19.10.2009 APPENDIX 1

PRELIMINARY SAFETY ASSESSMENT OF THE FENNOVOIMA NUCLEAR POWER PLANT PROJECT

APPENDIX 1: FEASIBILITY ASSESSMENT FOR PLANT OPTIONS

Unofficial translation

INTRODUCTION

Fennovoima submitted to STUK, as supplements to its application for a decision-in-principle, descriptions of the technical design of each alternative power plant unit together with its estimate of how each unit fulfills the requirements presented in the Government Decree on the Safety of Nuclear Power Plants (733/2008). The following is the assessment of STUK as to how the design objectives and principles of each of the power plant unit alternatives presented in the application for a decision-in-principle comply with Finnish safety requirements.

The preliminary safety assessment concerns two nuclear power plant units with a boiling water reactor, ABWR and KERENA (formerly SWR1000), and one nuclear power plant unit with a pressurized water reactor, EPR. These units employ both active and passive safety systems. An active system is a system based on devices that rely on an uninterrupted external power source. A passive system is a system whose operation does not depend on operator action or an external power source apart from the actuating function (e.g. valve position change), or which in the event of power loss automatically enters a safe state. The component performing the actuating function must have a passive power source such as an electrical battery or a pressure accumulator. The safety functions of the KERENA unit are largely based on passive systems. In the ABWR unit, the role of passive systems has been substantially increased in comparison with currently existing similar units. The safety functions of the EPR unit do not materially differ from those of currently existing similar units. In all unit alternatives, severe accidents are taken into account in the design. The principal data on these alternatives are given in Table 1.

Table 1. Power plant unit alternatives.

Unit	Supplier	Type	Thermal output	Electrical output
ABWR	Toshiba-Westinghouse	Boiling Water Reactor (BWR)	4300 MWt	c. 1600 MWe
KERENA	Areva	Boiling Water Reactor (BWR)	3370 MWt	c. 1250 MWe
EPR	Areva	Pressurized Water Reactor (PWR)	4590 MWt	c. 1700 MWe

The boiling water and pressurized water reactor units are presented each in a separate section, in alphabetical order.

BASIS FOR ASSESSMENT OF PLANT ALTERNATIVES

The assessment is based on the requirements provided for in the Government Decree on the Safety of Nuclear Power Plants (733/2008). The following is a

discussion of the requirements against which the power plant unit alternatives were assessed.

Assessment and verification of safety (Government Decree 733/2008, section 3)

Section 3 of the Decree specifies how nuclear power plant safety and the technical solutions of its safety systems shall be substantiated by using experimental and calculational methods.

The preliminary safety assessment notes with regard to the requirements in section 3 that the power plant unit supplier employs deterministic and probabilistic calculation methods that have been appropriately qualified and that these models have been employed in earlier power plant projects. The assessment also addresses how the power plant unit supplier has proven the functionality of new, previously unused features through experimental methods.

Limitation of radiation exposure and release of radioactive materials (Government Decree 733/2008, sections 8 to 10)

Sections 8 to 10 of the Decree set the limits for the annual dose of an individual in the population during normal operation, in case of an anticipated transient and in case of an accident. The preliminary safety assessment addresses the question of whether the power plant unit supplier employs appropriate analysis methods and compares analyses performed on the reference power plant to the limits set.

Engineered barriers for preventing the dispersion of radioactive materials (Government Decree 733/2008, section 13)

Pursuant to section 13 of the Decree, the engineered barriers preventing dispersion of radioactive materials from the nuclear power plant into the environment are the fuel cladding, the primary circuit and the containment building. These successive barriers implement what is known as the principle of defense in depth.

On the one hand, the preliminary safety assessment addresses the supplier's potential for manufacturing high-quality barriers to dispersion that can be relied on to maintain their integrity and seal. On the other hand, it is assessed whether the design principles for the safety functions of the power plant unit take sufficiently into account all postulated situations in which the mechanical and thermal loads on the barriers to dispersion must remain within the design limits.

Safety functions and provisions for ensuring them (Government Decree 733/2008, section 14)

Pursuant to section 14 of the Decree, the key safety functions are reactivity management, cooling the reactor, and retaining radioactive materials within the plant. The power plant units are assessed for how well they fulfill the principles of

redundancy, separation and diversity. It is important to take these principles into account early on in the design process of the power plant, because implementing them through changes made later would be extremely difficult and demanding.

The principle of redundancy refers to the design of safety systems so that they consist of multiply redundant sub-systems. The most important safety systems must be operable even if any one of the individual system components fails and any other component of the same system is simultaneously unavailable.. Multiple redundancy must similarly be provided for essential support functions of the safety system devices. Also, the electricity supply must be designed so that both external and internal power sources can be employed. An external power source is understood to mean a connection to the normal power grid, while an internal power source means any alternative power source within the power plant itself.

The principle of separation means that the multiply redundant components of the safety systems must be housed in different parts of the power plant, or at the very least separated from one another with robust structures. Also, critical safety systems must be housed in a different building or space from other parts of the power plant. This increases protection against internal and external threats to the power plant.

The principle of diversity means that the safety systems must be backed up with systems or devices based on different operating principles than the primary systems. This helps improve the reliability of plant safety and avoid consequences caused by simultaneous failures across the safety systems. The principle of diversity must be applied to those safety systems designed to contain the consequences of an anticipated transient and a Class 1 postulated accident. An anticipated transient and a Class 1 postulated accident refer to initiating events expected to occur more frequently than once every 1,000 years. Events concerning the behavior of the power plant during a transient or a Class 1 postulated accident combined with a common-cause failure in the safety systems are described as design extension conditions (DEC). Any rare accident or external event or a complex combination of failures shall also be considered a DEC event. The design principles for the systems required for managing the situations examined (diverse systems) and the design principles ensuring the independence of the primary safety systems and their diverse systems must be presented in assessing the feasibility of the power plant unit alternatives. STUK presented the DEC requirements in its separate decision Y55/3 (April 8, 2009) and its supplement.

Protection against external events (Government Decree 733/2008, section 17)

Section 17 of the Decree gives requirements for how the safety functions of a nuclear power plant must be protected against external events. External events may threaten the integrity of systems, structures and devices related to safety functions, cause a transient or an accident, or prevent safety functions from being executed. Such events include at least various weather phenomena (high or low temperatures,

high winds, blizzard), earthquakes, high sea level (flooding) and illegal activities undertaken to damage the plant, including a large airliner crash. Here, it is assessed how the aforementioned events have been taken into account in the power plant design.

Protection against internal events (Government Decree 733/2008, section 18)

Section 18 of the Decree specifies how the systems related to safety functions must be protected against internal events, as section 17 specified for external events. Internal events include fires, pipe breaks, container breakages, missiles, explosions, falling of heavy objects and flooding due to leakage. Here, it is assessed how the aforementioned events have been taken into account in the power plant design.

Monitoring and control of nuclear power plants (Government Decree 733/2008, section 19)

Section 19 of the Decree contains requirements on the protection automation, control room, emergency control post and local control systems of a nuclear power plant. Here, the implementation of the requirements of section 19 and the principles of redundancy, separation and diversity specified in section 14 in key automation systems are assessed.

POWER PLANT UNIT ALTERNATIVES WITH A BOILING WATER REACTOR

ABWR – Advanced Boiling Water Reactor, Toshiba-Westinghouse

General

ABWR is a boiling water reactor with an electrical output of about 1,600 MWe designed by Toshiba-Westinghouse of Japan. The first ABWR power plant unit designed and implemented by Toshiba was built in Kashiwazaki-Kariwa in Japan in the early 1990s (KK6) and the second immediately afterwards (KK7). The reference plant for the plant type being proposed for Finland is Hamaoka 5, completed at the beginning of 2005. In addition to the aforementioned plant units, there is one further ABWR plant unit in use in Japan, two under construction and several more planned.

In its feasibility study for Finland, Toshiba-Westinghouse have improved on the reference plant unit by adding certain safety features required in Finnish safety provisions. The planned service life of the plant is 60 years. The basic design of the plant unit is fairly advanced. The design objectives and principles largely comply with Finnish safety requirements.

Both active and passive safety systems are employed in the ABWR plant unit.

Assessment and verification of safety (Government Decree 733/2008, section 3)

Deterministic analysis methods and preliminary results

For evaluating and verifying safety, the plant supplier has access to the deterministic analysis methods of Toshiba and Westinghouse Electric Sweden (formerly ABB ATOM). The Westinghouse analysis methods were and are used in the design and operation of the Olkiluoto 1 and 2 power plant units. The methods have been appropriately maintained and qualified for their purpose. Analyses conducted on the ABWR unit indicate that transient and accident analyses compliant with Finnish requirements can be performed for this unit alternative.

Probabilistic analyses

Toshiba employs level 1 and 2 probabilistic risk analysis (PRA) methods that have been used for PRA analyses on the plants built by Toshiba in Japan. The analyses are primarily based on Japanese and American component failure databases. The analyses conducted by Toshiba on Japanese plants cover all events related to external and internal threats at the plants in all operating states. The analysis methods and information about the ABWR analysis results indicate that analyses compliant with Finnish PRA requirements can be performed for this unit alternative. If necessary, the methods can be further developed on the basis of Finnish detailed requirements. The probabilistic risk analyses will be conducted in connection with detailed planning of the power plant, and the fulfillment of Finnish safety requirements will be assessed at that point.

Qualification of new types of systems

Passive systems of a type not previously used in a nuclear power plant are planned for the Toshiba ABWR unit. These include isolation condensers (IC) cooling the reactor circuit directly and a passive containment cooler system (PCCS) used for extraction of residual heat in case of a transient or an accident. Toshiba has qualified these systems experimentally. The test program comprised tests on an individual heat transfer tube from a condenser associated with residual heat removal and tests on full-scale condensers. The tests involved experimentation on heat transfer mechanisms and the impact of non-condensing gases over a wide range of parameters. Based on these tests, a correlation of the effect of non-condensing gases on the heat transfer capacity of the condenser was developed. Tests and theoretical analyses have shown that both the IC and the PCCS will function reliably in accident conditions.

Limitation of radiation exposure and release of radioactive materials (Government Decree 733/2008, sections 7 to 10)

Toshiba has made a preliminary calculation of the radiation exposure of the population in the vicinity of the plant in the case of an accident. The calculations are based on a Class 2 accident (where the initiating event is assumed to occur less than once every 1,000 years). The analyses are based on Toshiba analysis methods previously used in the licensing of similar power plants in Japan. The analysis results indicate that the doses remain below the dose limits set for Class 2 accidents in Finland.

The analysis results and the design features of this power plant concept indicate that analyses compliant with Finnish requirements can be conducted for this unit alternative at a later stage in the licensing process and that the dosages will remain below the dose limits set in Finland in case of other occurrences and accidents too.

Engineered barriers for preventing the dispersion of radioactive materials (Government Decree 733/2008, section 13)

Reactor and fuel

The ABWR unit is a boiling water reactor with main circulation pumps inside the reactor pressure vessel; in terms of its operating parameters and safety properties, it is comparable to existing large boiling water reactors. There are 10 main circulation pumps in all. There are 872 fuel assemblies and 205 control rods. The reactor is intended to use fuel types already in use in existing boiling water reactors or developed from them. Reactivity is controlled during the operating cycle with the main circulation pumps, solid burnable absorbers in the fuel and the control rods.

The stability of the reactor is ensured using the same methods as in existing boiling water reactors: partial scram, core and fuel design, and protective functions. Stability control will be assessed in more detail at later stages in the licensing process. No operational occurrences related to reactor stability problems have occurred at the ABWR power plants in operation in Japan.

The planned fuel burn-up is greater than the maximum fuel assembly burn-up allowed in Finland, 45 MWd/kgU. However, the reactor can be adapted to conform to the Finnish burn-up limit. If approval is sought for a higher burn-up level, the applicant must be able to demonstrate experimentally that the fuel fulfills Finnish design criteria regarding accident situations.

The reactor and fuel designs fulfill Finnish requirements. Certain details such as reactor stability and the maximum fuel burn-up will require further analyses and possibly further testing at later stages in the licensing process.

Main nuclear components

The main nuclear components of the primary circuit of the ABWR unit are based on solutions proven in terms of materials and manufacturing technology. The reactor pressure vessel is made of low-alloy steel, which is shaped into forgings and welded together to produce the pressure vessel. The inside of the pressure vessel is lined with welded stainless steel. Nickel alloys with high durability are also used for corrosion protection of the main components.

The demands placed on the materials and welds in the reactor are set with a view to the planned service life of the plant. Radiation embrittlement of the reactor core area is taken into account in the material choices and will be monitored by means of a program based on normal practice. Proven materials are used in components associated with the reactor, such as the main circulation pumps, the control rod drive mechanisms, the pipe nozzles and the reactor internals to mitigate the detrimental effects of stress corrosion, thermal fatigue, ageing and other runtime phenomena. Attention will also be paid in the main component material choices to the maximum amount of additives increasing the activity of the primary circuit.Erosion corrosion in the main steam and feedwater lines will be minimized through control of flow and environmental factors.

Breaks in pipes connected to the primary circuit are taken into account in the design of the primary circuit. The dynamic effects (pressure shocks) of these breaks on other components and structures will be analyzed using methods approved in Finnish safety requirements. The safety systems are designed to take into account the pipe break with the largest diameter in the primary circuit. The main steam tunnel over the main control room will be provided with adequate protection.

The design objectives and principles proposed for the main nuclear components comply with Finnish safety requirements.

Reactor pressure control

The ABWR unit has 18 safety/relief valves for reactor pressure control. All 18 valves are used for restricting pressure; they are opened by a pneumatic pilot valve controlled by the reactor protection automation or in direct response to reactor pressure against a spring load.

Out of the 18 valves, 8 are reserved for depressurization; they open in response to a low water level in the reactor pressure vessel. Only two valves are required for rapid pressure reduction in the reactor. In order to improve reliability, the pneumatically controlled safety/relief valves have their own nitrogen tanks.

The isolation condensers (IC, 4 x 33%) can be used for pressure control in transient and accident situations. The isolation condensers are connected to the

steam and feedwater pipes. Once the system starts up, the steam flowing from the reactor to the steam pipes is drained into the heat exchanger and condensed into water, which is fed through the feedwater pipes back to the reactor. There are two parallel valves with different operating principles between the isolation condenser and the feedwater line. Only one of these valves needs to open to activate the isolation condenser. The isolation condenser is designed to respond to a short blow-down (just once) from the safety/relief valves in a dimensioning pressure transient. This restricts the blow-down of coolant from the primary circuit into the suppression pool, meaning that the water level in the reactor is simple to maintain in the case of a transient or an accident.

The design objectives and principles of reactor pressure control comply with Finnish safety requirements.

Containment building

The containment building is a conventional pressure suppression containment building typical of boiling water plants. During power operation, a nitrogen atmosphere is present within it. In loss of coolant accidents, the steam discharged from the reactor circuit into the containment building is forced by the differential pressure into the suppression pool. The residual heat generated in the reactor is removed from the suppression pool by means of the residual heat removal system. The containment building is designed to retain its integrity in compliance with the approval criteria in the case of a transient or an accident.

Severe accidents

Severe reactor accidents in the ABWR unit are managed by reducing pressure in the primary circuit before the reactor pressure vessel bursts, cooling the core melt in the core catcher under the reactor pressure vessel, and controlling pressure in the containment building with the passive residual heat removal system.

There are eight pneumatically controlled and four motor-operated valves for depressurization in the primary circuit. The power for opening these is supplied by the severe accident power supply system, which has a battery backup. The system prevents high-pressure melt discharge, which could otherwise happen if the reactor pressure vessel bursts and could damage the containment building.

During operation, the gas space of the containment building is filled with nitrogen, which ensures that the hydrogen generated in a severe accident during power operation cannot cause a hydrogen fire. Shutdown situations are discussed below under ‘Shutdown safety’. If all the zirconium in the fuel cladding and the fuel channels of a boiling water reactor becomes oxidized during a severe accident, a substantial volume of hydrogen will be generated. This hydrogen will pressurize the containment building. Dimensioning of the primary containment building of an

ABWR unit allows for hydrogen generation in a situation where all the zirconium in the reactor becomes oxidized.

In case of a severe accident, residual heat is removed from the ABWR containment building using a passive containment cooling system (PCCS). This system operates without an external power source. The PCCS consists of four natural circulation condensers that transfer heat along pipelines running in the air space of the containment building and directly into the water pools in the reactor building located above the primary containment building. There are two water pools each with two PCCS natural circulation condensers in the reactor building. The condensers in the pools are separated from one another with thresholds, which guarantees that a pool cannot be completely drained in case a leak occurs. The water volume in the pools is sufficient for removal of residual heat for 24 hours without refilling. The pools are filled from a storage tank outside the containment building. The functioning of the PCCS has been experimentally proven using a large-scale test assembly.

A core catcher is installed under the reactor pressure vessel to cool and solidify the core melt escaping from the pressure vessel. The core catcher operates without an external power source. The discharge of core melt into the core catcher will open the flooding valves through which water from the suppression pool will flow into the channels running under the catcher and later onto the melt pool. The steam generated in the core catcher will be condensed in the PCCS, and the resulting water will flow back into the core catcher.

The functioning of the core catcher will be experimentally proven. In the design process, the unit supplier has estimated the flow and temperature distribution of the core melt in the core catcher and the natural circulation conditions in the cooling channels of the core catcher in order to determine the thermal load on the structures of the core catcher. Based on these calculated values, the unit supplier has drawn up a testing program for heat transfer tests. The tests began with small-scale test assemblies to examine local heat transfer from the core melt to the cooling channels and the void fraction in the water pool above the core melt. The unit supplier then built a full-scale test assembly in early 2009. This test assembly models one flow channel in the core catcher, the elevations of the core catcher and the water pool being identical to those of the actual proposed design. Full-scale testing will ensure the functioning of the core catcher in circumstances replicating actual use as closely as possible.

A filtered containment venting system will be installed at the plant for long-term management of non-condensing gases.

The ABWR unit containment building and the design objectives and principles of the systems for managing severe accidents comply with Finnish requirements. The functioning of the core catcher remains to be experimentally proven. The unit supplier is currently running a test program concerning this.

Safety functions and provisions for ensuring them (Government Decree 733/2008, section 14)

Both active and passive safety systems are employed in the ABWR plant unit. Safety functions related to reactor core shutdown and removal of residual heat involve both an active and a passive system. The supply of make-up water to the reactor in case of transients and accidents is ensured through emergency cooling systems based solely on active components.

Reactivity management

Under normal conditions, the reactor power level is controlled with the control rods and main circulation pumps as in existing boiling water reactors.

Reactor shutdown in case of a transient or an accident is effected with a hydraulic scram system. This is a passive system based on water tanks pressurized with nitrogen that will insert the control rods into the reactor core when the scram valve opens. Each pressurized water tank controls two control rods. The total number of scram modules – each consisting of a nitrogen tank, a scram valve, a water tank and the necessary piping – is 120. This system fulfills the principle of multiple redundancy required in the Government Decree.

The scram system is backed up by a standby liquid control system (SLCS, 2 x 100%) with a pressurized borated water tank feeding borated water directly into the reactor core. This system fulfills the principle of diversity required in the Government Decree.

The reactor protection automation initiates the passive scram system whenever the process parameters exceed the protection limit. Reactor scram is secured by the alternate rod insertion (ARI) system, which also fulfills the principle of diversity with respect to automation. The system is implemented using hardwired technology. The ARI system controls the same scram valves and pressure accumulators as the normal protection automation system. Reactor shutdown is further ensured through the possibility of inserting the control rods into the reactor core using an electric motor drive in case the hydraulic system fails.

Reactor power can be decreased by reducing the reactor coolant flow rate, i.e. by stopping four or six out of the ten main circulation pumps, depending on the initiating event.

The design objectives and principles related to reactivity management comply with Finnish safety requirements.

Cooling of the reactor

Cooling of the reactor in shutdown conditions

During normal shutdown, the residual heat generated in the reactor is removed directly from the reactor pressure vessel using the residual heat removal system (RHR, 3 x 100%). The RHR system includes a subsystem for the cooling of a shut down reactor which takes care of the removal of residual heat during shutdown. This system is also used to supply make-up water to the reactor. From the RHR system, the residual heat is removed through the recirculating water system (RCWS, 3 x 100%) and the backed-up reactor service water system (RSWS, 3 x 100%) to the ultimate heat sink. The RHR system is used for cooling both when the reactor pressure vessel is closed and when it is open.

In transient conditions of the RHR system, the principle of diversity is fulfilled by the coolant cleanup system (CUW, 2 x 100%), by means of which the residual heat can be removed using two non-regenerative heat exchangers (NRHX, 2 x 100%). The NRHXs remove the residual heat to the reactor building normal cooling water system (RNCW, 2 x 100%), which in turn is cooled by the HVAC normal cooling water system (HNCW). From the HNCW system, the residual heat is transferred through the ventilation stack to the atmosphere. Make-up water for the reactor is obtained from the RNCW system.

Cooling of the reactor in accident conditions with the reactor primary circuit intact

In accident conditions where the reactor primary circuit is intact, the reactor is primarily cooled using an active high pressure core flooder system (HPCF, 3 x 100%).

Residual heat is removed from the reactor by conveying the steam through the primary circuit relief valves to the suppression pool in the containment building, where the residual heat is primarily removed using the residual heat removal system (RHR, 3 x 100%). The RHR uses the same pumps as the low pressure core flooder system (LPCF). The residual heat is removed through the recirculating water system (RCWS, 3 x 100%) and the backed-up reactor service water system (RSWS, 3 x 100%) to the ultimate heat sink.

The diversity principle with respect to the residual heat removal system is fulfilled by a system based on natural recirculation, which consists of four isolation condensers (IC, 4 x 33 %). The isolation condensers are connected to the steam and feedwater pipes. Once the system starts up, the steam flowing from the reactor to the steam pipes is drained into the heat exchanger and condensed into water, which is fed through the feedwater pipes back to the reactor. There are two parallel valves with different operating principles between the isolation condenser and the

feedwater line. Only one of these valves needs to open to activate the isolation condenser. The isolation condensers are located in two water pools in the reactor building, two condensers in each pool. The pools are separated by a threshold to prevent pool draining. From the pools in the reactor building, the residual heat is transferred to the atmosphere. The plant can be maintained in a controlled state using the isolation condensers. The water volume in the pools is sufficient for removal of residual heat for 24 hours without refilling. The pools can be refilled from a storage tank outside the containment building, and removal of residual heat can be continued for as long as necessary; it is, however, continued for at least 72 hours in any case.

The diversity principle can with respect to the residual heat removal system also be fulfilled using the passive containment cooling system (PCCS. The steam generated in the reactor can be led through the relief valves in the primary circuit to the suppression pool in the containment building, and the residual heat then transferred to the atmosphere through the PCCS.

An alternative way of providing make-up water for the reactor is to replace the high pressure core flooder system (HPCF) with a low pressure core flooder system (LPFL) by using the automatic pressure control system to lower the reactor pressure to a level where the low pressure core flooder pumps can function. The HPCF system gets its coolant from a separate make-up water tank, and the LPFL system from a suppression pool inside the containment building through suction filters in the pool. In order to improve the performance of the emergency cooling system, Toshiba is investigating the possibility to supply water from the flushing system of the hydraulic scram system to the reactor pressure vessel.

Cooling of the reactor in loss of coolant accidents

In a loss of coolant accident, the reactor is cooled using the high pressure core flooder system (HPCF, 3 x 100%) and the low pressure flooding line system (LPFL, 3 x 100%) and also the automatic pressure reduction system which uses relief valves.

The HPCF system gets its coolant from a separate make-up water tank, and the LPFL system from a suppression pool inside the containment building through suction filters in the pool. The suction filters prevent impurities from entering the reactor.

In order to ensure the reliable operation of the low pressure core flooder system in a loss of coolant accident, it is important that the suction filters of the pumps in the suppression pool do not become clogged as a result of impurities in the pool during the accident. Toshiba has developed the suction filters and experimentally verified their operation in accident conditions. The anti-clogging properties of the filters are due to their large surface area. The filters are also equipped with a flushing system

in case of clogging. It may become necessary at a later stage in the licensing process to conduct analyses or tests to ensure the functioning of the suction filters.

The steam discharged from the primary circuit in a loss of coolant accident is drained into the suppression pool by means of separate blow-down lines. Residual heat is transferred from the suppression pool into the ultimate heat sink in the same manner as in situations where the primary circuit is intact.

The diversity principle with respect to the removal of residual heat is fulfilled by the passive containment cooling system (PCCS), which is ready to run and does not need an initiating event from an active component. The PCCS consists of four natural circulation condensers that transfer heat along pipelines running in the air space of the containment building and directly into the water pools in the reactor building located above the primary containment building. The natural circulation condensers of the PCSS are located in two pools in the reactor building, two in each pool. The pools are separated by a threshold to prevent pool draining. From the pools in the reactor building, the residual heat is transferred to the atmosphere. The water volume in the pools is sufficient for removal of residual heat for 24 hours without refilling. The pools can be refilled from a storage tank outside the containment building, and removal of residual heat can be continued for as long as necessary; it is, however, continued for at least 72 hours in any case.

The design objectives and principles of the systems required for core cooling and removal of residual heat comply with Finnish safety requirements. Details of the emergency cooling systems, such as experimentally demonstrating the reliable functioning of the suction filters in the low pressure core flooder system, require further testing, and the final solution for observing the principle of diversity in the emergency cooling systems requires further design.

Containment building isolation

In the ABWR unit, containment building isolation is effected by means of two isolation valves in the pipelines penetrating the containment building, except for the inlet pipes of the low pressure core flooder system, which have one isolation valve outside the containment building. No common cause failure analysis has been performed in isolation valves of the same type, which means that observation of the principle of diversity required in the Government Decree cannot be proven.

The principles of multiple redundancy and diversity can be fulfilled with respect to the containment isolation through valve choices at a later stage in the project.

Loss of ultimate heat sink

If the normal removal of heat into seawater (the ultimate heat sink) is lost, residual heat can be removed from the reactor through isolation condensers (IC) into the water pools in the reactor building above the primary containment building and further through the ventilation stack into the atmosphere. This system enables the reactor to be brought into a controlled (hot shutdown) state and kept there. The water volume in the pools is sufficient for removal of residual heat for 24 hours without refilling. The pools can be refilled from a storage tank outside the containment building, and removal of residual heat can be continued for as long as necessary; it is, however, continued for at least 72 hours in any case. This system fulfills the principle of diversity required in the Government Decree.

In case of a transient in the RHR system, the principle of diversity is fulfilled by the coolant cleanup system (CUW, 2 x 100%), by means of which the residual heat can be removed using two non-regenerative heat exchangers (NRHX, 2 x 100%). The NRHXs remove the residual heat to the reactor building normal cooling water system (RNCW, 2 x 100%), which in turn is cooled by the HVAC normal cooling water system (HNCW). From the HNCW system, the residual heat is transferred through the ventilation stack to the atmosphere. Make-up water for the reactor is obtained from the RNCW system.

The design objectives and principles related to the management of loss of the ultimate heat sink comply with Finnish safety requirements.

Cooling of fuel pools

In the ABWR unit, the cooling of fuel pools, the control of pool water levels, water purification and radioactive materials handling are under normal conditions managed with the fuel pool cooling and cleanup system (FPC, 2 x 100%). If necessary, the pools can be refilled from the condensate storage tank. In case of a transient or an accident, residual heat removal and the control of pool water levels is effected using the residual heat removal system (RHR, 3 x 100%), which pumps water from the suppression pool in the containment building into the fuel pool through the FPC system. The fire protection system (FPS) and the suppression pool cleanup system (SPCU) may also be used to feed make-up water into the pools.

The design objectives and principles related to the cooling of the fuel pools comply with Finnish safety requirements.

Shutdown safety

It is ensured that the reactor will remain subcritical in all shutdown states by keeping the control rods inserted into the reactor.

Maintenance to be carried out during shutdown, particularly maintenance of the main circulation pumps, is planned with multiple layers of protection to prevent the coolant from leaking onto the floor of the containment building. The lower access doors to the containment building are protected against leaks with double doors, one of which is always closed. This prevents water from leaking from the reloading pool and the reactor to the outside of the containment building through these doors.

In case of a major coolant leak during a refueling outage, the cooling of the reactor is secured using the pumps of the residual heat removal system (RHR, 3 x 100%) and the high pressure core flooder system (HPCF, 3 x 100%). The pumps start up if the water level in the reactor falls, filling the lower drywell in the containment building and the reactor itself to above the top of the core. Maintaining the water at this level requires the RHR and HPCF pumps of one subsystem. Coolant is supplied to the RHR pump from the suppression pool and to the HPCF pump from a tank outside the containment building.

The design objectives and principles of systems related to shutdown safety comply with Finnish safety requirements.

Electrical systems

The external power source of the ABWR unit is a connection from the 400 kV grid through auxiliary transformers and a main transformer, or from the 110 kV grid through two standby auxiliary transformers. If necessary, power can be supplied from the standby auxiliary transformers directly to the distribution boards of the safety systems, bypassing distribution boards with no nuclear safety classification (EYT systems).

In case the external power source fails, power to the safety systems of the plant is supplied alternately from:

- the auxiliary diesel generators (3 x 100%) of subsystems 1 to 3 designed for the power supply of the active safety systems, and the auxiliary diesel generator (100%) of subsystem 4, designed for the power supply of the passive safety systems and automation
- gas turbine driven standby auxiliary generators (2 x 100%), which implement the diversity principle.
- batteries during the startup of the auxiliary power sources (rated discharge time 2 h).

According to the electrical systems description, the severe accident management systems do not have separate internal power source systems.

The principle of separation applied to the electrical systems is not clearly described in the documentation. This issue may be reviewed when the application for the construction license is submitted.

The lesson learned from the design errors leading to the malfunction of the electrical system of the Forsmark nuclear power plant in 2006 shall be taken into account. In the design of electrical systems and components, special attention must be paid for instance to preventing voltage transients from spreading and the application of the principle of diversity in electricity distribution and in the power supply of automation systems. A full analysis must be made of what the worst case voltage transients and malfunctions in the plant's in-house power grid would be, and the power consumers and systems must be designed to withstand them. This issue will be reviewed in more detail at the construction licensing stage.

The design objectives and principles of the electrical systems largely comply with Finnish safety requirements. A separate power supply system for the severe accident management system and the general lessons learned from the Forsmark malfunction are issues that must be reviewed in more detail when applying for the construction license.

Building technology fire protection

The design basis for the buildings and building services of the ABWR unit is consistent with the Japanese plants that are used as references; the environmental conditions of these are in most cases assessed as more demanding than those in Finland. The unit supplier also has access to the design expertise required for boiling water reactor plants in northern areas, and the current design basis thus ensures an adequate command of Finland's winter conditions in the detailed design of buildings and building services.

The design objectives and principles regarding earthquakes and resistance to vibrations induced by external threats comply with Finnish safety requirements. The detailed design includes an examination of structural frameworks so as to ensure the vibration resistance of the buildings and the appropriate vibration characteristics of the structures and component anchorages for vibration resistance of the components of the power plant.

The design objectives and principles regarding fire protection of the ABWR unit comply with Finnish safety requirements. The fire extinguishing systems are designed to be earthquake-proof, securing control over fires that earthquakes may cause.

Protection against external events (Government Decree 733/2008, section 17)

The protection strategy of the ABWR unit against the impact of a large passenger aircraft is to retain the coolability of the reactor core, the integrity of the containment building, the coolability of spent fuel and the integrity of the fuel pools. The buildings to be protected against an aircraft crash are the reactor building, the control room building and the pump station buildings of the residual heat removal systems. The protection measures used for the ABWR unit are strengthened reinforced concrete structures, physical separation of parallel systems critical to safety, physical protection provided by other structures, and the placement of components in underground facilities in the buildings.

Protection against external floods is provided by external wall structures able to withstand the pressure of groundwater. Penetrations below the flood limit are equipped with flood shields, and tunnel penetrations are built to be watertight.

The design objectives and principles presented comply with Finnish safety requirements.

Protection against internal events (Government Decree 733/2008, section 18)

Internal threats such as floods and fires are taken into account in the room and layout planning of the ABWR unit by placing the key safety systems in three separate areas. These areas are physically separated with reinforced concrete walls for which a rated fire resistance of two hours is indicated. The areas on the bottom floor of the reactor building, which house the pumps of the essential service water system (ESWS), are completely separated from one another with walls to prevent the spreading of internal flooding. The subsystem separation principle is also observed in the control room building. On the upper floors of the reactor building, there are doors between the areas for operating and maintenance purposes.

Pressure loads caused by breaks in high energy pipes are taken into account as part of the design requirements for the structures of the reactor building. The lower maintenance access to the containment building consists of two successive airlock doors, which ensure that the coolant discharged in a loss of coolant accident will remain inside the containment building and can be recovered into the coolant circuit.

The design principle of the ABWR unit involves running the main steam and feedwater pipes from the containment building to the turbine building along continuous channels through the control room building. Feasibility analyses have included a study of the effects on plant safety of breaks in these high energy pipelines. The plan is to divide the pipe channel into two tunnel sections. One of these would be a compartment inside the reactor building and the other a compartment running through the control room building. The management of the

consequences of pipe breaks in the compartment inside the reactor building has been analyzed. The construction of the compartment running through the control room building has been reinforced, and the compartment is provided with a steel lining to prevent a potential flood from affecting operations in the control room building. Further analysis is required, however.

The compact layout of the plant is challenging for protection against internal events such as floods and fires. The consequences of major internal floods, such as flooding of the essential service water system (ESWS) in one area of the reactor building, must be analyzed at later stages in the licensing process. It must be ensured that the impact of such events is limited to the area in question.

The design objectives and principles presented comply with Finnish safety requirements.

Monitoring and control of nuclear power plants (Government Decree 733/2008, section 19)

In the documentation of the application for a decision-in-principle, the safety principles of the automation systems are described on a rather general level. Before the design and the design materials are brought further to the technical stage, the discussion of safety principles is largely a discussion of goals, and on the basis of the documentation it is not possible to fully assess whether these goals will be attained. True attainment of the safety principles in the technical design of the power plant must be ensured as the design work progresses at later stages in the project. The construction license procedure will be the first official procedure in the power plant project that deals with concrete technical I&C solutions.

Automatic safety functions

The automation in the ABWR unit involves several lines of defense based on the 'defense in depth' principle. The first line comprises the normal process automation, control systems and limitation systems. The second line comprises the reactor protection system (RPS) and the engineered safety features actuation system (ESFAS). The third line includes the diverse actuation system (DAS) based on the principle of diversity. Finally, there is the severe accident management system.

The automation systems in the various lines of defense automatically seek to maintain the plant parameters within a safe range during operating transients and to limit the consequences of accidents.

The design objectives and principles regarding automation systems comply with Finnish safety requirements.

The principle of multiple redundancy in automation

The RPS and the ESFAS consist of four parallel subsystems. The protection function is actuated if a protection signal is received from any two of the four parallel protection channels. The systems fulfill the principle of multiple redundancy required in the Government Decree.

The number of parallel subsystems in the DAS based on the principle of diversity is not given.

The most important process automation control systems – the feedwater supply system, the control system of the main circulation pumps, the turbine bypass control system, the steam pressure control system and the reactor power control system – are implemented using three parallel subsystems.

The design objectives and principles regarding automation systems comply with Finnish safety requirements. Redundancy principles are not given for the DAS. This issue may be reviewed when the application for the construction license is submitted.

The principle of separation in automation

The automation subsystems are physically and functionally separated from one another.

Safety class 2 systems are physically and functionally separated from all other systems and components. Safety class 3 systems are functionally separated from systems and components in lower security classes.

The separation of the severe accident management automation and monitoring system from other automation systems is not presented. This issue may be reviewed when the application for the construction license is submitted.

The design objectives and principles regarding automation systems comply with Finnish safety requirements as far as the principle of separation is concerned. However, the separation of severe accident management from other automation systems is not presented. This issue may be reviewed when the application for the construction license is submitted.

The principle of diversity in automation

In the reactor protection system, the principle of diversity is observed by the signals indicating accident and transient conditions coming alternatively from two different process parameters. The design objectives and principles presented comply with Finnish safety requirements.

It is not clear at this stage of design which computer-based system platforms will be used in the various automation systems. This issue may be reviewed when the application for the construction license is submitted.

The ABWR plant concept incorporates a diverse actuation system (DAS), which is designed against common cause failures in the computer-based protection system. The DAS can control reactivity management, overpressurization protection, emergency core cooling, residual heat removal from the reactor and the containment building, containment isolation and emergency power sources. The DAS consists of two parts, one to back up the reactor protection system (RPS) and the other to back up the engineered safety features actuation system (ESFAS). The RPS backup part of the DAS system is based on hardwired technology, while the ESFAS backup part is based on programmable automation. The DAS system has its own sensors for the measurement of process parameters. The DAS can be used to bring the plant into a controlled (hot shutdown) state. The documentation does not present a procedure for bringing the plant into a safe (cold shutdown) state in the case of common cause failure of the programmable automation system.

The design objectives and principles presented largely comply with Finnish safety requirements. It must be clarified in connection with applying for the construction license how the plant can be brought into and maintained in a safe state in case of common cause failure of the programmable automation systems.

Control room

The control room of the ABWR unit contains the main control console, the display panel and the shift supervisor's console.

The main control console is used to control the plant under normal operating conditions, transient conditions and accident conditions. Also, all the information needed by the operators for the execution of control actions under the aforementioned conditions is transmitted to the main control console.

The display panel comprises fixed indicators and switches as well as a widescreen display. The purpose of the display panel is to show a summary of the status of the plant and its principal components and key alert data. There are also control functions for less frequently used functions such as in-service testing.

The shift supervisor's console is for monitoring the parameters and status of the plant, but no control actions can be performed here.

The design objectives and principles of the control room comply with Finnish safety requirements.

Emergency control room

The plant has an emergency control room where safety-critical systems can be controlled independently of the main control room. Here, the plant can be brought into a controlled (hot shutdown) state and further into a safe (cold shutdown) state.
The emergency control room is located in a different fire compartment and building than the main control room.
The design objectives and principles of the emergency control room largely comply with Finnish safety requirements. The possibility of controlling and monitoring the cooling of the fuel pools is not described in the documentation. This issue may be reviewed when the application for the construction license is submitted.

Reactor pressure vessel level measurement

The reactor pressure vessel level measurement is a normal differential pressure measurement that in turn controls the reactor protection automation. There are four measurements. The system is actuated when any two channels give the opening command. This system observes the principle of multiple redundancy.
The principle of diversity is realised by two floats located in the reactor water cleanup system.

Summary

The design objectives and principles of this power plant unit alternative largely comply with Finnish safety requirements. There are certain technical details that need further analysis, empirical qualification and further design; this can be performed at later stages in the licensing procedure. It is the considered opinion of STUK that none of these is such that it would constitute an obstacle to fulfilling the requirements of the Government Decree on the Safety of Nuclear Power Plants (733/2008). These technical details include:

- experimental verification of the functioning of the suction filters in the low pressure core flooder system
- implementation of the principle of diversity in the isolation of the containment building for all pipelines
- experimental demonstration of the operability of the core catcher required for severe accident management
- a residual heat removal system realizing the principle of diversity in shutdown situations
- taking the general lessons of the Forsmark malfunction into account in the electrical systems
- independence of the severe accident management automation and monitoring systems from other automation systems
- separate power supply system for the severe accident management system

– bringing the plant into a safe state in case of loss of the computer-controlled automation system.

KERENA - An Advanced Boiling Water Reactor with passive Safety Features, Areva

General

KERENA is a boiling water reactor with an electrical output of about 1,200 MWe designed by Areva of Germany. Areva (formerly Siemens) has extensive experience in designing boiling water reactor units since the 1960s. Every boiling water reactor ever built in Germany was designed by Areva. The reference plant for the plant type being proposed for Finland, concerning the basic processes, is Gundremmingen C, completed in 1985. At Gundremmingen C, safety functions are based on safety systems that require an external power source.

KERENA is a plant unit based on German boiling water reactor technology; its design is based on structural simplicity and a reduction in the number of components requiring maintenance. The planned service life of the plant is 60 years. KERENA is a power plant unit alternative that is still being designed. Its design is less complete than that of the other alternatives. Construction has not yet begun on a single plant unit of this type.

Safety in the KERENA unit is based not on active systems but on new kinds of natural properties and on passive safety systems.

Assessment and verification of safety (Government Decree 733/2008, section 3)

Deterministic analysis methods and preliminary results

Areva has analysis methods for safety assessment and verification developed over several decades. The methods have been appropriately maintained and qualified for their purpose. Analyses conducted on the KERENA unit indicate that transient and accident analyses compliant with Finnish requirements can be performed for this unit alternative.

Probabilistic analyses

Areva employs level 1 and 2 PRA methods used for the PRA analyses of plants in operation or under construction. So far, one level 1 PRA analysis has been conducted on the KERENA unit. The analysis methods and information about the KERENA analysis results indicate that analyses compliant with Finnish PRA requirements can be performed for this unit alternative. If necessary, the methods can be further developed on the basis of Finnish detailed requirements. The probabilistic risk analyses will be conducted in connection with detailed planning

of the power plant, and the fulfillment of Finnish safety requirements will be assessed at that point.

Qualification of new types of systems

The KERENA plant unit alternative features several new kinds of passive safety systems that have not been previously used in a nuclear power plant. These include the hydraulic reactor scram system (JDE) and its backup boron extinguisher system (JDJ), an isolation condenser cooling the reactor circuit directly (JNB), passive containment building cooling condensers (JNC), a passive reactor core flooder system (JNG) and a passive pressure transmitter (JRA).

The functioning of the systems has been qualified using test components at the unit design stage. Integral tests and full-scale component tests are in progress. Because the testing has not yet been completed, further information or possibly further testing will be required on certain details at later stages in the licensing procedure.

Runtime testing procedures for passive systems are not described in the application documentation. This issue may be addressed when applying for the construction license.

Limitation of radiation exposure and release of radioactive materials (Government Decree 733/2008, sections 8 to 10)

In the KERENA design process, the plant supplier has made a preliminary calculation of the radiation exposure of the population in the vicinity of the plant in the case of an accident. These calculations indicate that radiation dosages will remain below the dosage limits set in Finland for accident situations.

The analysis results and the design features of this power plant concept indicate that analyses compliant with Finnish requirements can be conducted for this unit alternative at a later stage in the licensing process.

Engineered barriers for preventing the dispersion of radioactive materials (Government Decree 733/2008, section 13)

Reactor and fuel

The reactor is a boiling water reactor with internal main circulation pumps; in terms of its operating parameters, it is similar to existing boiling water reactors. The reactor and its cooling circuit are designed so that the plant can, in principle, function on natural circulation without the main circulation pumps. The main circulation pumps are inside the pressure vessel to improve regulation of the reactor output during startup and power operation. There is also a chimney above the reactor to enhance natural circulation in the primary circuit. These design features have improved reactor stability in particular. The stability of the reactor is

also ensured using the same methods as in existing boiling water reactors: core and fuel design, and protective functions.

Under normal conditions, the reactor output is controlled using the main circulation pumps and control rods. There are 664 fuel assemblies in the core and 157 control rods. The reactor is intended to use fuel assemblies similar to those used in existing boiling water reactors, except slightly larger in cross-section and about one meter shorter. Reactivity is controlled during the operating cycle with solid burnable absorbers in the fuel and the control rods.

The reactor core is clearly lower than in existing reactors with a similar rating and is located lower in the pressure vessel than in existing boiling water reactors. The power density of the reactor core is also somewhat smaller. These features improve the unit's natural safety compared with existing plants. Because of the large volume of the reactor pressure vessels, pressure transients develop more moderately than in existing boiling water reactors. The isolation condenser (JNB) helps clear these up so that the need for the relief valves to function during the worst case pressure transient can be limited so that only a short blow-down of the safety/relief valves is needed at the beginning of the transient. This restricts the blow-down of coolant from the primary circuit into the suppression pool, meaning that the water level in the reactor is simple to maintain in the case of a transient or an accident.

The planned fuel burn-up is greater than the maximum fuel assembly burn-up allowed in Finland, 45 MWd/kgU. The operation of the reactor can, however, be designed to be consistent with the Finnish burn-up limit. If approval is sought for a higher burn-up level, the applicant must be able to demonstrate experimentally that the fuel fulfills Finnish design criteria regarding accident situations.

The design objectives and principles of the reactor and fuel comply with Finnish safety requirements.

Main nuclear components

The main nuclear components of the KERENA unit will be built based on technological solutions deriving from the unit supplier's extensive experience. The reactor pressure vessel is of low-alloy steel, made of rotationally symmetrical forgings welded together and with a welded stainless steel lining. Tested materials and validated welding methods are used in the manufacture to ensure the required service life of 60 years. Radiation embrittlement of the reactor core area is taken into account in material selection, and embrittlement is also monitored using a runtime monitoring program.

Compliance with requirements regarding material choices and manufacture will also be ensured for other main components such as the main circulation pumps, the control rod devices, the inner parts of the reactor and the primary circuit piping.

The reliability of the primary circuit is also ensured through continuous monitoring of the water chemistry of the coolant in the primary circuit.

The main steam and feedwater pipes are made of the same type of (ferrite) steel as the reactor pressure vessel, so that technically demanding dissimilar metal joints are not needed for the primary nozzles. Pipe breaks will be taken into account in the design and implementation of the principal pipes using the break preclusion (BP) principle, which includes applying the 'leak before break' concept (LBB). Also, the dynamic impact of a sudden pipe break in high energy pipes on other components and structures will be taken into account. The safety systems are designed to take into account the pipe break with the largest diameter in the primary circuit.

The design objectives and principles proposed for the main nuclear components of the KERENA unit comply with Finnish safety requirements.

Reactor pressure control

There are eight safety and relief valves (SRV) for reactor pressure control. There are four valves for pressure control and four for pressure reduction. The two groups of valves operate on different principles. All valves can be used for reactor pressure control in case of a transient or an accident if necessary.

The four pressure control valves are opened by a pilot valve controlled by the reactor protection automation or in direct response to reactor pressure against a spring load.

The four pressure reduction valves are opened by a passive pressure transmitter actuated directly by the water level in the reactor pressure vessel or by the reactor protection automation, which observes the principle of diversity with regard to the actuating signal. Both systems control the same control valve. Passive pressure transmitters need no external energy source or automation system; they react directly to the lowering of the water level in the reactor, which is always a symptom of the need to actuate a safety function. The pressure reduction valves have a mechanism ensuring that they stay open.

The number of safety and relief valves is so high that the safety function can be guaranteed even assuming the malfunctioning of several valves, as per Finnish requirements.

The isolation condensers (JNB, 4 x 50%) can be used for pressure control in transient and accident situations. The isolation condensers are connected directly to the reactor pressure vessel through dedicated nozzles. Once the system starts up, the steam flowing from the reactor to the steam pipes is drained into the heat exchanger and condensed into water, which is fed through the feedwater pipes

back to the reactor. If the water level in the reactor pressure vessel drops, this is enough to actuate the isolation condensers without action from a single active component. Because of the large volume of the reactor pressure vessels, pressure control transients develop more moderately than in existing boiling water reactors. The isolation condenser (JNB) helps clear these up so that the need for the relief valves to trip during the worst case pressure transient can be limited to a few trips at the start of the transient. In such cases, at least one safety/relief valve needs to trip for a short length of time to control the pressure.

The design objectives and principles regarding pressure control comply with Finnish safety requirements.

Containment building

The KERENA unit containment building is a conventional pressure suppression containment building made of reinforced concrete with suppression pools, typical of boiling water plants. During power operation, a nitrogen atmosphere is present within it. There are two kinds of pools in the containment building: the reactor core flooder pools and the suppression pool. The reactor core flooder pools are used as the water storage for the gravity-driven passive flooder system and for condensing the steam conveyed to the suppression pools through safety and relief valves in case of a transient or an accident. The isolation condensers (JNB) are also located in these pools and transfer the residual heat through the passive cooling condensers (JNC) in the containment building to the storage pools outside the containment building in the reactor building and from there to the environment.

In the postulated accidents (pipe breaks), the steam discharged from the reactor circuit into the containment building is forced by the differential pressure into the suppression pool. The residual heat from the reactor is removed from the suppression pool using a passive cooling condenser (JNC) in the containment building or through the residual heat removal system (RHR, 2 x 100%) and its related heat transfer chain to the ultimate heat sink. The containment building is designed to retain its integrity in compliance with the approval criteria in the case of a transient or an accident.

Severe accidents

The key safety functions in the management of severe reactor accidents in the KERENA unit are pressure reduction in the primary circuit, catching and cooling core melt within the reactor pressure vessel, and removing residual heat from the containment building.

Pressure reduction in the primary circuit is effected by overriding the safety and relief valves used for reactor pressure control. The purpose of pressure reduction is to relieve tension in the reactor pressure vessel and thus to ensure that the core melt remains within the pressure vessel. The KERENA unit has eight safety and

relief valves, all of which can be used to reduce pressure. The main valves operate on two different principles. All main valves have three parallel pilot valves operating on three different principles; any two of these are available for reactor pressure reduction. Four valves have a locking device that ensures that the valve remains open once pressure in the primary circuit has equalized with the pressure in the containment building. The tripping of just one of these valves is sufficient to bring the pressure in the primary circuit down close to the level of pressure in the containment building. The pressure reduction function is highly reliable, as the valve capacity is great and the system employs valves operating on two different principles.

The plant does not have separate valves for pressure reduction in the case of a severe accident, since the same valves are used both for protecting the primary circuit against overpressure and for pressure reduction in case of a postulated accident. This represents a deviation from the Finnish safety requirements, which insist that the systems designed for the management of severe accidents must be independent of the systems designed for the plant's operational occurrences and postulated accidents. However, the design solution presented in the KERENA unit is acceptable, since the pressure reduction function as presented rests on a highly reliable principle, and reducing pressure in the primary circuit is not essential for retaining core melt. The pressure vessel would remain intact despite a meltdown even if pressure in the primary circuit were not reduced. Pressure reduction does, however, substantially increase the safety margin.

During operation, the gas space of the containment building is filled with nitrogen, which ensures that the hydrogen generated in a severe accident during power operation cannot cause a hydrogen fire. Shutdown situations are discussed below under 'Shutdown safety'. If all the zirconium in the fuel cladding and the fuel channels of a boiling water reactor becomes oxidized during a severe accident, a substantial volume of hydrogen will be generated. This hydrogen will pressurize the containment building. Dimensioning of the primary containment building of a KERENA unit allows for hydrogen generation in a situation where all the zirconium in the reactor becomes oxidized.

In the KERENA unit, the core melt generated in a severe accident is contained and cooled within the reactor pressure vessel by cooling the vessel from the outside. The reactor pit around the pressure vessel is flooded using water tanks in the upper drywell. There are two parallel pipes in the flooder line leading from the water tank to the reactor pit, both with two consecutive flooding valves. These open automatically as guided by the reactor protection system or can be opened manually if necessary. The flooder line capacity is sufficient to raise the level of the coolant in the reactor shaft to above the core within 20 minutes of the valves being opened. The size of the reactor pressure vessel in the KERENA unit relative to the output of the reactor is so large that there is a high safety margin for heat transfer. The unit supplier has experimentally verified that the external pressure vessel cooling system works.

In case of a severe accident, removal of residual heat is effected through the containment building cooling condenser system. This system operates without an external power source. It consists of four natural circulation condensers installed in the ceiling of the drywell above the core flooder pool. These transfer heat to the storage pool above the primary containment building. The pool can be refilled through its cleanup system. The functioning of the condensers has been verified through large-scale tests. The joint functioning of the isolation condensers and the containment building condensers will be verified in a large-scale test assembly in due course.

The KERENA unit does not have a filtered containment building venting system for long-term management of non-condensing gases. The unit supplier has declared that significant amounts of non-condensing gases raising the pressure in the containment building would not be generated in a severe accident apart from hydrogen. There is a separate hydrogen removal system based on recombination. The sufficiency of this system for long-term management of non-condensing gases must be demonstrated at the eventual construction license stage.

Safety functions and provisions for ensuring them (Government Decree 733/2008, section 14)

In the KERENA unit, the safety functions required for the management of transients and accidents can be effected both using active systems and using only independent passive systems. The active systems are always actuated first in case of transients and accidents. If these are unable to contain the consequences of the event, safety is ensured through the passive safety systems. The passive safety functions of the KERENA unit are designed so that their activation and operation do not require an external power source. The purpose of the passive systems is to bring the power plant into a controlled state in case of an accident and keep it in that state for as long as necessary. Therefore the design of the automation and electrical systems, for instance, can be much simpler.

Reactivity management

In the KERENA unit, the reactor power level is controlled with the control rods and main circulation pumps as in existing boiling water reactors.

Reactor shutdown in case of a transient or an accident is effected with a passive scram system (JDE, 2 x 100%). The scram is achieved by the insertion of the control rods into the reactor by a hydraulic system. The hydraulic scram system is powered by steam pressure tanks. There are two component systems each with two steam pressure tanks and parallel valves governing them; the opening of just one of these valves is sufficient for the safety function. The actuation of just one of the component systems is sufficient to shut down the reactor.

The scram system is backed up by a standby boron system (JDJ, 2x100 x %) with a pressurized borated water tank feeding borated water directly into the reactor core. There are two component systems each with a pressurized borated water tank and parallel valves governing them; the opening of just one of these valves is sufficient for the safety function. Once the valve is open, pressurized nitrogen will force the borated water into the reactor.

The reactor protection automation initiates the scram system whenever the process parameters exceed the protection limit. Actuation is effected normally through the active reactor protection automation system or by its backup system, which relies on a passive pressure transmitter actuated directly by the water level in the reactor pressure vessel (JRA). The passive pressure transmitters actuate the hydraulic scram system without the intervention of any automation system. Passive pressure transmitters need no external energy source, not even control power; they react directly to the lowering of the water level in the reactor, which is always a symptom of the need to actuate a safety function. The borated water system, on the other hand, is only actuated by the reactor protection system.

Reactor shutdown is further ensured through the possibility of inserting the control rods into the reactor core using an electric motor drive in case the hydraulic system fails.

The design objectives and principles related to safety functions in reactivity management comply with Finnish safety requirements.

Cooling of the reactor

Cooling of the reactor in shutdown conditions

During normal shutdown, the residual heat generated in the reactor is removed directly from the reactor pressure vessel using the residual heat removal system (JNA, 2 x 100%). Make-up water is fed into the reactor by the low pressure core flooder system (JND, 2 x 100%). The JND system uses the same pumps as the JNA system. The residual heat is removed through the component cooling water system (CCWS, 2 x 100%) and the service water system (SWS, 2 x 100%) to the ultimate heat sink. The JNA system is used for cooling both when the reactor pressure vessel is closed and when it is open.

The principle of diversity in removal of residual heat during shutdown (when the pressure vessel is open) is realized with a third diverse redundant sub-system in the residual heat removal system (JNA) and the fuel pool cooling system (FAK). The details of this system will be decided at a later design stage and can be assessed in connection with the construction license application.

Cooling of the reactor in accident conditions with the reactor primary circuit intact

In accident conditions where the reactor primary circuit is intact, the reactor is primarily cooled using passive natural circulation isolation condensers (JNB, 4 x 50%). The isolation condensers are connected directly to the reactor pressure vessel through dedicated nozzles. Once the system starts up, the steam flowing from the reactor to the steam pipes is drained into the heat exchanger and condensed into water, which is fed through the feedwater pipes back to the reactor. If the water level in the reactor pressure vessel drops, this is enough to actuate the isolation condensers without action from a single active component. The isolation condensers are located in the four reactor flooder pools in the containment building. They transfer the residual heat through the passive cooling condensers (JNC, 4 x 50%) in the containment building to the storage pools outside the containment building in the reactor building and from there to the environment. With the isolation condensers, the reactor can be maintained in a controlled (hot shutdown) state.

Alternatively, residual heat in the reactor may be removed by conveying steam through the primary circuit pressure control valves and the blow-down pipes to the flooder pool in the containment building, condensing the steam into water and then removing the residual heat through the residual heat removal system (JNA, 2 x 100%), the component cooling water system (CCWS, 2 x 100%) and the service water system (SWS, 2 x 100%) into the ultimate heat sink. Make-up water is fed into the reactor by the low pressure core flooder system (JND, 2 x 100%). With these systems, the plant can be brought into a safe (cold shutdown) state.

Make-up water can also be fed into the reactor by the gravity-operated reactor flooder system (JNG, 4 x 100%) in case the isolation condenser fails. The JNG is actuated by the tripping of a spring-loaded check valve. There are four flooder pools in the system; each is connected to the reactor with pipes, and each pipe has a spring-loaded check valve. Pressure in the reactor is vented through relief valves to an area where the JNG system can operate.

Cooling of the reactor in loss of coolant accidents

In case of a loss of coolant accident, the reactor is cooled using the gravity-operated reactor flooder system (JNG, 4 x 100%), which is actuated by the opening of a spring-loaded check valve. There is enough water in the JNG system to flood the containment building to above the top of the reactor core. Once the containment building is flooded, no more water will leak out of the reactor pressure vessel. If the leak is so small that it does not relieve pressure in the reactor, the pressure will be reduced through the automatic pressure reduction system, and the steam generated in the reactor will be conveyed to the flooder pool in the containment building. The residual heat is transferred through the passive cooling condensers (JNC, 4 x 50%) in the containment building to the storage pools outside the containment building in the reactor building and from there to the environment. The water volume in the pools is sufficient for removal of residual heat for 24 hours without refilling. The pools can be refilled from a storage tank

outside the containment building, and removal of residual heat can be continued for as long as necessary; it is, however, continued for at least 72 hours in any case.

Alternatively, the residual heat removal system (JNA, 2 x 100%) may be used if the reactor flooder system fails. The residual heat is removed through the component cooling water system (CCWS, 2 x 100%) and the service water system (SWS, 2 x 100%) to the ultimate heat sink. Make-up water is fed into the reactor through the low pressure core flooder system (JNG, 2 x 100%), which uses the same pumps as the JNA system.

The design objectives and principles of the systems required for core cooling and removal of residual heat comply with Finnish safety requirements.

Containment building isolation

There are two isolating valves operating on two different principles for sealing off the containment building in case of a transient or an accident.

On the main steam line there are self-actuated isolating valves which receive a closing signal either from the reactor protection automation system or directly from a passive pressure transmitter actuated by the water level in the reactor pressure vessel.

On the feedwater line, isolation is effected through a self-actuated valve and a check valve. Check valves are forced shut by the medium in the pipe, with no external actuation. A self-actuated valve receives a closing signal either from the reactor protection automation system or directly from a passive pressure transmitter actuated by the water level in the reactor pressure vessel.

In other systems whose pipes penetrate the containment building, isolation is effected with motor-actuated or self-actuated isolating valves. Motor-actuated valves receive a closing signal only from the reactor protection automation system. A closing signal is generated by two mutually replaceable process parameters. The extent of diversification among these isolating valves and their actuation will be decided at a later design stage and can be assessed in connection with the construction license application.

The design objectives and principles of the containment building isolation comply with Finnish safety requirements.

Loss of ultimate heat sink

If the normal removal of heat into seawater (the ultimate heat sink) is lost, residual heat can be removed from the reactor through isolation condensers (JNB, 4 x 50%)

into the reactor flooder pools, then through the passive containment building residual heat removal system (JNC, 4 x 50%) to water pools in the reactor building above the primary containment building, and further through the ventilation stack into the atmosphere. Using the isolation condensers, the reactor can be brought into a controlled (hot shutdown) state and kept there. The water volume in the pools is sufficient for removal of residual heat for 72 hours without refilling.

The principle of diversity in removal of residual heat during shutdown (when the pressure vessel is open) is observed with a third and different component system in the residual heat removal system (JNA) and the fuel pool cooling system (FAK). The details of this system will be decided at a later design stage and can be assessed in connection with the construction license application.

The design principles related to the management of loss of the ultimate heat sink comply with Finnish safety requirements.

Cooling of fuel pools

The fuel pools are cooled by the fuel pool cooling system (FAK, 2 x 100%). Residual heat is transferred through the component cooling water system (CCWS, 2 x 100%) and the service water system (SWS, 2 x 100%) to the ultimate heat sink. This system fulfills the principle of multiple redundancy required in the Government Decree.

The principle of diversity in removal of residual heat during shutdown (when the pressure vessel is open) is realized with a third diverse redundant sub-system in the residual heat removal system (JNA) and the fuel pool cooling system (FAK). Make-up water is obtained from the coolant storage tank through the nuclear component flushing system (KWB) and the fuel pool cleaning system (FAL). Fire extinguishing systems can also provide make-up water for the fuel pools. The details of this system will be decided at a later design stage and can be assessed in connection with the construction license application.

The design objectives and principles related to the cooling of the fuel pools comply with Finnish safety requirements.

Shutdown safety

It is ensured that the reactor will remain subcritical in all shutdown states by keeping the control rods inserted into the reactor.

Loss of coolant during shutdown is prevented by designing the access doors to the containment building so that no water can escape from the containment building and by ensuring that there is always enough water in the pools in the containment building to flood the reactor core in case of an accident.

The design objectives and principles of systems related to shutdown safety comply with Finnish safety requirements.

Electrical systems

The passive safety functions of the KERENA unit are designed so that their activation and operation do not require an external power source. The purpose of the passive systems is to bring the power plant into a controlled state in case of an accident and keep it in that state for as long as necessary. Therefore the safety relevance of the electrical systems is lower, and their design can be much simpler.

The external power source of the KERENA unit is a connection from the 400 kV grid through auxiliary transformers and a main transformer, or from the 110 kV grid through a standby auxiliary transformer.

In case the external power source fails, power to the safety systems of the plant is supplied alternately from:

- auxiliary diesel generators (2 x 100%)
- battery arrays (4 x 100%) with a rated discharge time of 2 h
- battery arrays in the severe accident management system (2 x 100%) with a rated discharge time of 24 h

The number of auxiliary diesel generator systems is sufficient, because they are used to provide electricity for active safety systems which observe the principle of diversity and back up the passive safety systems.

The severe accident management systems have their own independent battery-based power source with a rated discharge time of 24 h. No procedures for recharging these battery arrays are given.

The subsystems of the emergency electrical systems are physically and functionally separated from one another. There is no mention in the documentation of how the four parallel DC systems with battery backup in the two component systems are separated from each other within their respective component systems. Safety class 2 and 3 cabling is isolated from all other cabling in accordance with the IEEE 384 principles.

The lesson learned from the design errors leading to the malfunction of the electrical system of the Forsmark nuclear power plant in 2006 shall be taken into account. In the design of electrical systems and components, special attention must be paid for instance to preventing voltage transients from spreading and the application of the principle of diversity in electricity distribution and in the power supply of automation systems. A full analysis must be made of what the worst case voltage transients and malfunctions in the plant's in-house power grid would be, and the power consumers and systems must be designed to withstand them.

The design objectives and principles of the electrical systems largely comply with Finnish safety requirements. Electrical system separation principles, a separate power supply system for the severe accident management system and the general lessons learned from the Forsmark malfunction are issues that must be reviewed in more detail when applying for the construction license.

Building technology and fire protection

The basic design requirements for the buildings and building services with regard to external threats are basically sufficient; the current design basis ensures an adequate command of Finland's winter conditions in the detailed design of buildings and building services.

For earthquakes, the design parameter used is the PGA value 0.23 g, which exceeds the Finnish requirement of 0.1 g. The design objectives and principles regarding earthquakes and resistance to vibrations induced by external threats comply with Finnish safety requirements. The detailed design includes an examination of structural frameworks so as to ensure the vibration resistance of the buildings and the appropriate vibration characteristics of the structures and component anchorages for vibration resistance of the components and devices of the power plant.

The design objectives and principles regarding fire protection of the KERENA unit comply with Finnish safety requirements. Regarding the management of fires possibly caused by an earthquake, the need for ensuring that the fire extinguishing systems of the power plant are earthquake-proof, and the related design principles, must be ascertained at the eventual construction license stage.

Protection against external events (Government Decree 733/2008, section 17)

In the aircraft crash protection strategy of the KERENA unit, the outer wall of the reactor building acts as a crash barrier and protects the containment building itself as well as all the safety systems inside the reactor building. The auxiliary building, which houses the central control room, has not been protected against a plane crash. The eventual destruction of this building is not cited as having an impact on the functioning of the automatic or natural safety functions, the idea being that the plant may be controlled from the emergency control room, protected by distance separation and shadowing separation. Finnish requirements state that the structures and safety systems of the control room must also be designed so as to allow work to continue safely even in case of an accident. The control room must be designed so that the plant may be controlled from there in case of an operational occurrence or an accident.

In the single-unit concept, the diesel system buildings and sea water pumping stations are located at opposite corners, observing the shadowing separation principle. In the twin-unit concept, the pumping stations are on the same side of the plant site, but the second pumping station for each unit is located entirely underground.

It is the considered opinion of STUK that the fulfillment of Finnish safety requirements with regard to control room functions has not yet been demonstrated. The proposed solution requires more detailed designs and analyses, and also changes to the plant concept.

Protection against internal events (Government Decree 733/2008, section 18)

Internal threats such as floods and fires are taken into account in the room and layout planning of the KERENA unit with physical separation of key safety systems.

The subsystems are located in separate areas in the containment building. Outside the containment building, the residual heat removal systems are located in two separate areas below the containment building and connected to the control rod well. There are doors separating these areas. The main steam and feedwater lines are clearly separated in the reactor and containment buildings.

In the reactor building, the control and electrical systems of the safety systems are located above the ceiling structure of the containment building. The subsystems are physically separated in their own areas on different sides of the reactor pool and are connected to the auxiliary building (UKB). There are dedicated cable ducts to areas above the containment building near the outer wall of the reactor building. There are separate ducts and tunnels connecting the residual heat removal system to the diesel generator and pumping station buildings.

As presented, the design principles regarding protection against internal events largely comply with Finnish requirements. STUK estimates that the room and layout planning of the plant is in a preliminary stage. The observation of the principle of separation in the room and layout design of the plant can be assessed in connection with the construction license application.

Monitoring and control of nuclear power plants (Government Decree 733/2008, section 19)

The passive safety functions of the KERENA unit are designed so that their activation and operation do not require an external power source. The purpose of the passive systems is to bring the power plant into a controlled state in case of an accident and keep it in that state for as long as necessary. Therefore the safety relevance of the active automation systems is lower, and their design can be much simpler.

In the documentation of the application for a decision-in-principle, the safety principles of the automation systems are described on a rather general level. Before the design and the design materials are brought further to the technical stage, the discussion of safety principles is largely a discussion of goals, and on the basis of the documentation it is not possible to fully assess whether these goals will be attained. True attainment of the safety principles in the technical design of the power plant must be ensured as the design work progresses at later stages in the project. The construction license procedure will be the first official procedure in the power plant project involving concrete appraisal of automation technology.

Automatic safety functions

The unit automation consists of several lines of defense based on the 'defense in depth' principle. The first line comprises the normal process automation, control systems and limitation systems. The second line consists of the primary protection system which actuates safety functions as required and a parallel system involving passive pressure transmitters which does not require an external power source to actuate key safety functions. Finally, there is the severe accident management system.

Passive pressure transmitters actuate these protection functions:

- reactor scram
- isolation of steam and feedwater lines
- reactor pressure control

The automation systems in the various lines of defense automatically seek to maintain the plant parameters within a safe range during operating transients and to limit the consequences of accidents.

The design objectives and principles regarding automation systems comply with Finnish safety requirements regarding the automatic actuation, control and monitoring of safety functions during operating transients and accidents.

The principle of multiple redundancy in automation

The KERENA unit protection system has four parallel subsystems. The protection function is actuated if a protection signal is received from any two of the four parallel protection channels. The systems fulfill the principle of multiple redundancy required in the Government Decree.

The passive pressure transmitter systems have two parallel subsystems. The activation of either of these will actuate a safety function. Internally, the subsystems employ a 2/2 tripping principle.

The observation of the principle of multiple redundancy in the key operating automation systems is not presented in the application documentation.

The severe accident management systems can tolerate individual faults.

The design objectives and principles presented largely comply with Finnish safety requirements regarding the principle of multiple redundancy. It must be established during the construction license application procedure how the requirement of multiple redundancy for key operating automation systems will be fulfilled.

The principle of separation in automation

In the KERENA unit, the automation systems are divided into two physically separated redundant compartments. However, the protection system consists of four parallel subsystems, and this means that two subsystems would have to be housed in one redundant compartment. This arrangement does not fulfill the Finnish requirements for separation.

The separation of automation systems and components with different safety classes between and within the subsystems is not described in the application documentation. The only related mention is that safety class 2 and 3 cabling is isolated from all other cabling in accordance with the IEEE 384 principles. The separation of the severe accident management automation and monitoring system from other automation systems is also not discussed.

The design objectives and principles regarding the separation of automation systems in the unit could not be considered to comply with Finnish safety requirements. The separation of automation systems of different safety classes from one another, and the separation of the severe accident management system from other automation systems, must be described and explained in the construction license application procedure. The principles for separating the parallel subsystems of automation systems must also be explained. If the reliability of the automation systems and the consequences of the simultaneous loss of two subsystems cannot be justified through the added backup provided by the passive systems, the separation must be redesigned.

The principle of diversity in automation

Finnish safety requirements stipulate that the reactor protection system must measure at least two different process parameters, both of which are physically dependent on a transient or accident situation and for both of which the tripping level can be set so as to ensure early intervention. The protection system and the passive pressure transmitters taken together fulfill the principle of diversity.

The active automation system is based on two computer-based system platforms. The reactor, plant protection and control systems run on one of these platforms and the other automation systems on the other one.

In the power plant concept, there is a protection system actuated by passive pressure transmitters to back up the software-based protection system in case of a common cause failure, and also passive safety systems.

The design objectives and principles presented comply with Finnish safety requirements regarding the principle of diversity.

Control room

The control room contains operator workstations with display terminals and a display screen for the safety systems. The information needed by the operators for the execution of control actions is transmitted to their workstations. The general status of the power plant can also be shown on a widescreen display.

The design objectives and principles of the control room comply with Finnish safety requirements.

Emergency control room

The KERENA unit has an emergency control room where safety-critical systems can be controlled independently of the main control room. Here, the plant can be brought into a controlled (hot shutdown) state and further into a safe (cold shutdown) state.

The emergency control room is located in a different building than the main control room.

The design objectives and principles of the emergency control room comply with Finnish safety requirements.

Reactor pressure vessel level measurement

Passive pressure transmitters actuated by a drop in the water level in the reactor pressure vessel directly actuate safety functions. There are four passive pressure transmitters. These are divided into two groups (two transmitters each), and the tripping of either group actuates the safety function.

The reactor pressure vessel level measurement is a normal differential pressure measurement that in turn controls the reactor protection automation. There are four measurements. The protection function is actuated if a protection signal is received from any two of the four parallel protection channels. The system is actuated when any two channels give the opening command.

The design objectives and principles for systems regarding reactor water level measurement largely comply with Finnish safety requirements.

Summary

The design objectives and principles of this power plant unit alternative largely comply with Finnish safety requirements.

The chosen design strategy in case of a crash by a large passenger aircraft is that principal protection is provided by the outer shell of the reactor building, which protects the containment and the safety systems in the reactor building itself. The auxiliary building, which houses the central control room, has not been protected against a plane crash; it is accepted that in such an event this building would be damaged. It is the considered opinion of STUK that the fulfillment of Finnish safety requirements with regard to protecting the control room against a crash by a large passenger aircraft has not yet been demonstrated.

There are certain technical details that need further analysis, empirical qualification and further design at a later stage in the licensing process. It is the considered opinion of STUK that none of these is such that it would constitute an obstacle to fulfilling the requirements of the Government Decree on the Safety of Nuclear Power Plants (733/2008). These technical details include:

- experimental demonstration of the functioning of the passive systems
- runtime testing procedures for the passive systems
- extent of diversification in the case of the isolating valves of the containment building
- details of the fuel pool cooling system realizing the principle of diversity
- design objectives and principles regarding the principle of separation for electrical and automation systems
- general lessons learned from the Forsmark malfunction
- observing the principle of multiple redundancy in operating automation systems

POWER PLANT UNIT ALTERNATIVES WITH A PRESSURIZED WATER REACTOR

EPR – European Pressurized Water Reactor, AREVA

General

EPR is a pressurized water reactor with an electrical output of about 1,700 MWe designed by the Franco-German consortium AREVA. The reference plant for this plant type is Olkiluoto 3. EPR is originally based on the German 1,300 MWe plants in the Konvoi series and the French 1,450 MWe plants in the N4 series. The safety assessment for the EPR unit is based on the documentation submitted for the Olkiluoto 3 unit.

The primary circuit of the EPR unit consists of four main circuits, each with a vertical steam generator and a main circulation pump.

The secondary circuit in this unit is essentially the same as in existing pressurized water reactors. There are four steam generators of the vertical U-tube type. These are technically similar to the newest steam generators at existing power plants.

Safety functions in the EPR unit are provided mainly through active systems, backed up by passive pressurized water tanks required for emergency cooling, as is typical for pressurized water reactor units. The planned service life of the plant is 60 years.

The design objectives and principles comply with Finnish safety requirements.

Compared with Olkiluoto 3, the EPR unit proposed here has an output about 7% higher. The power uprate affects the design of the unit's safety functions and its behavior in cases of transient and accident. The potential for a power uprate must be further assessed at a later stage in the licensing process.

Assessment and verification of safety (Government Decree 733/2008, section 3)

Deterministic analysis methods and preliminary results

Areva has analysis methods for safety assessment and verification developed over several decades and used for instance in the design of the Olkiluoto 3 unit. The methods have been appropriately maintained and qualified for their purpose.

Analyses conducted on the EPR unit indicate that transient and accident analyses compliant with Finnish requirements can be performed for this unit alternative.

Probabilistic analyses

AREVA employs level 1 and 2 probabilistic risk analysis (PRA) methods that have been used for PRA analyses on the Olkiluoto 3 unit, for instance. The analyses cover all events related to external and internal threats at the plant in all operating states. The analysis methods and information about the EPR analysis results indicate that analyses compliant with Finnish PRA requirements can be performed for this unit alternative.

Limitation of radiation exposure and release of radioactive materials (Government Decree 733/2008, sections 7 to 10)

As part of the design process, AREVA has calculated the radiation exposure of the population in the vicinity of the plant in accident situations. The calculations show that the radiation doses of the population remain below the dose limits set for accidents in Finland.

Engineered barriers for preventing the dispersion of radioactive materials (Government Decree 733/2008, section 13)

Reactor and fuel

The EPR unit reactor is essentially the same in structure as in existing pressurized water reactor units. There are 241 fuel assemblies and 89 control rods in the reactor. Fuel assembly and core design follow the same principles as for large existing pressurized water reactor units. The fuel assemblies are 17x17 assemblies typically used nowadays in large pressurized water reactors. Reactivity is managed during the operating cycle with boron in the primary coolant and burnable absorbers in the fuel.

A ‘heavy reflector’ surrounds the reactor core to flatten the power distribution and to improve the fuel economy; this was used for the first time in the Olkiluoto 3 unit currently under construction. The heavy reflector is a cylindrical steel structure which surrounds the reactor core and reflects leaking neutrons back into the reactor core to flatten power distribution and to protect the reactor pressure vessel against embrittlement caused by neutron radiation.

The planned fuel burn-up is greater than the maximum fuel assembly burn-up allowed in Finland, 45 MWd/kgU. However, the reactor can be adapted to conform to the Finnish burn-up limit. If approval is sought for a higher burn-up level, the applicant must be able to demonstrate experimentally that the fuel fulfills Finnish design criteria regarding accident situations.

The design objectives and principles of the reactor and fuel comply with Finnish safety requirements.

Main nuclear components

The material and structural design of the EPR unit are essentially similar to those of the Olkiluoto 3 unit. The reactor pressure vessel is of low-alloy steel, made of rotationally symmetrical forgings welded together using normal methods and clad on the inside with stainless steel welded on the surface. The requirements set for the analyses and properties of the most important materials used in the main components include the maintenance of adequate ductility throughout the service life of the unit. The heavy reflector included in the reactor internals reduces the neutron dosage to which the reactor shell is exposed as well as radiation embrittlement. A monitoring program based on normal practice is in place to monitor radiation embrittlement in the core area forgings and weld.

The methods chosen for the reactor pressure vessel are also observed, as applicable, in the manufacture of the steam generators and the pressurizer. The primary chamber of the steam generator is clad with stainless steel welded on the surface and partly with a nickel-based alloy. The heat transfer tubes are made of Inconel 690 TT alloy, which according to current knowledge is a clearly more durable solution than earlier material choices.

The main circuit piping is made of welded stainless steel forgings with good ductility properties. Although this choice of material requires the use of demanding dissimilar joints in the connections to the main components, this can be satisfactorily implemented with current technical solutions. Runtime monitoring of the dissimilar joints must be described in detail in the construction license application.

The integrity of the primary circuit is secured by means of high quality requirements for design and manufacture and by applying the ‘leak before break’ (LBB) principle based on Finnish safety requirements. The safety systems are also designed to take into account the pipe break with the largest diameter in the primary circuit. The main circulation pipes can if necessary be equipped with sufficient protection against pipe breaks, limiting the lateral and longitudinal shifting of a broken pipe and hence the magnitude of the leak.

The design objectives and principles proposed for the main nuclear components comply with Finnish safety requirements.

Primary circuit pressure control

There are three safety valves for pressure control in the primary circuit in the EPR unit. In pressure control for the primary circuit, the principle of diversity is realized in the auxiliary pressurizer spray system, which operates on the pressure differential in the main circulation pumps.

The design objectives and principles regarding pressure control comply with Finnish safety requirements.

Containment building

The primary containment building of the EPR unit is a 'dry containment' made of pre-stressed reinforced concrete and provided with a tight steel liner. It is designed to maintain the tightness compliant with its acceptance criteria even in case of a transient or an accident. A secondary concrete containment building is designed around the primary containment building to protect it against external threats.

Severe accidents

Severe accident management for the EPR unit is based on depressurization of the primary circuit, residual heat removal from the containment building using the spray system, spreading the core melt into a thin layer and cooling it in a separate spreading area, and hydrogen removal by means of recombinators.

The purpose of depressurizing the primary circuit is to prevent high-pressure discharge of core melt in the event of reactor pressure vessel failure. In the EPR unit, primary circuit pressure can be reduced using two parallel depressurization valves independent of other plant systems, discharging into the relief tank located in the containment building. There are two valves in line on both discharge pipes. In case of an accident, the opening of just one of these pipes will be sufficient to lower the pressure in the primary circuit to the design level. The power for opening these is supplied by the severe accident power supply system, which has a battery backup.

Residual heat removal is effected with the containment building spray system (JMQ), which is only used in case of a severe accident. As the system is only designed for severe accident management, it is not needed for managing postulated accidents. The JMQ system consists of two redundant trains, either of which is sufficient for removing the residual heat released into the containment building in case of an accident and transferring it to the ultimate heat sink. The containment building residual heat removal system and its support systems are powered by the severe accident power supply system.

In the EPR unit, the core melt is cooled in the core melt spreading area located on the base level of the containment building. The floor and walls of the spreading area are lined with thick iron elements with cooling ducts running in the bottom or

rear part. The floor elements are covered with a concrete layer designed to protect the elements at the melt discharge stage. If the reactor pressure vessel fails, the core melt is first discharged into the reactor pit and, when the metal gate at the bottom melts, through a short tunnel into the spreading area. The core melt discharging into the spreading area trips the flooding valves leading to the emergency cooling water pool, causing the coolant to flow into the cooling ducts under and behind the floor and wall elements in the spreading area and finally on top of the core melt itself. The steam generated in the spreading area rises into the dome of the containment building, where it is condensed using the containment building spray system. No external power is required to direct the core melt into the spreading area and to cool it with water from the emergency cooling pool.

During a severe accident, a substantial amount of hydrogen is generated which pressurizes the containment building. At a sufficiently high concentration, the hydrogen may combust or explode. The containment building of a pressurized water reactor is filled with air during operation and thus contains oxygen needed for combustion. However, pressurized water reactors have a large containment building made of pre-stressed concrete that is highly resistant to hydrogen fires or explosions. For hydrogen removal, the EPR unit is equipped with some 50 passive autocatalytic recombinators. The recombinators require no external power source, and they remove hydrogen at such low levels that a combustible gas mix cannot be generated.

The EPR unit currently under construction in Finland (Olkiluoto 3) is equipped with a filtered containment building venting system as specified in Finnish requirements. The purpose of this system is to remove non-condensing gases from the containment building following an accident and to equalize the pressure inside the containment building to normal atmospheric pressure.

The design objectives and principles of the systems for managing severe accidents comply with Finnish requirements.

Safety functions and provisions for ensuring them (Government Decree 733/2008, section 14)

Safety functions in the EPR unit are provided mainly through active systems. Passive systems are used for some details such as the reactor scram system and the pressurized water tanks typically used in emergency cooling systems in pressurized water reactor units.

Reactivity management

In the EPR unit, reactivity management is effected actively through control rods, boron in the primary coolant and burnable absorbers in the fuel.

In case of a transient, the reactor is shut down as in all other pressurized water reactors by dropping the control rods into the reactor core. The reactor scram system is a passive system. The control rods drop into the reactor core by gravity once the reactor protection automation system disconnects the power to the electromagnets holding them up. This system fulfills the principle of multiple redundancy required in the Government Decree.

The principle of diversity is realized with the emergency borating system (EBS), 3 x 100% in its active parts (the system comprises two trains to the reactor).

Because of the burnable absorber mixed in the fuel, the boron content of the primary coolant can be kept relatively low even after refueling. However, despite the lower boron content of the primary coolant and a more effective scram, the reactor design must allow for the possibility of the boron content of the coolant being erroneously diluted. The management of what is known as a boron-free water plug is taken into account in the design regarding shutdown states, startup, transients and accidents. The presented design fulfills Finnish requirements.

Recriticality of the reactor in cooling situations is prevented by means of the control rods and the boron solution pumped into the reactor cooling circuit by the medium head safety injection system (JND).

The design objectives and principles related to safety functions in reactivity management comply with Finnish safety requirements.

Cooling of the reactor

Cooling of the reactor in shutdown conditions

In a hot shutdown, residual heat is removed from the reactor through the steam generators directly into the turbine condenser using the turbine bypass lines, as is typical for pressurized water reactors. If this is not possible, residual heat may be removed by pumping water into the steam generators through the emergency feedwater system and by venting the steam into the atmosphere through the relief valves in the secondary circuit. This will be discussed below in connection with transients.

After lowering the pressure and temperature in the primary circuit, residual heat is removed from the reactor using the residual heat removal system (RHR, 4 x 100%), which uses the same pumps as the low head safety injection system. The

residual heat is removed through the component cooling water system (CCWS, 4 x 100%) and the service water system (SWS, 4 x 100%) to the ultimate heat sink. These systems are also used as the primary residual heat removal systems in case of a transient or an accident.

If the normal residual heat removal system (RHR) is not available in a situation where the reactor pressure vessel head is open, residual heat may be removed by evaporating water into the containment building for the first 24 hours and then removing residual heat into the atmosphere through the filtered containment building venting system. Make-up water for the reactor is realized from the IRWST tank using the JND system.

Cooling of the reactor in accident conditions with the reactor primary circuit intact

If a transient or an accident prevents normal removal of residual heat to the turbine condenser, residual heat can be transferred from the primary circuit to the atmosphere by using the secondary circuit emergency feedwater system (EFWS, 4 x 100%) and the steam generator relief valves (MSDV). The emergency feedwater system pumps water from the emergency feedwater tank to the steam generators, and the resulting steam is vented into the atmosphere through relief valves. The emergency feedwater system has four trains. This system enables the reactor to be brought into a controlled (hot shutdown) state and kept there for at least 72 hours.

If removal of residual heat through the secondary circuit is not possible and pressure and temperature are high in the primary circuit, residual heat can be removed directly from the primary circuit by pumping cold boron-containing water from the IRWST tank through the pumps of the medium head safety injection system (JND) and by removing hot water from the system through the safety valves back to the IRWST tank (‘feed and bleed’). Residual heat is further removed from the IRWST tank using the residual heat removal system (RHR, 4 x 100%). The residual heat is removed through the component cooling water system (CCWS, 4 x 100%) and the service water system (SWS, 4 x 100%) to the ultimate heat sink.

In case of a transient or an accident where the reactor primary circuit is intact, make-up water to compensate for lower volume due to cooling is primarily pumped into the reactor through the normal make-up water system (KBA, mainly 2 x 100%).

Alternatively, make-up water can be obtained through the medium head safety injection system (JND, 4 x 100%), which gets its water from the IRWST tank inside the containment building.

Cooling of the reactor in loss of coolant accidents

In accidents where reactor coolant is lost as the result of a leak, the reactor can be cooled with the safety injection system designed for this purpose.

In the EPR unit, emergency cooling of the primary circuit is effected through the active medium head safety injection system (JND, 4 x 100%) and the low head safety injection system (JNG, 4 x 100%), and four safety injection accumulators. Pressure in the primary circuit is reduced to within the operating range of the medium head safety injection pumps by means of the relief valves in the secondary circuit. This system forms part of the emergency cooling function. The medium and low head safety injection systems share common supply nozzles to the cold legs of the primary circuit. If necessary, the cooling water supply can be diverted to the pipes leading to the hot leg and thereby to cool the reactor core. The pumps of the emergency cooling system take coolant from the tank in the containment building (IRWST) through suction filters. Any reactor coolant leaking into the containment building will be drained back into the IRWST tank. The suction filters in the IRWST tank are designed so that they will not be clogged by debris generated in an accident or otherwise present in the containment building. The filters are also equipped with a flushing system in case of clogging. Partial clogging of the suction filters has been appropriately taken into account in determining the required suction head of the safety injection pumps. The performance of the suction filters has also been proven experimentally.

With regard to the emergency cooling system described above, the principle of diversity is observed for small coolant leaks by having the primary circuit cooled quickly using the relief valves in the secondary circuit and lowering the pressure in the primary circuit to a point where the JNG system and the safety injection accumulators can function. The JNG system can be replaced by the JND system. The systems take their cooling water from the IRWST tank.

Residual heat is removed from the IRWST tank using the residual heat removal system (RHR, 4 x 100%), which uses the same pumps as the low head safety injection system. The residual heat is removed through the component cooling water system (CCWS, 4 x 100%) and the essential service water system (ESWS, 4 x 100%) to the ultimate heat sink.

The presented design for the reactor core cooling and residual heat removal systems fulfills the Finnish requirements in principle.

Removal of residual heat from the containment building

In the EPR unit, residual heat can be removed from the containment building if necessary in case of a leak from the primary or secondary circuit by removing residual heat from the IRWST tank and transferring it through the component

cooling water system (CCWS) and the backed-up essential service water system (ESWS) to the ultimate heat sink.

When the reactor pressure vessel head is open, the normal residual heat removal system may be replaced by evaporating water into the containment building for the first 24 hours and then removing residual heat into the atmosphere through the filtered containment building venting system. Cooling water for the reactor is obtained from the IRWST tank using the JN system.

The design objectives and principles regarding removal of residual heat from the containment building comply with Finnish safety requirements.

Containment building isolation

The isolation of the pipelines penetrating the containment building is effected by two isolating valves operating on two different principles in case of a transient or an accident.

The design objectives and principles of the containment building isolation comply with Finnish safety requirements.

Loss of ultimate heat sink

If the ultimate heat sink, i.e. the possibility of removing residual heat through the turbine condenser or essential service water system to the sea, is lost while the reactor circuit is closed, residual heat may be removed from the reactor cooling circuit by pumping water into the secondary side of the steam generators through the emergency feedwater system and venting the resulting steam into the atmosphere. This will enable the reactor to be kept in a controlled state for at least 72 hours.

When the reactor pressure vessel head is open, the normal residual heat removal system may be replaced by evaporating water into the containment building for the first 24 hours and then removing residual heat into the atmosphere through the filtered containment building venting system. Cooling water for the reactor is obtained using the JNG system.

The design objectives and principles related to the management of loss of the ultimate heat sink comply with Finnish safety requirements.

Cooling of fuel pools

The fuel pools are cooled by the fuel pool cooling system. The system has two trains, each with two pumps (FAK). The fuel pool is divided into two physical pools.

In case of loss of other possibilities, the fuel pools could be cooled by removing residual heat through evaporating water in the pools. As the pressure would increase in the fuel building, the rupture disk would break, and the steam would be vented into the atmosphere through the ventilation stack. Make-up water for the fuel pools is available from a number of sources: the fire water distribution system (SGB), the fuel pool cleaning system (FAL) or the demineralized water distribution system (GHC).

The design objectives and principles related to the cooling of the fuel pools comply with Finnish safety requirements.

Shutdown safety

It is ensured that the reactor will remain subcritical in all shutdown states by keeping the control rods inserted into the reactor and by adding boron solution with an adequate concentration to the coolant. Subcriticality is monitored during shutdown with neutron flux detectors outside the reactor and through administrative procedures.

The safety valves of the primary circuit and safety valves in the residual heat removal system prevent the cold pressurization of the primary circuit.

The removal of residual heat from the primary circuit and the containment building in a shutdown situation with the reactor pressure vessel head open or closed is managed as noted above under ‘Cooling of the reactor’.

The presented design for shutdown safety systems fulfills the Finnish requirements in principle.

Electrical systems

The external power source of the unit is a connection from the 400 kV grid through auxiliary transformers, or from the 110 kV grid through two standby auxiliary transformers.

In case the external power source fails, power to the safety systems of the plant is supplied alternately from:

- auxiliary diesel generators (4 x 100%)
- alternative auxiliary diesel generators realizing the principle of diversity (2 x 100%)
- batteries during the startup of the auxiliary power sources (rated discharge time 2 h).

The severe accident management systems have their own separate battery arrays (rated discharge time 12 h) as internal power sources.

The design objectives and principles of the electrical systems comply with Finnish safety requirements.

Building technology and fire protection

The basic design of the buildings and building services and of fire protection is similar to that of the Olkiluoto 3 unit. The design objectives and principles regarding building technology, building services and fire protection comply with Finnish safety requirements.

Protection against external events (Government Decree 733/2008, section 17)

The protection strategy for the EPR unit against a crash by a large passenger aircraft is to design and build the containment building, fuel building and safeguard buildings 2 and 3 to withstand such a crash. Safeguard buildings 1 and 4 are located on either side of the containment building, and their protection is thus based on distance separation and shadowing separation. The two pumping stations of the essential service water system are protected on the basis of distance separation. The auxiliary diesel generator buildings are also located on different sides of the containment and safeguard building mass, and their protection is thus based on distance separation and shadowing separation. The isolating valves of the main steam and feedwater systems are located on different sides of the containment building and are thus protected by distance separation and shadowing separation. The turbine building is not designed to withstand an aircraft crash, as it houses no safety-critical systems.

The design objectives and principles of the solution comply with Finnish safety requirements.

Protection against internal events (Government Decree 733/2008, section 18)

Internal threats such as floods and fires are taken into account in the room and layout planning of the unit with physical separation of the four redundant key safety subsystems. Most of the four subsystems constituting the safety systems are housed in the four safeguard buildings. The main design principle in the EPR unit is that an initiating event in one subsystem must not compromise the operating of the other subsystems. The rated fire resistance of the structures between the subsystems is two hours. Fire hazard and flooding analyses have been carried out in the Olkiluoto 3 project, based on detailed design of the EPR unit, and STUK has reviewed these as part of the review process during the construction stage.

The design objectives and principles of the solution comply with Finnish safety requirements.

Monitoring and control of nuclear power plants (Government Decree 733/2008, section 19)

Automatic safety functions

The unit automation consists of several lines of defense based on the 'defense in depth' principle. The first line comprises the normal process automation, control systems and limitation systems. The second line consists of the primary protection system which actuates safety functions as required. The third line includes the safety automation system (SAS) and another backup system operating on a different principle, the hardwired backup system (HBS). Finally, there is the severe accident management system.

The automation systems in the various lines of defense automatically seek to maintain the plant parameters within a safe range during operating transients and to limit the consequences of accidents.

The design objectives and principles of the systems comply with Finnish safety requirements.

The principle of multiple redundancy in automation

The primary protection system has four parallel subsystems. The protection function is actuated if a protection signal is received from any two of the four parallel protection channels. The HBS backup, the reactor control and surveillance limitations systems (RCSL) and the SAS each also consist of four parallel subsystems.

The design objectives and principles of the systems comply with Finnish safety requirements.

The principle of separation in automation

Safety class 2 systems are physically and functionally separated from all other systems and components. Safety class 3 systems are functionally separated from other systems.

The severe accident management automation and monitoring system is separated from other automation systems.

The parallel automation subsystems are physically and functionally separated from one another.

The design objectives and principles of the separation of automation systems comply with Finnish safety requirements.

The principle of diversity in automation

In the reactor protection system, the principle of diversity is observed by the signals indicating accident and transient conditions coming alternatively from two different process parameters.

The unit automation is based on two computer-based system platforms. The protection, control and limitation actions operate on one of the platforms and other automation functions on the other one.

The plant concept incorporates a hardwired backup system (HBS) realizing the principle of diversity in case of a common cause failure in computer-based automation.

The design objectives and principles of the systems comply with Finnish safety requirements.

Control room

The control room of the EPR unit contains control consoles and a display panel. The control consoles of the turbine operator and the reactor operator are used to control the plant under normal operating conditions, transient conditions and accident conditions. Also, all the information needed by the operators for the execution of control actions is transmitted to the main control console.

The display panel comprises fixed indicators, control switches and widescreen displays. The purpose of the display panel is to show a summary of the status of the plant and its principal components and key alert data. The display panel also features hardwired push buttons for controlling the plant in case of a common cause failure in the digital automation systems or in case of a severe accident.

The design objectives and principles of the control room comply with Finnish safety requirements.

Emergency control room

The unit has an emergency control room where safety-critical systems can be controlled independently of the main control room. Here, the plant can be brought into a controlled (hot shutdown) state and further into a safe (cold shutdown) state.

The emergency control room is located in a different fire compartment than the main control room.

The design objectives and principles of the emergency control room comply with Finnish safety requirements.

Summary

The design objectives and principles comply with Finnish safety requirements. Compared with Olkiluoto 3, the EPR unit proposed here has an output about 7% higher. The power uprate affects the design of the unit's safety functions and its behavior in cases of transients and accidents. The potential for a power uprate must be further assessed at a later stage in the licensing process.