Unofficial translation

PRELIMINARY SAFETY ASSESSMENT OF THE FENNOVOIMA OY NUCLEAR POWER PLANT PROJECT

APPENDIX 1: SUITABILITY ASSESSMENT OF THE AES-2006 PLANT ALTERNATIVE

INTRODUCTION

Fennovoima has signed a plant delivery contract with Rusatom Overseas CJSC on the AES-2006 nuclear power plant alternative. Fennovoima did not discuss the AES-2006 plant alternative in its application for a Decision-in-Principle dated January 14, 2009.

On September 23, 2013, Fennovoima requested the Radiation and Nuclear Safety Authority (STUK) to review reports concerning the plant project by virtue of Section 55 of the Nuclear Energy Act. The reports submitted by Fennovoima describe the changes that have taken place in the Fennovoima project since 2009 in terms of the matters that were discussed in STUK's preliminary safety assessment (9/J42211/2009). Fennovoima also requested STUK to review the reports in the extent that STUK observes when preparing a preliminary safety assessment as part of the Decision-in-Principle processes. Fennovoima later supplemented the material and submitted reports on the AES-2006 plant alternative on October 10, 2013. In connection with the technical reports on the plant alternative, Fennovoima submitted its own assessment of how the plant alternative fulfils the requirements presented in the Government Decree on the Safety of Nuclear Power Plants. Fennovoima's assessment of the safety of the AES-2006 plant alternative, dated October 8, 2013, was based on the draft decree dated August 26, 2013 and submitted to Fennovoima during a decree amendment process. The revised Government Decree on the Safety of Nuclear Power Plants (717/2013) entered into force on October 25, 2013.

STUK initiated the preparation of a preliminary safety assessment of the new plant alternative and submitted a request for clarification on the aforementioned reports on November 27, 2013. Fennovoima submitted additional reports on February 7, 2014 in response to the request for additional information..

On March 4, 2014, Fennovoima submitted to the Government an application for a supplementary decision on the nuclear power plant. The new decision would supplement the valid Decision-in-Principle issued in 2010, confirming that the Fennovoima project is still in line with the overall good of society, as set forth in Section 11 of the Nuclear Energy Act. Therefore, the Ministry of Employment and the Economy has submitted a request for a statement (TEM/11/08.04.01/2014) on March 6, 2014 and requested STUK to issue a preliminary safety assessment of the project outlined in the application under Section 12 of the Nuclear Energy Act. In its request for a statement, the Ministry requested STUK to especially focus on the changes that have taken place in the project. Furthermore, the Ministry reminded that STUK must append a statement from the Advisory Commission on Nuclear Safety to the safety assessment in accordance with the Nuclear Energy Act. The Ministry set a target deadline of May 25, 2014 for the preliminary safety assessment and the statement from the Advisory Commission.

The following is an assessment by STUK as to how the design objectives and design principles of the plant alternative presented in the application for a Decision-in-Principle comply with the Finnish safety requirements.

The preliminary safety assessment concerns the AES-2006 nuclear power plant equipped with a pressurized water reactor. The plant alternative employs both active and passive safety systems. An active system is a system based on components that rely on an uninterrupted external power source. A passive system is a system whose operation does not depend on operator action or an external power source apart from the actuating function (such as valve position change), or one that automatically switches to a state that is beneficial for safety in the event of a power loss. The component performing the actuating function must have a passive power source, such as an electrical battery or a pressure accumulator. The key data of the plant alternative are given in Table 1.

Table 1. Key data of the AES-2006 plant alternative.

Unit	Supplier	Type	Thermal output [MW_{th}]	Electrical output [MW_e]
AES-2006/V491	Rusatom Overseas CJSC	Pressurized Water Reactor	3,220	approx. 1,200

BASES FOR ASSESSING THE PLANT

The regulations concerning the safety of nuclear power plants are set forth on a general level in Government Decree 717/2013 and in more detail in the YVL Guides issued by the Radiation and Nuclear Safety Authority. The outset for the Radiation and Nuclear Safety Authority's preliminary safety assessment is that meeting the fundamental safety regulations laid down in the Government Decree means compliance with Section 6 of the Nuclear Energy Act. The following presents the requirements against which the power plant unit alternative was assessed.

Assessment and verification of safety (Government Decree 717/2013, Section 3)

Section 3 of the Decree lays down the requirements for the justifications to be presented for the safety of nuclear power plants and the technical solutions of their safety systems using experimental and analytical methods. Analytical methods include transient and accident analyses, analyses of internal and external hazards, strength analyses, failure resistance analyses, failure mode and effect analyses and probabilistic risk assessments (PRA).

The preliminary safety assessment verifies, with regard to the requirements laid down in Section 3 of the Decree, that the plant supplier employs deterministic and probabilistic analysis methods that have been appropriately qualified and that these models have been employed in earlier power plant projects. The assessment also studies how the plant supplier has substansiated the functionality of new, previously unused features through experimental methods.

Limitation of radiation exposure and of release of radioactive materials (Government Decree 717/2013, Sections 8–10)

Sections 8–10 of the Decree set forth the limits for the annual dose of an individual in the population during normal operation and in case of anticipated operational occurrences and accidents. The preliminary safety assessment addresses the question of whether the plant supplier employs appropriate analysis methods and compares the results of the analyses of the reference power plant to the set limits.

Prevention of accidents and mitigation of consequences (Government Decree 717/2013, Section 12)

Section 12 of the Decree presents requirements for implementing the operational defence-in-depth principle in the design, construction and operation of a nuclear power plant. The levels of defence shall be as independent of one another as is reasonably achievable. Carefully examined, tested, high quality technology that is empirically proven shall be employed at the defence-in-depth levels. The measures necessary to bring a situation under control or to prevent radiation hazards shall be planned in advance. The implementation of the defence-in-depth principle in the AES-2006 plant alternative is discussed in this preliminary safety assessment in connection with assessing how the requirements of Sections 13–14 and 17–18 of the Decree are met.

Engineered barriers for preventing the dispersion of radioactive materials (Government Decree 717/2013, Section 13)

Pursuant 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 fuel cladding, the primary circuit and the containment. These successive barriers implement what is known as the defence-in-depth principle.

On the one hand, the preliminary safety assessment addresses the prerequisites for manufacturing high-quality dispersion barriers that reliably maintain their integrity and leaktightness. On the other hand, it is assessed whether the design bases of the safety functions of the plant take sufficiently into account all the circumstances in which the mechanical and thermal loads on the dispersion barriers must remain within the design limits.

Safety functions and provisions for ensuring them (Government Decree 717/2013, Section 14)

In order to prevent accidents and to mitigate the consequences thereof, a nuclear power plant shall have the systems to shut down the reactor and maintain it in a subcritical state, to remove the residual heat generated in the reactor, and to retain radioactive materials within the plant. The principles of redundancy, separation and diversity shall be applied in the design of these systems in order to ensure the implementation of the safety function even in the event of malfunctions. It is important to consider these principles early on in the design process of the plant because im-

plementing them through changes made later would be extremely difficult and demanding.

The redundancy principle refers to the implementation of systems necessary for the safety functions using several parallel subsystems so that the system will be able to function as required even if individual subsystems are out of operation due to maintenance, failure or other reasons. Multiple redundancy must also be provided for the essential support functions of the safety system components in similar fashion. Furthermore, a nuclear power plant shall have on-site and off-site electrical power supply systems for anticipated operational occurences and accidents. It shall be possible to supply the electrical power needed for safety functions using either of the two electrical power supply systems. An off-site power source refers to a connection to the normal power grids, while an on-site power source refers to substituting power sources.

In accordance with the aforementioned principle of redundancy, it shall be possible to execute the main safety functions necessary to switch to, and remain in, a controlled state in which the reactor is shut down and the removal of residual heat is secured, even if any single component of a system related to the function is inoperable and even if any other component of a system related to the execution of the same safety function or a component of a support or auxiliary system necessary for the operation of the system, is simultaneously out of use due to repair or maintenance. Furthermore, the impacts of common cause failures must remain minimal.

The separation principle refers to the implementation of physical separation and functional isolation in the design of the nuclear power plant. Physical separation refers to separating systems or components from one another by means of adequate barriers, distance or location or combinations thereof. Functional isolation refers to the isolation of systems from one another so that the operation or failure of one system does not adversely affect another system; functional isolation also includes electrical isolation and the isolation of information processing between systems. Following the separation principle provides for protection against internal and external hazards to the power plant.

Diversity principle refers to securing the safety functions through systems or components that are based on different operating principles or that are otherwise different from one another, which can implement the function individually. Following this principle improves the reliability of the safety function and avoids the consequences of common cause failures that are related to the safety function in question.

The nuclear power plant shall have the necessary components and procedures for securing the removal of residual heat from the spent fuel in the reactor and storage pools for a period of three days independently of the off-site supply of electricity and water in a situation caused by a rare external event or a disruption in the on-site electrical distribution system.

The plant shall be equipped with systems to control and monitor severe reactor accidents. These systems shall be independent of the systems designed for normal opera-

tion, anticipated operational occurrences and postulated accidents. The systems necessary to ensure the leaktightness of the containment in a severe reactor accident shall be capable of performing their safety functions even in the event of a single failure.

Protection against external events (Government Decree 717/2013, Section 17)

Section 17 of the Decree lays down the requirements for how the safety functions of a nuclear power plant must be protected against external events. External events may compromise the integrity of the systems, structures and components related to safety functions, cause a transient or an accident or prevent safety functions from being executed. Such events include various weather phenomena (high or low temperatures, high winds, blizzards), earthquakes, high sea level (flooding) and illegal activities undertaken in order to damage the plant, including a large commercial airliner crash. According to the requirement laid down in the Decree, the systems, structures and components shall be designed, located and protected so that the external events that are deemed possible have a minimal impact on plant safety. Here, it is assessed how the aforementioned events have been taken into consideration in plant design.

Protection against internal events (Government Decree 717/2013, Section 18)

Similarly to how Section 17 of the Decree lays down the arrangements for protection against external events, Section 18 of the Decree specifies how the systems, structures and components that are related to the safety functions must be designed, located and protected so as to minimise the probability of internal events and their impact on plant safety. The operability of the systems, structures and components shall be demonstrated in their design basis interior ambient conditions. Internal events include fires, flooding, explosions, electromagnetic radiation, pipe breaks, container breakage, falling of heavy objects, and missiles resulting from explosions and component failures. Here, it is assessed how the aforementioned events have been taken into consideration in plant design.

Monitoring and control of nuclear power plants (Government Decree 717/2013, Section 19)

Section 19 of the Decree sets out the requirements for the protection I&C systems, control room, emergency control room and local control systems of a nuclear power plant. Here, the implementation of the requirements of Section 19 and the principles of redundancy, separation and diversity laid down in Section 14 are assessed with regard to the essential I&C systems.

PLANT ALTERNATIVE AES-2006/V491 EQUIPPED WITH A PRESSURIZED WATER REACTOR

General

The AES-2006 is a pressurized water reactor with an output of approximately 1,200 MW_e marketed by the Russian Rusatom Overseas CJSC company. There are two different development versions of the AES-2006 plant: AES-2006/V392M and AES-

2006/V491. This preliminary safety assessment discusses the AES-2006/V491 development version presented in Fennovoima's application.

The AES-2006 is based on the VVER 91/99 plant, which is developed from the operating VVER-1000 plants. Plants of the VVER type have been constructed in Russia and many other countries for more than 30 years. The Loviisa 1 and 2 plant units are based on the VVER-440 plant type. A reference plant of the Fennovoima plant alternative is the Leningrad NPP-2, which is currently under construction in Russia. The Leningrad NPP-2 comprises two plant units, which, together with the Novovoronesh-2 plant unit (AES-2006/V392M), are the first AES-2006 type plants in Russia. In Russia, one more unit is under construction in Kaliningrad (AES-2006/V491) in addition to the Leningrad NPP-2 plant units. The construction of the Leningrad NPP-2 was started in 2008. The design service life of the plant is 60 years.

The safety functions of the AES-2006 have been improved compared to the VVER-91/99. The safety functions are mainly implemented by means of active systems and supplemented, as is typical with pressurized water reactors, with pressure accumulators. The AES-2006 plant's new passive systems for removing residual heat during disturbances and accidents are the residual heat removal system that is connected to the steam generators for cooling the primary circuit and the passive containment residual heat removal system. Both of these are based on natural circulation. The AES-2006 also features severe accident management systems. The basic design of the plant is at an advanced level. The design objectives and design principles mainly comply with the Finnish safety requirements.

The primary circuit of the AES-2006 plant consists of four main circuits, each with a horizontal steam generator and a main circulation pump. The technology of the steam generators of the plant is equivalent to the steam generators currently in use at the VVER-440 plants in Loviisa, and the operating experiences on this steam generator type are mainly positive. The secondary circuit is essentially the same as in the existing VVER type pressurized water reactors.

ASSESSMENT AND VERIFICATION OF SAFETY (GOVERNMENT DECREE 717/2013, SECTION 3)

Deterministic analysis methods and preliminary results

For the assessment and verification of the safety of the AES-2006 plant, the plant supplier employs analysis methods that have been maintained and qualified for their purpose of use. The methods have been used during the design and construction of currently operating VVER plant units. The analyses conducted on the AES-2006 plant indicate that transient and accident analyses compliant with the Finnish requirements can be performed for this plant alternative. The fulfilment of the Finnish requirements shall be assessed in the construction licence phase.

Probabilistic assessments

A probabilistic risk assessment will be conducted in connection with the detailed design of the plant. The licensee shall submit the probabilistic risk assessment (PRA)

for the design phase to STUK when applying for a construction licence and the PRA for the final design when applying for an operating licence.

The plant supplier employs internationally known and generally used probabilistic risk assessment methods for level 1 (reactor core damage) and level 2 assessments (release of radioactive materials into the environment). These methods have been used to conduct a level 1 PRA for the AES-2006 plant. An assessment of the reference plant covers the most important initiating events in all operational states of the plant. The analysis methods and the information concerning the PRA conducted on the reference plant indicate that probabilistic assessments can be conducted on the plant alternative in compliance with the Finnish requirements. When processing the construction licence applications, STUK assesses whether the PRA is sufficient and in compliance with the related Finnish requirements.

Qualification of new types of systems

New passive systems have been designed for the AES-2006 plant. The new systems to be used during disturbances and accidents are the residual heat removal system that is connected to the steam generators for cooling the primary circuit and the passive containment residual heat removal system. Both of these are based on natural circulation. Experimental substansiation of the functionality of the new passive systems is a prerequisite for their approval. Calculation methods and testing on different test equipment have been used to ensure the functionality and design of the systems. The results of such tests have been used for the qualification of the calculation models. The proper functioning and the sufficiency of the tests and qualifications completed can only be verified when the test results are available. The fulfilment of the Finnish requirements shall be assessed in the construction licence phase.

LIMITATION OF RADIATION EXPOSURE AND OF RELEASE OF RADIOACTIVE MATERIALS (GOVERNMENT DECREE 717/2013, SECTIONS 8–10)

The plant supplier has provided results of the population radiation dose analyses required for the AES-2006 plant.

According to the plant supplier's estimate, the radiation dose to the population surrounding the Hanhikivi plant site as a result of the normal release of radioactive materials by the AES-2006 plant would not be higher than the actual dose to the population surrounding the currently operating Finnish nuclear power plants. In this case, the values would clearly be below the limit set for the radiation exposure of the population specified in Section 8 of Government Decree 717/2013.

In terms of anticipated operational occurrences and postulated accidents, the results are clearly below the limits for the radiation exposure of the population specified in Sections 9–10 of Government Decree 717/2013.

A reference plant of the AES-2006 has also undergone design extension conditions radiation dose analyses. The results are below the limit value specified in Section 9 of

Government Decree 717/2013, but the situations analyzed are not entirely in compliance with the Finnish requirements. A large commercial airliner crash has not been analyzed. The fulfilment of the Finnish requirements shall be assessed in the construction licence phase.

The results of the design basis severe accident analyses conducted on the reference plant of the AES-2006 are below the emission limit set for Cs-137 specified in Section 10 of Government Decree 717/2013, and there is no need for large-scale population protection measures. No analysis results were obtained on the probability of a release at an early stage of a severe accident that would require population protection measures. This probability shall be extremely low.

Full population radiation dose analyses for normal operation, anticipated operational occurences and accidents shall be submitted to STUK in connection with the construction licence application. STUK will review them utilising reference analyses that STUK conducts or commissions, as necessary.

Based on the analysis results and the design features of the plant concept presented in the Decision-in-Principle phase, population radiation dose analyses that are in compliance with the Finnish requirements can be conducted on the AES-2006. The fulfilment of the Finnish requirements shall be assessed in the construction licence phase.

PREVENTION OF ACCIDENTS AND MITIGATION OF CONSEQUENCES (GOVERNMENT DECREE 717/2013, SECTION 12)

The implementation of the defence-in-depth principle in the AES-2006 plant alternative is discussed in connection with assessing compliance with the requirements of Sections 13–14 and 17–18 of the Decree.

ENGINEERED BARRIERS FOR PREVENTING THE DISPERSION OF RADIOACTIVE MATERIALS (GOVERNMENT DECREE 717/2013, SECTION 13)

Reactor and fuel

In the AES-2006 plant, the reactor essentially has the same structure as the VVER-1000 plants that are currently in operation. Due to the higher output, the active length of the fuel assemblies has been increased so as to maintain the same maximum fuel load. The fuel design and core design follow the same practices as the large pressurized water reactors that are currently in operation. The plan is to load fuel into the core every 12 months by replacing one quarter of the assemblies loaded with fresh assemblies.

The number of control rods has also been increased in order to improve safety. The core of the AES-2006 has 121 control rods. The rods use boron carbide and dysprosium titanate as neutron absorbing material. Reactivity is managed during the operation period using boron in the primary coolant, control rods and burnable absorbers

in the fuel (Gd2O3). The use of burnable absorbers reduces the need for a high boron concentration at the beginning of the operation period.

Hexagonal fuel assemblies, which are typical of VVER reactors, are used as fuel. There are 163 fuel assemblies in total in the core, each of which has 312 fuel rods. The fuel rod assemblies are equipped with a foreign material sieve in order to prevent foreign material damage.

In connection with the plant delivery contract, Fennovoima signed a separate contract on the procurement of nuclear fuel including the initial core loading and the reloading in the first operation period. Currently, the only manufacturer of fuel for the AES-2006 reactor is the Russian TVEL company.

Fennovoima has stated that it is negotiating on the use of reprocessed uranium, which is obtained from spent fuel, as a source of uranium. The source for uranium does not affect the behaviour of the fuel in the reactor.

In reprocessed uranium, the concentration of the fissile U-235 isotope (0.5–1.0%) is close to that of natural uranium (0.7%). With both sources, the U-235 concentration must be enriched to a level of approximately 4% for use as reactor fuel. Reprocessed uranium contains small amounts of the U-236 isotope, which has a negative impact on reactivity. Therefore, any fuel manufactured from reprocessed uranium must have a slightly larger U-235 concentration than fuel that is manufactured from natural uranium.

Furthermore, reprocessed uranium contains small amounts of the U-232 isotope, the decay chain of which generates high-energy gamma radiation. Due to U-232, radiation protection must be taken into account in fuel fabrication and storage at the plant. The fresh fuel manufactured from reprocessed uranium must be stored in a water tank at the plant, whereas fresh fuel manufactured from natural uranium can be stored in a dry storage. An appropriate storage system shall be built at the plant.

The design objectives and design principles of the reactor and fuel comply with Finnish safety requirements. The acceptability of the nuclear fuel design shall be demonstrated before the manufacture of the fuel is started by submitting a fuel type-specific suitability report to STUK for approval.

Main nuclear components

The material and structural solutions of the main nuclear components of the AES-2006 utilize approximately 30 years' operating experience of VVER-1000 reactors. The reactor pressure vessel is manufactured of modern pressure-grade steel, which is typical of the reactor type. Forged objects made of such steel are welded into a pressure vessel using known and qualified methods. The inside of the pressure vessel is lined with welded stainless steel. The internal parts of the reactor pressure vessel are manufactured with stainless steel and other materials that are suitable for their purpose of use.

Material choices for the main components and monitoring of operation takes the typical ageing phenomena into consideration. Radiation embrittlement of the reactor pressure vessel core area has been taken into account, and it is monitored with a radiation embrittlement monitoring programme. Attention shall be paid to the analysis requirements (P, Cu and Ni) for the steel for used in the reactor pressure vessel, 15Х2НМФА class 1, 15Х2НМФА and 15Х2НМФА-А, in order to keep the radiation embrittlement of the pressure vessel core area within the allowed range during the 60-year service life. Radiation embrittlement shall be assessed at the later phases of the licence application process, as well as during the operation of the plant. Furthermore, it is the opinion of STUK that detailed examinations concerning the radiation embrittlement of the pressure vessel steel should be started already at the design phase of the plant.

The other main components, such as the steam generators and the pressurizer, shall be manufactured similarly to the reactor pressure vessel. The heat transfer tubes of the steam generators are of stainless steel, which has been found to be a reliable solution in these plants when coupled with good water chemistry monitoring. The damage identified previously of the collector weld joints in the steam generators of VVER-1000 plants have been addressed in the new steam generator type intended for the AES-2006 through material selections.

The primary coolant piping is manufactured from low-alloy pressure equipment steel, which is lined on the inside with stainless steel. Therefore, demanding dissimilar metal joints are not needed between the main nozzles of the primary circuit and the primary coolant piping. Several smaller pipes for auxiliary and emergency systems are welded on the primary coolant circuit pipes. Verifying the integrity of the weld joints may pose a challenge in connection with processing the strength and ductility analyses, as well as the in-service inspections and the implementation of the related radiation protection objectives. Attention shall be paid to this matter in the construction licence phase.

The Leak Before Break principle (LBB) shall be applied in the design of the primary coolant piping. This eliminates the postulated break of a design basis pipe with the highest diameter. However, the potential break has been taken into consideration in the design of the safety injection systems and the containment. The procedure presented is not fully in compliance with the Finnish requirements; a complete break of the largest primary pipe shall be analyzed as a design extension condition. The analysis requirement pertains to the internal parts of the reactor and its support structures, fuel, heat transfer tubes of the steam generator and the flywheel mass of the reactor coolant pump of the pressurized water reactor. Furthermore, taking into account the dynamic effects of primary coolant circuit pipe breaks and break preclusion (BP) requires additional clarifications, especially if no whip restraints are to be installed in the primary circuit.

The design objectives and design principles of the main nuclear components of the AES-2006 are mainly in compliance with the Finnish safety requirements. The effects that the reactor pressure vessel material and especially its nickel alloys and impurities have on radiation embrittlement and the radiation embrittlement rate requires

additional clarifications that shall be described in the construction licence application. If the manufacture of the reactor pressure vessel is started before the construction licence is issued, the matter shall be described in the construction plan, which shall be submitted to STUK in accordance with Section 55 of the Nuclear Energy Act. In this connection, a statement is required on how the plant is to be operated in order to minimize embrittlement. A clarification on the effects that postulated, sudden pipe breaks of the primary coolant circuit have on the durability of the internal parts of the reactor, and a clarification on the implementation, inspection and radiation protection principles of the primary coolant circuit nozzles, are required in the construction licence phase.

Pressure control in the primary circuit and the secondary circuit

During normal operation, the primary pressure is controlled using the thermal resistors of the pressurizer and by means of spraying. The pressurizer can be sprayed using the reactor coolant pumps (normal operation), volume control system or the boron injection system pumps.

Overpressure protection of the AES-2006 primary circuit shall be ensured by three safety/blowdown valves in the pressurizer. The valves that are necessary to limit pressure are opened by a pneumatic pilot valve, which is controlled by the reactor protection I&C systems, or in direct response to reactor pressure against a spring load. There are two spring-loaded pilot valves per one safety valve. The diversity principle of the overpressure protection of the primary circuit is proposed to be met through pressurizer spraying using either the volume control system or the boron injection system pumps depending on the operational state of the plant.

Overpressure protection in the secondary circuit shall be ensured using safety and blowdown valves in the pressurizer. The live steam system features an overpressure protection system for the secondary circuit.

The design objectives and design principles of the systems participating in pressure control comply with the Finnish safety requirements. The suitability of pressurizer spraying for implementing the diversity principle in the primary circuit overpressure protection as well as the detailed implementation of the safety valves and relief lines shall be assessed in the construction licence phase.

Containment

The primary containment of the AES-2006 plant is a so called 'large dry containment made of pre-stressed reinforced concrete and provided with a sealing steel liner. It is designed to maintain its leaktightness in compliance with its acceptance criteria even in case of a anticipated operational occurence or an accident. A secondary concrete containment is designed around the primary containment to protect it against external hazards.

The top of the outer containment features the space for the water tanks of the passive residual heat removal systems of the inner containment and the primary circuit

steam generators. The pipes of the water tanks penetrate the inner pre-stressed protective shell in the dome area. The design of these penetrations and the tendon system of the protective shell is a demanding task. The detailed design principles and analyses will be reviewed in the construction licence phase.

Severe accidents

The primary objective of the severe accident management strategy of the AES-2006 plant is to prevent accidents resulting in core meltdown. In case an accident leads to core meltdown and the failure of the reactor pressure vessel, the purpose of the strategy is to retain and cool the molten core in the core catcher, and to ensure the integrity of the containment and to limit releases. The functions relevant in terms of the strategy objectives include pressure management and the removal of residual heat in the containment, sufficient heat removal from the core catcher, the prevention of a high-pressure melt discharge in the event of a pressure vessel failure, and the elimination of steam and hydrogen explosions.

In a severe accident, it shall be possible to sufficiently decrease the primary circuit pressure before the pressure vessel fails in order to avoid a high-pressure melt discharge that would compromise the integrity of the containment. According to the designs concerning the AES-2006 plant, the decrease of the primary circuit pressure is ensured in the event of severe accidents with the safety/blowdown valves of the pressurizer and the emergency gas removal system. The solution is not in compliance with the Finnish safety requirements, because the systems designed for managing severe accidents shall be independent of the systems that are designed for the operational conditions and postulated accidents of the plant. In accordance with the Finnish requirements, the plant shall be equipped with independent valves that are intended for pressure reduction.

The AES-2006 plant is equipped with a core catcher under the reactor pressure vessel, which retains and cools the molten material (core melt, the molten reactor internals, and the molten bottom structures of the pressure vessel) and maintains it in a subcritical state. The core catcher operates passively without an external power source. The core catcher will be cooled from the outside by flooding the reactor pit with boron water from the coolant tank located inside the containment. Furthermore, water from the reactor internals inspection shaft is injected into the core catcher from above. The steam generated in the core catcher is guided to the dome section of the containment, where it is condensed by the passive containment residual heat removal system. The condensate flows back to the reactor pit and cools the core catcher. The core catcher of the AES-2006 has been developed based on the previous solution used at the VVER-91 plant, and its functionality has been verified with an extensive test programme. The scope of the test programme will be ensured in the construction licence phase.

Long-term residual heat removal from the containment takes place by the passive containment residual heat removal system. The system includes heat exchangers on the containment walls, through which the system transmits heat to the water pools on top of the containment and from there into the atmosphere. In the system, water

flows by the force of gravity from the pools to the condensers installed in the top space of the containment. Water vaporizes inside the condenser pipes and rises back to the pool via the return pipe. There, some of the vapour re-condenses to water, while some is released into the atmosphere. The water pools on the roof of the containment are also shared by the steam generator passive residual heat removal system. The water in the pools is sufficient for removing residual heat for 24 hours, after which they must be refilled from the storage tank located outside the containment. The passive containment residual heat removal system has four redundant subsystems whose rated capacity meets the Finnish requirements. In accordance with the Finnish requirements, the systems that are necessary for ensuring the leaktightness of the containment in the event of a severe reactor accident shall be capable of performing their safety functions even in the case of a single failure.

During a severe accident, a substantial amount of hydrogen is generated, which pressurizes the containment and may combust or explode in large quantities. The containment hydrogen management and removal systems are designed to prevent the formation of a dangerous hydrogen concentration in the containment. The hydrogen removal system of the AES-2006 plant containment is based on passive autocatalytic recombiners that do not require a power source and that remove hydrogen in such low concentrations that a combustible gas mixture cannot be generated. The dimensioning of the systems ensures that the hydrogen concentration remains on a safe level throughout the accident.

The suitability report did not discuss the procedure for reducing the pressure of the containment in order to reach a long-term safe state following a severe accident. In accordance with the Finnish requirements, it shall be possible to sufficiently decrease the pressure in the containment after a severe accident so as to ensure that the leak from the containment is minor, even if the containment is not completely leaktight. At several operating nuclear power plants, the function can be implemented by a filtered relief system of the containment. The YVL Guides do not necessarily require that the function be implemented using a filtered relief system of the containment, if another solution is in place which is in compliance with the Finnish requirements. The implementation of the function at the AES-2006 plant shall be specified in connection with the construction licence application.

The systems and strategy for managing severe accidents at the AES-2006 plant are not entirely in compliance with the Finnish safety requirements. According to the Finnish requirements, the systems that are designed for managing severe accidents shall be independent of the systems designed for managing the normal operational conditions, anticipated operational occurrences and postulated accidents of the plant.

STUK finds that it is possible to implement the systems and strategy for managing severe accidents in compliance with the Finnish safety requirements. The implementation of the functions for severe accidents by independent systems in compliance with the Finnish requirements shall be verified in the construction licence phase.

SAFETY FUNCTIONS AND PROVISIONS FOR ENSURING THEM (GOVERNMENT DECREE 717/2013, SECTIONS 12 AND 14)

In the AES-2006 plant, both active and passive systems are used for the implementation of safety functions. As with all other pressurized water reactors, passive systems are employed in the control rods used to achieve a reactor scram and in the pressure accumulators. The new passive systems that will be used during disturbances and accidents are the residual heat removal system that cools the reactor circuit via the steam generators and the passive containment residual heat removal system. Both of these are based on natural circulation.

Reactor reactivity management

In the AES-2006 plant, reactivity is managed using control rods, boron in the primary coolant and burnable absorbers in the fuel. In the normal operation of the reactor, reactivity is controlled by adjusting the boric acid concentration of the coolant.

In case of a transient, the reactor is shut down by releasing the control rods into the reactor core. The reactor scram system is a passive system. The control rods drop into the reactor core by the force of gravity once the protection I&C system of the reactor disconnects the power to the electromagnets holding the rods. The reactor core of the AES-2006 has 121 control rods. The rods use boron carbide and dysprosium titanate as neutron absorbing material.

The control rods are able to stop the reactor and maintain it in a subcritical state even if it is assumed that the most effective rod is inoperable. Therefore, the system fulfils the principle of redundancy required in the Government Decree. Due to the high number of control rods, the re-criticality temperature of the reactor in the event of a cooling accident is exceptionally low, at approximately 100°C. This characteristic is beneficial in terms of managing anticipated operational occurences and accidents that result in inadvertent cooling.

With regard to reactor shut-down, the diversity principle is implemented with a boron injection system. The boron injection system comprises four redundant subsystems. Two subsystems are enough to stop the reactor and maintain it in a subcritical state even if it is assumed that the control rods are inoperable.

The burnable absorbers in the fuel (Gd_2O_3) absorb neutrons and reduce the need for maintaining a high boron concentration of the primary coolant at the beginning of the operation period. The Gd_2O_3 concentration of the fuel shall be selected such that it is fully consumed during the first year of operation of the fuel.

The design objectives and design principles of the safety functions related to reactivity management comply with the Finnish safety requirements. However, the plans presented for the sudden dilution of the boron concentration in the primary circuit, for example, shall be supported with supplementary analyses and/or tests in the construction licence phase.

Cooling of the reactor

Cooling of the reactor during shutdowns

In a hot shutdown, residual heat is removed from the reactor through the steam generators directly into the turbine condenser using the turbine bypass lines, as is typical for pressurized water reactors. If this is not possible due to a disturbance, the residual heat may be removed by pumping water into the steam generators through four redundant emergency feed water subsystems and by venting the steam into the atmosphere through the blowdown valves in the secondary circuit.

After lowering the pressure and temperature in the primary circuit, the residual heat is removed directly from the primary circuit using a residual heat removal system that uses the same pumps as the low head safety injection system. The residual heat is removed through the intermediate cooling system and the seawater system to the ultimate heat sink. The systems comprise four subsystems, each of which is capable of implementing the function required of the system. These systems are also used as the primary residual heat removal systems in transient and accident conditions.

During shutdowns where the pressure vessel is open and the residual heat removal system is unavailable due to a disturbance, the residual heat can be removed from the reactor using the passive containment residual heat removal system that is based on natural circulation. In this case, the residual heat is removed from the reactor by vaporizing water into the containment and conveying the heat further into the atmosphere through the condensers of the passive containment residual heat removal system and the water pools that are located outside the containment. The pools are also used by the steam generator passive residual heat removal system. Starting the passive containment residual heat removal system does not depend on the functionality of any active component. The system is capable of removing residual heat from the reactor for 24 hours after an accident without operator intervention. Further measures can extend this time to 72 hours at minimum by pumping water from the storage tanks of the make-up water system into the water pools of the passive containment residual heat removal system. Compliance with the Finnish requirements, especially in terms of sufficient make-up water storage in the event of a prolonged disturbance as well as the independence of the systems, shall be assessed in the construction licence phase.

The cooling water for the reactor is provided by the make-up water system of the primary circuit from the make-up water tank or by the low head safety injection system from the coolant tank inside the containment.

Cooling of the reactor during accidents when the reactor primary circuit is intact

If a transient or an accident prevents the normal removal of residual heat to the turbine condenser, the residual heat can be transferred from the primary circuit into the atmosphere using the emergency feed water system of the secondary circuit and the blowdown valves of the steam generator. The emergency feed water system pumps water from the emergency feed water tank to the steam generators, and the resulting

steam is vented outside through blowdown valves. Each of the four subsystems of the emergency feed water system have sufficient pumping capacity to implement the safety function of the system. This system enables the reactor to be brought into a controlled (hot shutdown) state and kept there for at least 24 hours. Further measures may extend this time to 72 hours at minimum, by pumping water from the alternative storage tank into the emergency feed water tank. Compliance with the Finnish requirements, especially in terms of sufficient make-up water storage in the event of a prolonged disturbance as well as the independence of the systems and operational reliability for three days, shall be assessed in the construction licence phase.

Alternatively, the residual heat can be transferred into the atmosphere using the steam generator passive residual heat removal system. The safety function can be implemented with three out of the four subsystems. The steam generator passive residual heat removal system can remove the residual heat from the reactor into the atmosphere via steam generators and the heat exchangers that are located in the water pools outside the containment for 24 hours without operator intervention. The system enables bringing the reactor into a controlled state (hot shutdown). Compliance with the Finnish requirements, especially in terms of sufficient make-up water storage in the event of a prolonged disturbance as well as the independence of the systems and operational reliability for three days, shall be assessed in the construction licence phase.

In case of a disturbance or an accident where the reactor primary circuit is intact, the make-up water to compensate for lower volume due to cooling is primarily pumped into the reactor using the normal make-up water system of the primary circuit. Alternatively, the make-up water can be obtained from the high head safety injection system, which takes its make-up water from the cooling water tank inside the containment.

The passive residual heat removal systems are also capable of cooling the reactor independently of off-site power and water supply, which is required in Section 14(7) of Government Decree 717/2013. In addition to this, the residual heat removal system of the containment can act as a heat sink if the fuel pool cooling is lost. STUK finds that the requirement can be met through technical solutions, and the matter can be reviewed in the construction licence phase. In connection with this, it is also necessary to process the capability of the essential systems to function in an event caused by a rare external event or a disruption in the on-site electrical distribution system.

The plant supplier proposes the use of a new system for events where the normal residual heat removal systems in the safeguard building or cooling via the primary circuit are unavailable. Using the feed water pumps, the system recirculates the water that has been cooled by the intermediate cooling system of the turbine building to the steam generators via the feed water tanks. The necessary make-up water is obtained from the make-up water tank. The assessment requires more detailed information. The issue will be processed in the construction licence phase.

Cooling of the 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 the safety injection systems that have been designed for this purpose.

In the AES-2006 plant, the emergency cooling of the primary circuit is implemented with four safety injection accumulators as well as an active high head safety injection system and a low head safety injection system, both of which comprise four redundant subsystems. The pumps of the safety injection systems obtain the coolant from the coolant tank inside the containment through suction strainers. Any reactor coolant that leaks into the containment is drained back into the tank. The structure and design bases of the suction strainers are not presented in the material. The suction strainers shall undergo tests in compliance with the Finnish requirements. However, STUK finds that the safety injection systems can be implemented in compliance with the Finnish requirements through verifiable technical solutions. The issue will be reviewed in the construction licence phase.

With regard to the safety injection system described above, the principle of diversity is ensured in small coolant leaks by decreasing the pressure in the primary circuit, for example with the relief valves of the steam generators, low enough to reach a level at which the low head safety injection system and the pressure accumulators can function.

Residual heat is removed from the reactor using a residual heat removal system that uses the same pumps as the low head safety injection system. The residual heat is removed through the intermediate cooling system and the seawater system into the ultimate heat sink.

The design objectives and design principles of the systems related to the cooling of the reactor core and the removal of residual heat comply with the Finnish safety requirements.
In the construction licence phase, it must also be ensured that the Finnish requirements are met in terms of the auxiliary and support systems that are necessary for the function.

Removal of residual heat from the containment

In the AES-2006 plant, the removal of residual heat from the containment in the event of an anticipated operational occurence or an accident is implemented with an active containment spray system for removing residual heat through the intermediate cooling system and the seawater system into the ultimate heat sink.

With regard to residual heat removal, the diversity principle is implemented by the passive containment residual heat removal system, which removes residual reactor heat from the containment into the atmosphere via water pools that are located outside the containment. Starting the system does not require an external power source. The water pools of the system are also shared by the steam generator passive residual heat removal system. The passive containment residual heat removal system is

capable of removing residual heat for 24 hours after an accident without operator intervention.

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

Containment isolation

The containment isolation of the AES-2006 plant is presented to be implemented in each pipeline that penetrates the containment using two isolation valves that operate on different principles. As planning advances, more information will be needed, for example, on the power supply and control of the isolation valves.

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

Loss of the ultimate heat sink

If the ultimate, primary heat sink, i.e. the possibility of removing residual reactor heat through the turbine condenser or seawater system into the sea, is lost while the reactor circuit is closed, residual heat may be removed from the reactor cooling circuit by pumping water into the secondary side of the steam generators through the emergency feed water system and by venting the resulting steam into the atmosphere. This enables the reactor to be brought to a controlled state and kept there for at least 24 hours. Compliance with the Finnish requirements, especially in terms of sufficient make-up water storage in the event of a prolonged disturbance, as well as the independence of the systems and operational reliability for three days, shall be assessed at the construction licence phase.

Alternatively, residual heat can be removed from the reactor into the atmosphere using a steam generator passive residual heat removal, which can function for 24 hours after an accident without operator intervention. Further measures may extend this time to 72 hours at minimum, by pumping water from the alternative storage tanks into the water pools. The cooling water for the reactor is provided by the make-up water system of the primary circuit from the make-up water tank or by the low head safety injection system from the cooling water tank inside the containment.

The removal of residual reactor heat is discussed in more detail under section “Cooling of the reactor”, including the scenarios when the reactor pressure vessel is open.

The design objectives and design principles of the systems involved in the management of a loss of the ultimate heat sink at the AES-2006 plant comply with the Finnish safety requirements. Compliance with the Finnish requirements, especially in terms of the sufficient make-up water and the cooling of auxiliary systems when removing residual heat into an alternative heat sink, shall be assessed in the construction licence phase.

Cooling of fuel pools

The fuel pools are cooled by the fuel pool cooling system. The system comprises two subsystems.

The containment spray system can be used as a fuel pool cooling system that complies with the diversity principle. Alternatively, the passive containment residual heat removal system can be used for removing residual heat by vaporising water in the fuel pools. The material does not specify the source of make-up water.

Under design extension conditions, water can be supplied into the fuel pools from the make-up water system tanks using the pump of the steam generator passive residual heat removal system.

The design objectives and design principles of the systems participating in the cooling of the fuel pools mainly comply with the Finnish safety requirements. In the construction licence phase, it must also be ensured that the Finnish requirements are met in terms of the auxiliary and support systems that are necessary for the function.

Shutdown safety

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

The blowdown valves the primary circuit are used to prevent the cold pressurization of the primary circuit.

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

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

Electrical systems

The external power source of the AES-2006 plant is a connection from the 400 kV grid through auxiliary transformers and a main transformer, or from the 110 kV grid through standby auxiliary transformers.

In case the external power sources are unvailable, power to the safety systems of the plant is supplied from:

- Safety Class 2 auxiliary diesel generators (4 x 100%);

- Safety Class 2 batteries with a minimum discharge time of 2 h during the start-up of auxiliary power sources in all four subsystems;
- Safety Class 3 batteries (72 h) that implement the diversity principle (2 x 100%) and, as a redundancy to these batteries, a Safety Class 3 diesel generator;
- Furthermore, a Class EYT (non-nuclear-classified) diesel power station will be implemented at the site.

The design documentation does not clearly specify the separation principles of the defence-in-depth levels of the electrical systems or how the AC power supply that ensures the diversity principle and, therefore, the design extension conditions will be taken care of with regard to electrical engineering. These issues can be reviewed in the construction licence phase.

The design objectives and design principles of the electrical systems mainly comply with the Finnish safety requirements. Issues that shall be reviewed in more detail in the construction licence phase include the AC power supplies that ensure the diversity principle, the separation principles of the electrical systems and the separate power supply system of the severe accident management system.

Building technology and fire protection

The basic design requirements of the buildings and building services of the AES-2006 plant are sufficient in terms of external hazards. The basic design provides a sufficient basis for managing the design requirements and for the detailed design of the buildings and building services.

The design objectives and design principles related to the resistance to vibrations induced by earthquakes and other external hazards comply with the Finnish safety requirements. The fulfilment of the plant site-specific earthquake resistance requirement shall be verified in the construction licence phase. With regard to earthquakes, the basic design uses the PGA values of the reference plants for components (0.2 g) and buildings (0.12 g). By implementing minor changes, the plant can be designed to satisfy the requirements set for the plant site. The basic design is based on the preliminary planning of the durability and vibration characteristics of the frame structures against all vibrations that are caused by external hazards. This provides a good basis for detailed design also in terms of the vibration resistance of the components. The requirements presented in the basic design are sufficient with regard to the Decision-in-Principle.

The design objectives and design principles of fire protection at the AES-2006 plant are in compliance with the Finnish safety requirements, with the exception of the separation between the safety divisions of safeguard buildings, whose design requirements are not fully in compliance with the Finnish requirements. Regarding this aspect and the management of any fires caused by an earthquake, the need to ensure

that the fire protection systems of the plant are earthquake-proof shall be verified along with the related design bases in the construction license phase.

PROTECTION AGAINST EXTERNAL EVENTS (GOVERNMENT DECREE 717/2013, SECTION 17)

The protection strategy of the AES-2006 plant against a crash of a large passenger aircraft is to construct the outer containment to withstand such a crash. Furthermore, the strategy uses shielding and separation by distance with regard to the main steam valve, safeguard, control room and auxiliary diesel generator buildings.

In the absence of more extensive structural protection, it is difficult to demonstrate the adequate retention of the safety functions in the event of an aircraft crash. The plant supplier has presented options for the reinforcement of the structural protection of the buildings that are deemed the most important to safety.

STUK finds that conformity with the Finnish safety requirements with regard to an aircraft crash has not yet been demonstrated. The solution presented requires more detailed designs and analyses as well as plant modifications that will be discussed in the construction licence application.

Other external events that threaten the plant are discussed in the preliminary safety assessment under 'Site'. STUK it finds that the plant can be designed in compliance with the Finnish requirements on protection against external hazards.

PROTECTION AGAINST INTERNAL EVENTS (GOVERNMENT DECREE 717/2013, SECTION 18)

The safety systems of the AES-2006 comprise four redundant subsystems that are mutually replaceable. The subsystems have been physically separated from one another into safety divisions. The safety divisions are generally divided into separate fire compartments. In the containment, physical separation includes separation by distance of safety divisions and the possibility to use local fire protection. The fire compartments of structures that are important to safety are in compliance with the Finnish requirements.

According to the Finnish requirements, system design shall apply the separation principle to ensure the implementation of the safety functions even in the event of a failure and during internal and external hazards. The redundant parts of a system implementing safety functions shall be assigned to separate safety divisions. Doors, hatches and penetrations between the safety divisions shall be avoided.

In the safeguard building of the AES-2006 plant, the fire compartments that contain safety systems are located side by side and connected by service corridors and ventilation system channels. These connections between the redundant subsystems are separated by doors and dampers, rendering the adequate implementation of physical separation questionable. Ensuring safety in this respect will be reviewed at the construction licence phase.

The bottom floors of the safeguard building contain the seawater heat exchangers and the related piping for the nuclear intermediate cooling system. The management of a major flood caused by a failure of these components in the layout design of the safeguard building is challenging. Similarly, in the safeguard building, the low and high head safety injection pumps and their related components and piping of each subsystem are located in the same room without physical separation. In this respect, the ensuring of safety shall be reviewed in the construction licence phase.

Conformity with the Finnish safety requirements with regard to internal events, including flooding and fires, has not yet been demonstrated. The solution presented requires more detailed designs and analyses as well as plant modifications. In the construction licence application, STUK will assess the fire protection design instructions and the more detailed design bases together with other authorities.

MONITORING AND CONTROL OF NUCLEAR POWER PLANTS (GOVERNMENT DECREE 717/2013, SECTION 19)

In the documentation submitted with the application for a Decision-in-Principle, the safety principles of the I&C systems are described on a rather general level. Before the design and the design materials are specified to the level of technical design, the discussion of several safety principles is largely a discussion of goals and, on the basis of the Decision-in-Principle documentation, it is not possible to fully assess whether these goals will be attained. The fulfilment of the safety principles in the technical solutions of the plant must be verified as design work progresses.

Automatic safety functions

The I&C systems of the AES-2006 plant provide several lines of defence in depth. The first line comprises the normal process I&C and the control systems. The second line consists of the primary protection system that actuates all safety functions when so required. It divides into two diverse parts, A and B, that are mutually replaceable. The third line has a different protection system, HW-Div (Hard Wired), that is based on different technology and that actuates the most essential safety functions. The system features the same functions as protection system diversity A. The last line of defence is the severe accident management system.

The I&C systems in the various lines of defence automatically seek to maintain the plant parameters within a safe range during transients and to limit the consequences of accidents.

The design objectives and design principles of the I&C systems comply with the Finnish safety requirements as far as the automatic actuation, control and monitoring of safety functions during transients and accidents are concerned.

The principle of redundancy in I&C

The primary protection system of the AES-2006 plant comprises four redundant subsystems. A protection function is actuated if a protection signal is received from any

two of the four redundant protection channels. The system meets the requirements set for the principle of redundancy laid down in the Government Decree.

The essential operational I&C systems shall tolerate single failures.

The protection system HW-Div implements the diversity principle in terms of I&C, and it comprises four redundant subsystems.

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

The principle of separation in I&C

The redundant reactor protection subsystems are physically and functionally separated from one another. The I&C system for managing severe accidents shall comprise two subsystems, use separate components and have a redundant power source that is independent of other electrical systems. The I&C functions for managing severe accidents shall be designed in compliance with the requirements during the construction licence application design phase. The separation of I&C systems and components of different safety classes between and within subsystems is not described in the application documentation.

The design objectives and design principles of the systems comply, on a general level, with the Finnish safety requirements.

The principle of diversity in I&C

According to the Finnish safety requirements, the reactor protection system shall measure at least two different process parameters, both of which are physically dependent on a disturbance or accident and the trip limits of which can be set to ensure early enough intervention. The application documentation does not describe how the diversity principle is applied in the measurements of the reactor protection system and the activation of protection. The issue can be reviewed in the construction licence phase.

The I&C of the AES-2006 plant is based on two computer-based system platforms. The reactor, plant protection and limitation systems are based on one platform, and the other I&C systems are based on the other.

The plant concept features a protection system, HW-Div, which is based on the diversity principle and designed for the computer-based protection system. The documentation supplied does not describe into which plant state the system can bring the plant in the event of an I&C common cause failure. The issue can be reviewed in the construction licence phase.

The design objectives and design principles of the system comply with the Finnish safety requirements as far as the principle of diversity is concerned. The scope of the HW-Div system and the diversity principle of the reactor protection system in meas-

urements and in the activation of protections can be further updated in the construction licence phase.

Control room

The control room contains control consoles and a display panel. The turbine, reactor and auxiliary system operators control the plant at their consoles during normal operating conditions, transients and accidents. Furthermore, all information that the operators need for the execution of control actions is transmitted to the control consoles.

Part of the display panel utilises fixed indicators and control switches. These include the protection system panel and the control panels of the components that are important to safety.

The preliminary safety assessment does not discuss the detailed security arrangements regarding the control room and the emergency control room. As the project progresses, the licence applicant shall take into consideration the detailed requirements concerning security arrangements, which will be reviewed in the construction licence phase.

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

Emergency control room

The AES-2006 plant has an emergency control room where the systems important to safety can be controlled independently of the main control room. From the emergency control room, the plant can be brought into a controlled state (hot shutdown) and further into a safe state (cold shutdown).

It is the considered opinion of STUK that the location of the emergency control room shall be reviewed with regard to an airliner crash. In other respects, the design objectives and design principles of the emergency control room comply with the Finnish safety requirements.

SUMMARY

Based on the reports presented, it can be stated that the AES-2006 plant alternative can be brought to meet the Finnish nuclear and radiation safety requirements following the implementation of design changes as well as additional analyses and qualification.

According to the Finnish requirements, the design of nuclear power plants shall take the crash of a large commercial airliner into consideration as an external hazard. The design of the plant shall take into account the direct and indirect effects of an airliner crash. The protection strategy of the AES-2006 plant against a large airliner crash is to construct the outer containment to withstand such a crash. Furthermore, the

strategy uses shielding and separation by distance to protect the safety functions. In the absence of more extensive structural protection, it is difficult to demonstrate the adequate retention of the safety functions in the event of an aircraft crash. The plant supplier has presented options for the reinforcement of the structural protection of the buildings that are deemed the most important to safety. STUK finds that conformity with the Finnish safety requirements with regard to an aircraft crash has not yet been demonstrated. The solution presented now requires more detailed designs and analyses as well as plant modifications to demonstrate compliance with the safety requirements.

In the AES-2006 plant alternative, the structural elements of the safeguard building that contain safety systems (safety divisions) are located side by side and connected by service corridors and ventilation system channels. These connections between the redundant subsystems are separated by doors and dampers, rendering the adequate implementation of fire compartmentation and other physical separation of the redundant subsystems of the safety systems questionable. According to the Finnish requirements, system design shall apply the separation principle to ensure the implementation of the safety functions even in the event of a failure and during internal and external hazards. The redundant parts of a system implementing safety functions shall be assigned to separate safety divisions. Doors, hatches and penetrations between the safety divisions shall be avoided. STUK finds that compliance with the Finnish safety requirements with regard to internal or external events, including flooding and fires, has not yet been demonstrated. The solution presented requires more detailed designs and analyses as well as plant modifications to demonstrate compliance with the safety requirements.

The AES-2006 features severe accident management systems. However, the depressurization of the primary circuit in a severe accident is not in line with the Finnish safety regulations because the depressurization is planned to be carried out using the emergency gas removal system and the safety valves in the primary circuit that are designed for the operational conditions and postulated accidents of the plant. The Finnish regulations require that the severe accident systems are independent of the systems designed for the plant's operational conditions and postulated accidents. The plant design shall be modified in this respect.

There are certain technical details that need further analysis, experimental qualification and further design. It is the considered opinion of STUK that none of these can be considered to constitute an obstacle to fulfilling the requirements of the Government Decree on the Safety of Nuclear Power Plants (717/2013). These technical details include:

- experimental substansiation of the functionality of the passive residual heat removal systems
- detailed demonstration of compliance with the Finnish requirements in terms of the redundancy, separation, and diversity principles of the systems that ensure safety functions
- the effect that the material of the reactor pressure vessel has on the radiation embrittlement rate requires additional clarifications

- the effects that postulated, sudden pipe breaks of the primary coolant circuit have on the durability of the internal parts of the reactor as well as the implementation, inspection and radiation protection principles of the primary coolant circuit nozzles
- the design of the penetrations of the top of the outer containment and the tendon system of the protective shell
- the suction strainers of the safety injection systems and experimental verification of their functionality
- the technical solutions that are related to obtaining the cooling water for the systems that implement the diversity principle in residual heat removal for a 72-hour period
- independence of the systems that implement the severe accident management strategy
- the procedure and systems for reducing the pressure of the containment in order to reach a long-term safe state following a severe accident
- the attainment of the safety principles and objectives in the technical solutions of the plant in terms of I&C systems
- the separation principles of electrical systems
- the scope of the HW-Div system
- the application of the diversity principle in the measurements of the reactor protection system and the activation of protection
- the cooling of auxiliary and support systems and substansiation of a sufficient cooling water supply.