Unofficial translation

PRELIMINARY SAFETY ASSESSMENT OF LOVIISA 3 NUCLEAR POWER PLANT PROJECT

APPENDIX 1: FEASIBILITY ASSESSMENT OF PLANT ALTERNATIVES

FOREWORD .........................................................................................................................................6

BASIS FOR THE ASSESSMENT OF THE PLANT ALTERNATIVES........................................7

BOILING WATER REACTOR PLANT ALTERNATIVES.................................................................9

ABWR - Advanced Boiling Water Reactor, Toshiba-Westinghouse............................................9

General ..............................................................................................................................................9

Assessment and verification of safety (Gov. Decree 733/2008 Section 3)....................................10

Deterministic analysis methods and preliminary results ..............................................................10

Probabilistic analyses .......................................................................................................................10

Qualification of new type of systems ..............................................................................................10

Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008

Sections 7–10).................................................................................................................................11

Reactor and fuel .................................................................................................................................11

Main nuclear components ..............................................................................................................12

Containment .....................................................................................................................................13

Severe accidents ..............................................................................................................................13

Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14)..............15

Reactivity management ....................................................................................................................15

Cooling of reactor ............................................................................................................................16

Cooling of reactor in shutdown conditions .....................................................................................16

Cooling of reactor in accident conditions with reactor primary circuit intact ...............................16

Cooling of reactor in loss of coolant accidents ..............................................................................17

Containment isolation ......................................................................................................................18

Loss of ultimate heat sink .................................................................................................................18

Cooling of fuel pools ........................................................................................................................19

Shutdown safety ...............................................................................................................................19

Electrical systems ...........................................................................................................................20

Civil engineering and fire protection .............................................................................................21

Protection against external events (Gov. Decree 733/2008 Section 17) ........................................21

Protection against internal events (Gov. Decree 733/2008 Section 18) .........................................22

Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19) ..............23

Automatic safety functions ............................................................................................................23

I&C redundancy principle ...............................................................................................................23

I&C separation principle .................................................................................................................24

I&C diversity principle ....................................................................................................................24

N.B. This is unofficial translation.

Original:
Control room .................................................................................................................. 25
Emergency control room ................................................................................................. 25
Reactor pressure vessel level measurement ................................................................. 26
Summary ........................................................................................................................... 26

ESBWR - Economical and Simplified Boiling Water Reactor, GE-Hitachi .................. 27
General ............................................................................................................................. 27
Assessment and verification of safety (Gov. Decree 733/2008 Section 3) .......... 27
Deterministic analysis methods and preliminary results ........................................ 27
Probabilistic analyses ...................................................................................................... 27
Qualification of new type of systems ............................................................................... 28
Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008 Sections 7–10) ................................................................. 28
Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008 Section 13) ................................................................. 28
Reactor and fuel ................................................................................................................ 28
Main nuclear components ............................................................................................... 30
Reactor pressure control ................................................................................................. 30
Containment .................................................................................................................... 31
Severe accidents ............................................................................................................. 31
Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14) ...................................................................................................................... 33
Reactivity management .................................................................................................. 33
Cooling of reactor .......................................................................................................... 34
Cooling of reactor in shutdown conditions ................................................................. 34
Containment isolation ..................................................................................................... 36
Loss of ultimate heat sink ............................................................................................... 36
Cooling of fuel pools ....................................................................................................... 36
Shutdown safety ............................................................................................................... 37
Electrical systems ........................................................................................................... 37
Civil engineering and fire protection ................................................................................ 38
Protection against external events (Gov. Decree 733/2008 Section 17) .................. 38
Protection against internal events (Gov. Decree 733/2008 Section 18) ................. 39
Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19) ...................................................................................................................... 40
Automatic safety functions ............................................................................................ 40
I&C redundancy principle .............................................................................................. 41
I&C separation principle ............................................................................................... 41
I&C diversity principle ................................................................................................... 42
Control room ................................................................................................................... 42
Emergency control room ............................................................................................... 43
Reactor pressure vessel level measurement ................................................................. 43
Summary ........................................................................................................................... 43

PRESSURISED WATER REACTOR PLANT ALTERNATIVES ................. 44

AES-2006 - Pressurised Water Reactor - Atomstroyexport ................................. 44
General ............................................................................................................................. 44
Assessment and verification of safety (Gov. Decree 733/2008 Section 18) .............. 45

N.B. This is unofficial translation.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deterministic analysis methods and preliminary results</td>
<td>45</td>
</tr>
<tr>
<td>Probabilistic analyses</td>
<td>46</td>
</tr>
<tr>
<td>Qualification of new type of systems</td>
<td>46</td>
</tr>
<tr>
<td>Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008 Sections 8–10)</td>
<td>46</td>
</tr>
<tr>
<td>Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008 Section 13)</td>
<td>46</td>
</tr>
<tr>
<td>Reactor and fuel</td>
<td>46</td>
</tr>
<tr>
<td>Pressure control of primary and secondary circuits</td>
<td>48</td>
</tr>
<tr>
<td>Containment</td>
<td>49</td>
</tr>
<tr>
<td>Severe accidents</td>
<td>49</td>
</tr>
<tr>
<td>Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14)</td>
<td>50</td>
</tr>
<tr>
<td>Reactivity management</td>
<td>51</td>
</tr>
<tr>
<td>Cooling of reactor</td>
<td>51</td>
</tr>
<tr>
<td>Removal of residual heat from the containment</td>
<td>54</td>
</tr>
<tr>
<td>Containment isolation</td>
<td>55</td>
</tr>
<tr>
<td>Loss of ultimate heat sink</td>
<td>55</td>
</tr>
<tr>
<td>Cooling of fuel pools</td>
<td>56</td>
</tr>
<tr>
<td>Shutdown safety</td>
<td>56</td>
</tr>
<tr>
<td>Electrical systems</td>
<td>57</td>
</tr>
<tr>
<td>Civil engineering and fire protection</td>
<td>58</td>
</tr>
<tr>
<td>Protection against external events (Gov. Decree 733/2008 Section 17)</td>
<td>58</td>
</tr>
<tr>
<td>Protection against internal events (Gov. Decree 733/2008 Section 18)</td>
<td>59</td>
</tr>
<tr>
<td>Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19)</td>
<td>59</td>
</tr>
<tr>
<td>Automatic safety functions</td>
<td>60</td>
</tr>
<tr>
<td>I&amp;C redundancy principle</td>
<td>60</td>
</tr>
<tr>
<td>I&amp;C separation principle</td>
<td>60</td>
</tr>
<tr>
<td>I&amp;C diversity principle</td>
<td>61</td>
</tr>
<tr>
<td>Control room</td>
<td>61</td>
</tr>
<tr>
<td>Emergency control room</td>
<td>62</td>
</tr>
<tr>
<td>Summary</td>
<td>62</td>
</tr>
<tr>
<td>APR1400 - Advanced Power Reactor 1400 - KHNP</td>
<td>64</td>
</tr>
<tr>
<td>General</td>
<td>64</td>
</tr>
<tr>
<td>Assessment and verification of safety (Gov. Decree 733/2008 Section 3)</td>
<td>65</td>
</tr>
<tr>
<td>Deterministic analysis methods and preliminary results</td>
<td>65</td>
</tr>
<tr>
<td>Probabilistic analyses</td>
<td>65</td>
</tr>
<tr>
<td>Qualification of new type of systems</td>
<td>65</td>
</tr>
<tr>
<td>Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008 Sections 7–10)</td>
<td>65</td>
</tr>
<tr>
<td>Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008 Section 13)</td>
<td>66</td>
</tr>
<tr>
<td>Reactor and fuel</td>
<td>66</td>
</tr>
<tr>
<td>Main nuclear components</td>
<td>66</td>
</tr>
<tr>
<td>Pressure control of primary and secondary circuits</td>
<td>67</td>
</tr>
<tr>
<td>Containment</td>
<td>68</td>
</tr>
</tbody>
</table>

N.B. This is an unofficial translation.

Original:
Severe accidents.................................................................................................................. 68
Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14)........ 69
Reactivity management ........................................................................................................ 69
Cooling of reactor .................................................................................................................. 70
Removal of residual heat from containment ......................................................................... 72
Containment isolation ............................................................................................................. 73
Loss of ultimate heat sink ....................................................................................................... 73
Cooling of fuel pools ............................................................................................................... 73
Shutdown safety ....................................................................................................................... 74
Electrical systems .................................................................................................................. 74
Civil engineering and fire protection ....................................................................................... 75
Protection against external events (Gov. Decree 733/2008 Section 17) ................................... 75
Protection against internal events (Gov. Decree 733/2008 Section 18) ................................. 76
Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19) .......... 76
Automatic safety functions ................................................................................................... 76
I&C redundancy principle ...................................................................................................... 77
I&C separation principle ......................................................................................................... 77
I&C diversity principle ........................................................................................................... 78
Control room .......................................................................................................................... 78
Emergency control room ....................................................................................................... 79
Summary .................................................................................................................................. 79

**EPR - European Pressurised Water Reactor - AREVA** .................................................................. 79
General ...................................................................................................................................... 79
Assessment and verification of safety (Gov. Decree 733/2008 Section 3) ............................... 80
  Deterministic analysis methods and preliminary results ...................................................... 80
Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008
Sections 7–10) ....................................................................................................................... 81
Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008
Section 13) .............................................................................................................................. 81
  Reactor and fuel .................................................................................................................. 81
  Main nuclear components .................................................................................................... 81
  Pressure control of primary circuit ....................................................................................... 82
  Containment ........................................................................................................................ 82
Severe accidents ....................................................................................................................... 83
Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14) ......... 84
Reactivity management .......................................................................................................... 84
Cooling of reactor .................................................................................................................. 85
Removal of residual heat from containment .......................................................................... 87
Containment isolation ............................................................................................................. 87
Loss of ultimate heat sink ....................................................................................................... 87
Cooling of fuel pools ............................................................................................................... 88
Shutdown safety ....................................................................................................................... 88
Electrical systems .................................................................................................................. 89
Civil engineering and fire protection ..................................................................................... 89
Protection against external events (Gov. Decree 733/2008 Section 17) ............................... 89

N.B. This is unofficial translation.
Original:
Protection against internal events (Gov. Decree 733/2008 Section 18)................................. 90
Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19)............ 90
   Automatic safety functions.................................................................................................. 90
   I&C redundancy principle................................................................................................... 90
   I&C separation principle..................................................................................................... 91
   I&C diversity principle......................................................................................................... 91
   Control room ...................................................................................................................... 91
   Emergency control room ................................................................................................... 92
Summary ................................................................................................................................... 92
FOREWORD

FORTUM submitted to STUK, as enclosures to the application for a decision-in-principle, descriptions of the technical solutions of each plant alternative and Fortum’s own assessment of how the plant alternatives meet the requirements set forth in the Government Decree on the safety of nuclear power plants (733/2008). This is a presentation of STUK’s assessment of how the design objectives and principles of each of the plant alternatives presented in the application for a decision-in-principle meet the Finnish safety requirements.

The preliminary safety assessment addresses two nuclear power plants with a boiling water reactor, ABWR and ESBWR, and three nuclear power plants with a pressurised water reactor, AES-2006, APR1400 and EPR. Both active and passive safety systems are used in these plant alternatives. Active systems refer to systems, which operation is based on components requiring an uninterrupted external power source. Passive systems refer to systems, which operation, with the exception of the actuating function (e.g. valve position change), is not dependent on an external power source or operator action and which, in consequence of a loss of power supply, will settle in a state preferable from the safety point of view. The power supply of the component performing the actuating function must be based on components passive in nature. The power source can be e.g. an electrical battery or a pressure accumulator. The safety functions of the ESBWR are mainly based on passive systems. In the ABWR and AES-2006 alternatives, the role of passive systems has been essentially increased compared with the existing plants. The safety functions of the APR1400 and EPR plant alternatives do not differ essentially from the existing plants. Severe accidents have been taken into account in all the plant alternatives. Table 1 presents the main technical data on the plant alternatives.

<table>
<thead>
<tr>
<th>Plant</th>
<th>Supplier</th>
<th>Type</th>
<th>Thermal power</th>
<th>Electrical output</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABWR</td>
<td>Toshiba-Westinghouse</td>
<td>Boiling water reactor</td>
<td>4300 MWt</td>
<td>ca. 1600 MWe</td>
</tr>
<tr>
<td>ESBWR</td>
<td>GE-Hitachi</td>
<td>Boiling water reactor</td>
<td>4500 MWt</td>
<td>ca. 1600 MWe</td>
</tr>
<tr>
<td>AES-2006</td>
<td>Atomstroyexport</td>
<td>Pressurised water reactor</td>
<td>3200 MWt</td>
<td>ca. 1200 MWe</td>
</tr>
<tr>
<td>APR1400</td>
<td>Korean Hydro &amp; Nuclear Power</td>
<td>Pressurised water reactor</td>
<td>4000 MWt</td>
<td>ca. 1400 MWe</td>
</tr>
<tr>
<td>EPR</td>
<td>Areva</td>
<td>Pressurised water reactor</td>
<td>4590 MWt</td>
<td>ca. 1700 MWe</td>
</tr>
</tbody>
</table>

The boiling water plants and the pressurised water plants are presented in separate sections in alphabetical order.

N.B. This is unofficial translation.

BASIS FOR THE ASSESSMENT OF THE PLANT ALTERNATIVES

The assessment is based on the key requirements of the Government Decree on the safety of nuclear power plants (Gov. Decree 733/2008). The requirements against which the plant alternatives have been assessed are presented here.

Assessment and verification of safety (Gov. Decree 733/2008 Section 3)

Section 3 of the Decree sets forth the requirements for the experimental and computational methods used to justify the safety and the technical solutions used in the safety systems of nuclear power plants.

As concerns the requirements set forth in Section 3 of the Decree, the preliminary safety assessment shall validate that the plant supplier uses deterministic and probabilistic computation methods, which have been appropriately qualified, and that the models have been used in earlier plant projects. The assessment also focuses on how the plant supplier has proven by means of experimental methods the functionality of any new plant features that have not been previously used.

Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008 Sections 8–10)

Sections 8-10 of the Decree define the limit values for the annual dose to an individual in the population resulting from normal operation of the plant, anticipated transients and accidents. The preliminary safety assessment includes an assessment of whether the plant supplier uses appropriate analysis methods as well as a comparison of analysis results for a reference plant with the defined limits.

Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008 Section 13)

According to Section 13 of the Decree, the engineered barriers for preventing the dispersion of radioactive materials from the nuclear power plant into the environment include the cladding of the fuel, the primary coolant circuit and the containment. Successive barriers constitute the so-called defence-in-depth principle.

On one hand, the preliminary safety assessment focuses on the capability of manufacturing high-quality barriers, which will reliably retain their integrity and leak-tightness. On the other hand, an assessment is made of whether all the situations in which the mechanical and thermal loads acting on the barriers must remain within the design limits are adequately taken into account in the design basis of the safety functions of the plant.

Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14)

N.B. This is unofficial translation.
Original:
Pursuant to Section 14 of the Decree, the most important safety functions include reactivity management, cooling of the reactor and prevention of the dispersion of radioactive materials. The assessment focuses on verifying how the principles of redundancy, separation and diversity have been implemented in the plant alternatives. Compliance with these principles is important already at the early plant design stage, as it would be extremely difficult and demanding to incorporate them in the designs at a later stage.

The redundancy principle refers to realising the systems required for safety functions, i.e. safety systems, as several redundant subsystems, which can replace each other. The most important safety systems must perform their function even if any one of the individual system components fails and any other component of the same system is simultaneously unavailable. The supporting functions essential to the safety system components must also be realised as redundant systems. Moreover, power supply must be implemented so that both an off-site and an on-site power supply system can be used. Off-site power supply systems refer to connections to normal power grids and on-site power supply systems to power supplies that can replace an off-site power supply.

The separation principle dictates that the parallel subsystems of safety systems, which back up each other, must be located in different parts of the plant or at least in facilities separated from each other by means of strong structures. In addition, systems critical to safety must be installed in different buildings or rooms from the other parts of the plant. The purpose of this is to ensure protection against internal and external events.

The diversity principle refers to securing systems related to safety functions with systems or components that are based on different operating principles. Compliance with this principle can improve the reliability of the safety function and eliminate the consequences of common cause failures related to safety functions. The diversity principle must be applied to the safety functions used to limit the consequences of anticipated operational transients or level 1 postulated accidents. Anticipated operational transients and level 1 postulated accidents refer to initiating events for which the anticipated frequency is higher than once in a thousand years. Situations in which the plant’s behaviour in transients or in level 1 postulated accidents is considered when some common cause failure of a safety system is related to them are called design extension conditions (DEC). Also a rare accident, external event or complex failure combination must be examined as a DEC event. The design principles of the systems (diverse systems) needed to manage situations examined and the design principles related to the primary safety systems and the independence of their diverse systems must be presented when assessing the feasibility of the plant alternatives. STUK presented the DEC requirements in its special decision Y255/3 (8.4.2009) and its appendix.

Protection against external events (Gov. Decree 733/2008 Section 17)

Section 17 of the Decree sets forth requirements for the protection of the safety functions of the nuclear power plant against external events. External events may
endanger the integrity of the systems, structures and components involved in safety functions, cause an operating transient or an accident and prevent the realisation of a safety function. External events may include various weather phenomena (high or low temperatures, strong winds, snowstorms), earthquakes, high seawater level (flooding) as well as hostile actions intended to damage the plant, including a large passenger airplane crashing into the plant. This paragraph assesses how the aforementioned phenomena are considered in the design of the plant.

Protection against internal events (Gov. Decree 733/2008 Section 18)

Section 18 of the Decree sets forth requirements for the protection of systems involved in safety functions against internal events, similarly to the presentation of requirements for protection against external events in Section 17. Internal events may include fires, pipe breaks, damages to tanks, missiles, explosions, heavy falling objects and flooding caused by a leak. This paragraph assesses how the aforementioned phenomena are considered in the design of the plant.

Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19)

Section 19 of the Decree sets forth requirements for the protection automation, the main control room, the emergency control room and the local control posts of the nuclear power plant. This paragraph assesses the realisation of the requirements presented in Section 19 and the principles of redundancy, separation and diversity presented in Section 14 in important automation systems.

BOILING WATER REACTOR PLANT ALTERNATIVES

ABWR - Advanced Boiling Water Reactor, Toshiba-Westinghouse

General

ABWR is a boiling water reactor with an electrical output of ca. 1600 MWe, designed by the Japanese Toshiba-Westinghouse. The first ABWR plant (KK6) designed and constructed by Toshiba was built in Kashiwazaki-Kariwa in Japan at the beginning of the 1990s and the second (KK7) immediately after the first one. The reference plant of the plant tendered to Finland is Hamaoka 5, which was completed at the beginning of 2005. In addition to the aforementioned plants, there is one more ABWR plant unit in operation in Japan, two under construction and several at design stage.

In the feasibility study for Finland, Toshiba-Westinghouse has developed the reference plant by adding certain safety features required by Finnish safety requirements. The rated service life of the plant is 60 years. The level of maturity of the plant with respect
to basic engineering is high. The design objectives and principles are, for the most part, consistent with Finnish safety requirements.

At the ABWR plant both active and passive systems are used for the implementation of safety functions.

Assessment and verification of safety (Gov. Decree 733/2008 Section 3)

Deterministic analysis methods and preliminary results

For the assessment and verification of safety, the plant supplier uses the deterministic analysis methods of Toshiba and Westinghouse Atom (previously ABB ATOM). The analysis methods of Westinghouse Atom have been used in the design and operation of the Olkiluoto 1 and 2 plant units. The methods have been appropriately maintained and qualified for the intended purpose of use. The analyses performed on the ABWR plant lead to the impression that transient and accident analyses consistent with Finnish requirements can be performed on this plant alternative.

Probabilistic analyses

Toshiba uses level 1 and 2 probabilistic risk analysis (PRA) methods, which have been applied in the PRA analyses of the plants Toshiba has constructed in Japan. The analyses are primarily based on Japanese and an American component failure database. The analyses performed on Toshiba's Japanese plants encompass all events associated with external and internal hazards in all operational states of the plant. Based on the data on analysis methods and the results of the PRA calculations pertaining to ABWR, it can be assessed that analyses consistent with Finnish PRA requirements can be performed on this plant alternative. If necessary, the methods can be developed on the basis of detailed Finnish requirements. Probabilistic risk analyses will be made in conjunction with the plant’s detailed design process, at which time the compliance with Finnish safety requirements will be assessed.

Qualification of new type of systems

The design concept of Toshiba's ABWR plant includes passive systems, which have previously not been used in nuclear power plants. These systems include an isolation condenser (IC) for direct cooling of the reactor circuit and a passive containment cooling system (PCCS) for the removal of residual heat in transient and accident conditions. Toshiba has experimentally qualified the systems. The test programme has encompassed both tests performed on a single heat transfer tube of a condenser associated with residual heat removal and full-scale tests on condensers. The tests have focused on studying heat transfer mechanisms and the effects of noncondensable gases over a large range of parameters. Based on the tests, a correlation of the effects of noncondensable gases on the heat transfer capacity of the condenser has been
developed. The tests and theoretical analyses have shown that both the isolation condenser and the containment cooling system operate reliably in accident conditions.

Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008 Sections 7−10)

Toshiba has performed a preliminary calculation of the radiation exposure of the population in the areas surrounding the plant in accident situations. The calculations have been performed for level 2 accidents (the frequency of the initiating event is assumed to be less than once in a thousand years). The analyses are based on Toshiba's analysis methods, which have previously been used in the licensing of plants of corresponding type in Japan. The analysis results show that in Finland the doses are below the dose limits defined for level 2 accidents.

Based on the analysis results and the design features of the plant concept, it can be assessed that analyses consistent with Finnish requirements can be performed on this plant alternative during later phases of the licensing process and that the doses will, also in other transient and accident conditions, remain below the dose limits defined in Finnish requirements.

Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008 Section 13)

Reactor and fuel

The ABWR boiling water plant is equipped with recirculation pumps inside the reactor pressure vessel. The operating parameters and the safety characteristics of the plant correspond to existing large boiling water reactors. The total number of recirculation pumps is 10. The number of fuel assemblies is 872 and the number of control rods 205. According to plans, the fuel types used in the existing boiling water reactors or fuel types further developed from these types will be used at the ABWR plant. Reactivity control during the operating cycle is implemented by means of the recirculation pumps, the solid burnable absorbers included in the fuel and the control rods.

The stability of the reactor is ensured using the same methods as in the existing boiling water reactors, i.e. partial scram, the design of the core and the fuel, and protection functions. Stability management will be assessed in more detail at later stages of the licensing procedure. No operating events related to reactor stability problems have taken place at the ABWR plants in operation in Japan.

The designed fuel discharge burn-up is higher than the maximum fuel assembly burn-up of 45 MWd/kgU approved in Finland. 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, the applicant must provide experimental proof of the consistency of the fuel with the Finnish design criteria pertaining to accident conditions.

N.B. This is unofficial translation.
The implementation solutions of the reactor and the fuel meet Finnish requirements. Certain details, such as reactor stability and maximum fuel burn-up, will require further analyses at later stages of the licensing procedure and possibly also experiments.

Main nuclear components

The main nuclear components of the primary circuit of the ABWR plant are based on solutions proven in terms of materials and manufacturing technology. The material of the reactor pressure vessel is low-alloy steel, which is used in the forgings welded together with certified methods to produce the pressure vessel. The interior of the vessel is clad with stainless steel welded on to the surface. Nickel alloys with good durability properties are also used in the corrosion protection of the main components.

The requirements for the materials and weld properties used in the reactor take into consideration the rated service life. Radiation embrittlement of the reactor core area has been taken into account in the material choices and will be monitored by means of a programme based on normal practice. Proven material choices are used in components associated with the reactor, such as recirculation pumps, control rod drive mechanisms, pipe nozzles and reactor internals, in order to mitigate the detrimental effects of stress corrosion, thermal fatigue, and ageing phenomena occurring during operation. The material choices of the main components also take into account the maximum amount of alloying elements increasing the primary circuit’s activity. By controlling flow and environmental factors, erosion corrosion of the main steam and feedwater lines is accounted for.

Breaks in pipes associated with the primary circuit have been taken into account in the design of the primary circuit. The dynamic effects (pressure shocks) of these breaks on other components and structures are analysed using methods approved by Finnish safety requirements. Provisions for a break in the pipe with the largest diameter in the primary circuit are made in the design of the safety systems. The main steam tunnel running above the main control room is provided with adequate protections.

The design objectives and principles presented for the main nuclear components are consistent with Finnish safety requirements.

Reactor pressure control

Reactor pressure control at the ABWR plant is implemented by 18 safety/relief valves. The valves required to restrict pressure are opened by a pneumatic pilot valve controlled by the reactor protection automation or directly on the basis of reactor pressure against a spring load.

A total of 8 of the 18 valves are reserved for depressurisation. They open on a low water level in the reactor pressure vessel. Only two valves are needed for rapid pressure
reduction in the reactor. In order to improve reliability, the pneumatically-controlled safety/relief valves are equipped with their own nitrogen tank.

The isolation condensers (IC, 4 x 33%) can be used for pressure control in transient and accident conditions. The isolation condensers are connected to the steam and feedwater pipes, and when the system starts up, the steam running from the reactor to the steam pipes is conducted into the heat exchanger and condensed into water, which then flows through the feedwater lines back to the reactor. Two parallel valves operating according to different principles are provided between the isolation condenser and the feedwater lines. Opening one of the valves is enough to activate the isolation condenser. The operation of the isolation condenser in transient conditions is designed so that only a short blow-down (just once) of the safety/relief valves is needed in a dimensioning pressure transient. This restricts the blow-down of coolant from the primary circuit into the suppression pool, i.e. maintaining the water level in the reactor is easy in transient and accident conditions.

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

Containment

The containment represents, by its basic type, conventional pressure suppression containment typical of boiling water plants. The containment is constructed of reinforced concrete and contains a suppression pool. During power operation, a nitrogen atmosphere is present in the containment. In loss-of-coolant accidents, the steam discharged from the reactor circuit into the containment 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 systems. The containment has been designed to retain its integrity in compliance with the approval criteria in transient and accident conditions.

Severe accidents

The management of severe reactor accidents at the ABWR plant is based on reducing pressure in the primary circuit before the reactor pressure vessel bursts, cooling the core melt in the core catcher underneath the reactor pressure vessel and controlling pressure in the containment by means of the passive residual heat removal system.

There are eight pneumatically-controlled and four motorised valves available for the depressurisation in the primary circuit. The power to open the valves is supplied from the severe accident power supply system, which is equipped with a battery backup. The depressurisation system prevents high-pressure melt discharge, which might otherwise take place when the reactor pressure vessel bursts and thus damage the containment.

N.B. This is unofficial translation.
During operation, the gas space of the containment is filled with nitrogen; thus the hydrogen generated in severe accident conditions cannot cause a hydrogen fire in accidents starting during power operation. A considerable amount of hydrogen is generated, if all the zirconium used in the fuel cladding and the fuel channels of boiling water reactors becomes oxidised during a severe accident. Shutdown conditions are reviewed in the section on shutdown safety. The hydrogen generated in the reaction pressurises the containment. Therefore, the design of the primary containment building of the ABWR plant takes into account hydrogen generation in a situation where all the zirconium in the reactor becomes oxidised.

In a severe accident, residual heat is removed from the ABWR containment using a passive containment cooling system (PCCS). The system operates without an external power source. The PCCS consists of four natural circulation condensers, which transfer heat directly along pipelines running in the air space of the containment into the reactor building’s water pools located above the primary containment. There are two water pools in the reactor building, each equipped with two PCCS natural circulation condensers. The condensers are in the pools that consist of two basins, which guarantees that the pools cannot be completely drained in the event of a leak. The volume of water in the pools is adequate for the removal of residual heat for 24 hours without refilling. The pools are filled from a storage tank located outside the containment. The operation of the PCCS has been experimentally verified in a large-scale test assembly.

A core catcher is installed under the reactor pressure vessel for cooling and solidifying the core melt. The core catcher operates without an external power source. The discharge of core melt into the catcher opens flooding valves through which water from the suppression pool flows into the channels running underneath the catcher and later onto the melt pool. The steam generated in the core catcher is condensed in the PCCS, and from there the water flows back to the catcher.

The functionality of the core catcher will be experimentally validated. In the design phase, the plant supplier has assessed the flow rate and temperature distribution of the core melt in the catcher as well as the natural circulation conditions in the cooling channels of the core catcher for the determination of the thermal loads on the catcher structures. The plant supplier has drawn up a test programme for heat transfer tests. The tests have been started in a small-scale test assembly to study local heat transfer from the core melt into the cooling channels as well as the void fraction in the water pool above the core melt. The plant supplier has produced a full-scale test assembly in the first half of 2009. The test assembly models one flow channel of the core catcher in such a way that the elevation differences between the core catcher and the feedwater pool are uniform with the designed equipment. The full-scale tests ensure functionality of the core catcher in conditions that are as close as possible to the equipment’s designed use.

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

N.B. This is unofficial translation.
The design objectives and principles of the ABWR plant’s containment as well as the systems designed for severe accident management are consistent with Finnish requirements. The functionality of the core catcher is still subject to verification experimentally. The plant supplier is currently running a test programme to study this.

Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14)

At the ABWR plant both active and passive systems are used for the implementation of safety functions. The safety functions associated with reactor core shutdown and removal of residual heat are implemented using both an active and a passive system. The supply of make-up water to the reactor in transient and accident conditions is implemented by emergency cooling systems based solely on active components.

Reactivity management

As with the existing boiling water reactors, reactor power level is controlled in normal conditions with control rods and recirculation pumps.

Reactor shutdown in transient and accident conditions is achieved with the hydraulic scram system. The system is passive and its operation is based on water tanks pressurised with nitrogen. When the scram valve opens, the pressure contained in the tanks inserts the control rods into the reactor core. Each pressurised water tank controls two control rods. There are a total of 120 scram units, each consisting of a nitrogen tank, a scram valve and a water tank as well as the required piping. The system fulfils the redundancy principle called for in the Government Decree.

The scram system is backed up by a standby liquid control system (SLCS, 2 x 100%) based on a pressurised borated water tank, which feeds borated water directly into the reactor core. The system fulfils the diversity principle with respect to reactivity management called for in the Government Decree.

Reactor protection automation initiates the passive scram system if process parameters exceed the protection limit. Reactor scram is ensured by the ARI system (Alternate Rod Insertion), which fulfils the diversity principle with respect to automation. The system is implemented using hardwired technology. The ARI system controls the same scram valves and pressure accumulators as normal protection automation. Reactor shutdown is further ensured by the possibility to insert the control rods into the reactor core with an electric motor, in case the hydraulic system has failed to do so.

Reactor power can be decreased by reducing the reactor coolant flow rate. This is achieved by completely stopping four or six out of the ten recirculation pumps, depending on the initiating event.
The design objectives and principles associated with reactivity management are consistent with Finnish safety requirements.

Cooling of reactor

Cooling of react in shutdown conditions

During normal shutdown conditions, 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 associated with the cooling of a shut down reactor, which implements the removal of residual heat during shutdowns. The same system is also used to supply make-up water to the reactor. Residual heat is removed from the RHR system via the reactor building cooling water system (RCW, 3 x 100%) and the reactor service water system (RSW, 3 x 100%) into 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 diversity principle is fulfilled by the reactor water cleanup system (CUW, 2 x 100%), by means of which residual heat can be removed with two non-regenerative heat exchangers (NRHX, 2 x 100%) into the ultimate heat sink.

Cooling of reactor in accident conditions with reactor primary circuit intact

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

Residual heat is removed from the reactor by conducting steam through the relief valves of the primary circuit into the containment suppression pool. Residual heat is removed from the pool primarily by means of the residual heat removal system (RHR, 3 x 100%), which uses the same pumps as the low-pressure core flood system. The residual heat is then transferred via the reactor building cooling water system (RCW, 3 x 100%) and the reactor service water system (RSW, 3 x 100%) into the ultimate heat sink.

With respect to reactor cooling, the diversity principle is fulfilled by a passive system based on natural recirculation; the system consists of four isolation condensers (IC, 4 x 33%). The isolation condensers are connected to the steam and feedwater lines; when the system starts up, the steam running from the reactor to the steam lines is drained into the heat exchanger and condensed into water. The water is then conducted along the feedwater lines back into the reactor. Two parallel valves operating with different principles are provided between the isolation condenser and the feedwater lines. The opening of one of the valves is enough to activate the isolation condenser. The isolation condensers are located in two water pools in the reactor building, and each pool has

N.B. This is unofficial translation.
Original:
two isolation condensers. The pools consist of two basins to prevent them from being completely drained. Residual heat is removed from the reactor building pools into the atmosphere. The isolation condensers make it possible to maintain the plant in a controlled state. The volume of water in the pools is adequate for the removal of residual heat for 24 hours without refilling. The pools can be refilled from a storage tank located outside the containment and can continue the removal of residual heat for as long as is necessary, and, in any case, for at least 72 hours.

With respect to the residual heat removal system, the diversity principle can also be fulfilled using the passive containment cooling system (PCCS). The steam generated in the reactor can be drained through the relief valves of the primary system into the containment suppression pool and the residual heat can be further transferred through the PCCS into the atmosphere.

Alternatively, the supply of make-up water into the reactor has been realised in such a way that the high-pressure core flooder system (HPCF) is replaced with a low-pressure core flooder (LPCF) system if necessary. This is done by reducing reactor pressure with the automatic depressurization system to a level at which the low-pressure safety injection pumps can operate. Cooling water is supplied to the HPCF system from a separate make-up water tank and to the LPCF system through suction strainers installed in the suppression pool inside the containment. In order to further improve the fulfilment of the diversity principle of the emergency cooling systems, Toshiba is investigating the possibility to supply water from the flushing system of the hydraulic scram system to the reactor pressure vessel.

**Cooling of reactor in loss of coolant accidents**

In loss of coolant accidents, the reactor is cooled using the high-pressure core flooder system (HPCF, 3 x 100%) and the low-pressure core flooder system (LPCF, 3 x 100%) as well as the automatic depressurization system, which utilises safety/relief valves.

Cooling water is supplied to the HPCF system from a separate make-up water tank and to the LPCF system through suction strainers installed in the suppression pool inside the containment. The suction strainers prevent impurities from entering the reactor.

In order to ensure reliable operation of the low-pressure core flooder system and reactor cooling in loss of coolant accidents, it is important that the suction strainer of the pumps in the suppression pool are not clogged as a result of impurities entering the pool during the accident. Toshiba has developed the suction strainers and has experimentally verified the operation of the strainers in conditions simulating accident conditions. The anti-clogging properties of the strainers are based on the large surface area of the strainer. In addition, the strainers are equipped with a flushing system for use if they become clogged. It may become necessary at later stages of the licensing procedure to perform some analyses or tests to verify the functionality of the suction strainers.

N.B. This is unofficial translation. Original:
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 the situation in which the primary circuit is intact.

The diversity principle with respect to the removal of residual heat is fulfilled by the passive containment cooling system, which is ready for operation and starts up without the need for any active component to function. Residual heat is removed from the containment by means of natural circulation condensers (PCCS, 4 x 33%), which transfer the heat directly into the reactor building’s water pools located above the primary containment along pipelines running in the air space of the containment. The natural circulation condensers of the passive containment cooling system (PCCS) are located in two water pools in the reactor building, and each pool has two PCCS condensers. The pools consist of two basins to prevent them from being completely drained. Residual heat is removed from the reactor building pools into the atmosphere. The volume of water in the pools is adequate for the removal of residual heat without refilling for 24 hours. The pools can be refilled from a storage tank located outside the containment and can continue the removal of residual heat for at least 72 hours.

The design objectives and principles of the systems required for the cooling of the reactor core and for the removal of residual heat are consistent with Finnish safety requirements. The details associated with the emergency core cooling systems, such as experimental demonstration of the reliable operation of the suction strainers in the low-pressure core flooder system, require further tests. Further design is also needed to implement the diversity principle in emergency core cooling.

Containment isolation

At the ABWR plant, containment isolation has been, as a rule, implemented in the pipelines penetrating the containment by means of two isolation valves. Exceptions are the suction lines of the pumps of the low-pressure core flooder system, which are provided with one isolation valve outside the containment. No common cause failure analysis has been performed on similar types of isolation valves, so fulfilment of the diversity principle called for in the Government Decree has not been demonstrated.

Principles of redundancy and diversity with respect to containment isolation can be fulfilled through valve choices at later stages of the project.

Loss of ultimate heat sink

If the normal opportunity to remove heat into seawater, acting as the ultimate heat sink, is lost, residual heat can be removed from the reactor with isolation condensers (IC)
into the reactor building’s water pools located above the primary containment. From these water pools, heat is removed through the ventilation stack into the atmosphere. This system makes it possible to bring the reactor into a controlled (hot shutdown) state and to maintain it in this state. The volume of water in the pools is adequate for the removal of residual heat for 24 hours without refilling. The pools can be easily refilled from a storage tank located outside the containment and the removal of residual heat can be continued for as long as is necessary, and at least for 72 hours. The system fulfils the diversity principle called for in the Government Decree.

The residual heat removal systems required for the loss of ultimate heat sink in shutdown situations are not described in the documentation. This matter can be reviewed when the application for the construction licence is submitted.

The design objectives and principles of the systems associated with the management of loss of ultimate heat sink are consistent with Finnish safety requirements.

*Cooling of fuel pools*

At the ABWR plant, the cooling of fuel pools, the control of pool water levels, the purification of the water and the management of radioactive materials in normal operating conditions is implemented with the fuel pool cooling and clean-up system (FPC, 2 x 100%). If necessary, the pools can be refilled from the condensate storage tank. In transient and accident conditions, residual heat removal and the control of pool water levels is achieved with the residual heat removal system (RHR, 3x100%), which pumps water from the suppression pool in the containment through the FPC system into the fuel pool. Additionally, make-up water to the pools can be pumped using the fire protection system (FPS) and the suppression pool clean-up system (SPCU).

The design objectives and principles of the systems involved in the cooling of the fuel pools are consistent with Finnish safety requirements.

*Shutdown safety*

The subcriticality of the reactor is secured in all shutdown situations by keeping the control rods inserted in the reactor.

Shutdown maintenance works, particularly recirculation pump service, has been planned to incorporate multiple layers of protection to prevent cooling water from leaking onto the floor in the containment. The lower access doors of the containment are protected against leaks with double doors, one of which is always closed. This prevents water from the reloading pool and the reactor from leaking to the outside of the containment through these access doors.

In case a major coolant leak occurs during a refuelling outage, the cooling of the reactor is ensured with the pumps of the residual heat removal system (RHR, 3 x
100%) and the high-pressure core flooder system (HPCF, 3 x 100%). As the water level falls, the pumps start up and fill the lower drywell in the containment as well as the reactor up to above the top edge of the core. The RHR pump and HPCF pump of one subsystem are needed to retain the water level above the core. Cooling water is supplied to the RHR pump from the suppression pool and to the HPCF pump from a tank located outside the containment.

The design objectives and principles of the systems associated with shutdown safety are consistent with Finnish safety requirements.

**Electrical systems**

The supply of off-site power is at the ABWR plant implemented through auxiliary transformers and a main transformer from the 400 kV grid or through two standby auxiliary transformers from the 110 kV grid. If necessary, power can be supplied from the standby auxiliary transformers directly to the switchgears of the safety systems bypassing switchgears with no nuclear safety classification (EYT systems).

In case off-site power supplies fail, power to the safety systems of the plant is supplied alternatively from

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

According to the description of the electrical systems, the severe accident management systems do not have their own on-site power supply systems.

The separation principles applied to the electrical systems have not been clearly described in the application documentation. This matter can be reviewed when the application for the construction licence is submitted.

The general lessons learned from the design errors leading to the malfunction of the electric system of Forsmark nuclear power plant in 2006, shall be taken into account. In the design of the electrical systems and components, special attention shall be paid to e.g. restraining voltage transients from spreading and the implementation of the diversity principle in the electricity distribution and in supplying power to I&C systems. Full analysis shall be made to find out the most severe possible voltage transients and malfunctions of the in-house grid. Power consumers and systems are to

N.B. This is an unofficial translation.

Original:
be designed to withstand these transients and malfunctions. The matter shall be reviewed in a more detailed manner at the construction licensing stage.

The design objectives and principles of the electrical systems are, for the most part, consistent with the Finnish safety requirements. A separate power supply system for the severe accident management system and the lessons learned from the Forsmark incidence must be further assessed when the application for the construction license is submitted.

Civil engineering and fire protection

The design basis for the buildings and building engineering systems at the ABWR plant are consistent with the Japanese plants used as references. The environmental conditions of the Japanese plants are in most cases assessed to be more demanding than conditions in Finland. The expertise required for the design of boiling water plants for the northern regions is also available to the plant supplier. This ensures that the current design basis provide an adequate basis regarding the Finnish winter conditions in the detailed design of buildings and building engineering systems.

The design objectives and principles associated with resistance to vibrations induced by earthquakes and external hazards are consistent with the Finnish safety requirements. Detailed design includes an assessment of the vibration resistance of the plant components. The analysis is based on the verification of the vibration resistance of the buildings as well as on the verification of the proper vibration characteristics of the frame structures and the component anchorage.

The design objectives and principles associated with the fire protection concept of the ABWR plant are consistent with Finnish safety requirements. The extinguishing systems of the plant are designed to be earthquake resistant, which secures control over fires caused by earthquakes.

Protection against external events (Gov. Decree 733/2008 Section 17)

The protection strategy of the ABWR plant against the impact of a large commercial airplane crash is to retain the coolability of the reactor core, the integrity of the containment, the coolability of spent fuel and the integrity of fuel pools. The buildings protected against aircraft crashes are the reactor building, the control room building and the pump station buildings of the residual heat removal systems. The protection measures in use at the ABWR buildings are strengthened reinforced concrete structures, physical separation of parallel systems critical to safety, the physical protection provided by other structures and the location of components in the underground facilities of the buildings.

N.B. This is unofficial translation. Original: http://www.stuk.fi/ydinturvallisuus/ydinvoimalaitokset/suomen_ydinvoimalaitokset/fi_FI/uidet_laitosyksikot/_files/82229809792876564/default/Alustava%20turvallisuusarvio_PAP-Forurn3_liite1_laitosvaihtoehdot.pdf
Protection against external floods is given by external wall structures, which withstand the pressure of groundwater. Penetrations below the flood limit are equipped with flood shields, and tunnel penetrations are built watertight.

The presented design objectives and principles are consistent with Finnish safety requirements.

Protection against internal events (Gov. Decree 733/2008 Section 18)

Internal hazards such as floods and fires are taken into account in the room and layout planning of the ABWR plant by locating the key safety systems in three different room areas. The room areas are physically separated by reinforced concrete walls, for which a rated fire resistance of two hours is indicated. The room areas on the bottom floor of the reactor building, which contain the pumps of the reactor service water system (RSW), are completely separated from each other with walls, which prevent the propagation of internal floods. The separation principle of the subsystems is also applied in the control room building. Doors between the room areas for operating and maintenance purposes have been designed for the upper floors of the reactor building.

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

The design basis of the ABWR plant is to run the main steam and feedwater pipes from the containment to the turbine building along undivided channels through the control room building. Feasibility analyses have included a study of the effects of breaks in these high-energy pipelines on plant safety. According to the designs, the pipe channel will be divided into two tunnel sections at the plant. One of the tunnels would constitute 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 occurring in the compartment inside the reactor building has been analysed. The structure 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. However, more analyses are required on this matter.

The compact layout of the plant results in requirements for protection against internal events, such as floods and fires. The consequences of major internal floods, for example flooding of the reactor service water system (RSW) in one room area of the reactor building, must be analysed at later stages of the licensing procedure. The analyses must prove that the effects of the events are limited within the room area in question.

N.B. This is unofficial translation.
The presented design objectives and principles are consistent with Finnish safety requirements.

Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19)

It should be noted that in the documentation of the application for a decision-in-principle, the safety principles of the I&C systems have been presented at a rather general level. Before the specification of the design and the design materials has reached the level of actual technical design, it is more a matter of the objectives of several safety principles, the fulfilment of which cannot be assessed based on the documentation of the decision-in-principle. On the basis of the material submitted for the decision-in-principle, it is impossible to fully assess whether or not these goals have been achieved. The genuine fulfilment of the safety principles in the plant’s technical solutions must be ensured also at the later stages of the project. Of these phases, the construction license process is the first regulatory phase of the plant project that deals with solid technical I&C solutions.

Automatic safety functions

ABWR plant automation includes several different lines of defence based on the defence-in-depth principle. The first line comprises normal process automation, control systems and limitation systems. The second line consists of 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 diversity principle, and the last line comprises the severe accident management system.

The automation systems of the different lines of defence aim to automatically maintain the plant parameters within a safe range during operating transients and to limit the consequences of accident conditions.

The design objectives and principles of automation systems are consistent with Finnish safety requirements.

I&C redundancy principle

The reactor protection system and the engineered safety features actuation system comprise of four parallel subsystems. The protection function is actuated if a protection signal is received from two of the four parallel protection channels. The systems meet the requirements set forth in the Government Decree for the redundancy principle.

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

N.B. This is unofficial translation.
Original:
The most important control systems included in process automation, such as the feedwater control system, the control system of the recirculation pumps, the control system of turbine bypass, the steam pressure control system and the reactor power control system are implemented with three parallel subsystems.

The design objectives and principles of the automation systems are consistent with Finnish safety requirements. Redundancy principles have not been presented for the diverse actuation system DAS. This matter can be reviewed when the application for the construction licence is submitted.

**I&C separation principle**

The subsystems of the automation systems have been physically and functionally separated from each other.

The separation of the I&C systems of different safety classes is based on the physical and functional separation of safety class-2 systems from other systems and equipment. Safety class-3 systems are functionally separated from lower safety class systems and equipment.

The separation of the severe accident management I&C and surveillance system from other I&C systems has not been presented. This matter can be reviewed when the application for the construction licence is submitted.

The design objectives and principles of the automation systems are consistent with Finnish safety requirements with respect to the separation principle. The separation of the severe accident I&C from other I&C systems has not been presented. This matter can be reviewed when the application for the construction licence is submitted.

**I&C diversity principle**

The diversity principle has been applied to the reactor protection system so that signals indicating accident and transient conditions come alternatively from two different process parameters. The design objectives and principles of the system are consistent with Finnish safety requirements.

At this design stage it is not clear which computer-based system platforms will be used in the different I&C systems. This matter can be reviewed when the application for the construction licence is submitted.

The ABWR plant concept incorporates the diverse actuation system (DAS), which is designed against common cause failures in the computer-based protection system. The DAS can control reactivity management, over-pressurisation protection, emergency core cooling, residual heat removal from the reactor and the containment, containment

N.B. This is unofficial translation.
Original:
isolation and emergency power sources. The DAS consists of two parts: one designed to back up the reactor protection system and the other the engineered safety features actuation system. The reactor protection backup part of the DAS is based on hardwired technology, while the engineered safety features actuation system backup part is based on programmable I&C. The DAS has its own sensors for the measurement 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 I&C system.

The design objectives and principles of the system are for the most part consistent with Finnish safety requirements. Clarification of how the plant is to be brought into a safe state and kept there in the case of common cause failure of the programmable I&C must be presented when the construction licence is applied for.

Control room

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

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

The display panel comprises fixed indicators and switches as well as a wide-screen display screen. The display panel is designed to present in one assembly the status of the plant and the most important components as well as the most important alarm data. The display panel also features control functions for less frequently used functions, such as in-service tests.

The shift supervisor's console can be used to monitor the plant parameters and status, but no control actions can be executed from this console.

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

Emergency control room

The plant features an emergency control room, which can be used for the control of safety-critical systems independently of the main control room. The plant can be brought into a controlled (hot shutdown) state and further into a safe (cold shutdown) state from the emergency control room.

N.B. This is unofficial translation.
Original:
The emergency control room is located in a different fire compartment and building from the main control room. The design objectives and principles of the emergency control room are, for the most part, consistent with Finnish safety requirements. The control and surveillance possibility of fuel pool cooling has not been described in the documentation. This matter can be reviewed when the application for the construction licence is submitted.

Reactor pressure vessel level measurement

Reactor pressure vessel level measurement is based on normal differential pressure measurement, which controls the reactor protection automation. There are four measurements, and the system is actuated on receiving an opening command from two channels. The system fulfils the redundancy principle. The diversity principle is realised by two floats located in the reactor water cleanup system.

Summary

The design objectives and principles of the plant alternative are, for the most part, consistent with Finnish safety requirements. Some technical details require further analyses and qualification based on tests as well as further engineering. These can be carried out at later stages of the licensing procedure. In STUK's opinion, none of these details can be foreseen to be an obstacle to the fulfilment of the requirements set forth in the Government Decree (733/2008). These technical details include

- experimental verification of the operation of the suction strainers of the low-pressure core flooder system
- implementation of the diversity principle for the containment isolation function with respect to all pipelines
- experimental demonstration of the functionality of the core catcher required for severe accident management
- residual heat removal system realising the diversity principle in shutdown conditions
- taking into account the general lessons from the Forsmark incidence in the electrical system design
- Separation of the severe accident management I&C and surveillance systems from other automation systems
- separate power supply system for the severe accident management system
- bringing the plant into a safe state (cold shutdown) in case the computer-based automation system is lost.

N.B. This is unofficial translation.
Original:
ESBWR - Economical and Simplified Boiling Water Reactor, GE-Hitachi

General

ESBWR is a ca. 1600 MWe boiling water reactor designed by General Electric/Hitachi (GEH). GE has gained extensive experience in the design of boiling water reactors since the 1960s. All the boiling water reactors constructed in United States as well as several plants all over the world, e.g. the oldest boiling water reactors in Japan and all the boiling water reactors in Spain and Switzerland, have been designed by GE. Hitachi has designed several boiling water reactors in operation in Japan. GE and Hitachi have founded GEH as a company that combines the expertise of the two companies.

The ESBWR plant is based on boiling water reactors previously designed and constructed by GE, and the objective of the design has been to simplify construction and to minimise the number of components requiring service and maintenance. No ESBWR plants have so far reached construction stage.

In the feasibility study for Finland, GEH has developed the plant concept used as a starting point by adding certain safety features required by Finnish safety requirements. The rated service life of the plant is 60 years. The level of maturity of the plant with respect to design is lower than the level of the other plant alternatives. The design objectives and principles are, for the most part, consistent with Finnish safety requirements.

The safety of the ESBWR plant is in many respects based on new types of inherent features and passive safety systems designed to replace active systems. However, thorough experimental and computational qualification of the presented new solutions is required.

Assessment and verification of safety (Gov. Decree 733/2008 Section 3)

Deterministic analysis methods and preliminary results

For the assessment and verification of safety analysis, GEH uses methods developed by the company over the decades. The analysis methods have been maintained and qualified for the intended purpose of use. The transient and accident analyses performed on the ESBWR plant gives the impression that transient and accident analyses consistent with Finnish requirements can be performed on this plant alternative.

Probabilistic analyses

N.B. This is unofficial translation.
GEH uses level 1 and 2 Probabilistic Risk Analysis (PRA) methods, which have been applied in the PRA analyses of the GE plants in operation in the USA. PRA methods have been used also right from the beginning of the designing of the ESBWR plant. The analyses encompass events associated with external and internal hazards in all operational states of the plant. Based on information on analysis methods and the results from ESBWR analyses, it can be assessed that analyses consistent with Finnish PRA requirements can be performed on this plant alternative. If necessary, the methods can be developed on the basis of detailed Finnish requirements. Probabilistic risk analyses are made in conjunction with the plant’s detailed design phase, at which time compliance with Finnish safety requirements will be assessed.

Qualification of new type of systems

The ESBWR plant concept includes several new passive safety systems, which have previously not been used at nuclear power plants. These new systems include an isolation condenser (IC) for direct cooling of the reactor circuit, a Passive Containment Cooling System (PCCS) for removal of residual heat, a passive Gravity Driven Core cooling System (GDCS) as well as depressurization valves.

The operation of the systems has been appropriately qualified by means of test assemblies. Although the test program has been quite comprehensive, further tests may be needed on some details at later stages of the licensing procedure.

Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008 Sections 7–10)

The plant supplier has, as part of the ESBWR engineering process, performed a computation of the radiation exposure of the population in the areas surrounding the plant in accident situations. The computations have been performed for a standard ESBWR plant. Based on these computations, the doses will remain clearly below the dose limits defined for accidents in Finnish requirements.

Based on the analyses performed on the standard ESBWR plant regarding radiation exposure and radioactive releases and based on the design characteristics of the plant concept, it can be assessed that an analysis fulfilling Finnish requirements can be made for the plant at later stages of the licensing procedure.

Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008 Section 13)

Reactor and fuel

N.B. This is unofficial translation.
The ESBWR plant design of the reactor and the associated cooling circuit relies on natural circulation and there are no recirculation pumps at the plant. Reactor power is in normal conditions controlled by means of the feedwater temperature and the control rods. The number of fuel assemblies in the core is 1132 and the number of control rods is 269. For the ESBWR plant, the intention is to use fuel assemblies that are identical in type but ca. one meter shorter than the fuel types used in existing boiling water reactors. Reactivity control during the operating cycle is implemented by means of feedwater temperature, the solid burnable absorbers included in the fuel and the control rods.

The height of the reactor core is clearly lower than the height of the existing reactors of similar size, and it is located inside the reactor pressure vessel at a level lower than in the existing boiling water plants. The power density of the reactor core is slightly lower than in the existing large boiling water reactors. These features improve inherent safety in comparison with the existing plants in terms of the thermal margins. In addition, the location of the core is advantageous with respect to transients and accidents. Owing to the large volume of the reactor pressure vessel, also transients in pressure control develop clearly slower than in the existing boiling water reactors. These transients can be managed with the isolation condenser (IC) so that safety or relief valves do not need to open during the worst possible pressure transient.

In reactors relying solely on natural circulation (reactor with no recirculation pumps), reactor stability is an essential factor in terms of safety. Existing boiling water reactors are able to operate on natural circulation to a power level of up to 50%, but have occasionally displayed stability problems. To ensure ESBWR reactor stability, a structure (chimney) above the reactor top has been designed to enhance the natural circulation of the reactor primary circuit. Some smaller boiling water reactors, based on the same principle, have been in operation and have showed good stability properties. The stability of ESBWR has been proven by theoretical calculations. The calculation method used has been qualified with operating experience for the natural circulation reactors mentioned above and with stability events from boiling water reactors in operation as well as by some stability tests in research facilities. These analyses show an adequate margin to power oscillations. However, the complex phenomena associated with reactor stability cannot be directly scaled according to reactor size. In these respects, further analyses are required for the plant alternative to prove reactor stability in all operating conditions.

The designed fuel discharge burn-up is higher than the maximum fuel assembly burn-up of 45 MWd/kgU approved in Finland. 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, the applicant must provide experimental proof of the consistency of the fuel with the Finnish design criteria pertaining to accident conditions.

The design objectives and principles of the reactor and fuel are consistent with Finnish safety requirements. Reactor stability requires further analysis and possibly also experiments in order to demonstrate that the Finnish requirement level is met.

N.B. This is unofficial translation.
Original:
Main nuclear components

The reactor pressure vessel of the ESBWR plant is built of low-alloy steel forgings, which are welded using proven methods typical in pressure equipment manufacture to produce the vessel. Tight ductility requirements based on the designed service life have been specified for the pressure equipment steel grades used in the main components.

The reactor core area consists of ring forgings assembled in a cylinder form using rotationally symmetrical welds. Longitudinal welded joints are also used in the top part of the large reactor pressure vessel (inner diameter 7.1 m, height 27.6 m). The inside of the reactor is clad with stainless steel welded onto the reactor surface. The structure (chimney), mounted above the core to enhance natural circulation as well as the other reactor internals are made of stainless steel.

The resistance of the main components and their welded joints due to the ageing problems encountered during operation, such as radiation embrittlement, thermal ageing, fatigue and various stress corrosion phenomena has been taken into account in the design and the material choices. The reactor core area’s embrittlement caused by radiation is monitored with a monitoring program that is compliant with normal requirements and monitored with associated fracture analyses. The material choices of the main components also take into account the maximum amount of alloying elements increasing the primary circuit’s activity. Wear caused by erosion corrosion of the main steam and feedwater lines is accounted for by controlling flow and environmental factors.

Breaks in the primary circuit and in pipes connected to the primary circuit have been taken into account in the design of the primary circuit and the associated safety systems. The design of the safety system takes into account a break of the pipe with the biggest diameter in the primary circuit. The dynamic effects (pressure shocks) of breaks assumed in different points on other components and structures are analysed using procedures approved by Finnish safety requirements.

The design objectives and principles of the main nuclear components are consistent with Finnish safety requirements.

Reactor pressure control

Reactor pressure control at the ESBWR plant is implemented by 18 safety/relief valves. The valves required to restrict pressure are opened by a pneumatic pilot valve controlled by the reactor protection automation or directly on the basis of reactor pressure against a spring load.

A total of 10 of the 18 valves are used for automatic depressurisation. They open on a low water level in the reactor pressure vessel. These ten valves feature both of the
aforementioned opening mechanisms. The other eight valves only feature the spring loaded opening.

The isolation condensers (IC, 4 x 33%) can be used for regulation of pressure in transient and accident conditions. The isolation condensers are connected to the steam and feedwater lines and when the system starts up, the steam running from the reactor to the steam lines is drained into the heat exchanger where the steam is condensed into water. The water is then led along the feedwater lines back to the reactor. Two parallel valves operating according to different principles are provided between the isolation condenser and the feedwater line. The opening of one of the valves is enough to activate the isolation condenser. The operation of the isolation condenser in transient conditions is designed so that the safety valves are not required to open in the dimensioning pressure transient. This restricts the blow-down of coolant from the primary circuit into the suppression pool, i.e. the water level in the reactor can be easily maintained in transient and accident conditions. The systems fulfil the principles of redundancy and diversity required by the Government Decree.

**Containment**

The ESBWR plant’s containment represents by its basic type conventional pressure suppression containment typical of boiling water plants. The containment is constructed of reinforced concrete and contains suppression pools. During power operation, a nitrogen atmosphere is present in the containment. In design-basis accidents (pipe breaks), the steam discharged from the reactor circuit into the containment is forced by the differential pressure into the suppression pool. The residual heat is removed from the suppression pool into the final heat sink by means of residual heat removal systems. The containment has been designed to retain its integrity in compliance with the approval criteria in transient and accident conditions.

**Severe accidents**

At the ESBWR plant, the management of severe reactor accidents is based on reducing pressure in the primary circuit before the reactor pressure vessel bursts, cooling the core melt in the core catcher underneath the reactor pressure vessel and regulating pressure in the containment by means of the passive residual heat removal system.

There are eight depressurization valves (DPV) available for the depressurisation of the primary circuit. The DPV valves are squib valves in type. The opening signal comes from a system that is equipped with battery backup, but is not reserved exclusively for severe accidents as prescribed in the Finnish requirements. The reduction of primary system pressure prevents high-pressure melt discharge, which might otherwise take place when the reactor pressure vessel bursts and could damage the containment.

During power operation, the gas space of the containment is filled with nitrogen, which means that the hydrogen generated in severe accident conditions cannot cause a

N.B. This is unofficial translation.
hydrogen burn in accidents starting during power operation. A considerable amount of hydrogen is generated, if all the zirconium used in the fuel cladding and the fuel channels of the reactor becomes oxidised during a severe accident. Shutdown situations are discussed in the Shutdown safety section. The hydrogen generated in the reaction pressurises the containment. In the original ESBWR concept, the containment is dimensioned in compliance with US norms, i.e. only the zirconium contained in the fuel cladding is assumed to become oxidised. According to Finnish requirements, all zirconium present in the core area must be considered as a source of hydrogen. For this reason, the plant supplier is considering adding an extra tank in the reactor building. Hydrogen would be drained into this tank in an accident. The plant supplier designs also to include some other actions to improve the effectiveness of containment pressure control.

In a severe accident, residual heat is removed from the containment using a passive containment cooling system (PCCS). The system operates without an external power source. At the ESBWR plant, the PCCS consists of six heat exchangers, which transfer heat directly along pipelines running in the air space of the containment into water pools located in the reactor building above the primary containment. The system has a high heat transfer capacity, 11 MW/circuit. The cooling capacity of the pool is adequate for at least 72 hours. The pools are filled from the makeup water system. The operation of the PCCS has been experimentally verified in a large-scale test assembly.

A core catcher is installed under the reactor pressure vessel for cooling of the core melt. The discharge of core melt from the pressure vessel initiates the flooding of the core catcher from the water storage pools of the gravity-driven cooling system (GDCS). Two pipelines run from each of the three GDCS pools to the core catcher. The pipes are provided with so-called squib valves, which receive the opening command on high temperature in the lower drywell. The power source of the opening logic is equipped with battery backup. Two batteries completely separated from all the other systems are used, each capable of opening all the required valves. The steam generated in the core catcher is condensed in the passive containment cooling system (PCCS) and the water is drained back to the core catcher. The documentation submitted for a decision-in-principle presents no data on experimental verification of the operability of the core catcher. Experimental verification is an absolute prerequisite for a construction license.

For long-term management of noncondensable gases accumulated in the containment, a venting line is provided from the wet well of the containment to the atmosphere. The original concept does not feature a filter unit in the venting line. According to the plant supplier, a filter unit designed for retention of radioactive materials can be incorporated in the plant to be built in Finland.

The containment at the ESBWR plant and the systems designed for severe accident management require further clarifications and plant modifications to demonstrate their consistency with Finnish requirements for severe accidents. The operability of the core catcher must be verified experimentally.
Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14)

At the ESBWR plant, both active and passive systems are used for the implementation of safety functions. Active systems are primarily designed for normal operation. However, they have been safety-classified. The safety functions associated with management of transients and accidents can be implemented both with the active systems designed for normal operation and exclusively with the passive systems. Active systems are always initiated first in transient and accident situations. If they are unable to limit the consequences of the event, safety is ensured by the passive safety systems.

Reactivity management

At the ESBWR plant, reactor power level is controlled with the control rods and by regulating the feedwater temperature utilising the feedwater preheater.

Reactor shutdown in transient and accident conditions is achieved with the passive scram system. A scram is implemented with control rods, which are inserted into the reactor core by a hydraulic system. Each hydraulic control unit controls two control rods. The total number of similar hydraulic control units, which consist of a high-pressure nitrogen tank, a scram valve and a water tank as well as the required piping, is 134. The system’s design principles fulfil the redundancy principle called for in the Government Decree.

The diversity principle is realised by a standby liquid control system (SLCS, 2 x 50%) that injects borated water directly into the reactor core. The system comprises two subsystems, both of which are required to operate to implement the safety function. The boron system is activated by squib valves, which only operate once by opening the line to the reactor. As a result of this, the nitrogen pressure present in the pressure tanks forces the borated liquid into the reactor. When boron mixes with the cooling water, the reactor shuts down. There are two parallel squib valves in each subsystem and only one of them is required to open to execute the safety function. The level control in the boron tank is also single failure tolerant. Each subsystem features two successive check valves, and the failure of either one can prevent the borated water from one boron tank from entering the reactor. The boron system does not completely fulfil the single failure criterion at present. The plant supplier has presented several alternatives to solve the problem.

Reactor protection automation initiates the passive scram system, if process parameters exceed the protection limit. Reactor scram is secured by the ARI system (Alternate Rod Insertion), which realises the diversity principle with respect to automation. The ARI system controls the same scram valves and high-pressure nitrogen tanks as the normal protection automation. Reactor shutdown is further ensured by a possibility to insert the control rods in the reactor core under control of an electric motor, in case the hydraulic system fails to do it.
The design objectives and principles of the safety functions associated with reactivity management are consistent with Finnish safety requirements. The boron system does not completely fulfil the single failure criterion at present, but the plant supplier has presented several alternatives to solve the problem. This matter can be resolved when the application for the construction license is submitted.

Cooling of reactor

Cooling of reactor in shutdown conditions

The residual heat generated in the reactor at the reactor cooling phase and in cold shutdown state is removed directly from the reactor pressure vessel using the reactor water cleanup/shutdown cooling system (RWCU/SDC, 2 x 100%). This system is used for cooling both when the reactor pressure vessel is closed and when it is open, and it is also used to supply make-up water to the reactor. Alternatively, residual heat can in shutdown conditions be removed with the fuel and auxiliary pool cleanup system (FAPCS, 2 x 100%). In both alternatives, residual heat is further transferred through the reactor component cooling water system (RCCWS) and the plant service water system (PSWS) into the ultimate heat sink. The RCCWS comprises two lines (2x100%), each equipped with three pumps (2x3x33%). The PSWS comprises two lines (2x100%), each equipped with two pumps (2x2x50%).

Cooling of reactor in accident conditions with reactor primary circuit intact

In accident conditions where the reactor primary circuit is intact, the removal of residual heat can be implemented with a passive system based on natural circulation, so-called isolation condenser (IC, 4 x 33%). The isolation condensers are connected to the steam and feedwater pipes and when the system starts up, the steam running from the reactor to the steam pipes is conducted into the isolation condenser where the steam is condensed into water. The water is then conducted along the feedwater pipes back to the reactor. The isolation condensers are located in two pools in the reactor building, and each pool has two isolation condensers. The isolation condenser is activated by a protection signal, which opens at least one of the two parallel valves operating according to different principles. The isolation condenser can be used to maintain the reactor in a controlled (hot shutdown) state. The design principles of the system realise the diversity principle called for in the Government Decree.

The diversity principle is with respect to the removal of residual heat realised by the reactor water cleanup/shutdown cooling system (RWCU/SDC, 2 x 100%). This system is also used to supply make-up water to the reactor. Residual heat can be removed 30 minutes after reactor shutdown using both lines. The safe (cold shutdown) state can only be achieved with the reactor water cleanup/shutdown cooling system, from which residual heat is further transferred through the reactor component cooling water system (RCCWS) and the plant service water system (PSWS, 2 x 100%) into the ultimate heat sink. The RCCWS comprises two lines (2x100%), each equipped with three pumps.
The PSWS comprises two lines (2x100%), each equipped with two pumps (2x2x50%). The control rod drive hydraulic system (CRDHS, 2 x 100%) can be used for cooling of the reactor.

Water supply to the reactor is also secured with the gravity-driven core cooling system (GDCS, 4 x 50%). The system has four subsystems that are placed in three pools. One pool is provided with two drain lines into the reactor and two pools with one drain line each. The squib valves mounted in each line needs to open to activate the system. The opening of one of the two parallel valves is enough. Reactor pressure is reduced by means of the automatic depressurising system (ADS). The water volume of the GDCS is adequate to fill the containment to a level ca. 1 m above the top level of the reactor core. This means that water would no longer flow out of the reactor pressure vessel through the relief valves.

The diversity principle can with respect to the residual heat removal system also be implemented using the passive containment cooling system (PCCS, 6 x 25%). Reactor pressure is reduced with the automatic depressurising system (ADS) and the steam generated in the reactor is drained into the suppression pool in the containment and further through the PCCS into the atmosphere.

**Cooling of reactor in loss of coolant accidents**

In a loss of coolant accidents, water supply to the reactor is secured by the gravity-driven cooling system (GDCS, 4 x 50%). The water volume of the GDCS is adequate to fill the containment to a level above the top level of the reactor core. Once the containment is filled, water will no longer flow out of the reactor pressure vessel. If the leak is so small that it does not reduce pressure in the reactor, the automatic depressurising system (ADS) is used to reduce pressure and the steam generated in the reactor is drained into the suppression pool in the containment. The residual heat transferred into the suppression pool is removed using the passive containment cooling system (PCCS, 6 x 25%). The design principles of the system realise the redundancy principle called for in the Government Decree.

In minor loss of coolant accidents, the diversity principle with respect to reactor water supply can be realised at high pressure with control rod drive hydraulic system (CRDHS, 2 x 100%) and at low pressure with the fuel and auxiliary pool cooling system (FAPCS, 2 x 100%). The fire water system can also be used in this situation.

The diversity principle with respect to residual heat removal is realised by both the fuel and auxiliary pool cooling system (FAPCS, 2 x 100%) and the reactor water cleanup/shutdown cooling system (RWCU/SDC, 2 x 100%). In both alternatives residual heat is further transferred through the reactor component cooling water system (RCCWS, 2 x 100%) and the plant service water system (PSWS, 2 x 100%) into the ultimate heat sink. The RCCWS comprises two lines (2x100%), each equipped with three pumps (2x3x33%). The PSWS comprises two lines (2x100%), each equipped with two pumps (2x2x50%).

N.B. This is unofficial translation.

Original:
The design objectives and principles of the systems required for the cooling of the reactor core and for the removal of residual heat are consistent with Finnish safety requirements. However, the design process is still at a very initial stage and further design is needed, particularly with respect to using systems that realise the diversity principle for the management of transients and accidents.

**Containment isolation**

At the ESBWR plant, containment isolation has been implemented in the pipelines penetrating the containment by means of two isolation valves of the same type. No common cause failure analysis has been performed on isolation valves of the same type, which means that the fulfilment of the diversity principle called for in the Government Decree cannot be proven with respect to the isolation valves. The realisation of the diversity principle with respect to containment isolation can be implemented through valve choices at later stages of the project.

**Loss of ultimate heat sink**

In case the normal removal of heat into seawater acting as the ultimate heat sink is lost, residual heat can be removed from the reactor by means of isolation condensers into the water pools in the reactor building located above the primary containment and further through the ventilation stack into the atmosphere. The isolation condensers (IC, 4 x 33%) are passive natural circulation condensers in type with which the reactor can be brought into a controlled (hot shutdown) state and maintained in this state. The water volume in the pools is adequate for the removal of residual heat for 24 hours without refilling. The pools can be refilled from a storage tank located outside the containment to continue the removal of residual heat for as long as is necessary, and in any case for at least 72 hours. The system realises the redundancy principle called for in the Government Decree.

The design principles of the systems involved in the management of the loss of the ultimate heat sink are consistent with Finnish safety requirements.

**Cooling of fuel pools**

The cooling of fuel pools is implemented with the fuel and auxiliary pool cooling system (FAPCS, 2 x 100%). Each subsystem consists of a pipeline, a pump and a heat exchanger. Residual heat is further transferred through the reactor component cooling water system (RCCWS, 2 x 100%) and the plant service water system (PSWS, 2 x 100%) into the ultimate heat sink. The system fulfils the redundancy principle called for in the Government Decree. The RCCWS comprises two lines (2x100%), each equipped with three pumps (2x3x33%). The PSWS comprises two lines (2x100%), each equipped with two pumps (2x2x50%).

N.B. This is unofficial translation.

Original:
Regarding the cooling of the fuel pools, the diversity principle is implemented in a way that if the water in the fuel pools begins to boil, make-up water is supplied through fixed connections from the fire water systems and residual heat is transferred through ventilation stack into the atmosphere.

The design objectives and principles of the systems involved in the cooling of the fuel pools are consistent with Finnish safety requirements.

**Shutdown safety**

The subcriticality of the reactor is ensured in all shutdown states by keeping the control rods inserted into the reactor.

The loss of reactor coolant during shutdowns is prevented by designing access doors to the containment so that they prevent water from leaking outside the containment and the water volume in the containment water pools is at all times adequate to flood the reactor core in accident conditions.

The design objectives and principles of the systems associated with shutdown safety are consistent with Finnish safety requirements.

**Electrical systems**

The supply of off-site power at the ESBWR plant is realised through auxiliary transformers from the 400 kV grid or through two standby auxiliary transformers from the 110 kV grid. If necessary, power can be supplied from the transformers directly to the switchgears of the safety systems bypassing switchgears with no nuclear safety classification (EYT systems).

In case off-site power supplies fail, power to the safety systems of the plant is supplied alternatively from

- auxiliary diesel generators (2 x 100%)
- batteries (rated discharge time 72 h), which supply direct current systems that are single failure tolerant within the subsystem

According to the description of the electrical systems, the severe accident management systems do not have their own on-site power supplies. Some of the on-site power supply systems, such as the auxiliary diesel generators, are assigned to safety class 3. The lower-than-normal safety class is based on the many passive safety functions incorporated in the plant concept. Auxiliary diesel generators are only needed to supply power to the active safety systems, which realise the diversity principle. Active safety systems are also used in normal operating conditions. The actual passive safety systems only need power for start-up. The required power can be supplied from batteries. In STUK's opinion, the lower safety class of the auxiliary diesel generators is justified.

N.B. This is unofficial translation.

Original:
The separation principle applied to the electrical systems is based on the separation referred to in standard IEEE 384, which only recognises one safety class 1E. Further analyses are required regarding decoupling between safety class 3 and class EYT, since the electrical systems of the auxiliary diesel generators and the sub-distribution have not been assigned to class 1E.

The general lessons learned from the design errors leading to the malfunction of the electric system of Forsmark nuclear power plant in 2006, must be taken into account. In the design of the electric systems and components, special attention must be focused on e.g. preventing voltage transients from spreading and the implementation of the diversity principle in the electricity distribution and in supplying power to I&C systems. Full analysis must be made to determine the most severe possible voltage transients and malfunctions of the in-house grid. Power consumers and systems are to be designed to withstand these transients and malfunctions.

The design principles of the electrical systems are consistent with Finnish safety requirements with respect to the off-site and on-site power supply system and the redundancy principle. Issues that need to be reviewed in more detail when the application for the construction license is submitted include the separation principles of the electrical systems, the separate power supply systems for the severe accident management system, and the general lessons learned from the Forsmark incidence.

Civil engineering and fire protection

The requirements defined for basic design of the buildings and the building engineering systems in terms of external threats are, for the most part, adequate. The temperatures and snow loads encountered in Finland in winter have not been separately discussed in the application documentation. However, the design basis provides an adequate basis for the consideration of Finnish winter conditions in the detailed design of buildings and building engineering systems.

The design basis regarding earthquakes is PGA 0.3 g, which exceeds the corresponding Finnish requirement of 0.1 g. The design objectives and principles associated with resistance to vibrations induced by earthquakes and other external hazards are consistent with Finnish safety requirements. Detailed design includes, first of all, verification of the vibration resistance of the actual buildings and, secondly, an analysis of the suitability of the vibration characteristics of the frame structures and the equipment anchorages to determine the vibration resistance of the plant components.

The design objectives and principles associated with the fire protection concept of the ESBWR plant are mainly consistent with Finnish safety requirements. The extinguishing systems of the plant are designed to be earthquake resistant, which ensures the management of consequential fires possibly caused by earthquakes.

Protection against external events (Gov. Decree 733/2008 Section 17)
The protection strategy of the ESBWR plant against aircraft crashes is, with respect to the reactor, the control room and the fuel buildings, designed so that the effects of an impact by a large commercial airplane on the integrity of the containment and on the removal of residual heat from the reactor and the fuel pools are limited to an acceptable level.

The fuel rods are protected against secondary missiles caused by the aircraft crash. In other parts of the plant, it has been demonstrated that internal missiles and the aircraft fuel, which may gain access through the damaged point, will not damage components to such an extent as to prevent the plant from being brought into a safe state or the removal of residual heat. According to the strategy, physical separation of the four redundancies of the plant ensures the operation of safety functions in an airplane crash situation.

The control room, which is located below ground level, is protected against damages resulting from damages sustained by the upper floors.

In the ESBWR plant concept, some residual heat removal systems are located in the turbine building, which is not protected against airplane crashes. To meet Finnish safety requirements in case of a loss of the turbine building, a Loviisa 3-specific residual heat removal system needs to be designed.

The chosen strategy in the ESBWR plant option is one in which structures do not fully withstand an airplane crash, but accept partial damage to structures. The implications of the presumed damages have on the required safety functions is evaluated and it is shown that the plant can be brought into a safe (cold shutdown) state despite the damage. According to STUK's assessment, the fulfilment of Finnish safety requirements has not yet been demonstrated. The proposed implementation requires more detailed design and analyses as well as plant modifications.

Protection against internal events (Gov. Decree 733/2008 Section 18)

Internal hazards such as floods and fires are taken into account in the room and layout planning of the ESBWR plant by placing the key safety systems in four different room areas. The room areas on the underground floors are provided with doors between the room areas for operating and maintenance purposes. The room areas are separated by means of reinforced concrete walls, for which a rated fire resistance of three hours is indicated.

The design premise at the ESBWR plant is to run main steam and feedwater pipes from the reactor building to the turbine building along undivided channels. According to Finnish requirements, impacts from a broken pipe, spray streams and missiles must not cause such damage or other coolant leaks to the equipment and structures that, in the case of a pipe break, can endanger the successful implementation of the necessary
safety functions, such as the removal of residual heat and the isolation of the containment. According to STUK’s assessment, the fulfilment of Finnish safety requirements in conjunction with pipe breaks in the main steam and feedwater lines has not yet been demonstrated. The proposed implementation requires more detailed design and analyses as well as plant modifications.

The compact layout of the plant results in requirements for protection against internal events, such as floods and fires. Major internal floods, for example floods of the essential service water system in one room area of the reactor building, must be analysed at later stages of the licensing procedure. The analyses must prove that the effects of the events are limited to the room area in question.

Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19)

It should be noted that in the documentation of the application for a decision-in-principle, the safety principles of the I&C systems have been presented at a rather general level. Before the specification of the design and the design materials has reached the level of actual technical design, it is more a matter of the objectives of several safety principles, the fulfilment of which cannot be assessed based on the documentation of the decision-in-principle. On the basis of the material submitted for the decision-in-principle, it is impossible to fully assess whether these goals have been achieved or not. The genuine fulfilment of the safety principles in the plant’s technical solutions must be ensured also at the later stages of the project. Of these phases, the construction license process is the first regulatory phase of the plant project that deals with solid technical I&C solutions.

*Automatic safety functions*

ESBWR plant automation includes several different lines of defence based on the defence-in-depth principle. The first line comprises normal process automation, control systems and limitation systems. The second line consists of the reactor protection system (RPS) and the safety system logic control/essential safeguards feature system (SSLC/ESF). The third line includes the diverse protection system (DPS) based on the diversity principle and the last line comprises the severe accident management system.

The reactor protection system (RPS) in the second defence line controls only the systems used to shut down the reactor and maintain it in a subcritical state. The SSLC/ESF system, on the other hand, operates in transient and accident conditions and actuates the passive safety systems, which include the isolation condenser, the automatic depressurising system and the gravity-driven core cooling system.

The DPS controls reactivity management, over-pressurisation protection, emergency core cooling, residual heat removal from the reactor and the containment as well as

N.B. This is unofficial translation.

Original:
containment isolation. The DPS is provided with process parameter measurement sensors, which are independent of the reactor and plant protection systems.

The automation systems of the different defence lines aim to automatically maintain plant parameters within a safe range during operating transients and to limit the consequences of accidents.

The design objectives and principles of the systems used for actuation, control and monitoring of safety functions during transients and accidents are consistent with Finnish safety requirements.

**I&C redundancy principle**

The reactor protection system and the safety system logic control/essential safeguards feature system comprise four parallel subsystems. The protection function is actuated if two of the four parallel protection channels give a protection signal.

There are three parallel subsystems in the diversity principle-based diverse protection system (DPS).

The most important process I&C systems, such as the reactor power control and limiting system, the feedwater supply control system, the control system of turbine bypass and main steam pressure, and the turbine control system are implemented with three parallel subsystems.

The design objectives and principles of the automation systems are consistent with Finnish safety requirements with respect to the redundancy principle.

**I&C separation principle**

The parallel subsystems of the automation systems have been physically and functionally separated from each other.

At the ESBWR plant, safety class 2 I&C systems are physically and functionally separated from the components of other safety classes. The separation of safety class 3 systems is not indicated in the appendices to the application.

At the ESBWR plant, the severe accident management I&C is part of the containment monitoring system. The application documentation does not indicate if the severe accident I&C and power supply to it are independent of the rest of the plant I&C, as prescribed in Finnish requirements.

The separation principles are, for the most part, consistent with Finnish requirements, with the exception of the separation of safety class 3 components and severe accident
systems, which couldn’t be verified from the application documentation. These matters can be reviewed when the application for the construction license is submitted.

**I&C diversity principle**

Finnish safety requirements prescribe that at least two different process parameters must be measured in the reactor protection system, both of which must be physically dependent on a transient or accident and the triggering limits of which can be selected so that they are reached early enough. According to the application documentation, the diversity principle has not been comprehensively applied to the reactor protection system so that signals indicating accident and transient conditions would come alternatively from two different process parameters.

At the ESBWR plant, automation is based on four different computer-based system platforms. The systems distributed to different system platforms include the reactor protection system (RPS), the safety system logic control/essential safeguards feature system (SSLC/ESF), the control system for severe accident management and the rest of the I&C.

The plant concept incorporates the diverse protection system (DPS), which backs up the reactor protection system (RPS) and the safety system logic control/essential safeguards feature system (SSLC/ESF). The DPS is implemented on the same system platform as the process automation. The documentation does not present a procedure for bringing the plant into a safe (cold shutdown) state in case the computer-based I&C system is lost.

The reactor protection system is backed up by the ATWS (Anticipated Transients Without Scram) control system, which is based on hardwired technology.

The design objectives and principles of the automation systems are, for the most part, consistent with Finnish safety requirements. When the construction permit is applied for, how the plant can be brought to a safe state (cold shutdown) and kept there in case programmable I&C is lost due to common cause failure must be clarified. Additionally, how the diversity principle is applied in the reactor protection system measurements must be clarified.

**Control room**

The control room of the ESBWR plant contains e.g. the main control console and the display panel.

The main control console is used to control the plant in normal operating conditions, transient conditions and accident conditions. In addition, all the information needed by the operators for the execution of the control actions in the aforementioned conditions is transmitted to the main control console.
The display panel comprises primarily wide-screen display screens. The display panel is designed to present in one assembly the status of the plant and the most important components as well as the most important alarm data.

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

**Emergency control room**

The ESBWR plant features two emergency control rooms, which can be used for the control of safety-critical systems independently of the main control room. The plant can be brought into a controlled (hot shutdown) state and further into a safe (cold shutdown) state from the emergency control room.

The emergency control room is located in a different fire compartment and building from the main control room.

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

**Reactor pressure vessel level measurement**

Reactor pressure vessel level measurement is based on normal differential pressure measurement, which controls the reactor protection automation. There are four identical parallel measurements, and the system is actuated on receiving a protection signal from two channels. The system realises the redundancy principle.

No common-cause failure analyses have been performed on the level measurement system and thereby the realisation of the diversity principle in this respect has not been analysed. The realisation of the diversity principle with respect to level measurement can be reviewed when the application for the construction license is submitted.

**Summary**

The design objectives and principles of the plant alternative are, for the most part, consistent with Finnish safety requirements.

In the ESBWR plant concept, some residual heat removal systems are located in the turbine building. These are the only systems that can be used to bring the plant from controlled (hot shutdown) state into safe (cold shutdown) state. Pursuant to Finnish safety requirements, it must be possible to bring the plant into a safe state also when the turbine building is lost as a result of e.g. a fire or an aircraft crash. In order to ensure fulfilment of the Finnish requirements in this respect, further design and plant modifications are needed.
The chosen strategy in the design of the containment in the event of an airplane crash is one in which structures are not designed to completely withstand an airplane crash, but partial damage to buildings is accepted. The strategy also encompasses an assessment of the significance of the assumed damages and demonstration of the ability to bring the plant into a safe state despite the damages. In STUK's opinion, fulfilment of Finnish safety requirements has not yet been demonstrated. In order to meet Finnish safety requirements in this respect, more detailed designs and analyses as well as plant modifications are needed.

Some technical details require further analyses and qualification based on tests as well as further engineering at later stages of the licensing procedure. In STUK's opinion, none of these details can be foreseen to be an obstacle to the fulfilment of the requirements set forth in the Government Decree (733/2008). These technical details include

- reactor stability
- reliability of the squib valve used in passive safety systems
- realisation of the diversity principle for the containment isolation function
- realisation of the diversity principle for reactor level measurement
- demonstration of the functioning of the core catcher required for severe accident management
- severe accident management I&C and the implementation of the external power source required for I&C independent of the rest of the plant I&C
- separate power supply system for severe accident management system
- realisation of the separation principle and general lessons learned from the Forsmark incidence taken into account in the electrical systems
- possibilities to bring the plant into a safe state in case the computer-based automation system is lost
- realisation of the diversity principle for reactor protection system’s measurements.

PRESSURISED WATER REACTOR PLANT ALTERNATIVES

AES-2006 - Pressurised Water Reactor - Atomstroyexport

General
AES-2006 is a ca. 1200 MWe pressurised water reactor marketed by the Russian Atomstroyexport (ASE). AES-2006 is based on the VVER 91/99 plant, which is developed from the VVER-1000 plants in operation. VVER type plants have been built in Russia and many other countries already for 30 years. Loviisa 1 and 2 plant units are based on the VVER 440 plant type. The reference plants for the plant alternative include Tianwan 1 and 2 in China, and Leningrad NPP-2 currently under construction in Russia. Leningrad NPP-2 consists of two plant units, which together with the Novovoronesh-2 plant unit are the first AES-2006 type plants in Russia. There are also several AES-2006 plants in the planning stage in different countries.

The AES-2006 plant’s safety functions have been improved compared to the VVER 91/99 plant. The safety functions are, as a rule, implemented by means of active systems that are supplemented, as is typical with pressurised water reactors, with passive, pressure accumulators for use in emergency cooling situations as well as passive systems designed for removing the plant’s residual heat and which have previously not been used at nuclear power plants. The new passive systems for residual heat removal in transient and accident conditions are the primary circuit cooling residual heat removal system based on natural recirculation and connected to the steam generator, and the natural circulation based containment residual heat removal system. The AES-2006 also has severe accident management systems. The rated service life of the plant is 60 years. The level of maturity of the plant with respect to basic engineering is high. The design objectives and principles of this plant are, for the most part, consistent with Finnish safety requirements.

The primary circuit of the AES-2006 plant comprises four reactor coolant loops, each with a horizontal steam generator and a reactor coolant pump.

The secondary circuit is essentially identical to the existing VVER-type pressurised water reactors. The plant has four horizontal steam generators, the technology of which corresponds to the steam generators already in use in Loviisa’s VVER 440 plants. The practical experiences with this type of steam generator are mostly positive.

Assessment and verification of safety (Gov. Decree 733/2008 Section 18)

_Deterministic analysis methods and preliminary results_

For the assessment and verification of safety of the AES-2006 plant, ASE uses analysis methods that have been maintained and qualified for the intended purpose of use. The methods have been used during the design and construction of the plant units in operation. Early versions of the analysis methods presented now have been used in the design of the Loviisa 1 and 2 plant units, among others. The analyses performed on the AES-2006 plant lead to the impression that transient and accident analyses consistent with Finnish requirements can be performed on this plant alternative.
Probabilistic analyses

ASE uses level 1 and 2 probabilistic risk analysis (PRA) methods. The methods have been used for a level 1 PRA analysis for the AES-2006 plant. The analyses cover the most important initial events in all the plant’s operational stages. Based on the data on analysis methods and the results of the PRA pertaining to AES-2006, it can be assessed that analyses consistent with Finnish PRA requirements can be performed on this plant alternative. If needed, the methods can be developed on the basis of detailed Finnish requirements. Probabilistic risk analyses are made in conjunction with the plant’s detailed designing, and at that time the compliance with the Finnish safety requirements will be assessed.

Qualification of new type of systems

Passive systems that have previously not been used at nuclear power plants have been planned for the AES-2006 plant. The passive systems to be used in transient and accident situations are the reactor circuit cooling residual heat removal system (PHRS SG) connected to the steam generators and based on natural recirculation, and the natural circulation based containment building’s residual heat removal system (PHRS C). The systems are in the process of testing-based qualification. Test assemblies exist and the testing is partially completed. The results of these tests have been and will be used in the qualification process for computation models. The correct functioning of the systems can be confirmed only after the test results are ready. This matter can be reviewed when the application for the construction licence is submitted.

Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008 Sections 8–10)

As part of the design process of the AES-2006 plant, ASE has calculated the radiation exposure of the population in the areas surrounding the plant in accident situations. The results of the calculation show that the radiation doses of the population will be below the dose limits defined for accidents in Finnish requirements.

Based on the analysis results and the design features of the plant concept, it can be assessed that analyses consistent with Finnish requirements can be performed on this plant alternative at later stages of the licensing procedure.

Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008 Section 13)

Reactor and fuel

N.B. This is unofficial translation.
Original:
The reactor in the AES-2006 plant is essentially identical in structure as in the VVER 1000 plants currently in operation. Because of the higher output, the active part of the fuel assemblies has been lengthened to keep the maximum load of the fuel unchanged. The design of the fuel and the core complies with similar practices applied in the existing large-scale pressurised water reactors. The number of control rods has also been increased to improve safety. Boron carbide and dysprosium titanium oxide are used in the rods as a neutron-absorbing material. The core contains 163 fuel assemblies and 121 control rods.

The fuel is typical hexagonal fuel assemblies used in VVER reactors. Reactivity during the operating cycle is managed by means of boron in the primary coolant, control rods, and burnable absorbers contained in the fuel.

The designed discharge fuel burn-up is higher than the maximum 45 MWd/kgU fuel assembly burn-up approved in Finland. 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, the applicant must provide experimental proof of the consistency of the fuel with the Finnish design criteria pertaining to accident conditions.

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

**Main nuclear components**

The material and structural engineering solutions of the main nuclear components of the AES-2006 utilise the practical data gained from about 30 years of VVER reactor operations. The reactor pressure vessel is made of modern pressure equipment grade steel typical for such reactors. The forgings are welded into pressure vessels using known and qualified methods. The interior of the vessel is clad with stainless steel welded on to the surface. The internals of the reactor pressure vessel are made of stainless steel and other applicable materials.

The typical aging phenomena have been taken into account in material selections for main equipment and in monitoring during operation. Radiation embrittlement in the core area of the reactor pressure vessel has been taken into consideration and is monitored with a program for radiation embrittlement during operation. Attention must be given to the analysis requirements (P, Cu and Ni) of the reactor pressure vessel steel 10 GH2MoA so that the radiation embrittlement of the reactor pressure vessel’s core area remains within the allowed limits during the 60-year rated service life of the plant. This must be ensured in later stages of the licensing process.

Other main components, like the steam generators and the pressuriser, are manufactured in the same way as the reactor pressure vessel. The heat transfer pipes of the steam generators are made of stainless steel, which has been found to be a reliable solution in these plants provided that the water chemistry is well controlled. The
damages detected earlier in the welding joints of VVER-1000 plant’s steam generator’s collectors have been addressed through the material selection of the new steam generator type for the AES-2006.

The reactor coolant piping is made of low-alloy pressure equipment grade steel, which is lined with stainless steel. Thus no demanding, dissimilar metal joints are needed in the joints between the reactor coolant nozzles and the reactor coolant pipes. The design of the reactor coolant piping applies the "break preclusion" (BP) principle, part of which involves the "leak before break" (LBB) principle. Thus the intention is to eliminate a design-basis postulated break in the pipe with the largest diameter. This is, however, taken into account in the design of the emergency cooling systems. Further clarifications are still needed to ensure consideration of the dynamic effects of pipe breaks in the primary circuit, particularly if pipe whip restraints are not to be installed in the primary circuit.

Numerous smaller pipelines related to auxiliary and emergency systems are connected to the reactor coolant loop with welded joints, the integrity verification of which can pose challenges in conjunction with processing strength and ductility analyses and the implementation of periodic inspections and the related radiation protection goals. This must be taken into account in later stages of the licencing procedure.

The AES-2006 design objectives and principles presented for the main nuclear components are, for the most part, consistent with Finnish safety requirements. The effect of the reactor pressure vessel material’s analysis requirements on the rate of radiation embrittlement requires additional analyses, which can be assessed at later stages of the licensing procedure. Also the effects of the reactor coolant loop’s postulated, sudden pipe breakages on the integrity of the reactor’s inner components, and the implementation, inspection and radiation protection principles of the reactor coolant loop joints must be clarified at later stages of the licensing procedure.

Pressure control of primary and secondary circuits

Pressure control of the AES-2006 plant’s primary circuit is implemented by 3 safety/relief valves (3x50%). The valves required to restrict pressure are opened by a pneumatic pilot valve controlled by the reactor protection automation or directly on the basis of reactor pressure against a spring load. There are 2 spring-loaded pilot valves per safety valve.

With respect to pressure control in the primary circuit, the diversity principle is realised by the pressuriser’s spray system, which can pump water in the pressuriser’s steam chamber with the recirculation pumps, the primary circuit volume control system (KBA) or the emergency borating system’s (JDH) pumps, depending on the operational status of the plant. Pressure is controlled in the secondary circuit with the steam generator’s dump valves (BRU-A) and with the steam generator’s safety valves.

N.B. This is unofficial translation.
Original:
The design objectives and principles of the systems involved in pressure control are consistent with Finnish safety requirements.

**Containment**

The primary containment of the AES-2006 plant is a so-called large dry containment built of pre-stressed reinforced concrete and provided with a tight steel liner. The containment is designed to maintain its integrity in compliance with approval criteria in transient and accident conditions. The primary containment is enclosed in a secondary concrete containment, which protects the primary containment against external hazards.

**Severe accidents**

In the severe accident management strategy of the AES-2006 plant, containment integrity is ensured by preventing the pressure vessel from bursting at high pressure, removing residual heat from the containment with the passive residual heat removal system, confining and cooling the core melt in the core catcher underneath the pressure vessel, and removing hydrogen with the recombinators.

The bursting of the pressure vessel at high pressure can be prevented by reducing pressure in the primary circuit by means of the relief valves. The purpose of the procedure is to prevent high-pressure discharge of core melt during reactor pressure failure, as such discharge could compromise the integrity of the containment. The AES-2006 plant does not have separate valves for depressurisation in severe accidents. Instead, depressurisation has been designed to occur using the primary circuit's pilot-controlled safety valves. As such, the solution is not consistent with Finnish safety requirements because the systems designed to control a severe accident must be independent of the plant's systems designed for the different stages of plant operation and for postulated accidents.

Core melt at the AES-2006 plant is retained and cooled in a core catcher installed underneath the reactor pressure vessel. The core catcher operates without an external power source. Coolant flows into the core catcher from a coolant tank inside the containment. The steam generated in the core catcher is condensed in the containment's passive residual heat removal system, from which the coolant flows via the coolant tank back to the core catcher. The AES-2006 core catcher has been developed from the previous VVER-91 plant’s solution, the functionality of which has been ensured with an extensive test program. Separate tests have been performed on the impact of the differences in the solutions.

The containment’s passive residual heat removal system (PHRS C) transfers heat from the containment into the atmosphere via the water pools on the containment roof. These water pools are shared with the steam generator’s passive residual heat removal system (PHRS SG). In the PHRS C system, the water flows by force of gravity from the pools.
into the condensers installed in the upper space of the containment. In the condenser, the water evaporates and rises through the return pipe back into the pool, where some of the steam recondenses into water and some of it is released into the atmosphere. The water inventory of the pools is sufficient for removing residual heat for 24 hours, after which they must be refilled from the storage tank outside the containment. The containment’s passive residual heat removal system has four parallel subsystems, each having the capacity of 33% of the required total capacity. The system’s capacity, 4x33%, fulfils Finnish requirements. They require that the systems needed to ensure the integrity of the containment in conjunction with a severe reactor accident must be able to perform their safety function also in the event of a single failure.

A considerable amount of hydrogen is generated during a severe accident. This hydrogen pressurises the containment and if present in high concentration, it may burn or explode. The containment of pressurised water reactors is filled with air during operation, which means it contains oxygen needed for the burning process. However, the large containment of pressurised water reactors, which is made of pre-stressed concrete, is quite strong against the effects of hydrogen burns and explosions. The AES-2006 plant will be equipped for the purpose of hydrogen removal with passive autocatalytic recombinators. The recombinators require no external power source and they remove hydrogen at such low levels that there is not enough time for a flammable gas mixture to be generated.

Finnish requirements call for nuclear power plants to be equipped with a filtered containment venting system to mitigate the consequences of severe accidents. A filtered containment venting system that can be used to remove noncondensable gases from the containment in a later phase of an accident is not planned for installation in the AES-2006 plant. According to the plant supplier, with the exception of hydrogen, there is not a significant amount of containment-pressurising noncondensable gases generated in a severe accident. Hydrogen can be removed using recombinators. The need for a filtered venting system must be assessed when applying for the construction license.

The systems designed for severe accident management of the AES-2006 plant do not, in their current state, meet Finnish safety requirements regarding primary circuit depressurisation because the depressurisation has been designed to be carried out using the ordinary safety valves of the primary circuit. Finnish requirements call for severe accident systems to be independent of the systems designed for the plant’s operating stages and postulated accidents. Additionally, the need for a filtered venting system must be assessed in later stages of the licensing process.

Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14)

At the AES-2006 plant both active and passive systems are used for the implementation of safety systems. As in all other pressurised water reactors, passive systems are used in control rods implementing reactor scram and in the emergency cooling system’s
pressure accumulators. Additionally, new passive safety systems, which have previously not been used at nuclear power plants, have been designed for the plant. The passive systems for residual heat removal in transient and accident conditions are the primary circuit cooling residual heat removal system based on natural circulation and connected to the steam generator, and the natural circulation based containment residual heat removal system.

Reactivity management

Reactivity management at the AES-2006 plant is implemented by means of control rods, boron contained in the reactor coolant, and burnable absorber contained in the fuel.

In a transient the reactor is shut down as in all other pressurised water reactors by dropping the control rods into the reactor core. The reactor scram system is passive in nature. The control rods drop into the reactor core by gravity after the reactor protection automation disconnects the power supply to the electromagnets, which hold the control rods. The system realises the redundancy principle called for in the Government Decree.

With respect to shutting down the reactor, the diversity principle is realised with an emergency borating system (JDH, 4 x 50%).

Owing to the burnable absorber mixed in the fuel, the boron content of the primary coolant can be kept relatively low also after fresh fuel has been loaded in the reactor. Despite the lower boron content of the primary coolant and the more effective scram, the possibility of the boron content of the coolant being erroneously diluted has been taken into account in the design of the reactor. The management of the boron-free water slug in shutdown and start-up situations as well as in transient and accident conditions has been taken into account in the design process. Supplementary analyses and/or tests are needed to support the presented plans.

In order to prevent the potential recriticality of the reactor in cooling situations, the efficiency of the control rods has been boosted by increasing the number of control rods in the reactor. After these measures, the reactor’s recriticality temperature during a cooling accident without additional boron is exceptionally low, about 100°C.

The design objectives and principles of the safety functions associated with reactivity management are consistent with Finnish safety requirements. However, the plans presented for e.g. the sudden dilution of boron concentration in the primary circuit require supplementary analyses and/or tests in later stages of the licensing process.

Cooling of reactor

N.B. This is unofficial translation.
Original:
Cooling of reactor in shutdown conditions

In hot shutdown conditions, as usual to pressurised water reactors, residual heat is removed from the reactor through steam generators directly to the turbine condenser using the turbine bypass lines. If this is not possible, residual heat can be removed by pumping water into the steam generators by means of emergency feedwater system (EFWS, 4 x 100%) and blowing steam into the atmosphere with the secondary circuit dump valves (BRU-A). This is discussed later in conjunction with transients.

After the pressure and temperature of the primary circuit is reduced, the residual heat is removed directly from primary circuit by means of the residual heat removal system JNA (4 x 100%), which uses the same pumps as the low-head safety injection system (JNG). The residual heat is transferred to the ultimate heat sink by means of the intermediate circuit cooling system (KAA, 4 x 100%) and the process water system for important consumers (PEB, 4 x 100%). These systems are used as the primary residual heat removal systems also in transient and accident conditions.

If the residual heat removal system JNA (4 x 100%) cannot be used in a situation where the reactor pressure vessel head is open (transient in residual heat removal e.g. in a "mid-loop operation" situation), it can be replaced with the containment's passive residual heat removal system (PHRS C, 4 x 33%). In this case, residual heat is removed from the reactor by evaporating water into the containment. The residual heat from the containment is transferred by means of the PHRS C condensers into the atmosphere via the water pools located outside the containment. The system is always ready for operation and starts up without the need for any active component to function. The pools outside the containment are shared with the PHRS SG. Residual heat can be removed with the PHRS C for 24 hours after the accident without measures by an operator. With additional measures, the time can be lengthened to 72 hours by pumping water from the alternative water storage into the water pools. This solution is not described in more detail in the documentation nor is it certain that the arrangement is completely consistent with Finnish requirements that call for fixed pipelines and a refilling pump from the alternative water storage to the water pool. This issue can be reviewed when applying for the construction license.

Cooling water for the reactor is supplied by means of the primary circuit’s volume and boron control system (KBA) from the make-up water tank or by means of the JNG system from the IRWST located inside the containment.

Cooling of reactor in accident conditions with reactor primary circuit intact

If a transient or an accident prevents normal residual heat removal to the turbine condenser, residual heat can be removed from primary circuit to atmosphere using the emergency feedwater system (EFWS, 4 x 100%) of the secondary circuit and the steam generator dump valves (BRU-A). The emergency feedwater system is used to pump water from the emergency feedwater tank into the steam generators; the steam
generated there is then transferred to the atmosphere through the dump valves. The emergency feedwater system features four lines (4 x 100%). The system can be used to bring the reactor into a controlled (hot shutdown) state and maintain it there for at least 24 hours. With additional measures, the time can be lengthened to 72 hours by pumping water from an alternative water storage into the water pools. This solution is not described in more detail in the documentation nor is it certain that the arrangement is completely consistent with Finnish requirements that call for fixed pipelines and a refilling pump from the alternative water storage to the emergency feedwater tank. This issue can be reviewed when applying for the construction license.

Residual heat can be transferred to the atmosphere alternatively also with the steam generator’s passive residual heat removal system (PHRS SG, 4 x 33%). With the PHRS SG, the reactor’s residual heat is transferred through the steam generators to the atmosphere via the heat exchangers in the water pools located outside the containment. The PHRS SG is activated from a protection signal, which opens the valve between the steam generator and the heat exchangers outside the containment. The heat is then transferred to the atmosphere via the water pools entirely without an external power source. The system can remove residual heat for 24 hours after an accident without measures by an operator. With the PHRS SG, the plant is brought to controlled (hot shutdown) state. With additional measures, the time can be lengthened to 72 hours by pumping water from an alternative water storage into the water pools. This solution is not described in more detail in the documentation nor is it certain that the arrangement is completely consistent with Finnish requirements that call for fixed pipelines and a refilling pump from the alternative water storage to the emergency feedwater tank. This issue can be reviewed when applying for the construction license.

In transient and accident conditions in which the reactor primary circuit is intact, the make-up water for the reactor and compensating for the volume decrease due to cooling is supplied primarily by means of the volume and boron control system (KBA). Alternatively, make-up water can be supplied by means of the high-head safety injection system (JND, 4 x 100%), which acquires the make-up water from the IRWST located inside the containment.

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 also be removed directly from the primary circuit. This is done by pumping cold boron-containing water into the circuit by means of the high-head safety injection system (JND) pumps from the IRWST, and by removing hot water from the circuit through the safety valves back to the IRWST (so-called feed and bleed cooling) via the containment. Residual heat is transferred to the ultimate heat sink by means of the intermediate circuit cooling system (KAA, 4 x 100%) and the process water system for important consumers (PEB, 4 x 100%).

Cooling of reactor in loss of coolant accidents

N.B. This is unofficial translation.
Original:
In accidents where reactor coolant is lost as a result of a leak, the reactor can be cooled with emergency cooling systems designed for this purpose.

At the AES-2006 plant emergency cooling of the primary circuit is implemented by means of active high-head safety injection system (JND, 4 x 100%) and a low-head safety injection system (JNG, 4 x 100%) as well as four pressure accumulators. The pumps of the safety injection system take coolant from the in-containment refuelling water storage tank (IRWST) through suction strainers. The reactor cooling water that has leaked into the containment drains back to the IRWST. The design of the suction strainers in the IRWST is not presented in the documentation. The design of the suction strainers and a test program for them is currently under way. The suction strainers will be equipped also with a back-flushing system. This issue can be reviewed when the application for the construction license is submitted.

For small coolant leaks, the diversity principle with respect to emergency cooling is realised so that the primary circuit is cooled quickly by means of the relief valves of the secondary circuit or with the safety valves of the primary circuit. The pressure in the primary circuit is reduced to a range where the JNG system and the safety injection accumulators can function. Cooling water for the JNG and JND systems is supplied from the IRWST.

The pumps of the high- and low-head safety injection system and the pressurised water tanks feed borated water directly into the reactor pressure vessel, both into the downcomer and above the reactor core. Additionally, with the high-head safety injection system pumps borated water is pumped to two cold legs, and with the low-head safety injection system pumps to the two cold legs and hot legs. This makes it possible to ensure the supply of cooling water to the reactor in case of small coolant leaks in the primary circuit that are associated with a common cause failure in the components related to reactor cooling.

Residual heat is removed from the reactor using the residual heat removal system JNA (4 x 100%), which uses the same pumps as the low-head safety injection system. The residual heat is transferred to the ultimate heat sink through the intermediate circuit cooling system (KAA, 4 x 100%) and the process water system for important consumers (PEB, 4 x 100%).

The design objectives and principles of the systems associated with the cooling of the reactor core and the removal of residual heat are consistent with Finnish safety requirements.

**Removal of residual heat from the containment**

At the AES-2006 plant the removal of residual heat from the containment in transient and accident conditions is implemented with the containment spray system (JMN, 4 x
50%), with which residual heat can be removed to the ultimate heat sink through the intermediate circuit cooling system and the process water system for important consumers.

The diversity principle for residual heat removal is realised by means of the containment’s passive residual heat removal system (PHRS C, 4 x 33%). The reactor’s residual heat is removed from the containment and into the atmosphere via the water pools located outside the containment by means of the PHRS C. System activation requires no external power source. The system’s water pools are shared with the PHRS SG. With PHRS C, the residual heat can be transferred for 24 hours after an accident without operator measures. With additional measures, the time can be lengthened to 72 hours as presented above.

The design objectives and principles of the systems involved in residual heat removal from the containment are consistent with Finnish safety requirements.

**Containment isolation**

At the AES-2006 plant the intention is to implement containment isolation in each of the pipelines penetrating the containment by means of two isolation valves that operate on different principles.

The design objectives and principles of the containment isolation are consistent with Finnish safety requirements.

**Loss of ultimate heat sink**

In case the ultimate heat sink, i.e. the possibility to transfer residual heat via the turbine’s condenser or the essential service water system into the sea is lost when the reactor circuit is closed, residual heat can be removed from the reactor cooling circuit by pumping water with the emergency feedwater system into the secondary side of the steam generators and releasing the steam into the atmosphere. With this arrangement, the reactor can be brought to and maintained in a controlled state (hot shutdown) for at least 24 hours. With additional measures, the time can be lengthened to 72 hours, as presented above.

Alternatively, the passive residual heat removal system (PHRS SG, 4 x 33%) of the steam generators can be used. The PHRS SG can remove residual heat 24 hours after an accident without operator measures. With additional measures, the time can be lengthened to 72 hours by pumping water from an alternative water storage into the water pools. With the PHRS SG, the plant can be brought to controlled state. Cooling water into the reactor is supplied by means of the primary circuit’s volume and boron.

N.B. This is unofficial translation.
Original:
control system (KBA) from a make-up tank or by means of the JNG system from the IRWST inside the containment.

When the reactor pressure vessel head is open, the normal residual heat removal system can be replaced by evaporating water into the containment and transferring the residual heat by means of the passive containment's residual heat removal system (PHRS C, 4 x 33%). Residual heat can be removed with PHRS C for 24 hours after an accident without measures by an operator. With additional measures, the time can be lengthened to 72 hours, as presented above. Cooling water for the reactor is supplied by means of the primary circuit’s volume and boron control system (KBA) from the make-up water tank or by means of the JNG system from the IRWST located inside the containment.

The design objectives and principles of the systems associated with managing the loss of ultimate heat sink are consistent with Finnish safety requirements.

Cooling of fuel pools

The cooling of fuel pools is implemented with the fuel pool cooling system, which features two train and two pumps in each train (FAK). The fuel pool is divided into two pools.

The containment spray system pumps and the emergency cooling system heat exchangers can be used as a fuel pool cooling system that realises the diversity principle.

Alternatively, residual heat can be removed by means of the PHRS C system by evaporating water in the fuel pools. In this case, the fuel pool purification system (FAL) is used to get make-up water to the fuel pools. The source of the make-up water is not mentioned in the documentation.

The design objectives and principles of the systems associated with the cooling of fuel pools are consistent with Finnish safety requirements.

Shutdown safety

The subcriticality of the reactor is ensured in all shutdown states by keeping the control rods inserted into the reactor and by adding boron solution with adequate concentration into the coolant water. The subcriticality of the reactor in shutdown states is monitored with neutron flux detectors positioned outside the reactor and with control procedures.

The dump valves of the primary circuit are used to prevent the cold pressurisation of the primary circuit.
The removal of residual heat from the primary circuit or the containment in a shutdown situation with the reactor pressure vessel head open or closed is implemented as described above in "Cooling of reactor".

The design objectives and principles of the systems associated with shutdown safety are consistent with Finnish safety requirements.

*Electrical systems*

The supply of off-site power at the AES-2006 plant is realised through auxiliary transformers and a main transformer from the 400 kV grid or through standby auxiliary transformers from the 110 kV grid.

In case off-site power supplies fail, on-site power to the safety systems of the plant is supplied from

- emergency diesel generators (4 x 100%)
- a gas turbine-driven generator, which realises the diversity principle (1 x 100%)
- batteries during the start-up of emergency power sources

The alternating current power source presented in the concept realises the diversity principle, but is not consistent with Finnish safety requirements in terms of the redundancy principle.

The severe accident management systems have their own separate on-site power supply systems. The description refers to own separate battery sets, which have a discharge time of 72 h. No procedures for recharging the battery sets have been presented.

The separation principle applied to the electrical systems has not been clearly described. This matter can be reviewed when the application for the construction licence is submitted.

The general lessons learned from the design errors leading to the malfunction of the electric system of Forsmark nuclear power plant in 2006, shall be taken into account. In the design of the electrical systems and components, special attention shall be paid to e.g. restraining voltage transients from spreading and the implementation of the diversity principle in the electricity distribution and in supplying power to I&C systems. Full analysis shall be made to find out the most severe possible voltage transients and malfunctions of the in-house grid. Power consumers and systems are to be designed to withstand these transients and malfunctions. The matter shall be reviewed in a more detailed manner at the construction licensing stage.

The design objectives and principles of the electrical systems are, for the most part, consistent with the Finnish safety requirements. The alternating current power source
realising the diversity principle, the separation principles of the electrical systems, the separate power supply system for the severe accident management system and the general lessons learned from the Forsmark incidence must be further analysed when the application for the construction license is submitted.

Civil engineering and fire protection

The requirements associated with external hazards defined for the basic design of the buildings and the building engineering systems at the AES-2006 plant are adequate. The basic design provides an adequate basis for the consideration of the design requirements in the detailed design of buildings and building engineering systems.

The design objectives and principles associated with resistance to vibrations induced by earthquakes and other external hazards are consistent with Finnish safety requirements. The reference plant used in the design basis for earthquakes is Tianwan’s PGA value of 0.2 g and Leningrad NPP-2’s PGA value 0.12 g, which exceed the corresponding Finnish requirement of 0.1 g. The starting point for the design basis has been the predesign of the durability of the frame structures and vibration characteristics against all vibrations caused by external threats. This provides good bases for the detailed design also regarding the vibration resistance of the components. In terms of the decision-in-principle, the requirements presented in the design basis are adequate. The design principles for the vibration resistance of components must be verified when submitting the construction license application.

The design objectives and principles associated with the fire protection concept of the AES-2006 plant are consistent with Finnish safety requirements, with the exception of the separation of the different room areas of the safety buildings, which, in terms of the design requirements, is not unambiguously consistent with Finnish requirements. In this respect, and in terms of controlling possible consequential fires caused by earthquakes, the need for seismic resistance of the plant’s fire extinguishing systems and the design basis must be verified in the possible construction licensing phase.

Protection against external events (Gov. Decree 733/2008 Section 17)

The protection strategy of the AES-2006 plant against the impact of a large commercial airplane is based on constructing the outer containment building to withstand the impact of a large airplane. Additionally, the strategy uses principles of shielding and distance for the buildings of main steam valves, safety systems, control rooms and emergency diesel generators. Strengthened reinforced concrete structures are used to protect the fresh fuel storage, and the tanks for radioactive waste are located in underground rooms.

Structural protection against collision by a large commercial airplane focuses on the outer containment and on the fresh fuel storage. The safety buildings and steam cells are not designed to withstand the impact of a large airplane. Demonstrating the
realisation of the safety functions in an event of an aircraft collision is thus difficult. The plant supplier has presented options for expanding the structural protection of the buildings deemed most significant in terms of safety.

In STUK’s opinion, fulfilment of Finnish safety requirements has not yet been demonstrated. The solution presented requires more detailed designs and analyses and plant modifications.

Protection against internal events (Gov. Decree 733/2008 Section 18)

The AES-2006 safety systems are divided into four parallel, redundant subsystems. The subsystems are physically separated from each other. Those components of the safety systems located in the safety building are placed in adjacent room areas. Physical separation in the containment has been realised by dividing the annulus into four fire compartments.

The safety building’s structural elements containing safety systems have been placed side by side and are connected by service corridors and channels for air-conditioning systems. These connections between the parallel subsystems are separated by doors and dampers and call into question the adequate realisation of physical separation.

The lower floors of the safety building contain the seawater heat exchangers and pipelines of the intermediate circuit cooling system. Controlling a major flood caused by the breakage of these components is challenging in the selected layout of the safeguard building. Likewise, in the safety building, each subsystem’s low- and high-head pressure injection pumps and related equipment and pipelines have been placed in the same room space without physical separation.

In STUK’s opinion, the fulfilment of Finnish safety requirements in terms of protection from internal incidents, such as floods and fires, has not yet been demonstrated. The solution presented requires more detailed designs and analyses and plant modifications.

Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19)

The safety principles of the automation systems have been presented at a rather general level in the documentation of the application for a decision-in-principle. Before the specification of the design and the design materials has reached the level of actual technical design, it is more a matter of the objectives of several safety principles, the fulfilment of which cannot be assessed based on the documentation of the decision-in-principle. The genuine compliance of safety principles in the technical solutions of the plant has to be ensured as the design work advances including the subsequent phases of the project. Of these phases, the construction license process is the first regulatory phase of the plant project that deals with concrete technical solutions of automation.
Automatic safety functions

AES-2006 plant automation includes several different lines of defence based on the defence-in-depth principle. The first line comprises normal process automation and control systems. The second line consists of the primary protection system that, if necessary, initiates all safety functions and is divided into two redundant, diverse parts, A and B. The third line includes a second protection system, HW (Hardwired)-Div., realised with a different technology and initiating the most important safety functions. The system includes the same functions as the protection system’s diversity A. The last line comprises the severe accident management system.

The automation systems of the different lines of defence are designed to automatically maintain the plant parameters within a safe range during operating transients and to limit the consequences of accident conditions.

The design objectives and principles of the automation systems used for actuation, control and monitoring of safety functions during transients and accidents are consistent with Finnish safety requirements.

I&C redundancy principle

The primarily operating protection system comprises four redundant subsystems. The protection function is actuated if two of the four redundant protection channels send a protection signal. The system meets the requirements of the Government Decree with respect to the redundancy principle.

The most important normal process automation systems are realised as single failure tolerant.

The protection system HW-Div realising the diversity principle for the automation has four redundant subsystem.

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

I&C separation principle

The parallel reactor protection systems have been physically and functionally separated from each other. The separation of the I&C systems and components of different safety classes from each other between and within subsystems has not been described in the documentation. Likewise, the separation of I&C and monitoring systems for severe accident management from other automation systems has not been addressed.
The documentation received does not provide adequate information regarding consistency with Finnish safety requirements in terms of design objectives related to the separation principle for I&C systems. The separation of automation systems of different safety classes from each other and the separation of the severe accident management system from the rest of the automation must be described and, if necessary, revised. Additionally, the separation principles of parallel I&C subsystems from each other must be clarified.

**I&C diversity principle**

Finnish safety requirements prescribe that at least two different process parameters must be measured in the reactor protection system, both of which must be physically dependent on a transient or accident and the triggering limits of which can be selected so that they are reached early enough. The application documentation does not indicate how the diversity principle is applied to the measurements of the reactor protection system and to the activation of protections. This matter can be reviewed when the application for the construction licence is submitted.

The AES-2006 plant’s automation is based on two computer-based system platforms. The reactor protection system, the engineered safety features system and the limiting system are based on one platform and the other I&C systems on the other platform.

The plant concept incorporates a HW-Div backup system for the computer-based protection system; the backup system is based on the diversity principle. The delivered documentation does not describe to what operational state the system can bring the plant in the case of common cause failure of the programmable I&C system. The issue can be reviewed when applying for the construction license.

The design objectives and principles of the system are consistent with Finnish safety requirements with respect to the diversity principle. The scope of the HW-Div system and the diversity principle of the reactor protection system with respect to measurements and activation of protections can be elaborated when the application for the construction licence is submitted.

**Control room**

The control room contains control consoles and a display panel. The control consoles of the turbine, the reactor and the auxiliary system operator are used to control the plant in normal operating conditions, transient conditions and accident conditions. In addition, all the information needed for execution of the control actions is transmitted to the control consoles.

N.B. This is unofficial translation.

Part of the display panel comprises fixed indicators and control switches. These include e.g. the protection system panel and the control panels for the safety-critical components.

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

Emergency control room

The AES-2006 plant features an emergency control room, which can be used for control of safety-critical systems independently of the main control room. The plant can be brought into a controlled (hot shutdown) state and further into a safe (cold shutdown) state from the emergency control room.

The emergency control room is located in separate building from the main control room.

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

Summary

The design objectives and principles of the AES-2006 plant alternative are, for the most part, consistent with Finnish safety requirements.

In the AES-2006 plant alternative, structural protection against collision by a large commercial airplane focuses on the outer containment and on the fresh fuel storage. The safety buildings and steam cells are not designed to withstand the impact of a large airplane. Demonstrating the realisation of the safety functions in an event of an aircraft collision is thus difficult. The plant supplier has presented options for expansion of the structural protection of the buildings deemed most significant in terms of safety. According to STUK's assessment, fulfilment of Finnish safety requirements has not yet been demonstrated. The solution presented requires more detailed designs and analyses and plant modifications.

In the AES-2006 plant alternative, the safety building’s structural elements containing safety systems have been placed side by side and are connected by service corridors and channels for air-conditioning systems. These connections between the parallel subsystems are separated by doors and dampers and call into question the adequate realisation of physical separation. According to STUK's assessment, the fulfilment of Finnish safety requirements in terms of protection from internal incidents, such as floods and fires, has not yet been demonstrated. The solution presented requires more detailed designs and analyses and plant modifications.
The design objectives and principles associated with the separation principles of the I&C systems were not found to be consistent with Finnish safety requirements. The separation I&C systems of different safety classes from each other and the separation of the severe accident management system from the rest of the automation must be described and, if necessary, revised. Additionally, the separation principles of parallel I&C subsystems from each other must be clarified.

Primary circuit depressurisation in severe accidents does not, in its current state, meet Finnish safety requirements because the depressurisation has been designed to be carried out using the ordinary safety valves of the primary circuit and emergency degassing system. Finnish requirements call for severe accident systems to be independent of the systems designed for the plant’s operating stages and postulated accidents.

Some technical details require further analyses and qualification based on tests as well as further engineering. In STUK's opinion, none of these details can be foreseen to be an obstacle to the fulfilment of the requirements set forth in the Government Decree on the safety of nuclear power plants (733/2008). These technical details include:

- Demonstration of the functionality of the passive residual heat removal systems (PRHR SG, PRHR C) with tests
- Analysis requirements of the reactor pressure vessel’s materials, and implementation, inspection and radiation protection principles for the pipe nozzles related to the reactor coolant loops
- Effects on the integrity of the reactor’s inner components in postulated, sudden pipe breaks in the primary circuit
- Need to equip the containment with a filtered containment venting system
- Emergency cooling system’s suction strainers and verification of their functionality with tests
- Technical solutions related to the supplying of cooling water for systems (EFWS, PRHR SG, PRHR C, FAL) that realise the diversity principle and are related to the 72-hour removal of residual heat
- Alternating current supply equipment realising the diversity principle
- Electric power supply system of the systems for management of severe accidents
- General lessons learned from the Forsmark incidence
- Separation principles for both electric and automation systems
- Scope of the HW-Div system
- Application of the diversity principle to measurements of the reactor protection system and to the activation of protections.

N.B. This is an unofficial translation.

APR1400 - Advanced Power Reactor 1400 - KHNP

General

APR1400 is a ca. 1400 MWe pressurised water reactor designed by the Korean KHNP. It is based on Combustion Engineering's System 80+ plant originally designed in the United States. KHNP started the construction of nuclear power plants of this type in Korea towards the end of the 1980s. Plant engineering and component manufacture were gradually transferred to Korea and each new plant was improved on the basis of the experience gained from the previous plants. As the degree of domestic origin rose to a significant level, the plants representing the same origin were referred to by a common abbreviation OPR1000. At present there are eight OPR1000 plant units in operation in Korea and four under construction.

APR1400 is an advanced reactor type based on the OPR1000 concept, a new generation reactor with higher electrical power output. The first APR1400 plant units, Shin-Kori 3 and 4, are currently under construction and expected to be completed in 2013–2014. Preparations have also been started in Korea for the construction of the next two APR1400 plant units.

KHNP has further developed the plant designed for the Korean market by adding certain safety features required by Finnish safety requirements. The rated service life of the plant is 60 years. The level of maturity of the plant with respect to basic engineering is high. The design objectives and principles are, for the most part, consistent with Finnish safety requirements.

Safety functions in the APR1400 plant have been improved over the OPR1000 plant and the plant concept includes severe accident management systems. Safety functions are as a rule implemented by means of active systems, supplemented, with passive, exceptionally large pressure accumulators for use in emergency cooling situations as is typical with pressurised water reactors.

The primary circuit of the APR1400 plant differs in design from other pressurised water reactors. The APR1400 plant concept features four cold legs, each with reactor coolant pumps. The cold legs are connected to very large steam generators, with two cold legs always connected to one steam generator. There are two hot legs that run from the reactor to the steam generators. Operating experience in this solution has been gained at power plants constructed by Combustion Engineering and KHNP.

The principle of the secondary circuit is identical with that used in existing pressurised water reactors. There are two exceptionally large steam generators based on vertical U-tubes. The technology of the steam generators corresponds to the newest steam generators at existing plants, with material choices and structural solutions used to
eliminate the problems typically encountered with the integrity of the heat transfer tubes in vertical steam generators.

Assessment and verification of safety (Gov. Decree 733/2008 Section 3)

**Deterministic analysis methods and preliminary results**

For the assessment and verification of safety, KHNP uses analysis methods reviewed and approved by the Korean nuclear safety authority and USNRC. The methods have been maintained and qualified for the intended purpose of use. The methods have been applied in the licensing of the existing plant units and in the design of the APR1400 plant. The analyses performed on the APR1400 plant lead to the impression that transient and accident analyses consistent with Finnish requirements can be performed on this plant alternative.

**Probabilistic analyses**

KHNP uses level 1, 2 and 3 probabilistic risk analysis (PRA) methods, which have been applied in the PRA analyses of the existing plant and the APR1400 plant. The analyses encompass all the operational states of the plant, including events associated with external and internal hazards. Based on the data on analysis methods and the results of the analysis pertaining to APR1400, it can be assessed that analyses consistent with Finnish PRA requirements can be performed on this plant alternative. If necessary, the methods can be developed on the basis of detailed Finnish requirements. Probabilistic analyses will be made in conjunction with the plant’s detailed design phase, at which time the realisation of Finnish safety requirements will be assessed.

**Qualification of new type of systems**

The design concept of the APR1400 plant alternative includes pressure accumulators of a new type for the emergency cooling system, never before used at nuclear power plants. The operation of the pressure accumulators has been appropriately qualified in a test assembly, and the analysis methods used have been updated on the basis of the test results. A test assembly based on the APR1400 plant and referred to as ATLAS is also in use in Korea. This test assembly has been and will be used in the development of analysis methods and in the verification of the operation of new plant features. Some new plant features may still require further tests.

Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008 Sections 7–10)

As part of the APR1400 design process, KHNP has performed a computation of the radiation exposure of the population in the areas surrounding the plant in accident
conditions. The analysis results show that the radiation doses of the population are below the dose limits defined in Finnish requirements.

The analyses results lead to the impression that analyses consistent with Finnish requirements can be performed on this plant alternative in later stages of the licensing procedure.

Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008 Section 13)

Reactor and fuel

At the APR1400 plant, the design of the fuel, the reactor core and the reactor complies for the most part with the practice applied in existing pressurised water reactors. KHNP designs and manufactures itself the fuel used in the reactor. The fuel assembly is based on a typical modern construction with construction materials, which correspond to other fuel types in use today. Burnable absorbers are used in the fuel to reduce the primary coolant boron concentration and in this way improve the dynamic properties of the reactor. The reactor contains 241 fuel assemblies as well as 76 full-length and 17 partial-length control rods, which are used together with the boron contained in the primary coolant to control reactor power. The partial-length control rods are used to control the xenon oscillations encountered in connection with reactor power changes in reactors of this size. The design of the loading patterns of the reactor corresponds to the practice applied in existing pressurised water reactors.

The designed discharge fuel burn-up is higher than the maximum fuel assembly burn-up of 45 MWd/kgU approved in Finland. 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, the applicant must demonstrate by means of testing that the fuel is consistent with the Finnish design criteria pertaining to accident conditions.

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

Main nuclear components

The reactor pressure vessel of the APR1400 plant is built of low-alloy pressure equipment steel joining together hemispherical forgings by welding using qualified methods typical to pressure equipment manufacture. The inside of the pressure vessel is lined with welded stainless steel and partly with nickel-based alloys. Good stress corrosion resistance is accounted for in the selection of the liner materials.

The limitation of radiation embrittlement taking place in the reactor core area has been taken into account in the material composition and analysis requirements.
Embrittlement is monitored with a monitoring programme compliant with normal practice. The reactor pressure vessel has been designed so that no weld joints exist in the centre areas of the reactor core.

Ageing phenomena during operation has been taken into account in the choice of building materials used in the reactor pressure vessel and in other main components. In the material choices for the main components, requirements are set also for the maximum concentration of alloy elements, like cobalt, affecting the activity of the primary circuit.

Proven requirements and implementation principles are adhered to also in the manufacture of the steam generators and the pressuriser. The heat transfer tubes of the steam generators are made of nickel-based alloy Inconel 690 TT (Thermally Treated), which, according to current knowledge, is a clearly more durable solution than earlier material choices.

The reactor coolant piping is made of low-alloy steel, which is lined with stainless steel welded onto the pipes. This means that no dissimilar metal joints are needed in the joints between the reactor coolant nozzles and the reactor coolant pipes. Other joints, in which the dissimilar metal joint technology is used, are welded using Inconel 690-type filler metal, which is proved to have better stress corrosion resistance than the filler metals used earlier.

In the design of the primary circuit, the "leak before break" (LBB) principle based on Finnish safety requirements is applied. Thus the intention is to eliminate a design-basis postulated break in the pipe with the largest diameter. This is, however, foreseen in the design of the emergency feedwater systems. Further clarifications are still needed to ensure consideration of the dynamic effects of pipe breaks in the primary circuit, particularly if pipe whip restraints are not to be installed in the primary circuit. The design objectives and principles presented for the main nuclear components are, for the most part, consistent with Finnish safety requirements. However, further analyses are needed to ensure the consideration of the dynamic effects of pipe breaks in the primary circuit.

**Pressure control of primary and secondary circuits**

At the APR1400 plant, pressure control in the primary circuit is implemented by four safety valves controlled by pilot valves. The valves blow the steam directly into the IRWST through the blow-down nozzles in the same way as in a boiling water reactor. If necessary, these valves can also be used to reduce pressure in the primary circuit in a controlled way if the possibility to pump water into the primary circuit in high pressure has been lost.

The diversity principle called for in the Government Decree is realised by the pressuriser's auxiliary spray system, through which water can be pumped with the

N.B. This is unofficial translation.
Original:
chemical and volume control system (CVCS, 2x100%) (emergency diesel backup for the electrical supply) to the pressuriser steam chamber and condensate steam.

Pressure control in the secondary circuit is implemented with the automatic dump valves of the steam generator (SG ADV) and the safety valves of the steam generator. The design objectives and principles of the systems involved in the pressure control are consistent with Finnish safety requirements.

**Containment**

The primary containment of the APR1400 plant is a so-called large dry containment built of pre-stressed reinforced concrete and provided with a tight steel liner. The containment is designed to maintain its integrity in compliance with approval criteria in transient and accident conditions. The primary containment is enclosed in a secondary concrete containment, which protects the primary containment against external hazards.

**Severe accidents**

Severe accident management at the APR1400 plant is based on depressurization of the primary circuit, the containment spray system, which removes residual heat, the retention and cooling of core melt with the core catcher located under the pressure vessel and recombinators, which remove hydrogen.

Depressurization of the primary circuit is part of severe accident management at the APR1400 plant. One of the objectives of this action is to reduce stress in the reactor pressure vessel and thereby secure the retention of core melt inside the pressure vessel. Another objective is to prevent high-pressure eruption of core melt should the reactor pressure vessel burst in any case. Pressure can be reduced in the primary circuit by means of two parallel pressure relief valves, which are independent of the other plant systems. The valves are mounted on the pressuriser head and they blow into the containment. The external power for the opening of the valves is supplied from the electrical system for severe accidents.

Residual heat is removed with the dedicated severe accident containment spray system (SACSS), which comprises two pumps operating in parallel and two parallel containment isolation valves, and a common heat exchanger. From the heat exchanger, residual heat is directed into the ultimate heat sink with the intermediate circuit with two parallel pumps dedicated for this system. Power to the SACSS system and the assisting intermediate circuit is supplied from the electrical system for severe accidents.

In the original APR1400 plant concept, the core melt is retained inside the reactor pressure vessel by cooling the pressure vessel from the outside. A similar solution has been applied e.g. at the Loviisa nuclear power plant, but the power of the Loviisa plant is only about one third of the power of the APR1400 plant. At a plant the size of the

---

N.B. This is unofficial translation.
APR1400, the residual heat of the core is so high that the safety margin of external cooling of the reactor pressure vessel is small. The plant supplier has launched a program in 2009 with the goal to develop a core catcher located under the pressure vessel of the plant tendered to Finland. A preliminary design of the core catcher does exist. In the design, the core catcher is flooded with water from a storage pool inside the containment by gravity. The melt discharge from the pressure vessel into the core catcher opens the flood-activation valve.

A considerable amount of hydrogen is generated during a severe accident. This hydrogen pressurises the containment and if present in high concentration, it may burn or explode. The containment of pressurised water reactors is filled with air during operation, which means it contains oxygen needed for the burning process. However, the large containment of pressurised water reactors, which is made of pre-stressed concrete, is quite strong against the effects of hydrogen burns and explosions. For the purpose of hydrogen removal, the APR1400 plant will be equipped with ca. 40 passive autocatalytic recombinators. The recombinators require no external power source and they remove hydrogen at such low levels that there is not enough time for a flammable gas mixture to be generated.

The APR1400 plant tendered to Finland will be equipped with a filtered containment venting system. By means of that filter, non-condensable gases can be removed from the containment in the late phase of an accident, and the containment can be depressurised to the level of outdoor air.

The containment of the APR1400 plant and the systems designed for severe accident management require further clarifications to meet Finnish safety requirements for severe accidents. The core catcher is in the design stage. The functionality of the core catcher must be demonstrated through testing in the construction licensing phase at the latest.

Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14)

The APR1400 plant’s safety functions are primarily implemented with active systems. Passive systems are used in some details, such as the control rods implementing reactor scram and in the exceptionally large pressure accumulators used in the emergency cooling system.

Reactivity management

Reactivity at the APR1400 plant is managed with control rods, boron contained in the reactor coolant, and burnable absorber contained in the fuel.

In a transient the reactor is shut down as in all other pressurised water reactors by dropping the control rods into the reactor core. The reactor scram system is passive in nature. The control rods drop into the reactor core by gravity after the reactor protection
automation disconnects the power supply to the electromagnets, which hold the control rods. The system realises the redundancy principle called for in the Government Decree.

The diversity principle with respect to the shutting down of the reactor is realised by the active emergency borating system (EBS, 2 x 100%). It is used only in situations when reactor scram implemented by means of the control rods fails.

In other transient and accident conditions, borated water of the safety injection system (SIS) is used to ensure that the reactor remains in a shutdown state and subcritical.

Owing to the burnable absorber mixed in the fuel, the boron content of the primary coolant can be kept relatively low also after fresh fuel has been loaded in the reactor. Despite the lower boron content of the primary coolant and the more effective scram, the possibility of the boron content of the coolant being erroneously diluted has been taken into account in the design of the reactor. The management of the so-called clean water slug in shutdown and start-up situations as well as in transient and accident conditions has been taken into account in the design process, which prepares for those. However, supplementary analyses and/or tests are needed to support the presented plans.

The design objectives and principles of the safety functions associated with reactivity management are, for the most part, consistent with Finnish safety requirements. However, supplementary analyses and/or tests are needed to support the strategy presented for the management of sudden boron dilution.

**Cooling of reactor**

**Cooling of reactor in shutdown conditions**

In hot shutdown conditions, residual heat is removed from the reactor in the manner typical for pressurised water reactors through steam generators directly to the turbine condenser using the turbine bypass lines. If this is not possible, residual heat can be removed by pumping water into the steam generators by means of auxiliary feedwater system and blowing steam into the atmosphere by means of the secondary circuit dump valves. This is discussed later in conjunction with transients.

After the pressure and temperature of the primary circuit is reduced, residual heat is removed directly from primary circuit by means of the shutdown cooling system and containment spray system (SCS/CSS, 4 x 50%). The residual heat is transferred to the ultimate heat sink by means of the component cooling water system (CCWS, 4 x 50%) and the essential service water system (ESWS, 4 x 50%). These systems are used as primary residual heat removal systems also in transient and accident conditions.
If the shutdown cooling system and the containment spray system (SCS/CSS, 4 x 50%) cannot be used in a situation where the reactor pressure vessel head is open (disturbance in residual heat removal, e.g. in "mid-loop operation" situation), residual heat can be removed by evaporating water into the containment and by transferring the residual heat into the atmosphere by means of the reactor containment fan coolers (RCFC, 2 x 100%). Make-up water to the reactor is supplied from the IRWST.

Cooling of reactor in transient and accident conditions with reactor primary circuit intact

If a transient or an accident prevents normal residual heat removal to the turbine condenser, residual heat can be removed from primary circuit to atmosphere using the auxiliary feedwater system (AFWS, 2 x 100%) of the secondary circuit and the steam generator dump valves (SGADV). The auxiliary feedwater system is used to pump water from the auxiliary feedwater storage tank into the steam generators and the generated steam is then transferred out through the dump valves. The auxiliary feedwater system features two parallel subsystems. Both subsystems have their own auxiliary feedwater storage tank and one supply line, each equipped with two pumps; one electric pump and one steam-driven pump and each of them can supply a sufficient amount of water in every situation. If necessary, the tanks can be cross-connected. The system can be used to bring the reactor into a controlled (hot shutdown) state and maintain it 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 also be removed directly from the primary circuit. This is done by pumping cold boron-containing water into the circuit by means of the safety injection system (SIS) high pressure pumps (SIP) from the IRWST, and by removing hot water from the circuit through the safety valves back to the IRWST (so-called feed and bleed cooling). Residual heat is removed further from the IRWST with the shutdown cooling system and containment spray system (SCS/CSS, 4 x 50%). The residual heat is transferred to the ultimate heat sink by means of the component cooling water system (CCWS, 4 x 50%) and the essential service water system (ESWS, 4 x 50%).

In transient and accident conditions in which the reactor primary circuit is intact, the make-up water for the reactor and compensating for the volume decrease due to cooling is supplied primarily by means of the chemical and volume control system (CVCS, 2 x 100%).

Alternatively, make-up water can be supplied by means of the safety injection system (SIS, 4 x 100%), which acquires the coolant from the IRWST-tank located inside the containment.

Cooling of reactor in loss of coolant accidents

In accidents where primary coolant is lost as a result of a leak, the reactor can be cooled with reactor emergency cooling systems designed for this purpose.
At the APR1400 plant, the safety injection system (SIS, 4 x 50%) comprises four parallel separate subsystems. Each is equipped with a high-head safety injection pump (SIP) and a passive, large pressurised safety injection tank (SIT). Flow regulation devices (vortex) designed for the pressure accumulators regulate the flow to the reactor core in an optimum manner during an accident. Each subsystem of the SIS supplies the cooling water through its own nozzle directly into the reactor pressure vessel. The safety injection system pumps acquire the coolant from the in-containment refuelling water storage tank (IRWST) through suction strainers. The reactor cooling water that leaks into the containment is drained back into the IRWST. The suction strainers of the IRWST are designed so that loose debris produced in the accident or otherwise present in the containment will not clog the suction strainers. The strainers are also equipped with a flushing system to account for clogging. Partial clogging of the suction strainers has also been appropriately taken into account in the determination of the required suction head for the safety injection pumps. The performance of the suction strainers has so far not been proven experimentally, but this can be done at later stages of the licensing procedure.

The diversity principle with respect to emergency cooling for small coolant leaks is realised by quickly cooling the primary circuit by means of the dump valves of the secondary circuit and, at the same time, pressure of the primary circuit is reduced to a range where the safety injection tanks, the shutdown cooling system and containment spray system (SCS/CSS, 4 x 50%) can operate. SCS/CSS takes the cooling water from the IRWST as does also the high-head safety injection system. The SCS is also used for long-term cooling of the reactor core in design-basis accidents.

Residual heat is removed from the IRWST with the shutdown cooling system and containment spray system (SCS/CSS, 4 x 50%). The residual heat is transferred to the ultimate heat sink by means of the component cooling water system (CCWS, 4 x 50%) and the essential service water system (ESWS, 4 x 50%).

The design objectives and principles of the systems associated with reactor core cooling are, for the most part, consistent with Finnish safety requirements. The performance of the suction strainers of the safety injection system has not yet been proven experimentally. The presented implementation solution requires further tests.

Removal of residual heat from containment

At the APR1400 plant, the removal of residual heat from the containment in primary or secondary circuit leaks can be implemented with the shutdown cooling system and containment spray system (SCS/CSS, 4 x 50%) with which residual heat can be transferred to the IRWST and from there further to the ultimate heat sink by means of the component cooling water system (CCWS) and the essential service water system (ESWS).
The diversity principle with respect to the removal of residual heat from the containment in small coolant leaks is realised by means of the reactor containment fan coolers (RCFC).

The design objectives and principles of the systems associated with the removal of residual heat from the containment are, for the most part, consistent with Finnish safety requirements.

**Containment isolation**

Containment isolation at the APR1400 plant has been implemented in the pipelines penetrating the containment by means of two isolation valves. The implementation of the diversity principle can be realised with respect to containment isolation through valve choices at later stages of the project.

**Loss of ultimate heat sink**

In case the ultimate heat sink is lost, which means that a possibility to transfer residual heat to the turbine condenser or through essential service water system to the sea is lost when the reactor circuit is closed, residual heat can be removed from the reactor cooling circuit by pumping water into the secondary side of the steam generators by means of the auxiliary feedwater system and blowing the steam into the atmosphere. With this arrangement, the reactor can be kept in a controlled state for at least 72 hours.

When the reactor pressure vessel head is open, the shutdown cooling system and containment spray system (SCS/CSS, 4 x 50%) and the cooling chain that transfers heat from these systems further into the sea can be replaced by evaporating water into the containment and by transferring the residual heat into the atmosphere by means of the reactor containment fan coolers (RCFC). The cooling water to the reactor is supplied from the IRWST.

The design objectives and principles of the systems associated with the management of the loss of ultimate heat sink are consistent with Finnish safety requirements.

**Cooling of fuel pools**

The cooling of fuel pools is implemented with cooling and clean-up system (FC, 2 x 100%) of those pools, to which make-up water is supplied from the boric acid storage tank (BAST). The system realises the redundancy principle.

The diversity principle called for in the Government Decree can be realised by transferring residual heat into the atmosphere by evaporating water in the fuel pools. Make-up water to the fuel pools is supplied alternatively by gravity from the storage tank of the auxiliary feedwater system or by means of the boron pumps from the storage tank of the boron system. The design objectives and principles of the systems

N.B. This is unofficial translation.

Original:
http://www.stuk.fi/ydinturvallisuus/ydinvoimalaitokset/suomen_ydinvoimalaitokset/fi_FI/uu...
associated with the cooling of fuel pools are consistent with Finnish safety requirements.

**Shutdown safety**

The subcriticality of the reactor is ensured in all shutdown states by keeping the control rods inserted into the reactor and by adding boron solution with adequate concentration into the cooling water. The subcriticality of the reactor in shutdown states is monitored with neutron flux detectors positioned outside the reactor and with control procedures.

The overpressure protection of the primary circuit at low temperatures has been implemented with dump valves during plant shutdown and start-up as well as in outage states when the shutdown cooling system (SCS) is in operation.

The removal of residual heat from the primary circuit or the containment in a shutdown situation with the reactor pressure vessel head open or closed is implemented as described above in "Cooling of reactor".

The design objectives and principles of the systems associated with shutdown safety are consistent with Finnish safety requirements.

**Electrical systems**

The supply of off-site power at the APR1400 plant is realised through auxiliary transformers and a main transformer from the 400 kV grid or through standby auxiliary transformers from the 110 kV grid.

In case off-site power supplies fail, on-site power to the safety systems of the plant is supplied alternatively from

- emergency diesel generators (4 x 100%)
- standby emergency generators (2 x 100%), which realise the diversity principle
- batteries during the start-up of the emergency power sources

The severe accident management systems have their own separate on-site power supply systems.

The separation principles applied to the electrical systems have not been clearly described in the documentation. This matter can be reviewed when the application for the construction licence is submitted.

The general lessons learned in connection with the malfunction of the electrical system at the nuclear power plant of Forsmark in 2006 must be taken into account. In the design process of the electrical systems and equipment, attention must be paid to e.g. the prevention of voltage transient propagation and the realisation of the diversity
principle for the electrical power supplies and power supplies of I&C systems. The worst possible voltage transient situations and transient situations in the plant’s electrical network must be analysed. Electrical equipment and systems must be dimensioned to tolerate these situations. This matter will be examined in a detailed manner in the construction licensing phase.

The design objectives and principles of the electrical systems are, for the most part, consistent with Finnish safety requirements. Matters to be studied in a more detailed manner when an application for the construction licence is submitted include the separation principles applied to the electrical systems and general lessons learned from the Forsmark incident.

Civil engineering and fire protection

The requirements associated with external hazards defined for the basic design of the buildings and the building engineering systems at the APR1400 plant are adequate except that the temperatures and snow loads associated with Finnish winter conditions have not been separately discussed in the requirements. The basic design provides an adequate basis for the consideration of also these design requirements in the detailed design of buildings and building engineering systems.

The design objectives and principles associated with resistance to vibrations induced by earthquakes and other external hazards are consistent with Finnish safety requirements. The design basis regarding earthquakes is PGA 0.3 g, which clearly exceeds the corresponding Finnish requirement of 0.1 g. The detailed design incorporates an analysis of the frame structures, including verification of, first of all, the vibration resistance of the actual buildings and, secondly, an analysis of the suitability of the vibration characteristics of the frame structures and the equipment anchorages to determine the vibration resistance of the plant components. This applies to vibrations induced by all external hazards.

The design objectives and principles associated with the fire protection concept of the APR1400 plant are consistent with Finnish safety requirements and the design bases for structural fire protection are adequate. The extinguishing systems of the plant are designed to be earthquake resistant, which ensures the management of consequential fires possibly caused by earthquakes.

Protection against external events (Gov. Decree 733/2008 Section 17)

The protection strategy of the APR1400 plant against the impact of a large commercial airliner is based on constructing the outer containment and auxiliary buildings aircraft crash-resistant and tight so that the aircraft fuel spilled as a result of the crash does not enter the protected buildings.
The control room of the plant is located in the auxiliary building, as are also two separate diesel generator sets and the fuel pools. The two backup diesel buildings and the two essential service water pumping stations are protected through distance separation.

The design objectives and principles of the presented implementation solution are consistent with Finnish safety requirements.

Protection against internal events (Gov. Decree 733/2008 Section 18)

Internal hazards such as floods and fires are taken into account in the room and layout planning of the APR1400 plant by locating the four parallel redundancies of the key safety systems in different room areas separated from each other. The room areas are separated by means of reinforced concrete walls, for which a rated fire resistance and flooding class of three hours is indicated. The adjacent room areas on the bottom floor of the reactor building, which contain e.g. the pumps of the safety injection and essential service water systems, are separated by means of walls to prevent the propagation of internal floods. The separation principle is also applied in the control room building. The cable channels running to the control room are separated into different fire compartments, and the various channels do not meet until they reach the control room, where they are also appropriately separated from each other.

The design premise in the APR1400 plant is to run the main steam and feedwater pipes from the containment to the turbine building along two separate routes. Each main steam and feedwater route runs along its own reinforced concrete channel.

Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19)

It should be noted that the safety principles of the automation systems have been presented on a fairly general level in the documentation of the application for a decision-in-principle. Before the specification of the design and the design materials has reached the level of actual technical design, it is more a matter of the objectives of several safety principles, the fulfilment of which cannot be assessed based on the documentation of the decision-in-principle. The genuine compliance of safety principles in the technical solutions of the plant has to be ensured as the design work advances including the subsequent phases of the project. Of these phases, the construction license process is the first regulatory phase of the plant project that deals with concrete technical solutions of automation.

Automatic safety functions

APR1400 plant automation includes several different defence lines based on the defence-in-depth principle. The first line comprises normal process automation and control systems. The second line consists of the protection system, which is the
primarily active system that initiates all safety functions when needed. The third line includes the diverse protection system (DPS), which is implemented using different technology and can initiate the most important safety functions. The last line comprises the severe accident management system.

The automation systems of the different defence lines have been designed to automatically maintain plant parameters within a safe range during operating transients and limit the consequences of accidents.

The design objectives and principles of the automation systems used for actuation, control and surveillance of safety functions during transients and accidents are consistent with Finnish safety requirements.

**I&C redundancy principle**

The primarily operating protection system of the APR1400 plant comprises four parallel subsystems. The protection function is actuated if two of the four parallel protection channels give a protection signal. The systems meet the requirements of the Government Decree with respect to the redundancy principle.

The diversity principle with respect to automation is realised by the diverse protection system (DPS), for which the number of parallel subsystems has not been indicated in the application documentation.

The design objectives and principles of the automation systems are, for the most part, consistent with Finnish safety requirements. The redundancy principle of the DPS must be clarified when the application for the construction licence is submitted.

**I&C separation principle**

At the APR1400 plant, safety class-2 I&C systems are physically and functionally separated from components of other safety classes. The functional separation of safety class-3 systems from other safety classes is not described. This matter can be handled when the application for the construction licence is submitted. The severe accident management I&C and surveillance system is separated from the rest of the plant I&C.

The parallel subsystems of the I&C systems are physically and functionally separated from each other.

The design objectives and principles associated with the separation principle of I&C systems are consistent with Finnish safety requirements. The functional separation of safety class-3 systems from other safety classes must be described when the application for the construction licence is submitted.
I&C diversity principle

Finnish safety requirements prescribe that at least two different process parameters must be measured in the reactor protection system, both of which must be physically dependent on a transient or accident and the triggering limits of which can be selected so that they are reached early enough. The application documentation does not indicate how the diversity principle is applied to the measurements of the reactor protection system and to the activation of protections. This matter can be reviewed when the application for the construction licence is submitted.

At the APR1400 plant, automation is based on two computer-based system platforms. The reactor protection system and the engineered safety features system are based on one platform and the other I&C systems, including the diverse protection system DPS, on the other platform. According to the current designs, the DPS only covers certain initiating events and it is possible that new functions will need to be added. The possibility of a common cause failure in the system platforms of computer-based automation has also been taken into account in the plant concept by providing hardwired manual controls for the most important safety systems. The plant can be brought into a safe (cold shutdown) state by means of these manual controls.

The design objectives and principles of the system are consistent with Finnish safety requirements with respect to the diversity principle. The scope of the DPS and the diversity principle of the reactor protection system with respect to measurements and activation of protections can be elaborated when the application for the construction licence is submitted.

Control room

The control room contains control consoles, a display panel and a control console for safety systems. The control consoles of the turbine and reactor operators are used to control the plant in normal operating conditions, transient conditions and accident conditions. In addition, all the information needed by the operators for the execution of the control actions is transmitted to the control consoles.

The control console for safety systems is used to control the plant with hardwired manual controls in case the digital I&C systems fail.

The display panel comprises fixed indicators and wide-screen display screens. The display panel is designed to present in one assembly the status of the plant and the most important components as well as the most important alarm data.

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

N.B. This is unofficial translation.
Original:
Emergency control room

The APR1400 plant features an emergency control room, from which safety-critical systems can be controlled independently of the main control room. The plant can be brought into a controlled (hot shutdown) state and further into a safe (cold shutdown) state from the emergency control room.

The emergency control room is located in a different fire compartment and on a different floor from the main control room.

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

Summary

The design objectives and principles of the APR1400 plant alternative are, for the most part, consistent with Finnish safety requirements. The core catcher included in the plant tendered to Finland is the design stage. The functionality of the core catcher must be demonstrated with tests in the construction licence phase at the latest.

Some other technical details require further analyses and qualification based on tests as well as further engineering. In STUK's opinion, none of these details can be foreseen to be an obstacle to the fulfilment of the requirements set forth in the Government Decree on the safety of nuclear power plants (733/2008). These technical details include

- management of sudden boron dilution in the primary circuit
- consideration of the dynamic effects of pipe breaks in the primary circuit
- experimental verification of the performance of suction strainers in the emergency cooling system
- realisation of the diversity principle for the containment isolation function
- separation principles applied for the electrical systems and consideration of general lessons learned from the Forsmark incident in electrical systems
- redundancy principle for the DPS and the scope of functions
- application of the diversity principle to the measurements of the reactor protection system and to the activation of protections.

EPR - European Pressurised Water Reactor - AREVA

General

N.B. This is unofficial translation.
Original:
EPR is a ca. 1700 MWe pressurised water plant designed by the German-French AREVA. The reference plant for this plant alternative is Olkiluoto 3. EPR is originally based on the German 1300 MWe Konvoi series plants and the French 1450 MWe N4 series plants. The safety assessment of the EPR plant is based on the documentation submitted for the Olkiluoto 3 plant.

The safety functions of the EPR plant are, for the most part, implemented by means of active systems, supplemented with passive pressure accumulators for use in emergency cooling situations as is typical with pressurised water reactors. The rated service life of the plant is 60 years.

The design objectives and principles of this plant alternative are consistent with Finnish safety requirements.

The output of the tendered EPR plant has been increased by ca. 7 percent compared to Olkiluoto 3. The power increase affects the design of the plant's safety functions and the behaviour of the plant in transient and accident events. The effects of the power increase must be taken into account at later stages of the licensing procedure.

The primary circuit of the EPR plant comprises four reactor coolant loops, each with a vertical steam generator and a reactor coolant pump.

The secondary circuit in this plant type is essentially identical with existing pressurised water plants. There are four vertical, U-tube steam generators and the technology of the steam generators corresponds to the newest steam generators at existing plants.

Assessment and verification of safety (Gov. Decree 733/2008 Section 3)

**Deterministic analysis methods and preliminary results**

For the assessment and verification of safety, AREVA uses analysis methods used in the design process of the Olkiluoto 3 plant unit. The methods have been maintained and qualified for the intended purpose of use. The analyses performed on Olkiluoto 3 lead to the impression that transient and accident analyses consistent with Finnish requirements can be performed on this plant alternative.

**Probabilistic analyses**

AREVA uses level 1 and 2 probabilistic risk analysis (PRA) methods, which are applied in the PRA analyses of the Olkiluoto 3 plant unit. The analyses encompass all the operational states of the plant, including events associated with external and internal hazards. Based on the data on analysis methods and the results of the PRA calculations pertaining to Olkiluoto 3, it can be assessed that analyses consistent with Finnish PRA requirements can be performed on this plant alternative.
Limitation of radiation exposure and releases of radioactive materials (Gov. Decree 733/2008 Sections 7–10)

As part of the design process of the Olkiluoto 3 plant unit, AREVA has performed a computation of the radiation exposure of the population in the areas surrounding the plant in accident situations. The analysis results show that the radiation doses of the population are below the dose limits defined in Finnish requirements.

Engineered barriers for preventing the dispersion of radioactive materials (Gov. Decree 733/2008 Section 13)

Reactor and fuel

The construction of the EPR plant reactor is essentially the same as that of existing pressurised water reactors. The reactor contains 241 fuel assemblies and 89 control rod assemblies. The design of the fuel and the core complies with the practices applied in the existing large pressurised water reactors. The fuel assemblies are 17x17 assemblies typically used in existing large pressurised water reactors. Reactivity is managed during the operating cycle by means of boron contained in the reactor coolant and burnable absorbers contained in the fuel.

A so-called heavy reflector surrounds the reactor core to equalise power distribution and to improve fuel economy. The heavy reflector, which has been used for the first time at the Olkiluoto 3 plant unit currently under construction, is a cylindrical steel structure, which surrounds the reactor core and reflects leaking neutrons back into the reactor core to equalise power distribution and to protect the reactor pressure vessel against embrittlement caused by neutron flux.

The designed discharge fuel burn-up is higher than the maximum 45 MWd/kgU fuel assembly burn-up approved in Finland. However, the operation of the reactor can be designed to be consistent with the Finnish burn-up limit. If approval is sought for a higher burn-up, the applicant must provide experimental proof of the consistency of the fuel with the Finnish design criteria pertaining to accident conditions.

The design objectives and principles of the reactor and the fuel are consistent with Finnish requirements.

Main nuclear components

The material and structural design choices of the main components of the EPR plant are essentially consistent with the principles used at Olkiluoto 3. The reactor pressure vessel is welded of rotationally symmetrical forgings made of low-alloy steel using qualified methods, and the inside of the vessel is clad with stainless steel welded onto the surface. The requirements set forth 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. The heavy reflector included in the reactor internals reduces the neutron dose to which the reactor shell is exposed as well as radiation embrittlement. A monitoring programme based on normal practice is in place to monitor radiation embrittlement in the core area forgings and weld.

The solutions selected for the reactor pressure vessel are also applied where applicable to the manufacture of the steam generators and the pressuriser. 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 nickel-based Inconel 690 TT alloy, which according to current knowledge is a clearly more durable solution than earlier material choices.

The reactor coolant piping is made of welded stainless steel forgings with good ductility properties. On the other hand, this material choice results in the use of demanding dissimilar welds in connections to main components, which, based on current experiences, can be fully implemented. However, the monitoring of dissimilar welds during operation must be reviewed when applying for the construction licence.

The integrity of the primary circuit is secured by means of increased quality requirements that are consistent with the break preclusion (BP) concept for pipe breaks, which includes the application of the "leak before break" (LBB) principle based on Finnish safety requirements. In addition, the effect that a break in the reactor coolant pipe with the largest diameter would have on the safety systems is taken into account in the design and adequate protections are provided for such a break.

The design objectives and principles of the main nuclear components are consistent with Finnish requirements.

Pressure control of primary circuit

Pressure control of the primary circuit of the EPR plant is implemented by three safety valves. The diversity principle with respect to pressure control of the primary circuit is realised by the auxiliary spray system of the pressuriser using the pressure difference of the reactor coolant pumps.

The design objectives and principles of the systems involved in the pressure control are consistent with Finnish safety requirements.

Containment

The primary containment of the EPR plant is a so-called large dry containment built of pre-stressed reinforced concrete and provided with a tight steel liner. The containment is designed to maintain its integrity in compliance with acceptance criteria for transients and accidents. It is enclosed in a secondary concrete containment, which protects the primary containment against external threats.

N.B. This is an unofficial translation.

Original:
http://www.stuk.fi/ydinturvallisuus/ydinvoimalaitokset/suomen_ydinvoimalaitokset/-fi_FI/uudet_laitosyksikot/_files/82229809792876564/default/Alustava%20turvallisuusarvio_PAP-Foruton3_liite1_laitosvaihtoehdot.pdf
Severe accidents

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

The purpose of the depressurisation of the primary circuit is to prevent high-pressure discharge of core melt during reactor pressure vessel failure. At the EPR plant pressure can be reduced by means of two parallel depressurisation valves, which are independent of the other plant systems and discharge into the relief tank to be located in the containment. There are two valves in series in each discharge pipe. In accident conditions one of the lines is opened, which is enough to reduce pressure in the primary circuit to the design level. The power needed to open the valves is supplied from the electrical system for severe accidents, which is provided with battery backup.

Residual heat is removed with the containment heat removal system JMQ designed for severe accidents. The system is only used in severe accident management and not needed in design-basis accidents. The JMQ system consists of two redundant trains, with one train adequate to remove the residual heat released into the containment in an accident and to transfer the heat into the ultimate heat sink. Power to the containment heat removal system and the systems supporting it is supplied from the electrical system for severe accidents.

At the EPR plant core melt is cooled in the core melt spreading area located on the base level of the containment. The floor and the walls of the spreading are lined with thick iron elements provided with cooling ducts running in the bottom and rear part of the element. The floor elements are covered with a concrete layer designed to protect the elements at the melt discharge stage. After reactor pressure vessel failure, the core melt is first discharged into the reactor pit and then through the metal gate at the bottom of the pit and along a short tunnel into the spreading area. The core melt discharged into the spreading area opens the flood valves leading to the emergency cooling water pool. The coolant flows through these valves to the cooling ducts running under the floor elements and behind the wall elements of the spreading area and finally onto the core melt. The steam generated in the spreading area rises up into the dome part of the containment, where it is condensed using the containment heat removal system. No external power is needed to direct the core melt into the spreading area and to cool it with water taken from the emergency cooling pool.

A considerable amount of hydrogen is generated during a severe accident. This hydrogen pressurises the containment and, if present in high concentration, it may burn or detonate. The containment of pressurised water reactors is filled with air during operation, which means it contains oxygen needed for the combustion process. However, the large containment of pressurised water reactors, which is made of pre-stressed concrete, is quite strong against the effects of hydrogen burns and detonations.
The EPR plant will be equipped for the purpose of hydrogen removal with ca. 50 passive autocatalytic recombinators. The recombinators require no external power source and they remove hydrogen at such low levels that there is not enough time for a flammable gas mixture to be generated.

The EPR plant under construction in Finland is equipped with a filtered containment venting system called for in Finnish requirements. By means of that filter, non-condensable gases can be removed from the containment in the late phase of an accident, and the containment can be depressurised to the level of outdoor air.

The design objectives and principles of the severe accident management systems are consistent with Finnish requirements.

Safety functions and provisions for ensuring them (Gov. Decree 733/2008 Section 14)

At the EPR plant active systems are primarily used for the implementation of safety functions. Passive systems are used in some details, such as the reactor scram system and the pressure accumulators used at pressurised water plants in the emergency cooling system.

Reactivity management

EPR plant reactivity management is implemented actively by means of control rods, boron contained in the reactor coolant, and burnable absorber contained in the fuel.

In a transient situation, the reactor is shut down as in all other pressurised water reactors by dropping the control rods into the reactor core. The reactor scram system is passive in nature. The control rods drop into the reactor core by gravity after the reactor protection automation disconnects power supply to the electromagnets, which hold the control rods. The system realises the redundancy principle called for in the Government Decree.

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

Owing to the burnable absorber mixed in the fuel, the boron content of the primary coolant can be held relatively low even after fresh fuel has been loaded in the reactor. Despite the lower boron content of the primary coolant and the more effective scram, the possibility of the boron content of the coolant being erroneously diluted must be taken into account in the design of the reactor. The management of the so-called pure water slug in shutdown states, start-up situations as well as in transient and accident events has been taken into account in the design. The presented design meets the Finnish requirements.
The recriticality of the reactor in cooling situations is prevented by means of the control rods and the boron solution pumped by the medium-head safety injection system (JND).

The design objectives and principles of the safety functions associated with reactivity management are consistent with Finnish safety requirements.

Cooling of reactor

Cooling of reactor in shutdown conditions

In hot shutdown conditions, residual heat is removed from the reactor in the manner typical for pressurised water reactors through steam generators directly to the turbine condenser using the turbine bypass lines. If this is not possible, residual heat can be removed by pumping water into the steam generators by means of auxiliary feedwater system and blowing steam into the atmosphere by means of the secondary circuit dump valves. This is discussed later in conjunction with transients.

After the pressure and temperature of the primary circuit is reduced, residual heat is removed from the reactor by means of residual heat removal system RHR (4 x 100%), which uses the same pumps as the low-head safety injection system. The residual heat is transferred to the ultimate heat sink through the component cooling water system (CCWS, 4 x 100%) and the essential service water system (ESWS, 4 x 100%). These same systems are used as primary residual heat removal systems also in transient and accident conditions.

If the normal residual heat removal system (RHR) cannot be used in a situation where the reactor pressure vessel head is open, the normal residual heat removal system can be replaced by evaporating water into the containment for the first 24 hours and then transferring the residual heat into the atmosphere with the filtered containment vent system. Make-up water to the reactor is supplied from the IRWST by means of the JND system.

Cooling of reactor in accident conditions with reactor primary circuit intact

If a transient or an accident prevents normal residual heat removal to the turbine condenser, residual heat can be removed from primary circuit to atmosphere using the emergency feedwater system (EFWS, 4 x 100%) of the secondary circuit and the steam generator dump valves (MSDV). The auxiliary feedwater system is used to pump water from the auxiliary feedwater storage tank into the steam generators and the generated steam is then transferred to the atmosphere through the dump valves. The auxiliary feedwater system features four lines. The system can be used to bring the reactor into a controlled (hot shutdown) state and maintain it there for at least 72 hours.

N.B. This is unofficial translation.

Original:
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 also be removed directly from the primary circuit. This is done by pumping cold boron-containing water into the circuit by means of the medium-head safety injection system’s (JND) pumps from the IRWST, and by removing hot water from the circuit through the safety valves back to the IRWST (so-called feed and bleed cooling). Residual heat is removed further from the IRWST with the residual heat removal system RHR (4 x 100%). The residual heat is transferred to the ultimate heat sink by means of the component cooling water system (CCWS, 4 x 100%) and the essential service water system (ESWS, 4 x 100%).

In transient and accident conditions in which the reactor primary circuit is intact, the make-up water for the reactor and compensating for the volume decrease due to cooling is supplied primarily by means of the chemical and volume control system (KBA, mainly 2 x 100%).

Alternatively, make-up water can be supplied by means of the medium-head safety injection system (JND, 4 x 100%), which acquires the coolant from the IRWST-tank located inside the containment.

Cooling of reactor in loss of coolant accidents

In accidents where reactor coolant is lost as a result of a leak, the reactor can be cooled with reactor emergency cooling systems designed for this purpose.

Emergency cooling of the primary circuit at the EPR plant is implemented by means of the active medium-head safety injection system (JND, 4 x 100%) and the low-head safety injection system (JNG, 4 x 100%) as well as 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 of the secondary circuit. This system is 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. In order to secure the supply of cooling water into the reactor in case a common cause failure occurs in the systems supply can be diverted to the pipelines running to the hot leg and through there supplied to cool the reactor core. The pumps of the emergency cooling system take coolant from the in-containment refuelling water storage tank (IRWST) through suction strainers. The reactor cooling water that leaks into the containment is drained back into the IRWST. The suction strainers in the IRWSTs are designed so that loose debris produced in an accident or otherwise present in the containment will not clog the screens. The strainers are also equipped with a back-flushing system to account for clogging. Partial clogging of the suction strainers has also been appropriately taken into account in the determination of the required suction head of the safety injection pumps. The performance of the suction strainers has also been proven experimentally.
For small coolant leaks, the diversity principle with respect to emergency cooling is realised so that the primary circuit is cooled quickly by means of the relief valves of the secondary circuit or with the safety valves of the primary circuit, and the pressure in the primary circuit is reduced to a range where the JNG system and the safety injection accumulators can function. The JNG system can be replaced by the JND system. Cooling water for the systems are supplied from the IRWST.

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

The presented design for the systems associated with reactor core cooling and residual heat removal meets Finnish requirements at the principle level.

Removal of residual heat from containment

At the EPR plant, if necessary, residual heat can be removed from the containment in conjunction with a primary circuit or secondary circuit leak from the IRWST and into the ultimate heat sink through the component cooling water system (CCWS) and the essential service water system (ESWS).

When the reactor pressure vessel head is open, the normal residual heat removal system can be replaced by evaporating water into the containment for the first 24 hours and then transferring the residual heat into the atmosphere with the filtered containment vent system. Cooling water to the reactor is supplied from the IRWST with the JNG system.

The design objectives and principles of the systems associated with the removal of residual heat from the containment are consistent with Finnish safety requirements.

Containment isolation

The isolation of the pipelines penetrating the containment in transients and accidents is implemented, as a rule, by means of two isolation valves operating with different principles. An exception is the suction lines of the high-head injection system’s pumps that have an isolation valve outside the containment.

The design objectives and principles of the containment isolation function are consistent with Finnish requirements.

Loss of ultimate heat sink

N.B. This is unofficial translation.
In case the ultimate heat sink, i.e. the possibility to transfer residual heat via the turbine’s condenser or the essential service water system into the sea is lost when the reactor circuit is closed, residual heat can be removed from the reactor cooling circuit by pumping water with the emergency feedwater system into the secondary side of the steam generators and releasing the steam into the atmosphere. With this arrangement, the reactor can be kept in a controlled state for at least 72 hours.

When the reactor pressure vessel head is open, the normal residual heat removal chain can be replaced by evaporating water into the containment for the first 24 hours and then transferring the residual heat into the atmosphere with the filtered containment vent system. Cooling water to the reactor is supplied by the JNG system.

The design objectives and principles of the systems associated with the management of the loss of ultimate heat sink are consistent with Finnish requirements.

Cooling of fuel pools

The cooling of fuel pools is implemented with the fuel pool cooling system, which features two trains and two pumps in each train (FAK). The fuel pool is divided into two pools.

After all other options are gone, the cooling of the fuel pools could be implemented by removing residual heat by evaporating water in the pools. When pressure increases in the fuel building, the rupture disk breaks and steam is removed into the atmosphere through the ventilation stack. Make-up water for the fuel pools would be supplied from several alternative sources: fire water distribution system (SGB), the fuel pool purification system (FAL) or the demineralised water distribution system (GHC).

The design objectives and principles of the systems associated with the cooling of fuel pools are consistent with Finnish requirements.

Shutdown safety

The subcriticality of the reactor is ensured in all shutdown states by keeping the control rods inserted into the reactor and by adding boron solution with adequate concentration into the coolant water. The subcriticality of the reactor in shutdown states is monitored with neutron flux detectors positioned outside the reactor and with control procedures.

The safety valves of the primary circuit and the safety valves included in the residual heat removal system are used to prevent the cold pressurisation of the primary circuit.

The removal of residual heat from the primary circuit and the containment in an shutdown situation with the reactor pressure vessel head open or closed is implemented as described above in "Cooling of reactor".

N.B. This is an unofficial translation.
Original:
The presented design of the systems associated with shutdown safety is consistent with Finnish requirements at the principle level.

**Electrical systems**

The plant’s off-site power supply is realised through auxiliary transformers from the 400 kV grid or through two standby auxiliary transformers from the 110 kV grid.

In case off-site power supplies fail, on-site power to the safety systems of the plant is supplied alternatively from

- emergency diesel generators (4 x 100%)
- standby emergency diesel generators (2 x 100%), which realise the diversity principle
- batteries during the start-up of the emergency power sources (rated discharge time 2 h)

The severe accident management systems have their own separate battery sets (rated discharge time 12 h) to secure the supply of on-site power.

The design objectives and principles of the electrical systems are consistent with Finnish requirements.

**Civil engineering and fire protection**

The basic design of the buildings, the building engineering systems and fire protection is consistent with the Olkiluoto 3 plant unit. The design objectives and principles of civil engineering, building engineering systems and the fire protection concept are consistent with Finnish requirements.

**Protection against external events (Gov. Decree 733/2008 Section 17)**

The protection strategy of the EPR plant against the impact of a large commercial airplane is based on designing and constructing the containment, the fuel building and safeguard buildings 2 and 3 to withstand an airplane crash. Safeguard buildings 1 and 4 are located on either side of the reactor building, i.e. their protection is based on distance separation and shielding separation. The two pumping stations of the essential service water system are protected by distance separation. The emergency diesel buildings are also located on different sides of the complex consisting of the reactor building and the safeguard buildings and are thus protected through distance separation and shielding separation. The isolation valves of the main steam and feedwater systems are located on different sides of the reactor building in accordance with the principles of distance separation and shielding separation. The turbine building is not designed to be aircraft crash-resistant, as it contains no systems critical to safety functions.
The design objectives and principles of the presented implementation solution are consistent with Finnish requirements.

Protection against internal events (Gov. Decree 733/2008 Section 18)

Internal hazards such as floods and fires are taken into account in the room and layout planning of the plant by placing the four parallel redundancies of the key safety systems in different areas separate from each other. Most of the safety systems consisting of four subsystems are located in the four safeguard buildings. The main principle in the design of the EPR plant is to ensure that an initiating event taking place in one subsystem will not jeopardise the operation of the other subsystems. The rated fire resistance of the structures between the subsystems is two hours. Fire hazard and flooding analyses have been performed in the Olkiluoto 3 project on the basis of the detailed plant design of the EPR plant, and STUK has reviewed these as part of the review process during the construction stage.

The design objectives and principles of the presented implementation solution are consistent with Finnish requirements.

Monitoring and control of a nuclear power plant (Gov. Decree 733/2008 Section 19)

*Automatic safety functions*

EPR plant automation includes several different lines of defence based on the defence-in-depth principle. The first line comprises normal process automation, control systems and limiting systems. The second line consists of the protection system, which is the primarily operating system that initiates all safety functions, if necessary. The third line includes the safety automation system (SAS), which can initiate the most important safety functions, and another backup system operating according to a different principle (HBS, Hardwired Backup System). The last line comprises the severe accident management system.

The automation systems of the different defence lines aim to automatically maintain plant parameters within a safe range during operating transients and to limit the consequences of accidents.

The design objectives and principles of the systems are consistent with Finnish requirements.

*I&C redundancy principle*

The primarily operating protection system comprises four redundant subsystems. The protection function is actuated if two of the four redundant protection channels are activated. The hardwired backup system (HBS), the reactor control, surveillance and
limiting system (RCSL) included in process automation and the I&C critical to safety (SAS) also comprise four redundant subsystems.

The design objectives and principles of the systems are consistent with Finnish requirements.

_I&C separation principle_

Safety class-2 I&C systems are physically and functionally separated from components of other safety classes. Safety class-3 systems are functionally separated from other systems.

The severe accident management I&C and surveillance system is separated from the rest of the plant I&C.

The I&C systems of the different redundancies are physically and functionally separated from each other.

The design objectives and principles associated with I&C systems are consistent with Finnish requirements.

_I&C diversity principle_

The diversity principle has been applied to the reactor protection system of the EPR plant so that signals indicating various accident and failure situations are received alternatively on two different process parameters.

The automation of the plant is based on two computer-based system platforms. Protection, control and limiting functions are implemented on one platform and other I&C functions on the other platform.

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

The design objectives and principles of the systems are consistent with Finnish requirements.

_Control room_

The control room of the EPR plant contains control consoles and a display panel. The control consoles of the turbine operator and the reactor operator are used to control the plant in normal operating conditions, transient conditions and accident conditions. In

N.B. This is unofficial translation.

Original:
addition, all the information needed for the execution of the control actions is transmitted to the control consoles.

The display panel comprises fixed indicators, control switches and wide-screen display screens. The display panel is designed to present the status of the plant and the most important components as well as the most important alarm data. The display panel also features manual push-buttons based on hardwired technology for the control of the plant in case of a common cause failure in the digital I&C systems and in severe accidents.

The design objectives and principles of the control room are consistent with Finnish requirements.

**Emergency control room**

The EPR plant features an emergency control room, which can be used for control of all safety-critical systems independently of the main control room. The plant can be brought into a controlled (hot shutdown) state and further into a safe (cold shutdown) state from the emergency control room.

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

The design objectives and principles of the emergency control room are consistent with Finnish requirements.

**Summary**

The design objectives and principles of the plant alternative are consistent with Finnish safety requirements. The power of the tendered EPR plant has been increased by ca. 7 percent compared to Olkiluoto 3. The power increase affects the design of the plant's safety functions and the behaviour of the plant in transient and accident events. The effects of the power increase must be taken into account if an application for a construction licence is to be submitted.