stopped at the channel boundary using the moderator heat sink to remove heat. The moderator system is an inherent backup to the front-line systems if they fail. The CANDU severe accidents strategy is to retain fuel channel debris within the calandria vessel and to maintain containment integrity.

In CANDU 6 design, 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 and design provisions are made to protect the containment function and to mitigate consequences in the containment. A good understanding of the severe accidents progression in CANDU 6 plants has been established based on the analytical, research and development work performed by AECL. The results of this earlier work demonstrate that significant time is available for operator interventions to arrest the severe accident progression of such events.

Defence-in depth Approach to Severe Accidents

The defence-in-depth approach in the CANDU design incorporates four major physical barriers to the release of radioactive materials to the environment, as follows:

- The fuel matrix. The bulk of the fission products generated in the fuel are contained within the fuel grains or on the grain boundaries, and are not readily available to be released even if the fuel sheath fails.
- The fuel sheath. There are large margins to fuel sheath failure under normal operating conditions.
- The primary heat transport system (PHT). Even if fission products are released from the fuel during an accident, they are contained within the PHT. The PHT is designed to withstand the pressure and temperature loading resulting from the accident conditions.
- Containment. In the event of an accident, automatic containment isolation will occur, ensuring that any subsequent release to the environment does not occur.

Consistent with the overall safety concept of defence-in-depth, the design of the CANDU aims to prevent, as far as practicable, challenges to the integrity of physical barriers; failure of a barrier when challenged, and failure of a barrier as a consequence of the failure of another barrier. This approach is structured in five levels, as presented below:

Level 1	Prevention of abnormal operation and of failures of structures, systems, and components (SSC) by conservative design and high quality in construction.
Level 2	Detection and control of deviations from normal operation by controlling plant behaviour with both inherent and engineered design features.
Level 3	Control of accidents within the design basis by provision of inherent safety features, fail safe design, engineered design features and procedures.
Level 4	Control of severe plant conditions to manage accidents and mitigate their consequences, as far as practicable, by the robust containment design, complementary design features and severe accident management procedures.
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials by emergency support centre and plans for on-site and off-site emergency response.

The levels of defence are implemented such that the reliability of each protection level is preserved to commensurate with the expected frequency and consequence of challenges. Should one level fail, it is compensated or corrected by the subsequent level.

The above objectives are accomplished by incorporating sufficient design margins, simplifying the design, adopting high quality standards, and providing preventative features that provide a high level of confidence that an initiating event that does occur will not progress to the point of Severe Core Damage Accident (SCDA).

Prevention of SCDA requires the minimum number or combinations of systems to operate, during a specified period of time, to ensure that the following critical safety functions are met within the limits of the acceptance criteria:

- Reactivity control, which is established by rapidly shutting down the nuclear reaction and maintaining the reactor subcritical;
- PHT pressure control, which is established by limiting the peak PHT pressure to the stress limit of the ASME Code for Level D;

- Core cooling and the PHT inventory control, which is established by rapidly flooding the core with water to limit fuel failures and keeping fuel channels inside the calandria vessel intact and cooled by the moderator;
- Containment pressure suppression, which is established by cooling the containment atmosphere such that containment pressure remains below the limits and controlling the flammable gases in the containment atmosphere.

As part of CANDU terminology "severe core damage" in CANDU reactors is an event in which the core structural integrity is lost. A "loss of core structural integrity" implies that many fuel channels have failed, resulting in fuel debris accumulating in the calandria vessel.

Therefore, it is useful to distinguish two categories of severe accidents:

<u>Severe accidents within the design basis</u> 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 all Limited Core Damage (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. The implication to CANDU Severe Accident management Guideline (SAMG) is that events involving limited fuel damage would not require the use of SAMG to mitigate consequences, as such events are already anticipated and addressed by Emergency Operating Procedures (EOPs) (or their equivalent).

<u>Severe core damage accidents, beyond the design basis</u> 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)".

3.7.2 Measures to Prevent Reactor Core Damage

The Cernavoda Unit 1 and 2 Nuclear Power Plants include multiple heat sinks for normal and abnormal modes of operation & configuration of the units as measures for defence-in-depth to protect against fuel and fuel channel damage. The transport and removal of residual heat at an appropriate rate is an important safety related function required to prevent radioactivity releases above prescribed limits during all operational states and acceptable limits during and after accident conditions. The Cernavoda NPPs employ various heat transfer systems to remove the residual heat from the reactor core to an ultimate heat sink (e.g., river, atmosphere) during normal, Design Basis Accident conditions as well as during Severe Core Damage Accident conditions. The important to safety systems that transport the residual heat from the fuel to the ultimate heat sink are shown schematically in Figure 3.7-1.

3.7.2.1 Normal Operation Heat Transfer Paths

During normal operation, including normal shut down conditions, the steam generators transfer the residual heat from the PHT system to the turbine condenser. The heat is then transferred to the ultimate heat sink through the condenser cooling water (CCW) system.

3.7.2.2 Design Basis Accident Heat Transfer Path

Under Design Basis Accident (DBA) conditions, the PHT pumps may not be operable. In this case the fuel is cooled by natural circulation, referred to as thermosyphoning. If both the condenser and the main feedwater system are not operable, water is supplied from other sources and the residual heat is rejected by discharging steam directly to the atmosphere by opening the main steam safety valves (MSSVs).

In case Class IV power is lost, water supply to the steam generators is available from other sources e.g. deaerator using auxiliary feedwater pump, Danube river water using emergency water system (EWS) pumps or dousing tank (by gravity) after depressurization of steam generators through MSSVs.

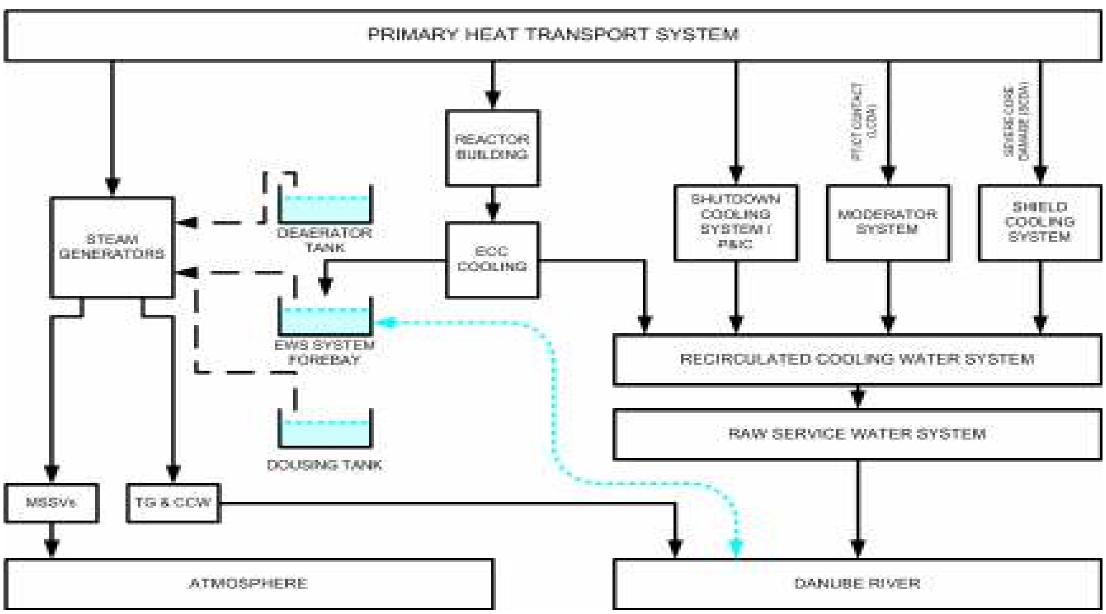

Figure 3.7-1 Schematic of Core Heat Sinks in CANDU 6

3.7.2.3 Limited Core Damage Accident (LCDA) Heat Transfer Path

For all LCDA cases considered, the pressure tubes will come in contact with the calandria tubes, but otherwise the fuel channels retain the fuel materials within an essentially normal fuel channel lattice geometry. Event progression may be halted or delayed at the LCDA stage using the moderator cooling system as a heat transfer path to the ultimate heat sink. Heat is removed via RCW / RSW systems.

3.7.2.4 Severe Core Damage Accident (SCDA) Path Heat Transfer

In case the moderator heat sink is lost following LCDA, the event will proceed into an SCDA stage- the fuel channels will fail and the core will eventually collapse to the bottom of the calandria. Event progression may be halted at this state by cooling the calandria vessel externally via the calandria light water inventory. The shield cooling system (SCS) is used to remove decay heat by cooling the exterior of the calandria vessel so that the hot core debris is retained within the vessel (i.e. calandria vessel failure is prevented). Heat is removed by the SCS heat exchangers and transferred to the RCW system.

3.7.3 Measures to Prevent Loss of Containment Integrity

This section describes the Cernavoda 1 and 2 design measures to address the three main challenges to containment integrity (i.e. containment pressurization, hydrogen control, and molten core-concrete interaction (MCCI)) resulting from progression of severe core damage to an ex-vessel state for which the calandria vessel has been breached and corium has relocated to the thick-walled concrete calandria vault.

The following structures and systems are designed as part of the Containment system for accident management:

3.7.3.1 Containment Envelope

The containment envelope; airlocks, containment penetrations and extensions, and containment isolation system provide a barrier to prevent off-site radiological releases.

a. Reactor Building;
b. Airlocks;
c. Containment Isolation System;

Reactor Building

The containments (reactor buildings) of the single unit CANDU plants are constructed with a design pressure of 124 kPa(g) (18 psig), and are proof tested at 1.15 times the design pressure during the commissioning phase of plant construction (design criteria is that there are no tensile stresses in the inner surfaces of the concrete at this pressure). In addition, full pressure reactor building leak tests are conducted at regular intervals (during plant outages) as part of the licensing requirements, while leak tests at lower pressures are conducted at more frequent intervals.

The existing CANDU 6 reactor passive design features to mitigate containment pressurization are the Containment strength (i.e., design and ultimate pressure capacity), its surfaces on which steam can condense, and its free volume. The containment structure is a single unit, single barrier, positive pressure, dry-type containment. It consists of an epoxy-lined, pre-stressed concrete cylindrical wall and a hemispherical dome structure supported on a reinforced concrete base slab. The surface area of the structures for condensation by cooling is 22,300 m^2 while the net total volume of the building within the containment envelope is approximately 48,000 m^3.

Airlocks

Containment access consists in two airlocks, the equipment airlock and personnel (emergency) airlock, and one spent fuel transfer containment door. The airlocks and spent fuel transfer containment door are designed such that access into the reactor building is possible without breaching the integrity of the containment. The airlocks are cylindrical steel structures with door assemblies at each end, one at the reactor building side and one at the service building side. For the equipment airlock, the door assembly consists of an equipment door with a personnel door mounted within it. The personnel airlock has a personnel door at each end. The spent fuel transfer containment door has the same size as the personnel doors of the airlocks.

The airlocks have electrometric double seals that are environmentally qualified to Loss of Coolant Accident (LOCA) condition on each door. Door closure can be monitored continuously and the performance of seals can be tested to assure that a fully capable barrier exists at all times. During a severe accident, the seals on the R/B side may be subject to degradation due to the extreme harsh environment. However, it is expected that the seal on the S/B will continue to provide the sealing capability, thus maintaining the containment integrity.

During a severe accident, the containment may be flooded with dousing water and D2O released from HTS and Moderator. The bottom of the airlock is at 2.1 m from the R/B basement floor. A dam of 20 cm, raises the protection level at 2.3 m from the basement floor and protects the airlock seal from exposure to water up to that level.

When water is supplied from an external source, the basement water level will rise eventually, and it should be monitored to prevent discharge of water through the airlock.

Containment Isolation System

The containment design ensures its containment structure and its internal compartments can accommodate pressurization, without exceeding the design leakage rate (the design target is ≤ 0.5% per day at design pressure). The containment envelope provides a barrier to prevent off-site radiological releases. Accident management, which includes automatic and manual containment isolation, seals the containment envelope after the initiation of an accident. The Containment Isolation System (CIS) ensures that, on demand, the containment boundary can be closed and maintained closed to limit radioactive releases to the environment. Containment isolation occurs when the R/B pressure exceeds 3.45 kPa(g) or a high radioactivity level is detected in either the ventilation exhaust from the R/B or the boiler room D_2O Vapour Recovery System exhaust line. The operator can also manually isolate the containment based on the indications and alarms from the area monitors (ensuring containment isolation is one of the first steps stipulated in the EOPs). For C1 and C2, EOPs are called Abnormal Plant Operating Procedures – APOPs). Failure to close of one or more of these pathways represents a potential release pathway to the environment.

3.7.3.2 Energy Suppression Systems

The energy suppression systems are used to control pressure and temperature of the containment atmosphere.

Dousing System

The dousing sprays are used for containment pressure suppression for a short-term following a LOCA. Dousing tank water inventory can also be used for SG make-up following a non-LOCA event. The dousing tank is filled with demineralized water dosed with catalyzed hydrazine. The tank stores 1560 m^3 for dousing water, 500m^3 for emergency core cooling plus an unused volume of 114 m^3. The dousing spray is distributed by a system of headers suitably arranged in the upper portion of the reactor building below the dousing water storage tank. For R/B pressure suppression, this system provides about 6804 kg/s into the containment via six (6) headers, each delivering spray flow of 1134 kg/s using 281 nozzles. The dousing system is normally operated automatically on high reactor building pressure; the system cycles on and off as pressure reaches 14 kPa(g) and reduces to 7 kPa(g), respectively.

The dousing valves are arranged in two independent groups. Group A valves (headers HD1, HD3, HD5) are installed in one subsystem controlled by electro-pneumatic instruments. Group B valves (headers HD2, HD4 and HD6) in the other subsystem controlled by pneumatic instruments that do not require electrical power for automatic actuation. The two dousing subsystems are completely independent and the valve actuators and instruments are of different types.
Dousing provides pressure suppression in DBAs giving rise to strong pressurization of containment, such as a main steam line break. In BDBAs, the dousing will provide initial pressure suppression when the containment pressure exceeds the initiation setpoint. For continued function during a BDBA, it is required that the dousing be provided with a long-term source of water, which can be an external source. Description to re-fill the dousing tank is discussed in the SAMG documentation.

Removal of fission products in containment atmosphere following a postulated accident is assisted by dousing water in the reactor building. The dousing system is capable of reducing the iodine and particulate fission product inventories in the containment atmosphere. Dousing (if available) also provides a means of scrubbing aerosols from the containment atmosphere in severe accidents.

Reactor Building Local Air Coolers

The containment cooling system comprises a system of local air coolers (LACs) in addition to a dousing system. The fuelling machine vault and steam generator room LACs are designed to condense the steam released from process systems to prevent over-pressurizing the R/B structure. Each LAC is comprised of a plate steel housing containing a finned tube air/water heat exchanger and a fan. Cold water from the Recirculating Cooling Water (RCW) System flows continuously through all LACs. Two manual isolation valves are provided on the water lines to each LAC. These valves are located in accessible areas. These air coolers are designed to control Reactor Building temperature during normal operation and to provide sufficient cooling to reduce R/B pressure to approximately atmospheric conditions and to bring the temperature to an acceptable level following a design basis accident. The environmentally qualified fuelling machine vault and steam generator room LACs are powered by Class IV (AC power) and supplementary for C2, LACs have a back-up power supply from EPS. Also, for C2 LACs have a additional feature to switch on low speed operation on detection of LOCA signal in order to prevent them from tripping due to the high density steam environment..

3.7.3.3 Atmospheric Control Systems

The composition of the containment atmosphere is controlled by the atmospheric control systems. Hydrogen control system is one of the atmospheric control measures.

Hydrogen Control System Design Features

Design measures used in operating CANDU to mitigate hydrogen are to dilute the containment atmosphere by inerting, or to remove the hydrogen by igniters, which provide controlled burn of hydrogen and/or passive autocatalytic recombiners
It is predicted that a LOCA with a loss of ECC and loss of moderator heat sink will produce the bounding hydrogen source term. Events involving a moderator drain are not expected to lead to as high a hydrogen source term because of a reduction in steam available to participate in the Zircaloy-steam oxidation reaction. The most significant hydrogen generation is during core disassembly.

Flammable gases such as hydrogen, if not removed or inerted can result in slow deflagrations, fast deflagrations, global or local transition from deflagration to detonation, and diffusion (standing) flames.

Inerting Containment

Currently, Cernavoda Unit 1 Severe Accident Management Guidelines (SAMG) strategy to reduce hydrogen volumetric concentration is by inerting the containment atmosphere so that in the longer term the containment integrity is not threatened. Since the containment volume is relatively large, dilution of hydrogen with containment steam or air is the most readily available means of dealing with a broad range of hydrogen releases. The containment structure is designed to promote natural circulation mixing. For both C1 and C2, PARs installation is considered in order to control long term hydrogen volumetric concentration.

Hydrogen Igniters

The Hydrogen management strategy for Cernavoda 2 is igniters and LAC fans. A network of 44 hydrogen igniters is installed within the reactor building, in the Fuelling Machine Vaults and the Steam Generator Room, areas anticipated to contain the highest hydrogen concentration after an accident. Each igniter consists of an electrically heated thermal coil, normally powered by Class II and manually backed up by the EPS, with a power dissipation of approximately 500W per igniter. All igniters are turned on automatically by LOCA signal. The LAC fans, if available, promote forced air circulation for hydrogen mixing to avoid pockets of locally high concentrations.

The hydrogen will be deliberately ignited and burned as soon as it reaches flammable concentration, avoiding its detonation at higher concentrations with consequential higher pressure within containment. Deflagrations and detonations arising from rapid generation of hydrogen can potentially be prevented by the deliberate ignition of the containment atmosphere at compositions near the flammability limit of air, hydrogen and H_2O vapour mixtures. Hydrogen igniters mitigate hydrogen generated by rapid sources, such as Zircaloy oxidation in severe accidents. Generally, hydrogen igniters burn hydrogen off when the concentration is low, or burns off pockets of locally high concentrations. Local burns do not pose challenge to containment integrity.

The hydrogen igniters may not initiate a hydrogen burn under high steam conditions when the atmosphere may be inerted, such as in an unmitigated severe accident. The use of igniters should reduce the overall risk to the containment and should not create new additional hazards such as a large pressure excursion that may challenge containment integrity. For this reason, guidelines recommend caution in the use of igniters in certain severe accident conditions, such as when LACs are available to condense steam from the containment atmosphere, which removed the inerting effect and increases the concentration of hydrogen in the containment atmosphere.

3.7.3.4 Containment Over-Pressurization

Potential challenges to the containment boundary can occur at any time during the severe accident progression and through a wide range of mechanical failures and physical phenomena.

The existing design provisions to protect the containment integrity against over-pressurization are as follows:

a. Large containment volume and passive condensation on R/B structures
b. Provisions to condense steam in the containment atmosphere: R/B Local Air Coolers (LACs) and Dousing Sprays

In order to eliminate containment integrity challenge due to over-pressurization, for both C1 and C2, an emergency filtering venting system is taken into account for installing.

3.7.4 Prevention of Re-criticality

3.7.4.1 Prevention of Re-criticality under Severe Accident Conditions

There is no requirement for engineered means to prevent re-criticality in the event of a severe accident, as described below.

The CANDU 6 reactor is heavy-water moderated and cooled. The reactor uses natural (non-enriched) uranium fuel in a 37-element bundle geometry. The fuel is located in horizontal channels in a square lattice of 28.5 cm lattice pitch, which is a design that is optimized for neutron economy. Approximately 2 channels per day are refuelled with eight bundles of fresh fuel to maintain the reactor critical with all reactivity control devices in their nominal positions. Any significant deviation from this geometry would result in a reduction in core reactivity and it would not be possible to maintain criticality. In a severe accident when the core might be in a molten state, the collapsing of fuel channels and fuel bundles into corium would reduce the overall core reactivity due to less neutron moderation which consequently leads to higher resonance absorption in uranium and keeps the molten core subcritical

3.7.4.2 Prevention of Criticality in the Spent Fuel Bay or New Fuel Storage Room

The Cernavoda Unit 1 and 2 NPPs spent fuel bays use light water to cool the spent fuel and provide shielding for operators. The 37-element natural-uranium fuel bundles in an infinite array in a light-water medium have been demonstrated to remain subcritical[1]. It has been shown that in the most reactive state of an infinite array of natural-uranium fuel bundles in light water, the maximum multiplication factor is 0.93. This condition bounds the storage arrangement of both fresh and irradiated fuel bundles since the fuel-bundle arrangement in the new fuel storage (NFS) room (and in the irradiated-fuel storage bay are less than optimal and consist of additional structural materials.

The NFS room located in the S/B is at elevation EL 100 m. There is no source of heavy water at higher elevation in the S/B. The only significant amount of heavy water in the S/B is located at a lower elevation (EL 93.9 m) on the opposite side of the S/B from the NFS room in heavy-water supply tanks. In the unlikely event that all the heavy-water supply tanks were to be damaged, there would be no flow path leading to the NFS room therefore it would not lead to nuclear criticality.

Therefore handling and storage of fresh and irradiated natural-uranium CANDU 37-element fuel bundles in a CANDU 6 NPP do not pose any out-of-core criticality hazard. Moreover, there is no credible way this could lead to a criticality accident.

3.7.5 Measures to Limit Radioactivity Release – Emergency Planning

On-site emergency plan takes into account radiological consequences, which can result from the design basis accidents (DBA) or severe accidents of a CANDU reactor type. For design basis accidents, the safety analysis shows limited radiological consequences by calculating doses, for each postulated accident, which are demonstrated to be within the approved limits.

For the CANDU plants, the paramount concern during the progression of a severe accident is radiological protection of the public and the environment, including the avoidance of land and aquatic contamination. This is achieved by managing all activities affecting the release of fission products. The airborne releases of fission products could originate from containment or from systems that by-pass containment. Release pathways from containment could include a failed penetration or general leakage through cracks in the containment structure. Releases that bypass containment could include releases from the secondary side such as from steam generator tube(s) rupture, or from a break in the primary system piping that extends outside containment (e.g., ECC piping). Release of waterborne radioactivity from inside containment into the external waterways is highly improbable as there is no direct pathway to the environment; multiple failures are required before waterborne releases to the environment were to occur.

In general, the mitigating strategies are in the following order:

- Isolate the leak path to the environment (close isolation valves, dampers, airlock seals, crimp);
- Reduce the driving force using a containment heat sink (local air coolers and dousing serve multiple purposes – they not only remove heat, but also condense steam to reduce pressure, and remove fission products by plate-out and wash-out);
- Reduce the driving force by venting through a filtered, monitored release path (this is the lowest priority strategy because there is a temporary increase in release rate until the driving force for leakage is reduced).

Emergency response activities sequence

In accordance with "On-site Emergency Plan", approved by CNCAN and reviewed by the Inspectorate for Emergency Situations "DOBROGEA" of Constanta County, any event, which involves an actual or potential release of radioactive materials into environment that require urgent protective actions off site, is classified by the affected unit Shift Supervisor (SS) as **"General Emergency"** (level 4 of the emergency classification system; other emergency levels are: level 1 – Alert, level 2 – Station Emergency, level 3 – On-Site Emergency).

The emergencies at Cernavoda NPP are classified on the basis of the following criteria:

a) station / systems / personnel status;
b) radiation hazards.

Therefore, General Emergency is declared in case of events with radiation consequences both on-site and off-site, caused by:

- loss of reactivity control, or
- loss of core structural integrity, or

- degradation of a process system, which make necessary to initiate the two special safety systems (ECC and Containment Isolation), simultaneously with the Containment Isolation System impairment.

Based on radiation hazards, General Emergency is declared in the following conditions:

- External dose rate ($\dot{H}_{ext}$) in normally occupied areas of the station*: $\dot{H}_{ext}$ > 10 mSv/h, or
- External dose rate ($\dot{H}_{ext}$) at off-site / beyond the site boundary: $\dot{H}_{ext}$ > 1 mSv/h, or
- Total activity released to stack (confirmed release), averaged on 15 minutes, which lead in 1 hour the off-site doses: H > 1 mSv, or
- Total activity in the containment, based on the results from Post Accident Sampling and Monitoring System: Λ_{GN} > 9E14 Bq / Λ_I > E13 Bq.

***a**reas (from 2 and 3 Radiological Areas) where in normal conditions the dose rates are smaller than 10 µSv/h

In case of emergency classified as "General Emergency", the On-site Emergency Organization (see Figure 3.7-2) is activated and emergency response activities are initiated in the following sequence:

- Shift Supervisor (SS) notifies plant personnel about the initiated event through the public address system and site siren system requiring on-site personnel to assemble in assembly areas (done in approx. 5 minutes after the event classification), and all non-essential personnel evacuate the site;
- SS activates the Intervention Support Center (ISC) from the main control room of the unit affected by the event: Intervention Coordinator arrives in the ISC, obtain information about the event from SS and set initial strategic objectives of response activities (done in approx. 10 minutes after the event classification.;
- Intervention Coordinator notify management and support staff in the emergency, which is composed of personnel working in the On-site Emergency Control Centre, staff working in the operational centers of the county and local public authorities and members of the on site / off-site monitoring teams (done in approx. 12-13 minutes after the event classification);
- Intervention Coordinator, with the approval of the SS, makes the initial notification of public authorities: communicating critical information on plant status and submitting recommendations on protective measures for the population to the authorities involved in off-site intervention, if the accident is type I (accidents with immediate loss of containment integrity). In this case, in order to establish and transmit quick recommendations on protective measures, the emergency procedure "Determination of Population Protective Measures" defined pre-established recommendations on protective measures for all identified accidents type I, depending on the meteorological conditions (wind direction), affected sectors, localities placed in those sectors, distances from the plant, anticipated whole body effective doses and anticipated thyroid committed doses (done in max. 30 minutes after the event classification ;
- Main control room personnel carry on operating activities in emergency situations, which aim to bring the plant into a safe state, ensure proper cooling of the fuel and reduce or stop radioactive emissions from the containment using APOPs or Severe Accident Control Room Guide 1 (SACRG-1) if the event directly leads to core damage, based on the criteria provided in the APOPs;
- Intervention Coordinator initiates the following emergency response activities: checking of the accounting results and implementing protective measures for on-site personnel, and monitoring of the affected unit;
- Up to the activation of the On-site Emergency Control Centre, the SS fulfills the Emergency Manager duties regarding management and coordination of activities whose purpose is to protect the public, the environment, the plant and on-site personnel;
- Activates the On-Site Emergency Control Centre: members of Command Unit (Emergency Manager, Emergency Technical Officer, Emergency Health Physicist and Emergency Administrative Officer) arrive in On-site Emergency Control Centre, get information (status of

plant, staff, notifications made, etc.) about the event from the SS and review the response activities strategic objectives (required time: 15 minutes after notification of the emergency management and support personnel during normal working hours / until 2 hours after notification of the emergency management and support personnel outside normal working hours ;

- Emergency Manager takes the lead in coordinating of the emergency response activities from the SS;
    - Emergency Health Physicist (EHP) establishes the on-site / off-site radiological monitoring strategy and coordinating of the monitoring teams (In-station Survey Team and two On-site / Off-site Monitoring Teams). The EHP, aided by the EHP Assistant processes the data received from the monitoring teams, Gaseous Effluent Monitors System (if the release is going on through the stack) and Off-site Gamma Monitoring System (this is an on-line gamma monitoring system which contains 15 gamma monitoring stations, two of them being installed at each stack of both units and 13 being installed in range of 3 km around the plant) and establishes protective measures for population and on-site personnel.;
- Emergency Administrative Officer coordinates the implementation of protective measures for staff on site;
- Emergency Health Physicist with the Emergency Notification Forms completed regularly updates information for Public Authorities regarding plant status and recommendations on protective measures for population;
- Emergency Technical Officer coordinates the Technical Support Group to provide technical advice in timely manner to the Emergency Manager and to the Shift Supervisor. If SAMG entry condition is met, the Technical Support Group use the SAMG, based on Diagnostic Flow Chart (DFC) and Severe Challenge Status Tree (SCST) parameter values, to evaluate and recommend recovery actions/or strategies to reach a controllable, stable plant state;
- In case of a severe accident, Main Control Room staff implements SAMG strategies recommended by the Technical Support Group, executing special SAMG Enabling Instructions and provide all necessary information about the status of plant equipment and conditions;
- Technical Support Group monitors all potential hazards on long-term and confirms / records if implemented strategies continue to function. When all the monitored parameters are stabilized or a steady decline, the Technical Support Group then assesses the Severe Accident Management Exit Guides for "exit" conditions.

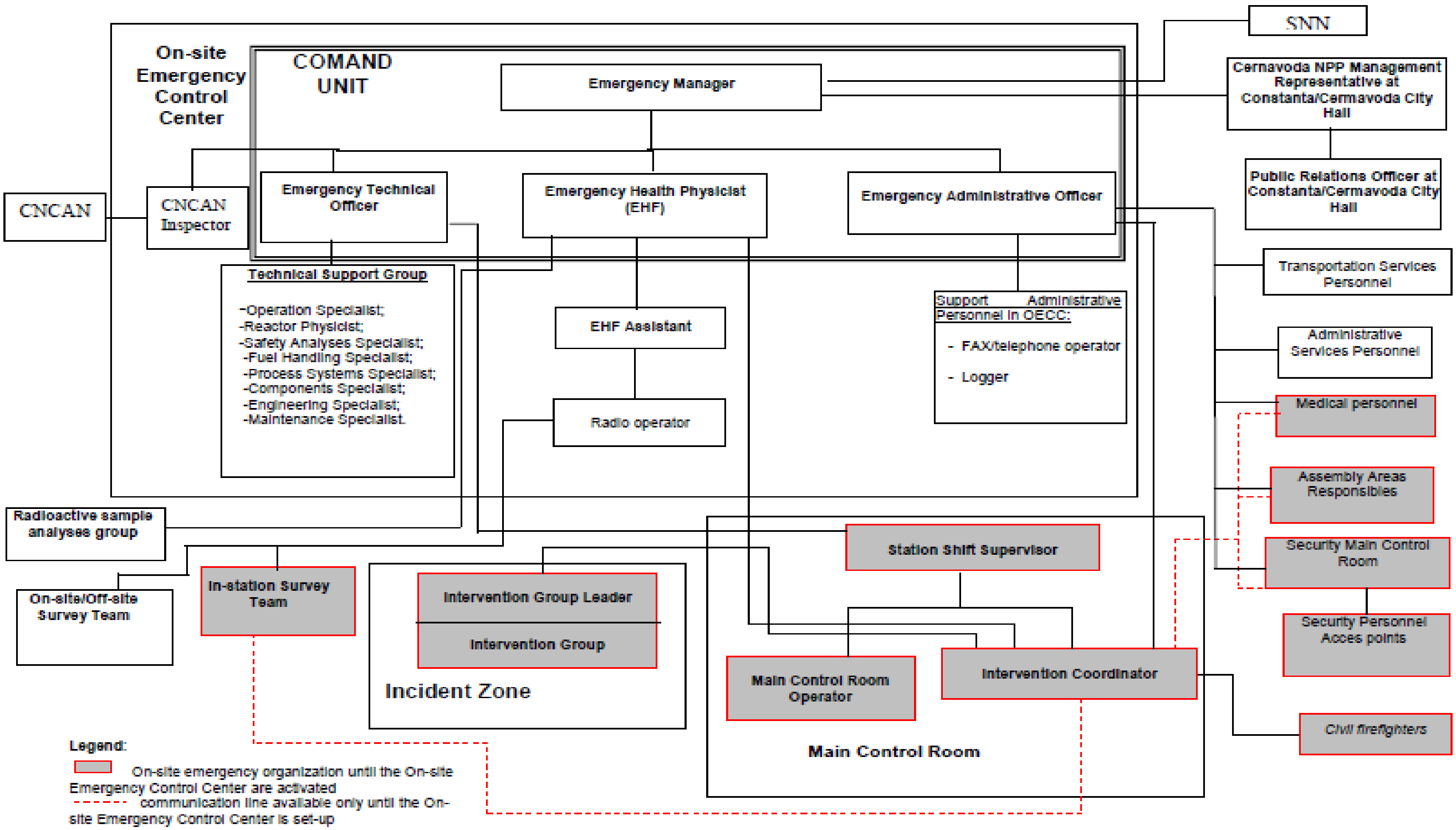

Figure 3.7-2 On-Site Emergency Organization

3.7.6 Loss of Spent Fuel Bay Cooling

3.7.6.1 System description

Spent Fuel Bay cooling and purification system provides cooling and purification of the water within the spent fuel bay. The Spent Fuel Bay system consists of 4 bays filled with water in which spent fuel is discharged from the core using fuelling machine facilities. Cooling and purification for these bays is ensured by 3 Class III power pumps, 3 heat exchangers, 2 purification lines with filters and ion exchange columns, associated piping and instrumentation.

The four Spent Fuel Bays are:

- discharge bay – walls and floor are covered with epoxy
- reception bay – stainless steel plated in Unit 2 and epoxy covered in Unit 1
- failed fuel storage bay – walls and floor covered with epoxy and
- spent fuel storage bay – stainless steel plated in Unit 2 and epoxy covered in Unit 1.

The spent fuel storage bay (sometimes referred to as the Spent Fuel Bay or SFB) is the largest and is a pool which is stainless steel plated in Unit 2 and epoxy liner covered in Unit 1. All Spent Fuel Bay s are filled with demineralized water that is circulated with the provision of pumps in order to cool the spent fuel stored on fuel racks inside the pool. The heat transferred from the spent fuel is removed by plate type heat exchangers using RCW - recirculated cooling water (in Unit 2) or RSW - raw service water (in Unit 1). The water in the Spent Fuel Bay also provides shielding from radiation fields emitted by the fuel.
Spent Fuel Bays and associated piping are DBE qualified in order to preserve their integrity after an earthquake.

CANDU 6 nuclear power plants use on-line refueling by design. During normal operation 2 fuel channels are refueled per full power day, refueling being executed during full power operation. During normal refueling operation 8 out of 12 fuel bundles are replaced for each fuel channel selected for refueling, meaning that 16 spent fuel bundles per full power day are removed from the reactor core and are stored in the Spent Fuel Bay for cooling. The spent fuel must be water cooled inside the Spent Fuel Bay for 5 to 10 years, and after this period the spent fuel is transported to dry storage facilities, when residual heat is low enough to be adequately removed by natural air circulation.

3.7.6.2 Loss of SFB Cooling

Based on a prolonged loss of spent fuel bay cooling, make-up water is required to prevent uncovering of the spent fuel and potential hydrogen generation. The calculations performed show that 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 (9 days until radiological fields in Spent Fuel Bay rooms start to increase significantly (to 1.7 mSv/h), and 15 days until first fuel bundles become uncovered), the loss of Spent Fuel Bay cooling event can be managed successfully following the applicable Abnormal Plant Operating Procedure. Therefore, 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.

3.7.7 Cernavoda Crew Response Preparedness

3.7.7.1 Human resources in case of emergency

The human resources appointed for emergency response activities include the followings:

- Operation personnel assigned to perform the emergency operation activities and to accomplish the emergency functions from Main Control Room and Incident Area;
- Emergency management and support personnel, assigned to accomplish the emergency functions from the On-Site Emergency Control Center, monitoring teams, Cernavoda NPP Management Representatives and Public Relations Officers at Constanta and Cernavoda town hall. For every emergency function there is appointed and trained personnel organized in 5 emergency management and support crews. In order to ensure the continuity of the human resources in case of emergency, the appointed personnel is scheduled in 3 shifts, both during normal working hours and after normal working hours (on-call). The On-site Emergency Control Center is considered set up when the minimum shift complement, constituted by the Command Unit members (Emergency Manager, Emergency Technical Officer, Emergency Health Physicist and Emergency Administrative Officer), is present in the Emergency Control Center (on-site/off-site).
- Personnel assigned to Assembly Area Responsible positions;
- Medical personnel which constitutes the necessary support in case of medical incidents;
- Professional civil firefighters which are part of the Response Team;
- For firefighting purpose, permanent support will be provided by Cernavoda Military Fire Brigade and other neighboring Military Fire Brigades.

3.7.7.2 Official agreements

There are also other documents and official agreements which support the Cernavoda NPP Emergency Planning and Preparedness Program:

- A protocol agreed with the Constanta County Inspectorate for Emergency Situations, Police County Inspectorate, National Roads and Bridges Company and County Roads and Bridges Company in order to provide the necessary support for the Cernavoda NPP personnel in case of emergency, when the roads are blocked due to extreme meteorological conditions, natural disasters (earthquakes, flooding etc) or other traffic restrictions.
- A contract with a transportation company in order to provide the necessary vehicles for the on-site personnel evacuation in case of emergency;
- A protocol agreed with “IOWEMED” Medical Centre in order to provide medical services (first aid, initial treatment and decontamination) for the injured and contaminated personnel prior to transfer them to the hospital;
- A protocol agreed with the Cernavoda Hospital in order to provide medical services (treatment and decontamination) for the injured and contaminated personnel;
- A protocol agreed with the Constanta Hospital in order to provide special medical services for radiation exposed personnel. This medical facility has all the necessary equipment for taking care of overexposed personnel.

All these station documents have been approved by Station Management and by equivalent external Organizations Management, as applicable.

3.7.7.3 Emergency facilities and equipment

Provisions for emergency response are designated facilities of adequate size and location, supplied with appropriate communication means and equipment that can be brought into operation without delay in the event of an emergency, to support the emergency response activities. The emergency equipment and resources cover the plant status and radiological hazard assessment, personnel protection, damage control, fire fighting, first aid, communication and data transfer requirements.

The **On-site Emergency Control Center** is a specially equipped area from which the emergency response activities are directed and coordinated.

The On-Site Emergency Control Center is brought into operation under emergency conditions and is appropriately equipped to ensure the continued management of the emergency activities:

- necessary equipment for technical assessment and strategically decisions making (critical safety parameters display, meteorological and on-site radiological data display, personnel accounting results display);
- data handling, processing and display equipment;
- copies of emergency plan, emergency procedures and all necessary technical documentation ;
- communication equipment (including backups);
- the site personnel and the neighboring population warning equipment;
- personnel protective equipment.

3.7.8 Conclusions

The Cernavoda NPP reactor design is based on the defence-in-depth principle, and it is equipped with safety systems, multiple and diverse heat sinks available to cater for severe core damage accidents. Each system uses a combination of passive and active features to ensure maximum reliability of the heat sinks during accident conditions.

Severe accident progression in CANDU reactors 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 surrounds the calandria vessel in CANDU 6 plants, provide a heat sink capability which, in many event sequences, will delay the progression sequence significantly. Such delays are of benefit in that they provide decision and action time for accident mitigation and management measures to be taken. The approximate inventory of heavy and light water, available for heat removal, is as follows: ~120 Mg heavy water in heat transport system (PHT), ~230 Mg heavy water in calandria and ~500 Mg of light water in calandria vault. These significant quantities of water inventories surrounding the fuel and the entire core as a heat sink to remove the decay heat after reactor shutdown, even if all engineered heat removal systems fail. There is no need for any operation of any valves or pumps as heat removal is through passive boil off. The large water volumes mean that such boil off times are long (many hours), extending time available for the implementation of severe accident management actions.

This allows time for decay heat to reduce, and for accident mitigation and management measures to be taken. Cernavoda NPP has adopted the CANDU Owners Group Severe Accident Management Guidelines-(SAMG) approach to develop and implement Cernavoda specific strategy to mitigate the effects of severe accidents. Severe Accident Management Guidelines provide the necessary guidance to operator to terminate the progression of such events. Mitigation strategies presented in SAMGs are considered adequate in order to manage a severe accident.

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. Its effectiveness requires limiting the interior temperature and pressure following such an event. In general, the main challenges to containment integrity in the event of a severe accident are: Containment slow over-pressurization, hydrogen control, and MCCI.

The challenge to containment integrity in the event of a severe accident is slow over-pressurization due to steam generation by decay heating as a result of a loss of the heat sinks. Multiple provisions are available to avoid steaming in to the containment; highly reliable, active, post-accident heat sinks are provided for the PHT, the calandria vessel, and the shield cooling, which would stop the steaming into the containment atmosphere when available. The reactor building has the Local Air Coolers dedicated to cool the containment atmosphere. The dousing sprays are used for containment pressure suppression. They are initiated automatically upon detection of high pressures that may challenge containment integrity.

Flammable gases such as hydrogen, if not removed or inerted can result in slow deflagrations, fast deflagrations, global or local transition from deflagration to detonation, and diffusion (standing) flames. Hydrogen detonations have potential to damage the containment envelope. For both units installation of passive autocatalytic recombiners is considered, due to the fact that these recombiners do not need any external power supply.

Containment structure designed to provide natural circulation mixing. The LAC fans, if available, promote forced air circulation for hydrogen mixing to avoid pockets of locally high concentrations. Cernavoda Unit 1, the provision for hydrogen control is to reduce hydrogen volumetric concentration is by inerting the containment atmosphere so that in the longer term the containment integrity is not threatened. Cernavoda 2 is equipped with igniters to deliberately ignited and burned the hydrogen as soon as it reaches flammable concentration; thus avoiding its detonation at higher concentrations with consequential higher pressure within containment.

In the unlikely case of ex-vessel core damage, potential molten corium-concrete interactions may challenge containment integrity by pressurization from non-condensable gases and steam production. The Cernavoda NPPs provides sufficient floor space for debris spread and means to keep the debris on the floor submerged in water.

The 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 On-Site Emergency Control Centre is the headquarter 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. Habitability and accessibility (radiation fields at vital areas of the plant) assessments have been performed. The assessments have shown that control room operating staffs can safely respond to the hypothetical severe accidents from the MCR or SCA without exceeding the allowable regulatory dose limits. Robust accident management program is in place, with APOPs mainly for prevention of severe accidents, and SAMGs for severe accident mitigation. Comprehensive SAMG training for all emergency response personnel have been completed or planned by the end of August 2011. SAMG drills are being incorporated in the overall Emergency Response Training Program.

The information presented in this section demonstrates that the comprehensive emergency response program and provisions for responding to emergencies, including severe accidents, are in place:

- 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 responses

All provisions of the emergency program, including the associated documentation, have been tested / rehearsed and approved by station management and the regulatory body.

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 (likely to involve the use of equipment in ways that are not intended by the design). 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. Note that two mobile diesel generators have been provided in a secure location on-site for hook-up to provide power when EPS is not available. 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.

4. Overall Conclusions

Based on the information contained in the preceding sections and the assessments made, it is concluded that both Cernavoda units, as designed, meet the safety design requirements as stipulated in the original design while having sufficient safety margins against severe earthquakes, flooding, loss of electrical power and the loss of ultimate heat sink. Potential improvements and enhancements to increase the available safety margins even more have been identified. A separate evaluation was performed using a risk-informed process to determine which improvements or enhancements were required for implementation on a priority basis. Plans are currently in place to implement the selected enhancements in both units.