European Stress Tests for Nuclear Power Plants

National Report

FINLAND

3/0600/2011

December 30, 2011

Tomi Routamo (ed.)

CONTENTS

Abbreviations

BWR	Boiling Water Reactor
CCWS	Component Cooling Water System
CDF	Core Damage Frequency
CET	Containment Event Tree
CHRS	Containment Heat Removal System
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EFW	Emergency Feed Water
EOP	Emergency Operating Procedure
EPR	European Pressurized water Reactor
ESWS	Essential Service Water System
EYT	Non-safety classified
HCLPF	High Confidence of Low Probability of Failure
HPSI	High-Pressure Safety Injection
IRWST	In-containment Refuelling Water Storage Tank
IVR	In-Vessel Retention (of core melt)
LOCA	Loss Of Coolant Accident
LHSI	Low-Head Safety Injection (corresponds to LPSI)
LOOP	Loss Of Offsite Power
LPSI	Low-Pressure Safety Injection (corresponds to LHSI)
LUHS	Loss of Ultimate Heat Sink
MCR	Main Control Room
MEE	Ministry of Employment and the Economy (of Finland)
MHSI	Medium Head Safety Injection
MSB	Main Steam Bypass
MSLB	Main Steam Line Break
MSRT	Main Steam Relief Train
NI	Nuclear Island
NPP	Nuclear Power Plant
PAR	Passive Autocatalytic Recombiner
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor

RCS	Reactor Coolant System
RCP	Reactor Coolant Pump
RHR	Residual Heat Removal
RHRS	Residual Heat Removal System
RPV	Reactor Pressure Vessel
SAM	Severe Accident Management
SBO	Station Blackout
SC	Safety Class
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SIS	Safety Injection System
SSCs	Structures, Systems and Components
SSS	Start-up and Shutdown System
TI	Turbine Island
VIRVE	Finnish authorities' secured radio network

Authors

The preparation of this report in STUK has been divided between several experts according to their expertise:

- Pekka Välikangas (earthquakes)
- Jorma Sandberg (flooding and extreme weather conditions)
- Ulla Vuorio (extreme weather conditions and loss of ultimate heat sink)
- Kim Wahlström and Samuli Hankivuo (electrical systems)
- Tomi Routamo (severe accidents)

The technical descriptions of the nuclear power plant sites and units are based on the Licensees' reports [Fortum 2011; TVO 2011]. The conclusions in this report present STUK's position at the Finnish NPPs, with respect to the issues dealt within this report.

Executive summary

Background

A severe accident took place in Japan at Fukushima Dai-ichi nuclear power plant in March 2011. The immediate cause of the accident was a tsunami caused by the earthquake and the fact that the consequences of large tsunamis were not adequately considered in the design of the plant.

Although tsunamis are not considered a real threat in Europe, the European Council requested on 25 March 2011 the European Nuclear Safety Regulators' Group (ENSREG) and the European Commission to undertake a comprehensive and transparent risk and safety assessment ("stress test") of European nuclear power plants [ENSREG 2011A].

This report is prepared to evaluate the safety provisions of Finnish Nuclear Power Plants as specified in the European "stress tests". The technical description is based on the Licensees' reports on the issues within these specifications [Fortum 2011; TVO 2011]. Furthermore, evaluation on the current situation carried out by Radiation and Nuclear Safety Authority (STUK) is provided, and the possibilities to further enhance safety in the Finnish NPPs are presented.

According to the ENSREG specifications, earthquakes, flooding and extreme weather conditions were studied in the stress tests. In addition, consequences of losses of some safety functions and finally management of severe accidents were studied, irrespective of their probabilities. The European stress tests cover in Finland all the operating nuclear power plants (Loviisa 1 and 2, Olkiluoto 1 and 2) and the unit under construction (Olkiluoto 3). The intermediate storages of spent fuel in Loviisa and in Olkiluoto are included in the stress tests. The new NPP units to be constructed which do not yet have a construction license, (Fennovoima 1, Olkiluoto 4) are not considered in the European stress tests.

Earthquakes

For civil construction, there are no general requirements on seismic design in the Finnish Building Code. In the Finnish nuclear safety regulations requirements concerning seismic design were defined first time in 1988. Because of that and due to the low seismicity in southern Finland earthquakes were not considered in the original design of the operating NPPs in Finland.

The first seismic PSA studies were completed in 1992 for Loviisa NPP and in 1997 for Olkiluoto NPP. In these studies certain structures were identified that were strengthened to withstand seismic loads. The seismic risk estimated in the latest PSA updates (Loviisa 2010, Olkiluoto 2008) is considered low.

The stress tests raised some new questions, and further studies will be conducted to confirm adequate robustness of certain vital structures such as the spent fuel pool structures and fire water systems.

Earthquakes were taken into account in the original design of Olkiluoto 3 and no need for design improvements was identified in stress tests.

Flooding

The Baltic Sea is an enclosed sea with moderate variations of seawater level. As the Baltic Sea is shallow (mean depth about 55 m), large tsunamis exceeding normal wave heights are not considered possible. The Baltic Sea is protected from strong impacts of a potential tsunami occurring at Atlantic Ocean by the shallow shelf of the North Sea and the Danish Straits. Also tidal effects are insignificant in the Baltic Sea.

The variations of the sea water level are determined by the total quantity of water in the Baltic Sea, air pressure, wind and seiche (standing waves across the Baltic basin). In the long term (decades) the land uplifting and the possible ocean level rise due to global warming also affect the seawater level. The maximum seawater level is assessed in the most pessimistic way.

Based on the studies, exceeding the critical seawater level at Olkiluoto site, +3.5 m is very unlikely. On the hand, the Loviisa NPP is more vulnerable to high seawater level especially if either of the plant units is in cold shutdown and the seawater system has been opened for maintenance. In this situation, the critical height is +2.1 m. However, the refuelling outages are usually scheduled for period from August to October when the seawater levels are significantly lower than during winter. Additionally, the open hatches of the seawater system can be closed in advance if the seawater level is rising. However, actions are needed to lower the risk of flooding in this situation. During power operation the critical level of the Loviisa NPP for flooding is +3.0 m. This level is well above the observed maximum and the estimated theoretical maximum, although the margin is smaller than at Olkiluoto. The licensee is considering either local protections of some safety significant spaces or flood banks. STUK is reviewing the different actions proposed by the licensee.

Extreme weather conditions

The original design of the operating NPPs in Finland did not take into account all possible aspects of weather phenomena or their possible combinations. Weather phenomena and other extreme external conditions including the combinations of phenomena relevant at the plant site have been comprehensively analysed at the operating NPPs in weather PSA, which is part of the overall PSA. The results of the weather PSA studies and operational experiences regarding the impact of extreme weather phenomena on plant operation have been taken into account in the design of preventive measures including technical modifications and plant procedures. Some further changes will be made at the operating NPPs based on the stress tests.

In the design of Olkiluoto 3 the latest results concerning weather phenomena have been used. Extreme weather conditions and extreme seawater levels, including the impact of climate change and global warming, are also studied within a project in the Finnish Research Programme on Nuclear Power Plant Safety [SAFIR2010, SAFIR2014]. The results of the programme are taken into account by reconsidering the safety margins for external phenomena, in particular air temperature, wind and rain.

Loss of electrical supply

Reliable supply of electrical power to the systems providing basic safety functions in Finnish NPPs is ensured by the Defence-in-Depth concept. As a result of the multiple and diversified electrical power sources at different levels, the probability of loss of all electrical supply systems is very low at the Finnish NPPs.

In normal operating state the AC power to the safety related systems is supplied from plants' main generators. In case of a disturbance in the NPP's own power production, it is possible to use either one of the two separate external grid connections as the second Defence-in-Depth level for AC power supply. If neither of these is available, the next Defence-in-Depth level for supplying AC power is fourfold redundant emergency diesel generators, of which one is adequate for supporting the important safety functions. In some very low probability accidents two of these diesel generators may be needed for a while. In addition to the emergency diesel generators, there is also an additional power supply unit located on-site: a gas turbine station on Olkiluoto site and a large air-cooled diesel generator on Loviisa site. The Finnish NPPs have also a possibility to supply electricity from a nearby hydropower plant.

In case all of the above systems should fail, the situation may lead to reactor core damage, i.e. severe accident. As the fourth level of Defence-in-Depth there are independent electrical power supply systems that are intended to protect containment integrity and thus prevent large radioactive releases during severe accidents. In Olkiluoto the severe accident management measures are independent of AC power. In Loviisa AC power is required for the management of severe accident situations and it is provided by two diesel generators that are separated and independent of other power supply and distribution systems. Each of these diesel generators has adequate capacity to supply power for all severe accident management systems. In some cases, these diesel generators could be connected to supply power also to systems applied for preventing the core damage.

Olkiluoto 3 has, similarly to Loviisa NPP, two so called station blackout (SBO) diesel generators with different manufacturer, different capacity and different voltage level compared to the four emergency diesel generators. These SBO diesel generators could be used as the last resort to prevent a severe accident, in addition to protecting containment integrity should a severe accident occur.

In case of a total loss of electrical supply the time margin at Loviisa 1 and 2 for the recovery of the AC power supply before fuel damage occurs is quite long. In this situation, there is also a possibility to use additional direct diesel driven feed water pump, which extends the time margin significantly.

An independent way of pumping water to the reactor pressure vessel is being planned in Olkiluoto 1 and 2 by the licensee. This is due to the short time margin before the reactor core damage in the case of a total loss of electricity, although considered as a very unlikely situation. STUK will review the detailed technical design of the system. At Olkiluoto 3, an independent way to feed water to the steam generators in case of a total loss of electricity supply is being studied. The time margin in case of loss of electricity is longer in Olkiluoto 3.

Other actions for increasing reliability of AC power supply at all plant units, including Olkiluoto 3, deal with enhanced provision of long term fuel and lubricating oil reserves for all emergency power units at the site, investigating the needs and possibilities to use mobile power supply units and securing adequate battery capacity. Concerning the batteries, the actions may, depending on the unit, deal with increasing the capacity of some critical batteries, improving possibilities to charge them and studying the possibilities to protect them better. Especially in the Loviisa NPP the adequate battery capacity of some safety significant systems needs to be reassessed.

Loss of ultimate heat sink

In the case of loss of normal ultimate heat sink, all plant units have some possibilities to remove the residual heat. Especially precautions have been taken against the cooling water intake blockage due to different impurities in sea water and frazil ice. Several improvements are being considered by the licensees concerning the alternate ultimate heat sink. For example, in Loviisa the licensee is investigating the possibility to install independent air-cooled cooling towers as an alternative ultimate heat sink. Concerning Olkiluoto 1 and 2 the licensee has presented a plan to secure the operation of the auxiliary feedwater system in case of a loss of normal heat sink. STUK is reviewing these plans. Additionally, further actions are needed to secure the long term supply of raw water for residual heat removal taking also into account the possibility of an accident affecting more than one unit on the site.

Severe accidents

A comprehensive severe accident management (SAM) strategy has been developed and implemented both at Olkiluoto 1 and 2 and Loviisa 1 and 2 plant units. Development of the strategies started after the accident in Chernobyl in 1986, and the latest measures were in place in 2003. These strategies are based on ensuring the containment integrity which is required in the existing national regulations. STUK has reviewed these strategies and has made inspections in all stages of implementation.

Severe accidents have been considered in the original design of Olkiluoto 3. STUK has reviewed the overall SAM strategy and the approach has been accepted. No changes to this approach are needed based on the stress tests.

Spent fuel pools

The approach for spent fuel pools at all units is to “practically eliminate” the possibility of fuel damage. This is achieved by ensuring sufficient water level in the spent fuel pools. Since the time delays of spent fuel heating up are relatively long in the case of loss of normal cooling systems, the strategy to practically eliminate the fuel damages can be based on using temporary connections to secure the cooling of the fuel located in the pools. The detailed actions at each unit, including Olkiluoto 3, need to be considered and necessary actions taken. Also improvements in the instrumentation (water level, temperature) of the pools are foreseen.

Emergency planning and preparedness

Accidents affecting simultaneously several units have not been explicitly considered in the emergency planning. Although the risk of a severe accident is small even at a single unit, it is now considered prudent to evaluate the applicability of the existing emergency plans for multiple unit accident. Especially organisational aspects as well as human and material resources need to be analysed in more detail. Furthermore, such analysis needs to take into account a possible degradation of the regional infrastructure that may complicate the situation.

A. BACKGROUND INFORMATION ON NATIONAL REPORT

A.1 General view on NPPs and nuclear power regulation in Finland

Currently there are two nuclear power plant (NPP) sites in Finland, one on Hästholmen island in Loviisa and the other one on Olkiluoto island in Eurajoki. Loviisa NPP is owned and operated by Fortum Power and Heat Oy (Fortum) and the Olkiluoto NPP by Teollisuuden voima Oyj (TVO).

Loviisa site has two VVER-440 reactors of Soviet design equipped with specific safety features including leak tight steel shell containment to meet Western nuclear safety requirements. The first unit Loviisa 1 (LO1) achieved its first criticality in January 1977 and it started commercial operation in May 1977, the second unit (LO2) in October 1980 and in January 1981, respectively.

In Eurajoki, there are two BWRs of AB Asea Atom design. The first unit Olkiluoto 1 (OL1) achieved first criticality in July 1978 and started commercial operation in October 1979, and unit 2 (OL2) in October 1979 and in July 1982, respectively. The third unit Olkiluoto 3 (OL3) currently under construction is AREVA's pressurized water reactor, European Pressurized Reactor (EPR). There is also Decision in Principle for construction of the fourth unit (Olkiluoto 4) at site, but the construction license has not yet been applied.

In future, Finland will have a third site for Fennovoima's NPP in Pyhäjoki municipality located on the northern part of Finnish coast of Gulf of Bothnia. There is a Decision in Principle for this plant, but the construction license has not yet been applied.

The Stress Tests considered here focus on the units in operation or under construction, but not on those that have not yet been licensed, as implied in the specifications on the Stress Tests [Oettinger 2011].

The two sites considered here, are dealt with in chapters B (LO1 & LO2) and C (OL1 & OL2), and a separate chapter (D) is provided for OL3 under construction. The technical descriptions of the NPP sites and units are based on the final Licensee Reports on the Stress Tests [Fortum 2011; TVO 2011]. The conclusions in this National Report present STUK's position at the Finnish NPPs, with respect to the stress test issues.

Of the Finnish legislation, the highest legal provisions concerning the use of nuclear power are set in Nuclear Energy Act [990/1987], which among other issues applies to the construction and operation of nuclear facilities. In Chapter 2a of this Act, the requirements concerning safety are given, and the first one of these sets the guiding principles (Section 7a):

> *The safety of nuclear energy use shall be maintained at as high a level as practically possible. For the further development of safety, measures shall be implemented that can be considered justified considering operating experience and safety research and advances in science and technology.*

This requirement can be considered as the driving force for ensuring continuous improvement of the nuclear safety, and it is further specified in Section 24 (Operational experience feedback and safety research) of Government Decree on the Safety of Nuclear Power Plants [733/2008]:

> *Nuclear power plant operational experience feedback shall be collected and safety research results monitored, and both assessed for the purpose of enhancing safety. Safety-significant operational events shall be investigated for the purpose of identifying the root causes as well as defining and implementing the corrective measures. Improvements in technical safety, resulting from safety research, shall be taken into account to the extent justified on the basis of the principles laid down in section 7 a of the Nuclear Energy Act.*

In Section 7r of Nuclear Energy Act [990/1987], the mandate for the Radiation and Nuclear Safety Authority (STUK) is given to make detailed requirements:

> *The Radiation and Nuclear Safety Authority (STUK) shall specify detailed safety requirements concerning the implementation of safety level in accordance with this Act.*
>
> *Further, the Radiation and Nuclear Safety Authority (STUK) shall specify the safety requirements it sets in accordance with the safety sectors involved in the use of nuclear energy, and publish them as part of the regulations issued by the Radiation and Nuclear Safety Authority (STUK).*
>
> *The safety requirements of the Radiation and Nuclear Safety Authority (STUK) are binding on the licensee, while preserving the licensee's right to propose an alternative procedure or solution to that provided for in the regulations. If the licensee can convincingly demonstrate that the proposed procedure or solution will implement safety standards in accordance with this Act, the Radiation and Nuclear Safety Authority (STUK) may approve procedure or solution by which the safety level set forth is achieved.*

New regulatory guides (YVL) apply to new NPP units to be built in Finland as such. According to the principle of continuous improvement of nuclear safety, they will be applied to existing plants to the extent possible. The applicability of new requirements to, as well as their fulfilment in the existing units is evaluated separately.

The responsibilities of STUK are further defined in Chapter 15 of the Nuclear Energy Decree [161/1988].

STUK is responsible for the regulatory control of nuclear safety in Finland. Its responsibilities include the control of physical protection and emergency response, as well as the safeguards for nuclear materials necessary to prevent nuclear proliferation. The general objective of STUK's regulatory activities is to ensure the safety of nuclear facilities, so that plant operation does not cause radiation hazards that could endanger the safety of workers or the population in the vicinity or cause other harm to the environment or property.

STUK contributes to the processing of applications for licences under the Nuclear Energy Act, controls compliance with the licence conditions, and formulates the detailed requirements. STUK also lays down qualification requirements for personnel involved in the use of nuclear energy and controls compliance with these requirements. In addition, STUK submits proposals for legislative amendments and issues general guidelines concerning radiation and nuclear safety according to section 7r of Nuclear Energy Act, as described above.

STUK's regulation of operating nuclear facilities ensures that the condition of the facilities is and will be in compliance with the requirements, the facilities function as planned and that they are operated in compliance with the regulations. The regulatory activities cover the operation of the facility, its systems, components and structures, as well as the operations of the organisation. In this work, STUK employs regular and topical reports submitted by the licensees, on the basis of which it assesses the operation of the facility and the plant operator's activities. In addition, STUK assesses the safety of nuclear power plants by carrying out inspections on plant sites and at component manufacturers' premises, and based on operational experience feedback and safety research. On the basis of the safety assessment during operation, both the licensee and STUK evaluate the need and potential for safety improvements. STUK also employs resident inspectors at the plants, who supervise and wit¬ness the construction, operation and condition of the plant and the operations of the organisation on a daily basis and report their observations. An overall safety assessment is conducted annually on each nuclear facility, dealing with the attainment of radiation protection objectives, the development of defence in depth, and the operation of organisations constructing or operating nuclear facilities and providing services to them.

In Finland, operating licences are granted for a fixed term, typically 10 to 20 years. A comprehensive safety assessment is required to renew the operating licence. If the operating licence is granted for a period exceeding 10 years, an interim safety assessment (Periodic Safety Review) is carried out during the licence period. The scope of the interim assessment is similar to that carried out in conjunction with renewing the operating licence. During the assessments, the state of the plant is investigated, paying particular attention to the effects of ageing on the plant and its equipment and structures. In addition, the capabilities of the operating personnel for continued safe operation of the plant are assessed. In both cases (renewal of the operating license or an interim safety assessment), safety assessment of a facility is made against the latest safety requirements set in force in Finland following the principle of continuous improvement of safety.

The issues within the "Stress Tests" are part of STUK's normal regulatory activities described above.

A.2 Earthquakes – seismicity in Finland and Finnish requirements

Finland is situated in the north-western part of Europe and belongs to the Baltic shield. Due to the intraplate location Finland is in low seismicity area. There are no seismically active fault lines and zones in Finland. No earthquake disasters in the area of Finland are mentioned in the written history. Loviisa and Olkiluoto sites are located in the lowest seismic hazard zone of Finland.

Seismic activity is higher in Northern Finland, but still remains in such low level that there are no seismic design requirements for other buildings or structures than nuclear facilities.

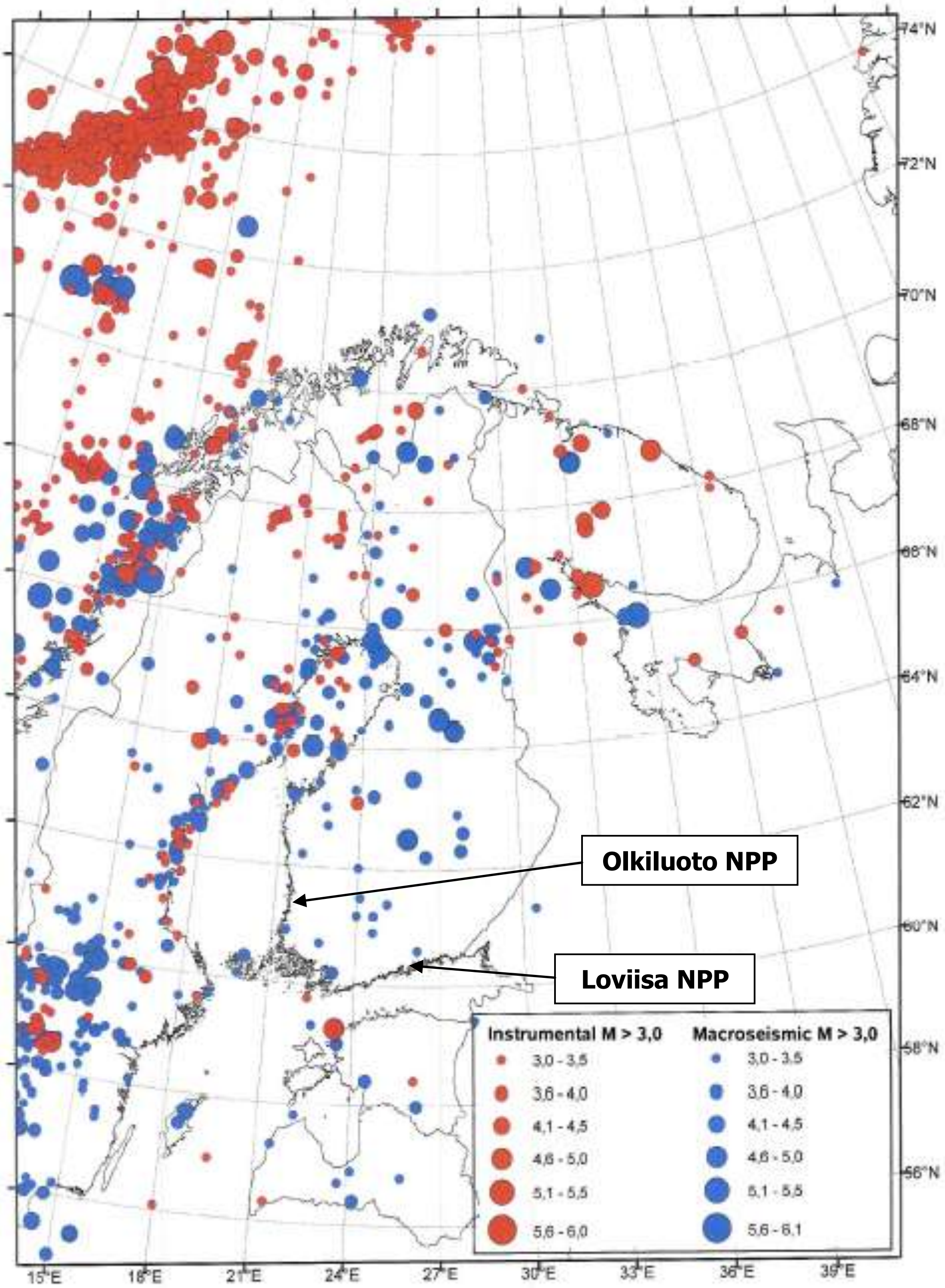


Figure A-1. Distribution of the magnitude above 3 M earthquake epicentres in northern Europe since 1375 according to FENCAT [FENCAT; Ahjos & Uski 1992; Mäntyniemi et al. 1992].

Figure A-1 illustrates earthquake epicentres according the catalogue of Northern Europe [FENCAT; Ahjos & Uski 1992; Mäntyniemi et al. 1992], maintained by the Institute of Seismology of the University of Helsinki. The catalogue includes all documented earthquakes in Fennoscandia and adjacent areas since 1375. Within 500 km of the sites, most of the earthquakes are small, less than 5.0 Magnitude (M). The most severe instrumentally registered earthquake in the vicinity is the 4.9 M earthquake in Estonia in 1976. Altogether, about ten earthquakes higher than 4.5 M have been observed in Finland. Only one event of 5.1 M, which occurred in 1894 in central Sweden, can be classified as a moderate (≥5.0 M) earthquake.

In general, the Government Decree on the Safety of Nuclear Power Plants [733/2008] sets requirement for siting of a plant in Section 11:

> *The safety impact of local conditions, as well as the security and emergency preparedness arrangements, shall be considered when selecting the site of a nuclear power plant. The site shall be such that the impediments and threats posed by the facility to its environment remain extremely minor and heat removal from the plant to the environment can be reliably implemented.*

STUK has issued guides YVL 2.6 (1988, replaced by update 2002) and YVL 2.8 (1996, replaced by update 2003) for giving general requirements for the design and demonstration of seismic resistance with corresponding nuclear safety as well as for the monitoring of earthquakes and their effects during the operation of the nuclear power plants. YVL 2.6 requires site and NPP specific design basis earthquake (DBE) criteria in order to ensure the safe shut-down including the cooling of the radioactive inventory. Those criteria are corresponding with IAEA NS-G-3.3 requirement 5.3 with footnote 1 [NS-G-3.3]. The goal has been to assure that seismic threats to safety remain extremely small.

DBE as site specific design criteria are defined so that, in the current geological circumstances, stronger earthquakes are anticipated not more often than once in a hundred thousand years (10^{-5}/a) on median confidence level. The definition of design basis earthquake has been presented and justified based on statistic study of the area's seismic history, regional and local geology as well as tectonics. Due to the fact that there are no registered strong motion acceleration recordings of earthquakes in Finland, earthquake recordings from Saguenay and Newcastle from Canada and Australia are taken as sources of initial data for the attenuation equations. The Saguenay and Newcastle regions have geological and tectonic similarity to Fennoscandia.

A decision tree is used for the treatment of uncertainties, and it stipulates the ground motion estimation in probabilistic seismic hazard studies in order to define reliable median spectra with 5% percentile and 95% percentile for mean return period of 100,000 years.

Site specific structural design parameter is seismic ground response spectrum, where the zero period value is peak ground acceleration (PGA). Corresponding horizontal component of PGA is analysed for Loviisa 0.056 g and for Olkiluoto 0.082 g. Both sites' ground responses are covered with enveloping spectra. Finally the PGA value in Finland is set 0.1 g as the minimum level suggested by IAEA [NS-G-1.6, NS-G-3.3]. The seismic ground response spectrum presented in Guide YVL 2.6 appendix is enveloping bedrock conditions both at Loviisa and Olkiluoto sites (see Figure A-2). Corresponding vertical component is 2/3 of the horizontal component. Current understanding is that the expected median frequency of DBE for Loviisa is less than 10^{-6}/a and for Olkiluoto less than $8 \cdot 10^{-6}$/a.

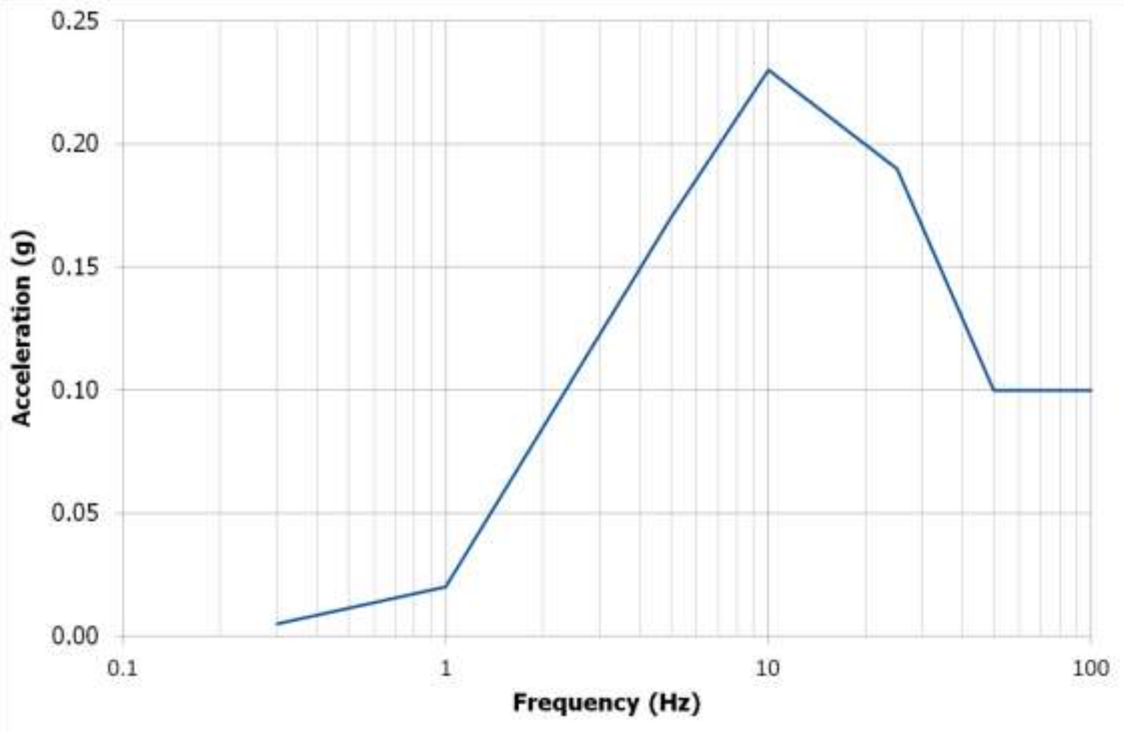


Figure A-2. Free field response spectrum (D = 5%) according to YVL 2.6

In Finland all buildings important to seismic safety have been founded directly on bedrock so that no further amplification from bedrock to base slab will develop. This is based on the fact that shear wave velocities from earthquakes are high (about 2,700 m/s) in Finnish bedrock. Such a fixed base assumption is also in accordance with USNRC Standard Review Plan Section 3.7.2. Good and coherent foundation conditions decrease the uncertainty of the estimation of design basis earthquake and dynamic interaction between buildings and the bedrock. In this respect Finland is in better position compared to many other areas, where foundation circumstances are more complicated. Under these circumstances horizontal PGA 0.1 g to foundations is estimated to develop from the approximated earthquake 4.2 M, if the anticipated epicentre is within 5 km distance from the site. Similar level of PGA will be developed from 5.0 M earthquake, if the epicentre is about 25 km from the site. If the 5.0 M earthquake epicentre is within 5 km distance from the site, corresponding PGA can be about 0.25 g.

For the purpose of time history analyses, artificial ground acceleration histories fulfilling corresponding response spectrum are adopted from the ASCE-98 design code recommendation for the earthquakes of magnitudes 5.5 to 6.0.

In conventional design structures, anchorage, mounting and equipment are designed to fulfil common static/dynamic stress-strain, stability, integrity and vibration requirements. Beyond that NPP safety design requires deterministic and stochastic qualification procedure in order to ensure the operability of safety activities during and after earthquake. Finally qualification of nuclear safety related SSCs against earthquakes is a combination of studies in different technical domains.

The design of building framework is based on acceleration profiles from the vibration analysis. Seismic loads cover also other external vibration loads in the design on building frameworks. The existence of big horizontal loads has effects on stability design and to minimum design requirement. Since the design basis earthquake is low in Finland they do not have much effect on structural design because of other design loads and creep and shrinkage effect in massive concrete structures.

Principles for qualification of equipment against earthquakes are based mainly on international standards from different technical domains, like IEC 60980 for electrical and I&C equipment. Vibration resistance studies of SSCs are based on enveloping design response spectrum for all analysed design response spectra representing locations and external load cases of SSCs. In principle there are three possible ways to verify vibration resistance: analysis, testing and combination of analysis and testing.

Nuclear safety against earthquakes of operating NPP units at Loviisa and Olkiluoto sites are demonstrated by full scope living PSA models. New NPPs, systems, structures and components (SSCs) built after YVL 2.6 was issued, are designed according to DBE and safe shutdown criteria described above. An important part of nuclear seismic safety is living seismic PSA, on which some modifications in SSCs has been based.

In order to develop and verify seismic design of NPPs in Finland, research project SESA has been established at the end of 2010 for the Finnish Research Programme on Nuclear Power Plant Safety 2010–2014 [SAFIR2014]. Safety design margins of NPPs are studied by assessing seismic hazards and the potential effect of earthquakes on plant safety requirements and design criteria for new installations. Therefore the whole seismic qualification process from seismic hazards to approved equipment qualification criteria will be reviewed in order to understand better the formation of seismic safety design margins of NPPs.

Further on guides YVL 2.6 and YVL 2.8 are under update in order to bring state-of-the-art knowhow available for seismic safety and nuclear safety design and PSA studies. Guidance for dealing uncertainties and use of expects are under consideration. STUK is following how USNRC recommendations [NUREG/CR-6372] are implemented when different Senior Seismic Hazard Analysis Committees are defining and updating DBE criteria for NPPs around the world. Finland is also participating on the work of IAEA's international seismic safety centre which was established 2008.

A.3 Flooding – Finnish requirements

The Government Decree on the Safety of Nuclear Power Plants [733/2008] states about siting of a plant in Section 11 that

> *The safety impact of local conditions, as well as the security and emergency preparedness arrangements, shall be considered when selecting the site of a nuclear power plant. The site shall be such that the impediments and threats posed by the facility to*

> *its environment remain extremely minor and heat removal from the plant to the environment can be reliably implemented.*

Furthermore, the Decree includes provisions for protection against external and internal hazards:

Section 17 (Protection against external events):

> *The design of a nuclear power plant shall take account of external events that may challenge safety functions. Systems, structures and components are to be designed, located and protected so that the impacts of external events on plant safety remain minor. External events to be accounted for include at least exceptional weather conditions, seismic events and other factors resulting from the environment or human activity. Design must also take account of illegal activities undertaken to damage the plant, and a large airliner crash.*

Section 18 (Protection against internal events):

> *The design of a nuclear power plant shall take account of any internal events that may challenge safety functions. Systems, structures and components shall be designed, located and protected so that the probability of internal events remains low and impacts on plant safety minor. Internal events to be considered include at least fire, flood, explosion, pipe breaks, container breakages, missiles, falling of heavy objects and component failures.*

Although flooding in not mentioned explicitly in the list of external hazards, it is covered by Section 17 above. The provisions on extreme weather conditions also apply to flooding because, at the Finnish NPP sites, flooding is in practice due to storms.

More detailed requirements are set forth in guides YVL 1.0 (Safety criteria for design of nuclear power plants), YVL 1.10 (Safety criteria for siting a nuclear power plant) and YVL 2.8 (Probabilistic safety analysis in safety management of nuclear power plants).

YVL 1.0; Section 3.12 (Environmental conditions)

> *All nuclear power plant structures, systems and components shall be so designed that they perform reliably under design basis environmental conditions. During design, it shall be defined under what environmental conditions the structure, system or component shall be capable of operating. The operability of a structure, system or component under the environmental conditions in question shall be demonstrated by the necessary tests and analyses.*
>
> *Requirements for the environmental qualification of electrical and instrumentation components are presented in Guide YVL 5.5 and the environmental qualification of other structures and components is prescribed in YVL Guides which apply to these structures and components.*

YVL 1.0; Section 3.14 (External events):

> *According to paragraph one, section 20 of the Council of State Decision (395/91) [has been replaced by Government Decree 733/2008], "the most important nuclear power*

plant safety functions shall remain operable in spite of any natural phenomena estimated possible on site or other events external to the plant. In addition, the combined effects of accident conditions induced by internal causes and simultaneous natural phenomena shall be taken into account to the extent estimated possible."

Natural phenomena include at least freezing which hinders the operation of the final heat sink or blockage due to some other reason, thunderstorm, earthquake, storm wind, flooding, exceptionally cold or warm weather, exceptionally hard rain or drought and exceptionally low sea level. Other events external to the plant are at least electromagnetic disturbances, oil leaks, crashing aeroplanes, explosions, releases of poisonous gases and unauthorised plant site entry.

Guide YVL 2.6 deals with how earthquakes are taken into account in nuclear power plant design.

Guide YVL 1.10; Section 3.1 (External events affecting safety)

The applicant for a licence shall list those external events that could pose a threat to safety at the site in question and shall also assess the risks arising from these events. Effects on the supply of cooling water and on electric power grid connections shall also be considered.

Hazardous industry, traffic and exceptional natural phenomena shall be considered. Examples of exceptional natural phenomena include

- *freezing or other clogging of the cooling water intake*
- *storms*
- *snow loads*
- *flood*
- *low sea level*
- *seismic events.*

The risks arising from external events are assessed by analyses conducted in accordance with Guide YVL 2.8.

Guide YVL 2.8; Section 2.2 (Design phase):

The applicant for a licence shall provide the Finnish Radiation and Nuclear Safety Autority (STUK) with level 1 and 2 design phase PSAs corresponding to the design and site of the plant for the application for a construction licence. These analyses shall meet the contentual requirements set forth in section 4 of this Guide.

The risks associated with various initiators and accident sequences, taking into account their uncertainties, shall be compared with the numerical safety objectives and with each other in order to ensure that no single or few prevailing risk factors will stay at the plant.

The design phase PSA shall be used for its part to demonstrate that the plant design basis is adequate and design requirements are sufficient.

> *Particularly, such phenomena whose frequency of occurrence and consequences include large uncertainties shall be carefully examined. These are for example exceptional weather conditions, other possible harsh environmental conditions and seismic events.*

Guide YVL 2.8; Section 4.2 (Level 1 PSA):

> *[…]*
>
> *Events such as internal failures, disturbances and faults, loss of off-site power, fires, floods, harsh weather conditions, seismic events and other external and human caused initiators shall be dealt with as initiating events.*
>
> *[…]*

The Finnish regulations do not include explicit quantitative requirements on the flood level which shall be considered in the design of NPPs. The design values shall be based on clarifications conducted or contracted by the licensee and reviewed by STUK in co-operation with the appropriate expert organizations, especially the Finnish Institute of Meteorology.

A.4 Extreme weather conditions – Finnish requirements

In the current regulatory guides no detailed quantitative requirements for meteorological and hydrological events are given. The only quantitative risk targets are given in the YVL 2.8 guide for Probabilistic Safety Analysis in Safety Management of NPPs. These are introduced in Section A.6 dealing with the requirements for severe accident management. The requirements in Section A.3 above concerning flooding also apply to extreme weather conditions.

A.5 Electrical power supply – Finnish requirements

The Government Decree on the Safety of Nuclear Power Plants [733/2008] presents general safety requirements for Finnish NPPs. This decree contains both general provisions for all safety systems and provisions for the electrical power systems of NPP. These are stated in more detail in Guide YVL 1.0. More detailed obligations for licensee about design bases and safety requirement pertaining to electrical systems and components are given in Guide YVL 5.2.

The Government Decree above gives a general design criterion in Section 14:

> *[…] The most important systems necessary for transferring to, and remaining in, a controlled state must be capable of fulfilling their function even if any individual system component is inoperable and even if any other component of the same system or of a supporting or auxiliary system necessary for its operation is simultaneously out of use due to required repair or maintenance.*

This is often referred to as “N+2-criterion”. As electrical systems provide power to many of the systems necessary for reaching a controlled state, this criterion is applied to electrical systems, as well.

Government Decree 733/2008 also states that

> *A nuclear power plant shall have on-site and off-site electrical power supply systems. The execution of safety functions shall be possible by using either of the two electrical power supply systems.*

Guide YVL 1.0 (Safety criteria for design of nuclear power plant) gives general requirements for the design of the electrical systems in Section 3.5:

> *In addition to these [on-site and off-site electrical power supply] systems, the plant shall be provided with systems which enable power supply from the main generator to the plant's safety significant systems in case the connection to the external transmission grid is lost.*
>
> *The on-site electrical power supply system serving the safety functions shall be capable of carrying out its functions during anticipated operational transients and postulated accidents even in the event of a single failure, although any component affecting the safety function would simultaneously be inoperable due to repair or maintenance.*
>
> *For electrical power supply, there shall be two separate, independent grid connections from the external grid to each parallel section of the on-site electricity distribution system. These grid connections shall be so designed that during operational conditions and postulated accidents, the simultaneous loss of both is unlikely. It must be possible to start operation of both grid connections quickly enough after the plant main generator has been separated from the grid.*
>
> *The plant's electrical power supply units shall be so designed that the loss of the remaining power supply units in case of the loss of a single power supply unit or caused by the same reason is highly unlikely.*
>
> *In nuclear power plant design, the possibility of the on-site and off-site power supply units being simultaneously lost shall be considered. As provision against such a situation, the plant shall have available a power supply unit which is independent of the electrical power supply units designed for operational conditions and postulated accidents. It must be possible to introduce this power supply unit into operation quickly enough and its capacity shall be sufficient to remove reactor decay heat, to ensure primary circuit integrity and to maintain reactor sub-criticality.*
>
> *Batteries backing up the operation of electrical systems important to safety shall maintain their capability to operate at least for two hours under any circumstances.*

Guide YVL 5.2 (Electrical power systems and components at nuclear facilities) gives more detailed requirements for the electrical systems, and the most important of these are presented below (the full requirements are more comprehensive). Section 2 sets the requirements for design bases of electrical power systems and components:

– General (Section 2.1)

The plant's off-site and on-site electrical power supplies shall be designed such that each can alone ensure reactor decay heat removal, primary circuit integrity and reactor sub-criticality.

– Off-site grid connections (Section 2.2)

The plant unit's off-site grid connections shall be electrotechnically dimensioned such that each connection alone has sufficient capacity to ensure the removal of decay heat, to assure primary circuit integrity and to maintain reactor sub-criticality.

The plant unit shall be provided with reliable, automatically starting change-over equipment for change-over switching between off-site grid connections. Change-over switching shall be designed to not unnecessarily start the plant's safety systems.

– Normal power supply systems (Section 2.3)

The plant's normal power supply systems supply the necessary electrical power to the plant units' electrical equipment and I&C systems, either from their own electrical power supplies or from the off-site power transmission grid. Normal power supply systems refer here to electrical power systems whose operation is not secured by auxiliary power supply systems.

The design of normal power supply systems shall ensure that the disturbance or failure of a Safety Class 4 or Class EYT (non-nuclear) normal power supply system does not endanger the designed operation of a Safety Class 2 or 3 electrical power or I&C system.

– Secured alternating current power systems (Section 2.4)

The operation of Safety Class 2 and 3 alternating current components shall be assured by supplying electric power from onsite emergency power supply systems. Those emergency power supply systems that carry out a safety function only shall be physically separated from plant sections for normal operation. Systems performing the same safety function, and their subsystems – whether they are similar to or different from one another – shall also be separated. The functional separation of safety-classified alternating current power systems shall be designed such that the deterioration, or failure, of their redundant subsystems due to the same electrical disturbance is unlikely.

The systems are to automatically engage to ensure uninterrupted power supply, or power supply if a voltage break of permissible duration has occurred, in case normal power supply is disrupted in a way endangering the operability of components. The on-site emergency power supply systems shall be designed to assure the availability of Safety Class 2 and 3 secured alternating current power systems according to the operating time requirements set to them. It shall be possible to reliably take the emergency power supply systems into service even from the main control room and from local control centres.

The emergency power supply systems shall be provided with sufficiently comprehensive, alarming condition monitoring systems to promptly detect and locate failures causing unavailability of the systems.

– Total loss of alternating current power (Section 2.5)

> *The design of an independent alternating current power supply unit shall be such that its failure simultaneously with the external power transmission grid connections, and due to the same cause, in consequence of weather phenomena or other external events is unlikely. In addition, auxiliary systems important for the operability of the supply unit and external grid connections, e.g. auxiliary power supplies and automatic switching systems, shall be designed such that the independent supply unit and external grid connections are as independent of each other as possible.*

– Direct current power systems (Section 2.6)

> *To assure the operation of Safety Class 2 and 3 direct current equipment, their electrical power supplies shall be ensured by reliable and sufficiently efficient batteries to ensure an uninterrupted supply of direct current power in case of a disturbance in the supply of alternating current power, which endangers their operability.*
>
> *Safety-classified direct current power systems shall be equipped with extensive enough alarming condition monitoring devices by which the operability of the systems can be continuously reliably monitored and failures causing their unavailability immediately detected and located.*

– Main control room, emergency control posts and local control centres (Section 2.7)

> *The main control room of a nuclear power plant shall be equipped with devices providing information about the operational state, and deviations from it, of the plant's electrical systems and the off-site power transmission grids; as well as with systems monitoring the operation of the plant's electrical systems during operational transients and accidents..*

– Unit-to-unit power supply (Section 2.8)

> *The design of the alternating current power supply systems of nuclear power plant units shall enable unit-to-unit supply of electrical power within the site such that, where necessary, one unit can be maintained in a safe state in case of the loss of the off-site grid.*

Furthermore, in Section 3 of Guide YVL 5.2 general requirements are set for redundancy, separation and diversity, as well as qualification for environmental conditions.

A.6 Severe accident management – Finnish requirements

Severe accident requirements are dealt within the Government Decree on the Safety of Nuclear Power Plants [733/2008], where it is stated that

Section 10:

> *The limit for the release of radioactive materials arising from a severe accident is a release which causes neither acute harmful health effects to the population in the vicinity of the nuclear power plant, nor any long-term restrictions on the use of extensive areas of land and water.*

The requirement applied to long-term effects will be satisfied if there is only an extremely small possibility that, as the result of a severe accident, atmospheric release of cesium-137 will exceed the limit of 100 terabecquerel (TBq).

Section 13:

In order to ensure containment building integrity,

- *the containment building shall be designed so as to maintain its integrity during anticipated operational occurrences and, with a high degree of certainty, during all accident scenarios;*
- *pressure, radiation and temperature loads, combustible gases, impacts of missiles and short-term high energy phenomena resulting of an accident shall be considered in the design of the containment building; and*
- *the possibility of fracturing of the reactor pressure vessel in a severe accident so that the leak-tightness of the containment building would be endangered shall be extremely small.*

The nuclear power plant shall be equipped with systems that ensure the stabilisation and cooling of molten core material generated during a severe accident. Direct interaction of molten core material with the load bearing containment structure shall be reliably prevented.

Section 14:

The plant shall be provided with systems, structures and components for controlling and monitoring severe accidents. These shall be independent of the systems designed for operational conditions and postulated accidents. Systems necessary for ensuring the integrity of the containment building in a severe accident shall be capable of performing their safety functions, even in the case of a single failure.

The plant shall be designed so that it can be brought into a safe state after a severe accident.

More detailed requirements on severe accidents are given in Finnish Regulatory Guides (YVL Guides), and these are introduced in the following.

<u>Design requirements</u>

Guide YVL 1.0 (Safety criteria for design of nuclear power plant) sets some general requirements for severe accident management systems on

– Reactivity control and reactor shutdown in Section 3.1:

The reactivity control systems shall be so designed that a reactor which has sustained damage in a severe accident, or its debris, are maintained sub-critical.

– Reactor coolant system in Section 3.2:

Pressure reduction [of the RCS] shall be so planned that a severe accident at high pressure can be reliably prevented.

– Containment in Section 3.3:

The containment shall be encased in a secondary containment building so that any radioactive substances which leak from the primary containment can be collected and treated as appropriate. In case the primary containment must be made non-leaktight due to reactor reloading or maintenance, the secondary containment shall be designed to function as an efficient technical barrier to the spreading of radioactive substances in accidents assessed possible under these operational conditions.

The primary containment and the secondary containment protecting it shall be so designed that the external events[1] do not jeopardise the operability of the containment systems and the primary containment leaktightness in accidents. These buildings shall also be so designed that they form an adequate physical shield against external events for the reactor and the systems relating to it.

It must be possible for systems ensuring containment leaktightness in connection with a severe accident to carry out their safety function also in the event of a single failure.

– Penetrations, access openings and isolation in Section 3.3:

The location, structure, protection and sealing materials of containment penetrations, access openings and isolation valves shall be so designed that they maintain operability and leaktightness during operational conditions and accidents. Particular attention shall be paid to the long-term durability of the sealing materials in severe accidents. In the design of the penetrations, loads transferred from piping shall be observed.

– Pressure and temperature management in Section 3.3

To ensure containment integrity in severe accidents, systems, structures and components shall be designed which are independent of systems designed for plant operational conditions and postulated accidents. When analysing pressure and temperature loads, the below facts in particular shall be considered

- *decay heat yielded by the reactor and its debris*
- *total volume of uncondensed gases*
- *heat loads arising from combustible gases.*

When evaluating the volume and timing of non-condensable gases released during severe accidents, particular attention shall be paid to how overheated reactor internals and fuel react with water. In estimating the volume, it shall be assumed that 100% of easily oxidising reactor core materials reacts with water. Furthermore, radiation-induced disintegration of water, chemical reactions considered possible in the con-

---

[1] Natural phenomena include at least freezing which hinders the operation of the final heat sink or blockage due to some other reason, thunderstorm, earthquake, storm wind, flooding, exceptionally cold or warm weather, exceptionally hard rain or drought and exceptionally low sea level. Other events external to the plant are at least electromagnetic disturbances, oil leaks, crashing aeroplanes, explosions, releases of poisonous gases and unauthorised plant site entry.

tainment and the primary circuit, and melted core-concrete interaction on the containment floor if the core melt has penetrated the reactor pressure vessel shall also be analysed.

The release into the environment of a steam-gas mixture accumulated in the containment shall not be designed as the primary measure of preventing containment pressurisation. A containment filtered venting system shall be designed which can be used to remove any overpressure caused by non-condensable gases possibly released in a later phase of an accident.

The effects of the core melt possibly discharged from the high-pressure primary circuit to the containment in consequence of a severe accident shall be taken into account in the containment design.

– Treatment of combustible gases in Section 3.3:

Containment systems shall be designed to reduce the concentrations of oxygen or combustible gases formed in accidents, or to prevent in some other way gas explosions or uncontrollable gas fires which may jeopardise containment leaktightness or the operability of accident management equipment inside the containment.

[…]

For the reduction of combustible gases, [such] systems and components shall be used in the first place [that] do not rely on external power supply.

– Management of the reactor debris in Section 3.3:

The containment lower space shall be so designed that a core melt possibly formed in a severe accident with high certainty does not cause a containment melt-through.

Provision shall be made for the cooling of the reactor debris on the bottom of the containment in such a way that radioactive substances released into the containment air space can be effectively restricted and that the radiation heat emitted by the reactor debris does not break the containment integrity.

The management of hot gases formed in severe accidents shall be so planned that the gases do not break the containment integrity via the steam generators or otherwise.

– Cleaning of the gas space in Section 3.3:

Containment systems shall be designed to remove radioactive substances from the gas space during accidents. In designing these systems, special attention shall be paid to radioactive iodine and radioactive substances in the form of solids and also to events including a containment leak during an accident.

It must be possible to clean the containment gas space during accidents even in the event of a single failure.

Safety classification

In Guide YVL 2.1 (Nuclear power plant systems, structures and components and their safety classification) SSCs mitigating the consequences of severe accidents are required to be classified in Safety Class 3, which is the same for e.g. *SSCs having an essential effect on the reliability of reactor cooling and decay heat removal from the reactor*. Furthermore, *systems by which the accomplishment of the safety functions mentioned above are monitored shall also be classified in Safety Class 3*.

Instrumentation and control

YVL 1.0, Section 3.6:

> *Monitoring equipment shall be designed for the nuclear power plant to manage and monitor the progress of severe accidents and to give data about*
> - *the possible re-criticality of the reactor or its debris*
> - *the threat of a reactor pressure vessel melt-through*
> - *the location of the reactor debris*
> - *other factors possibly endangering containment integrity.*
>
> *The measurement systems designed for accident monitoring and management shall maintain operability even in the event of a single failure.*

The requirement on instrumentation and control during severe accidents is supplemented in Guide YVL 5.5 (Instrumentation systems and components at nuclear facilities) as follows (Section 2.5.4).

> *The design of the monitoring instrumentation for severe accidents shall fulfil the following requirements:*
> - *The measuring methods chosen shall be suitable for monitoring severe accidents.*
> - *The instrumentation shall be independent from all the other instrumentation at the plant.*
> - *The power supply of the instrumentation (electricity, compressed air, etc.) shall be independent from all other power supplies of the plant.*
>
> *The requirements apply also to control actions possibly needed during a severe reactor accident.*

The requirements specifically on radiation monitoring systems are set in Guide YVL 7.11. In Section 3.3 it is required that

> *[…] it shall be possible to determine the activity concentration of the water inside the containment […] even during a severe reactor accident.*

Section 4.3 gives general requirements on radiation monitoring during severe accidents:

The measuring equipment for the external dose rate in the containment, which is designed to function during a severe accident, shall be capable of displaying the dose rate that is caused by the release of a significant fraction of the radioactive materials from the reactor core into the containment. The measuring range shall extend to a dose rate of 10^6 Gy/h (Sv/h).

The measuring range of the sampling and instrumentation intended to measure the concentrations of iodine isotopes and radioactive aerosols in the containment shall extend at least to a value of 10^{15} Bq/m^3. The locations of the sampling points shall be justified.

Continuous measurement of the air activity concentration in the areas close to the containment shall be conducted considering the necessary inspection and control measures in these areas during accidents.

A sufficient number of portable measuring instruments for external radiation whose upper limit of the measuring range is no less than 10 Gy/h (Sv/h) shall be available for measurements to be carried out during an accident.

The range of the measuring system for releases into the air shall be such that the system is capable of functioning even during a severe accident. The release measurement shall be protected in such a way that external background radiation does not prevent or disturb the measurement.

<u>Deterministic analyses</u>

Guide YVL 2.2 (Transient and accident analyses for justification of technical solutions at nuclear power plants) gives guidance on how to demonstrate the reliability of severe accident management. The requirements on events to be analysed are given for

– analyses of plant behaviour in Section 2.2:

The essential functions of the severe accident management strategy shall be justified by suitable experimental and analytic means. As part of the strategy, it shall be assured in particular that initiating events endangering containment integrity or the prevention of the dispersion of fission products as well as rapid and/or energetic physical phenomena have been prevented with a good certainty.

Severe accident analyses shall be conducted to study factors affecting containment integrity, leak tightness and the operability of containment systems. Analyses have to be carried out for cases which may be the worst from the viewpoint of the functioning of the containment. They could include e.g.

- *total loss of AC power*
- *total loss of feed water*
- *leak of primary coolant without emergency cooling during power operation; or during a maintenance, refuelling or other outage*
- *leak of primary coolant and blockage of coolant recirculation.*

In addition, for the purpose of emergency planning, safety analyses are to examine events not considered in the severe accident management strategy proper. These include severe accident sequences whose prevention has been implemented with such certainty that they are excluded from the severe accident management strategy.

– analyses of releases and radiation doses in Section 2.3:

Releases of radioactive substances and radiation doses caused by a severe accident shall be analysed. The analyses shall be carried out for cases which, on the basis of containment behaviour and conditions and the concentration of radioactive substances in the containment, are estimated to cause the most extensive releases. The analyses are to include events in accordance with the management strategy in the first place.

Guide YVL 2.2 also gives requirements on methods of analysis in Section 3:

If sufficiently reliable calculation methods are not available, the analysis shall be justified by experiments. This requirement applies especially to most phenomena essentially relating to severe accident management, for example, the long term coolability of reactor core debris after a severe accident.

and on assumptions used in analyses of plant behaviour in Section 4.1.6:

The analyses justify that the systems and actions designed to implement the severe accident management strategy are acceptable. The analyses may base on so called best estimate methods but apply conservatism in balance with the strategic significance of the function: the more essential the function, the better assurance for success shall be demonstrated. Also the conservative factors for the choices shall be justified.

In addition to the systems proper belonging to the actual management strategy, other systems whose functioning does not presuppose the operation of active components may be taken into account as factors mitigating accident conditions or restricting releases. An example of such a system is the heat transfer circuit in which the medium circulates by natural circulation. In addition, even such active components may be assumed operable whose operation is independent of the causes and consequences of a severe accident.

If relevant justification is provided, component faults that have resulted in a severe accident may be assumed to be fixed later, unless a high radiation level, or some other reason, prevents repairs. The time spent in repairs shall be chosen conservatively and be justified.

The time spent in actions in accordance with the management strategy and other factors connected to the implementation of the actions (e.g. accessibility of locally controlled equipment) shall be justified.

In addition, Section 4.2.4 in Guide YVL 2.2 sets some specific requirements on assumptions when analysing releases and radiation doses resulting from severe accidents.

Probabilistic targets

The demonstration of efficiency of severe accident management shall be supported by PSA studies as required in Guide YVL 2.8 (Probabilistic safety analysis in safety management of nuclear power plants) on level 2 PSA in Section 4.3. According to this guide (Section 2.1):

The following numerical design objectives cover the whole nuclear power plant:

- *The mean value of the probability of core damage is less than 10^{-5}/a.*
- *The mean value of the probability of a release exceeding the target value [of 100 TBq of cesium-137] must be smaller than $5 \cdot 10^{-7}$/a.*

Should substantial risk factors not recognised earlier appear during operation, the licensee shall upgrade the safety of the plant.

In conjunction with the design of safety upgrades the licensee shall demonstrate that the safety of the plant assessed after the upgrades is substantially at the same level or better than the objectives presupposed for the design phase.

Emergency preparedness

Guide YVL 7.4 (Nuclear power plant emergency preparedness) set general requirements for the plant organisation taking care of the emergency situation. Section 2.1 gives the overview of the issues to be included in the plants emergency plan, and the details are given in the further sections of the guide:

The emergency plan shall cover the following:

- *classification of emergency situations and description of events and accidents on which classification is based on*
- *description of the emergency organisation*
- *description of alert and communication arrangements*
- *management of an emergency situation and conducting situation assessments*
- *safety of workers and radiation protection*
- *on-site and off-site radiation measurements during an emergency situation*
- *provision of information to the public*
- *premises and equipment*
- *termination of an emergency situation and post-emergency measures*
- *report on the maintenance of preparedness.*

In addition, the emergency plan shall describe the licensee's actions related to rescue operations. Instructions on the emergency response activities shall also be attached to the plan.

A.7 Actions initiated in Finland after the Fukushima Dai-ichi accident

Radiation and Nuclear Safety Authority (STUK) received a letter from Ministry of Employment and the Economy (MEE) on the 15th of March 2011. The letter gave directions for STUK to carry out a study how Finnish NPPs have prepared against loss of electric power supply and extreme natural phenomena in order to ensure nuclear safety.

STUK sent a letter to Licensees on the 21st of March 2011 with specific directions to give a report to answer MEE's letter due on the 15th of April 2011. In some issues Licensees' reports go beyond the EU Stress Tests, but they support the Stress Test work, as well.

Based on the Licensees' reports, STUK gave a report to the ministry on the 16th of May 2011. The report was followed by letters to Licensees with requirements on further safety assessments as well as requests to improve safety where possible. These requirements are presented in sub-sections considering the "estimation of safety margins" or "conclusions of the adequacy" under each issue within this report.

Licensees gave their answers to the requirements mentioned above with plans to improve plant safety on the 15th of December 2011. These improvements and other issues identified are introduced in sub-sections considering "measures which can be envisaged to enhance" safety.

The experiences from the Fukushima accident will also be taken into consideration in the ongoing renewal of the Finnish Regulatory Guides (YVL Guides).

B. FORTUM – LOVIISA 1&2

B.1 General data about the site and nuclear power plant units

B.1.1 Brief description of the site characteristics

Loviisa town is located approximately 90 km east of Helsinki on the coast of Gulf of Finland, Baltic Sea. Loviisa NPP is located approximately 10 km south-east of the town centre on the island of Hästholmen. The island is connected with the mainland by a 200 m causeway including a short bridge.

Loviisa NPP and Hästholmen island is owned by the license holder Fortum Power and Heat Oy. The site consists of two reactors, two shared spent fuel storages, low an intermediate level waste storages, liquid waste solidification plant and all necessary facilities for support functions (offices, workshops, fire station etc.) Accommodation facilities and site gate are located at the mainland side of the causeway.

B.1.1.1 Main characteristics of the units

Loviisa NPP consists of two VVER-440 pressurized water reactor units that were heavily modified already in the design phase in comparison with original design. The process systems were mainly designed in Soviet Union. Large modifications included for example the containment system (leak tight ice-condenser containment with Westinghouse ice condenser), automation systems (Siemens) and safety systems. Significant modifications have been made throughout the plant lifetime as well. For example new systems have been constructed (e.g. auxiliary emergency feed water system, severe accident management systems) and many existing systems have been modified. Renewal of automation is currently under way. Loviisa NPP units differ significantly from other VVER-440 units.

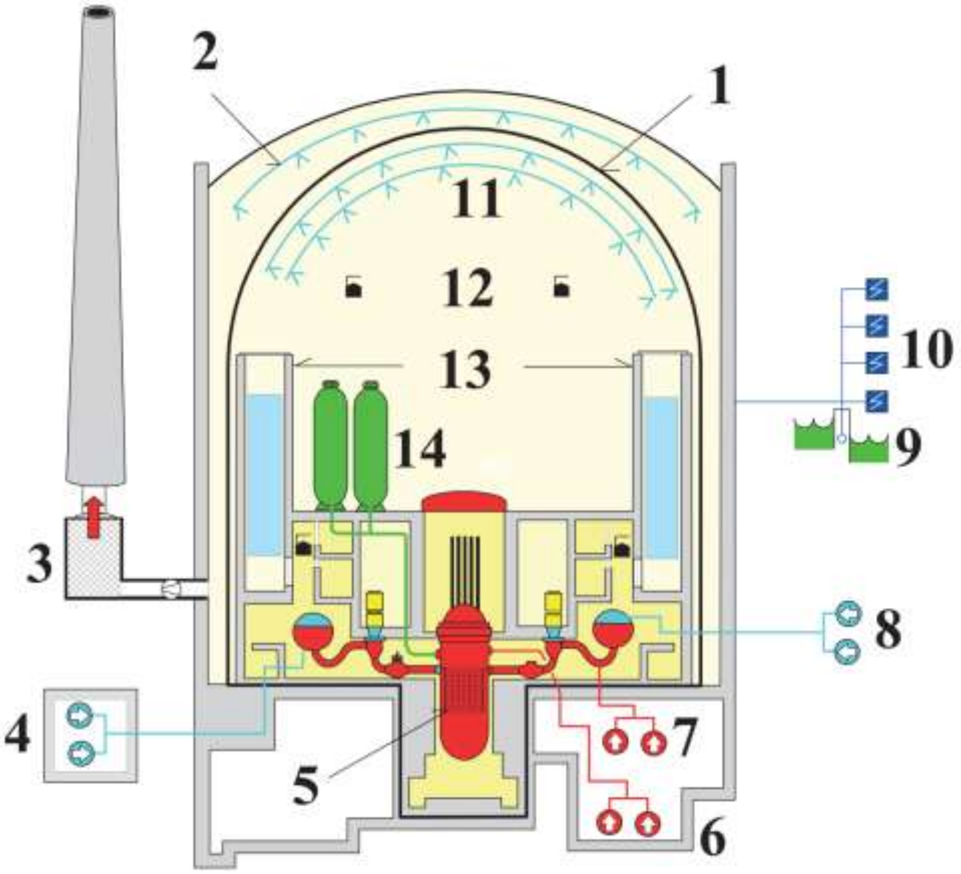
Loviisa NPP units were constructed from early 1970's to early 1980's. The first criticality was reached 21 January 1977 at Loviisa 1 (LO1) and 17 October 1980 at Loviisa 2 (LO2). The original thermal power of the units was 1375 MW per unit. In mid-90's Loviisa modernization program was implemented and the thermal power was uprated to 1500 MW per unit. At the same time significant plant modifications were implemented to enhance the safety level.

At Loviisa NPP there is a fuel storage consisting of one fuel pool inside each of the containment buildings. In addition the auxiliary building of Loviisa 2 contains two separate spent fuel storages (spent fuel storage 1 and spent fuel storage 2) including several individual pools, which can be separated by gates. The original plant design included only one spent fuel storage. The additional storage was constructed because transportation of spent fuel to Russia was stopped due to change in Finnish legislation.

One adverse feature of the ice-condenser containment of LO1 and LO2 is that the containment structure does not provide efficient protection against radiation to upward direction. Therefore, in case there are large amounts of radioactive material in the upper part of the containment, the radiation levels around the containment may be rather high due to scattered radiation from the air above the containment (skyshine) although the containment walls provide shielding against direct radiation.

B.1.1.2 Description of the systems for conduction of main safety functions

A general overview on the main layout and the main safety systems of Loviisa NPP is given in Figure B-1 below.



1 Steel containment
2 Containment external spray
3 Stack filters
4 Auxiliary EFW pumping station
5 Reactor
6 Low-pressure safety injection
7 High-pressure safety injection
8 Emergency feed water pumps
9 Electricity connection from a hydropower plant
10 Emergency diesel generators
11 Containment spray
12 Hydrogen recombiners and igniters*
13 Ice-condensers
14 Emergency hydro accumulators

Figure B-1. Main layout and main safety systems of Loviisa NPP [Fortum 2007]
*Hydrogen igniters only in the steam generator space (lower compartment)

The safety systems are discussed in more detail in the following.

<u>Reactivity control and safety injection</u>

Loviisa NPP has two independent reactivity control means: control rods and boron injection systems. Reactivity of the core is decreased either by inserting control rods or by increasing the boron content of the primary coolant.

Control rods are of safety class 2 (SC2), and they are driven by alternating current of electrical motors and they are kept in upper position by direct current of electrical motors. Control rods may be manoeuvred manually or automatically during normal operation. Reactor protection system (SC2) may actuate reactor trip by opening trip-breakers from DC system of electrical motors, causing control rods to drop into the core by gravity. Control rods are able to shut down the reactor from power operation to hot standby state.

There are several systems, which are able to increase the boron concentration of primary coolant. Two of these systems, make-up system and chemical/boron supply system, are the primary systems for boration during accident conditions.

The chemical/boron supply system's two redundant high-capacity pumps (SC2) provide boron control for the make-up system. The system has also two redundant low-capacity pumps (SC3), which are diverse from the high-capacity pumps and capable of injecting high concentration boron solution directly into the RCS at design pressure of 137 bar. The make-up system's (SC3) two high-capacity pumps inject boron solution from the boron/chemical supply system into the RCS up to pressures of 138 bar. In addition, the system has two redundant low-capacity pumps to provide boron injection into the RCS at elevated pressures up to 160 bar.

In addition, both the HPSI and LPSI (SC2) increase boron concentration in primary coolant when injecting water from the emergency core cooling system (ECCS) tank. Borax within the ice in the ice condensers ensures high enough boron concentration in the sump water also during the ECC recirculation mode. This applies also during the severe accident, when the reactor cavity is flooded with the water accumulated from the ice in the ice condensers. Criticality issues during severe accidents are discussed in more detail in Section B.6.3.4.

In-containment spent fuel storages and spent fuel storages were originally designed to ensure sub-critical conditions even with non-borated water. However, new fuel has higher enrichment and this has required additional measures to ensure sub-criticality. These measures include administrative measures to prevent storage of fresh fuel in spent fuel storage 1, to limit the fresh fuel bundle amount to six in spent fuel storage 2, where the fuel examinations are done, and plugging 21 positions in the in-containment spent fuel pool. These measures ensure original design basis of sub-criticality with non-borated water. Normally the pool water is borated in all spent fuel pools.

<u>Heat transfer from reactor to the ultimate heat sink</u>

The primary heat sink is sea water. It is possible to circulate sea water also from normal outlet channel to inlet of service water system. Secondary heat sink is atmosphere, which can be utilised by dumping steam from main steam header to atmosphere or by opening steam generator relief valves to atmosphere. The main safety systems are sea water cooled, but the auxiliary emergency feed water system is air cooled.

During normal power operation, heat from the core is transferred by circulating the water within the RCS by primary coolant pumps (PCP) to the secondary circuit through steam generators (SG), from where the heat is further transferred to the sea via the turbine and the condenser. The main steam line system is classified to SC2 up to main steam isolation valves, and the sea water systems are non-safety classified (EYT).

When cooling the plant to hot shutdown, the heat is transferred via steam generators to the secondary side. After turbine trip steam can be lead to the condensers via turbine bypass system. It is also possible to dump excess steam to the atmosphere via main steam header relief valves. Water inventory in the steam generators is maintained with normal feed water system (EYT) or emergency feed water (EFW) system (SC2). Using of EFW system as a normal procedure like auxiliary feed water system during cooldown are scheduled to be changed in 2014 (LO1) and 2016 (LO2), and thereafter the EFW system will serve only for EFW function.

After reaching a specific RCS pressure, the SGs are filled with water. During the filling steam can be led either to turbine by-pass system or to main steam header relief valves. When a specific water level in steam generator is reached, main steam lines are isolated and shutdown cooling system (SC3) is taken into use. This system is capable of operating both in steam and water phase, and it is cooled by the service water system. The water from the shutdown cooling system heat exchangers is pumped back to the SGs.

After the PCPs are stopped, the heat from the core is transferred to the SGs by natural circulation. Normally there are at least two of the six loops operating in natural circulation, but even one loop is capable to transfer residual heat in cold shutdown mode. Removal of reactor pressure vessel head does not affect the natural circulation in cold shutdown. After removal of the RPV head, the reactor shaft will be filled with water and connected to the in-containment spent fuel pool. During refuelling part of the residual heat is removed through steam generators and the rest by the spent fuel pool cooling system (SC3).

<u>Heat transfer from the reactor during accident conditions</u>

In case of incident or accident the reactor is assumed to trip either automatically actuated by reactor protection system or manually by the operator. ATWS scenarios have been taken into account, and in this case reactor cooling is not performed until sufficient boron concentration has been reached in order to minimize neutron power.

In case of LOCAs, cooldown to hot shutdown is performed as follows:

- Part of the residual heat is removed by the leakage itself into the containment.
- Leaked coolant is collected to LPSI system and containment spray system (SC2) sumps.
- In the beginning of LOCA, HPSI and LPSI systems inject water from ECCS tank. The injected water is colder than primary circuit water, which also cools down the reactor.
- Water from sumps is cooled with the containment spray system and LPSI system heat exchangers. These heat exchangers are cooled by the intermediate cooling system (SC3), which is cooled by the service water system (SC3).
- The operator can cool down the reactor with the secondary circuit by releasing steam through the main steam header relief valves or dumping steam into the condenser via the turbine by-pass system.

In case of primary-to-secondary leakage, cooldown to hot shutdown mode is performed from secondary side after isolation of leaking SG. Each of six primary coolant loops can be isolated by main gate valves. Closing of valves from one loop isolates the SG and thus stops the primary-secondary leakage. If the valves fail, EOPs guide operators to decrease the RCS pressure so that radioactive releases to the environment are terminated and the amount of diluted water from SGs to primary circuit is minimised. In case of secondary leakage, reactor first cools down by the leakage itself. The leaking SGs are isolated from secondary side and the reactor is cooled by the intact SGs.

In scenarios not involving primary or secondary leakages the reactor can be cooled down by the secondary circuit, which is performed similarly to normal cooldown. The steam generated in the SGs is either dumped to the condenser or to the atmosphere via different relief valves in the turbine by-pass or main steam header. Water inventory is maintained with normal feed water, EFW or auxiliary EFW pumps. Feed water is taken either from the feed water tank in closed cooling mode or from the demineralised water tanks (SC3) or condensate tanks (SC3) depending on the pump used. The turbine by-pass, however, requires systems that are not safety classified and need operable external grid connection.

In case of emergency the reactor is cooled down to the cold shutdown similarly to normal operation. It is possible to use the shutdown cooling system for accident management also. In addition to normal the shutdown cooling system a back-up shutdown cooling system (SC3) has been installed. This is mainly provided against turbine building fires, and was constructed in 1990's after PSA analyses showing a relatively high CDF due to turbine hall fires.

If either the shutdown cooling system or the back-up system is not available, plant is not taken to the cold shutdown but stabilized to hot shutdown. Means of stabilization are basically the same as cooldown means, i.e. dumping steam into the atmosphere and injecting water to the SGs. If the main turbine condenser and consequently the turbine by-pass are not available, the excess heat is released from the main steam header through two battery-backed power operated relief valves (SC3) to atmosphere. Water inventory in the SG is maintained by the normal feed water or EFW systems. The EFW pumps (SC2) are backed by emergency diesel generators, and the water supply is from the demineralised water tanks.

If the EFW system is not available, two auxiliary EFW pumps (SC3) can be used. These pumps may use same water reservoirs as the EFW pumps, primarily the condensate water tanks. It is possible to fill up the condensate tanks from the demineralised water tanks with a diesel backed transfer pump. In extreme situations it is possible to fill the demineralised water and condensate tanks from fire fighting water system’s diesel driven pumps.

If the reactor vessel head has been removed and the total loss of electrical power or loss of ultimate heat sink occurs, it may be challenging to use steam generators for residual heat removal. The auxiliary EFW system is able to inject more coolant to the secondary side, but leaking of secondary side water through SG relief valves would not remove enough heat in the long run. It would be possible to use steam generators for residual heat removal only if RPV head would be placed back to its position so that pressure in the RCS could be increased and boiling in the SG secondary side would become possible. Therefore it is more practical to let the water boil in the reactor shaft and fill up the shaft once in a while. Filling could be done for instance from the LPSI system hydro-accumulators after the leak tightness of reactor shaft has been ensured. It is also possible to inject water to reactor shaft from fire fighting system. These actions have not been described in the EOPs and shall be initiated by emergency preparedness organisation.

In some cases, if loss-of offsite power (LOOP) occurs, it is possible to cooldown the core feeding ECCS water to the primary circuit and opening pressurizer valves and letting steam and water to bleed from the circuit to the containment (feed & bleed). There are relief valves, safety relief valves and SAM relief valves connected to the pressurizer. The pressurizer relief valves are both diesel generator and battery backed and SAM valves are backed from SAM diesel generator charged batteries. Safety relief valves are spring loaded pilot operated valves. Functional safety class of these valves is SC3 and mechanical safety class SC1. Feed & bleed is possible either with the HPSI or with the LPSI system. Functioning of one large SAM line and one HPSI pump ensures core cooling after the reactor trip.

In addition, it is possible to support maintaining coolant inventory by injecting water from the make-up or chemical/boron supply systems, and at low pressures from the LPSI system. If the pressure in the primary circuit decreases below 35 bar, the hydro-accumulators will inject water to the RCS. Reactor pressure vessel head has a small valve for removing non-condensable gases from the RPV and the pressurizer relief valves could be used for steam venting. However, capacities of these systems are rather low compared to the residual heat produced in the core.

If the pressure in the RCS exceeds significantly the normal operating pressure of 123 bar, the pressurizer safety valves will open at 137 bar, and feed & bleed is possible with high pressure chemical/boron supply system pumps if some protection signals are overriden.

<u>Spent fuel pools</u>

At Loviisa NPP there are in total four different spent fuel pool areas, one in each of the containment (in-containment pool) and two separate spent fuel storages. In-containment fuel pools are connected to systems of the corresponding unit and spent fuel storages to LO2 systems. Each spent fuel pool area has its own cooling systems with two trains transferring heat to separate trains of the intermediate cooling circuits. One fuel pool cooling train and one intermediate cooling train are capable of providing adequate cooling for the corresponding spent fuel pool system.

Typically the spent fuel is stored in the in-containment fuel pools from one to two years before it is transported to spent fuel storages. In spent fuel storage 1 the fuel is stored in the transport casks (30 bundles in each cask) and in all other pools in fuel racks.

Boiling without compensation would gradually lower the water surface level and finally the water depth above the fuel would not be sufficient for radiation shielding thus increasing radiation levels. Increased radiation could also result from fuel damage in the reactor of corresponding or neighbouring unit. Increased radiation levels may prohibit or make more difficult the use of some systems to add water to the pools.

Spent fuel storage 2 structures were originally designed to allow boiling. For other spent fuel pools boiling was not the original design basis but analyses made afterwards show that in atmospheric pressure the structures can assure sufficient integrity of the pools despite of the loads due to boiling. Boiling of containment pools can occur also at pressures higher than atmospheric. Although detailed analyses are not available, it has been evaluated that sufficient pool integrity is maintained also in this case.

There are many systems available for water injection and some of them are backed up by emergency diesel generators or they are direct diesel driven. Unborated water can be used if borated water is not available as fuel storages are designed to stay sub-critical in unborated water. Some of the available systems require in the beginning access into the containment or spent fuel storages, and some others require temporary electrical connections and manual operation of valves located outside the containment or spent fuel storages. All these systems in current plant configuration require manual operations if electricity or I&C is lost. Summary of these available systems and their limitations are presented in Table B-1. This information will be described in detail in SAM handbook (see Section B.6.1.1). During refuelling outages the in-containment fuel pool may be connected to reactor, and in this case systems providing water injection into the RCS supply water for in-containment fuel pool, as well.

Table B-1. Alternative available systems for water injection into the in-containment fuel pools and into the spent fuel storages

System	Manual oper. [1]	EDG backup	Remarks
Pool filling pump (SC3)	No	No	This pump can also be used to circulate water between pools and ECCS tank. Decay heat can be removed from the tank by the containment internal spray system or the LPSI system.
Circulation pump of emergency core cooling system tank (SC3)	No	No	
Pool water treatment to pool cooling system (SC3)			
From clean condensate tanks with make-up water pumps (SC3)	No	Yes	
Liquid supply system directly by hose or to pool by water treatment system and pool cooling system (EYT)	Yes [2] No [3]	No	
Containment internal spray system (SC2)	No	Yes	Spray water falls partly into the pool. Can be used only for containment storages with pool covers removed. Water from ECCS tank or sumps
By hose from fire water system or from fire truck (SC4)	Yes (only to install the hose to hydrant)	No	Fire water system has pumps with direct diesel drive. Valves can be operated manually by hand wheels. Containment or spent fuel storage can not be closed permanently if fire truck is used.

1) Manual operation inside the containment or spent fuel storage required
2) hose installation
3) water treatment and pool cooling systems are used

In Table B-2 the durations to pool boiling, loss of radiation shielding and core uncovering are given. These time delays are mostly highly conservative because they don't assume any heat transfer from pool water to structures or gas (adiabatic case).

More detailed analyses are ongoing to assess the impact of heat transfer to structures or heat transfer through structures into the environment. Also efficiency of steam cooling will be assessed in these analyses. As the fuel bundles in Loviisa NPP are canned, steam flows upwards and cannot escape sidewards. According to preliminary results steam cooling is sufficient for a significant time, especially with low decay heat power.

Table B-2. Time to boiling, loss of radiation shielding and fuel damage in fuel pools in limiting cases after loss of decay heat removal

	Operating conditions	Start of boiling	Loss of shielding	Fuel uncovering
Containment pools	After fuel loading: Connected fuel pool & well 1	16.8 h	5 d 5 h	6 d 10 h
	Low pool surface during gate maintenance	43 h	8 d 20 h	10 d 16 h
	Core unloaded: Connected fuel pool & well 1	3.4 h	1 d 10 h	1 d 19 h
Spent fuel storage 1	Normal situation	99 h	25 d 4 h	35 d 0 h
	Less than 1 year cooled fuel	49 h	14 d 16 h	20 d 14 h
Spent fuel storage 2	Single pool decay power highest possible	90 h	21 d 12 h	29 d 20 h
	Pools combined; decay power highest possible	190 h	43 d 10 h	60 d 2 h

Heat transfer from the containment to the ultimate heat sink

The containment is made of steel and this allows heat to be efficiently transferred through the containment shell to the outer annulus of the reactor building. From the outer annulus heat is in the long term partially transferred through reactor building outer wall and roof into the environment. This means of heat transfer is fully passive and can not be prevented. The transferred power is not very high and is not sufficient alone for decay heat removal. Significant heat sinks in the containment in a short term are also two ice-condenser sections, steel structures and concrete structures creating significant time delay to the demand of other cooling means by ultimate heat sink.

Decay heat removal from the containment can be done by containment internal spray system, which automatically starts if the containment pressure exceeds 1.17 bar (abs), or by the containment external spray system, which is primarily planned to be used in severe accidents. Lowering the heat loads from primary circuit into containment can be done by the LPSI system by feed & bleed. With low decay power the steam generation is low and use of low pressure safety injection alone might be sufficient to keep the containment pressure below design pressure.

Electrical systems

Electrical systems are discussed in Section B.5.1.

B.1.2 Significant differences between units

The plant units have the following differences that may affect the accident management.

- There are two emergency feed water pumps in LO1 and four in LO2.
- There is an additional large-scale diesel generator common for both units at the site. The control of this device is only at LO1 MCR, but local operation is also possible.
- Two boron mixing tanks for borated water production are located only at LO1.
- The spent fuel storages and their cooling is connected with LO2 systems.
- The normal fire water control systems are located at LO1, and diesel powered fire water pumps at LO2.
- The containment external spray water cooling system pumps are located at the sea water pumping station of LO2.
- Equipment and electrical system room ventilation have differences between units.

Other differences between units are minor regarding their safety significance.

B.1.3 Use of PSA as part of the safety assessment

The level 1 PSA for Loviisa NPP was completed for the first time in 1989. Currently, it covers internal and external events including fires, floods, seismic, severe weather and man-made external events for full, low and non power states. Fire PSA for shutdown states was completed in November 2011 showing fire initiators during shutdown contributing 2% of the total core damage risk. The PSA of unit 2 will be made in the near future. No significant differences between the units have been identified concerning high sea water and other severe weather phenomena. The risks related to in-containment spent fuel pool cooling are not yet fully covered in the analyses.

The goal of the level 1 PSA is to assess the core damage frequency of the plant by identifying the relevant accident sequences, systems, equipments and actions. PSA is utilized extensively for the safety related decision making of the plant. Therefore it must be detailed enough and it is updated constantly and reported annually. Living PSA provides continuously support in at least the following areas:

- identification of dominating risk contributors and possible means for reducing risk by plant modifications and improved procedures or other means;
- supporting new design and modifications;
- presently the main effort is the renewal of plant automation in 4 stages and several other modifications being designed in the same connection;
- risk-informed evaluation of safety classification;
- economic optimization and prioritization of design options;
- improvement of operator training;
- justification of temporary (and permanent) configurations, extended test intervals and extended outage times;
- justification of certain rules of Technical Specifications;
- risk informed in-service inspection (RI-ISI) of piping;
- equipment categorization for the maintenance program;

– risk follow-up; and
– annual refuelling outage risk estimates.

The flood PSA covers leakages that submerge equipment in large areas causing an initiating event and also failing safety components that would be needed in case of such an initiating event. A systematic identification and mapping of flood sources and spreading routes as well as equipment vulnerabilities to external effects has been done in the PSA. The secondary effects of risen temperature and humidity have been analysed in the PSA when necessary. External floods due to high sea water level are included in the weather PSA.

The severe weather risk assessment began with an identification of potentially risky weather-related phenomena including hydrological, oceanographic, meteorological and biological phenomena as well as man-made phenomena (e.g. oil spill accidents). Detailed analysis was carried out for phenomena and combinations that passed certain screening criteria. The main principles in the screening analysis were the following.

1. The phenomenon must have strength exceeding the design basis at 50% confidence with a frequency higher than 10^{-8}/a.
2. The phenomenon that exceeds the design basis must lead to detectable consequences at the plant, site or power grid, so that a reactor trip is actuated or the plant is run into a safer operating state.
3. The effect of the event is analysed 24 hours or to a stabilized state.
4. If the identified phenomenon can be foreseen 12 h beforehand no power operation risk is considered. A potential shutdown risk has to be studied if the cold state is not safe due to this phenomenon.

The screening phase produced relevant thresholds for each phenomenon, exceeding of which causes an initiating event and weakening some relevant safety function. It was taken into account that the thresholds can be smaller or lower with certain phenomena together with additional failures, like e.g. with high or low temperature and HVAC failures, with excess sea vegetation and strainer failures or with high sea water level and erroneous installation of the bulkhead gates during shutdown. Ultimately many weather-related phenomena and their combinations were analysed in detail, such as sea level, extreme water and air temperatures, wind taking into account tornados and downbursts, rain, snow, lightning, sea vegetation, fouling and transportations in the vicinity.

The fire risk assessment is based on world-wide statistics on fires in different rooms and buildings of nuclear power plants. Plant-specific fire frequencies were determined by the empirical Bayes method and allocated to different rooms based on their con-tents and characteristics. Consequences of fires were evaluated based on the fire loads and by taking into account fire suppression means.

The seismic risk analysis was initially conducted in 1992 and was updated in 2010. The analysis included the estimation of earthquake frequencies, assessment of seismic responses of structures and components, identification of vulnerable components and other seismic risks, assessment of consequences of failures, PSA modelling and quantification. The seismic risks were estimated very low due to the small level of seismic activity in Fennoscandia, and they contribute to only 0.3% of the total CDF for Loviisa NPP.

The most important risk contributor to the CDF is internal events during shutdown. Weather initiated events contribute to 20% of the total CDF, and slightly more than half of this fraction is due to shutdown states. Current analyses show that fire events cause around one sixth of the total CDF.

The current level 2 PSA for LO1 covers full, low and non-power states and it analyses accident sequences initiated by internal events, internal floods and weather events. Fire events are currently under development and will be integrated into the level 2 PSA in the future. The level 2 fire analysis is based on the level 1 fire analysis and it considers the same initiating fire events. Seismic events are not covered in level 2.

The most important categories in current level 2 PSA for LO1 resulting in large releases are internal events during shutdown (60% of the LRF), weather initiator during shutdown (20%), internal events at power (10%), and weather initiators at power (<10%). These results do not include fire and seismic events.

B.2 Earthquakes

B.2.1 Design basis

B.2.1.1 Earthquake against which the plant is designed

Characteristics of the design basis earthquake (DBE)

Section A.2 describes the basis of DBE criteria. When the Loviisa NPP units were built there were no regulatory requirements on seismic design, and earthquake loads were not considered separately in the design. The new systems, structures and components (SSC) critical to safety constructed after 1997 are designed and qualified to withstand the DBE. The DBE response spectrum is described in Section A.2, in Figure A-2. The corresponding horizontal PGA is 0.10 g.

Latest seismic PSA has been done in 2010 for LO1 with a set of ground response spectra defining frequencies and fragilities. Five discrete earthquake acceleration levels between 0.04 g, 0.07 g, 0.10 g, 0.20 g, 0.30 g and over 0.30 g are set with corresponding median frequency. Corresponding fragility estimation points in these discrete levels are 0.055 g, 0.085 g, 0.15 g, 0.25 g and 0.40 g. In this set of spectra horizontal PGA value 0,056 g is estimated to take place on median frequency of 10^{-5}/a, which is following the DBE frequency according to Guide YVL 2.6.

Methodology used to evaluate the design basis earthquake

Section A.2 describes how DBE is based on statistical analysis of historical data with adjacent geological and tectonic information. Based on seismic PSA 2010 the horizontal PGA value 0.10 g is expected to take place at Loviisa NPP with median frequency less than 10^{-6}/a which is over 10 times less frequent than the required frequency level in current design criteria.

Conclusions on the adequacy of the design basis for the earthquake

Due to the low seismicity of the Loviisa area, the fact that originally plant has not been designed against earthquakes does not post a major risk on the seismic safety of the plant. The seismic CDF is $1.47 \cdot 10^{-7}$/a (about 0.3% share of total CDF $4.7 \cdot 10^{-5}$/a), which indicate that there is no instant need for updating probability studies concerning DBE specification.

Ongoing efforts to develop and verify seismic design of NPPs in Finland are described in Section A.2. Final conclusions in detail level will be achieved later.

B.2.1.2 Provisions to protect the plant against the design basis earthquake

SSCs that are required for achieving safe shutdown state are examined up to 0.4 g median PGA level. Following SSCs are evaluated to have adequate capacity against earthquakes: reactor pressure vessel, pumps, valves, pipelines, the horizontal heat exchangers, switchyards, diesel generators, turbines, the biological protection cylinder in the reactor hall, the new automation equipment, relays, lightning, work planes, pack discharge, the fracture zones of the sea water canals, buildings and their concrete structures, control rods, hydro accumulator tanks, diesel fuel oil storage tanks.

Fragilities are assessed of following SSCs that are identified critical to seismic safety: steam generators, diesel control panels, diesel fuel oil storage tanks, motor control centres, battery chargers, main transformers, auxiliary transformers, transformers 6/0.4 kV, relay cabinets, reactor protection cabinets, power substation, main control benchboard, monitors on main control benchboard, main operator panels, RHR heat exchangers, feed water tanks, boron water and other tanks, component cooling expansion tanks, EFW pumps lubrication water tank, deionization tanks, demineral water tanks, pressurizer, ECCS hydro-accumulators.

Main operating contingencies in case of damage that could be caused by an earthquake and could threaten achieving safe shutdown state are studied in seismic PSA. The most significant direct failures due to earthquake are presented below including consequential indirect effects of the failures. Reference PGA is 0.085 g from the fragility analyses as a closest value compared to the DBE value of 0.10 g.

The movement of steam generators could cause a large loss of coolant accident. The conditional failure probability in case of PGA 0.085 g is estimated $9 \cdot 10^{-3}$… $4 \cdot 10^{-2}$. The breakage of LPSI accumulator piping could prevent the use of the accumulators to control the loss of coolant accident. The conditional failure in PGA 0.085 g is estimated as $3 \cdot 10^{-4}$. The steam generator failure event is estimated to cover 54% of the seismic risk, which presents about 0.16% share of total CDF.

The rupture of the feed water tanks could cause flood, which can lead to the loss of I&C. If this happens, the decay heat removal depends on the auxiliary emergency feed water system. The conditional failure probability in PGA 0.085 g is estimated as $3 \cdot 10^{-3}$. The event is estimated to cover 32% of the seismic risk, which presents about 0.10% share of total CDF.

The monitors of the control room may fall on the main control benchboard, which limits the accident management possibilities. The conditional failure probability in PGA 0.085 g is estimated as $2 \cdot 10^{-4}$. The event is estimated to cover 8% of the seismic risk, which presents about 0.02% share of total CDF. This risk will be eliminated after the completion of the ongoing automation renewal.

The DC power could be lost due to moving of the electrical cabinets or the battery chargers. The conditional failure probability in PGA 0.085 g is estimated as $3 \cdot 10^{-5}$. The event covers roughly 2% of the seismic risk.

The movement of the pressurizer may cause a loss of coolant accident. The conditional failure probability of the pressurizer in PGA 0.085 g is estimated as $3 \cdot 10^{-5}$. The event covers roughly 1% of the seismic risk.

The significance of other seismic failures is very small. Other events cover roughly 3% of the seismic risk.

Loss of external power supply may be due to failure of the main transformer relay cabinets or other relay cabinets, or due to loss of the power substation. The frequency estimate for loss of offsite power due to earthquake is roughly $2 \cdot 10^{-8}$/a. By taking into account the possible failures of plant internal equipment due to the earthquake, the resulting CDF estimate is roughly $6 \cdot 10^{-10}$/a, which is 0.4% of the total seismic risk. The conditional probability of loss of offsite power in the case of the 0.085 g DBE is $9 \cdot 10^{-6}$.

The road access can be lost due to fall of trees or due to ruptures on the paving, which can delay access to site. In addition, the external power supply can be lost as described above.

There are no nearby industrial buildings that could pose a threat to the plant in case of a notable earthquake.

The movement of transformers could cause oil leaks and short-circuits that result to fires. The conditional probability of transformer failure in case of PGA 0.085 g earthquake is estimated as $2 \cdot 10^{-11}$. The total transformer failure frequency due to earthquakes is roughly $5 \cdot 10^{-10}$/a. The consequences of the resulting fires have not been analysed further because of the extremely low failure frequency, and thus, core damage is conservatively assumed in the seismic PSA.

B.2.1.3 Compliance of the plant with its current licensing basis

Due to the low seismicity of the site, no processes for ensuring seismic safety critical SSCs for achieving safe shutdown after earthquake, or limiting indirect effects are specified especially for earthquakes. Common maintenance, testing and monitoring of SSCs is considered to include also preparedness against seismic events.

The use of mobile equipment is considered to some extent in connection to severe accident safety functions in Section B.6.

Earthquake was not demanded as a design basis for Loviisa NPP. Seismic requirements are taken into account in modifications and building of new systems and structures since 2001. Living seismic PSA is used to verify appropriate safety level for safe shut down.

B.2.2 Evaluation of safety margins

B.2.2.1 Range of earthquake leading to severe fuel damage

In the seismic PSA, it has been assessed that the risk related to earthquakes smaller than 0.04 g is negligible. The conditional core damage probabilities (CCDP) at power operation after earthquakes of different level are presented in Table B-3.

Table B-3. CCDP related to different earthquake levels

PGA (g)	**0.04…0.07**	**0.07…0.10**	**0.10…0.20**	**0.20…0.30**	**0.30…**	**TOTAL**
Frequency (1/a)	$3.2 \cdot 10^{-5}$	$4.5 \cdot 10^{-6}$	$1.1 \cdot 10^{-6}$	$2.5 \cdot 10^{-8}$	$2.1 \cdot 10^{-9}$	$3.7 \cdot 10^{-5}$
CDF (1/a)	$7.5 \cdot 10^{-9}$	$1.6 \cdot 10^{-8}$	$6.5 \cdot 10^{-8}$	$1.1 \cdot 10^{-8}$	$2.0 \cdot 10^{-9}$	$1.0 \cdot 10^{-7}$
CDF Share	7.4%	16%	64%	11%	2.0%	100%
CCDP	0.024%	0.36%	6%	43%	96%	

According to the PSA of 2010, steam generators and feed water tanks are the most probable seismic contributors to cause core meltdown. The failure of the feed water tanks is estimated to cover 32% of the seismic risk, and the failure of the steam generators is estimated to cover 54% of the seismic risk. However, when the DBE 0.1 g to be applied for new structures is considered, the capacity of the feed water tanks and the steam generators can be considered adequate. The median capacity of the feed water tanks is estimated as 0.28 g and the median capacity of the weakest steam generators is estimated as 0.17 g. Corresponding high confidence of low probability of failure (HCLFP), 95% confidence of a less than 5% probability of failure values are for feed water tanks 0.10 g and for weakest steam generators 0.06 g.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a more detailed evaluation of the seismic stability of spent fuel pools and the fire fighting systems against earthquakes beyond the current DBE level at the Loviisa NPP site.

B.2.2.2 Range of earthquake leading to loss of containment integrity

The reactor containment has not been considered in seismic PSA studies conducted in 1991 and 2010. There are no PGA limit state estimations for the containment at the moment.

B.2.2.3 Earthquake exceeding the design basis earthquake for the plant and consequent flooding exceeding design basis flood

External floods due to an earthquake are not plausible in the Loviisa area as explained in detail in Section B.3.1.1. There are no nearby rivers or dams, and the probability of a tsunami in the Gulf of Finland is negligible.

B.2.2.4 Measures which can be envisaged to increase robustness of the plant against earthquakes

According to the seismic PSA of 2010, the share of the seismic core damage risk is 0.3% of the total risk of the plant. Consequently, the plant robustness against earthquakes can be considered adequate.

Certain plant modifications will decrease the seismic risk further. New sump strainers were installed in September 2011 to prevent fuel element clogging after large loss of coolant accidents. Although not related to lessons learned from Fukushima accident, this decreased the seismic risk by over 20% to $1.12 \cdot 10^{-7}$/a (0.3% of the total risk) because the risk related to loss of coolant accidents resulting from steam generator breakage was reduced. Currently, the most important contributors to seismic risk are: steam generators (44%), feed water tanks (38%) and control room monitors (10%).

Additionally, the ongoing automation renewal includes replacement of plant equipment with new, seismically qualified equipment. This will further decrease the seismic risk by roughly 10%.

To respond STUK's requirements after Fukushima accident, Licensee is studying seismic fragilities of pool structures of reload batching in reactor containment and pools in spent fuel storages. Analyses cover PGA levels of 0.1 g, 0.2 g, 0.3 g and 0.4 g in order to research seismic capacity such structures on and beyond current DBE level combined with possible boiling of pool water. Also seismic fragility of fire water systems is under study.

B.3 Flooding

The spent fuel storage pools in the reactor building and in the intermediate storage building are cooled with systems depending on the same electricity sources and seawater and intermediate circuits as the reactor. The following description covers both the reactor and the spent fuel pools.

The possibility of flooding due to exceptional precipitation is considered in connection with extreme weather condition in section B.4.

B.3.1 Design basis

B.3.1.1 Flooding against which the plant is designed

Loviisa NPP is situated in the Hästholmen Island on the coast of the Gulf of Finland. The Hästholmen Island is mainly bedrock, the area of the island is order of 1 km^2, and the maximum elevation is 16 m. The Hästholmen Island belongs to the inner Loviisa archipelago with typical sea depth of about 5 to 20 m. There are no bigger rivers or river dams in the vicinity of the plant. The open sea outside the archipelago starts about 10 km to the south from the plant. The width of the Gulf of Finland is less than 100 km and the depth about 50 m. The post-glacial uplift rate at Loviisa is 3 mm in a year which is comparable to the present global rise of the seawater level. It is predicted that in the future the rate of seawater level rise will exceed land uplift rate, but during the expected life of Loviisa NPP, i.e. before 2030, the difference will be small.

The water levels and elevations are given in the N60 coordinate system. At Loviisa the long term average seawater level has been +0.0 m with the accuracy of about 15 mm during the lifetime of the plant. Under certain conditions, seawater could rise to its peak level at a rate of 10 cm/h, possibly even faster.

The design basis of Loviisa NPP for high seawater level is +2.1 m but the actual flooding threshold level is higher during power operation. The consequences of flooding are different depending on whether residual heat removal is possible through the secondary circuit or not (unpressurized primary circuit).

The seawater level (mean sea level) refers to the average level over a measuring period of a few minutes as opposed to the momentary level caused by waves. Figure B-2 presents the estimated frequencies of exceeding specific water levels in 2000 and 2040.

The frequency distribution of the seawater level maxima is well justified at least up to a water level of +2.00 m. Exceeding this level requires a situation in which all the factors impacting the level would be at their maximum simultaneously. Factors impacting the seawater level and their expected maximum values are

a) Total volume of water in the Baltic Sea 0.83 m
b) Rise in the mean sea level as a result of strong wind 0.60 m
c) Specific phase of a standing wave (seiche) 0.20 m
d) Low air pressure 0.40 m
e) Tide 0.10 m

The sum of the maxima is 2.13 m.

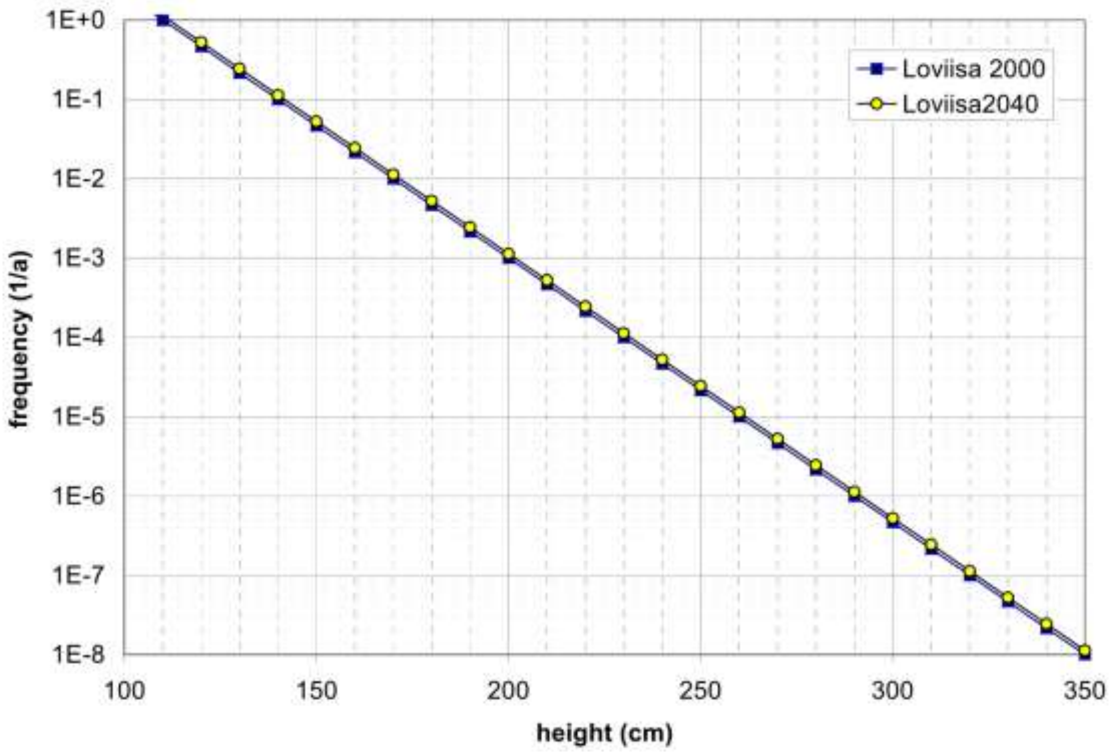


Figure B-2. The frequency distributions of the seawater level maxima in relation to the theoretical mean sea level at Loviisa in 2000 and 2040.

The phenomena listed above are well known and their occurrence can be predicted with high confidence at least one day in advance on the basis of routine weather forecast. Seawater is typically high at the end of the year and in winter (November to March).

The total volume of water in the Baltic Sea increases if storms raging in the North Sea push water through the Danish Straits into the Baltic Sea. After the storms have subsided, water flows back to the North Sea via the strait, but it takes several weeks until the surface returns to a normal height.

Without exception, an unusually high sea level is associated with high wind. In January 2005, the sea level at Loviisa NPP was +1.77 m and the wind speed was 11– 18 m/s as an hourly average. According to the estimate made by the Finnish Meteorological Institute in the early 1990’s, a height of +2.50 m at Loviisa NPP would require a wind speed of 30…40 m/s as a 10 minute average or 3-second gust speed of 40…60 m/s at a 10 metre elevation.

The seiche effect is a continuous phenomenon and refers to the free spill over of water across the Baltic (very long standing waves). High pressure on the Baltic Sea with a simultaneous low pressure on the Gulf of Finland will raise the water level in the Gulf of Finland. Strong winds are often associated with a low pressure front, so these phenomena can occur simultaneously.

The Baltic Sea is protected from strong impacts of a potential devastating tsunami occurring at Atlantic Ocean by its location behind the wave shadow of Norway and the shallow shelf of the North Sea and the Danish Straits. The strength of a tsunami originating from the Baltic Sea is efficiently restricted by the shallowness of the Gulf of Finland and the archipelago of the islands in front of the site.

Atmospherically generated meteotsunami is the most probable type of the tsunamis in the Gulf of Finland. The meteotsunami is caused by a travelling thunder front, but the phenomenon is not thoroughly investigated, yet. Meteotsunamis are not included in the weather forecasts and early warning at the plant cannot be assumed. Meteotsunamis could most likely occur during the summer season, when the average sea level is low in the Gulf of Finland. Thus, the sea level following the meteotsunami would not be very high. On the other hand, the annual refuelling outage of Loviisa NPP is normally scheduled for the summer or autumn, and a meteotsunami could occur when the critical flooding height of the plant is at its lower value, +2.1 m.

Plant response - Power operation

During power operation massive flooding is possible through doors and other hatches of the plant buildings. The grade level of the yard is about +2.9 m and the door sill level about +3.0 m. Flooding through doors is possible if the seawater level rises above +3.0 m or if seawater level exceeds +2.5 m and strong wind from an unfavourable direction drives water to the yard.

Water would first enter the turbine hall through doors and hatches. When the turbine halls of both units are filled up to the level of +1.0 m water starts to flow through cable tunnels into the reactor building basement. High and low pressure emergency core cooling pumps are situated in the reactor building basement and would be lost. Because components of the primary coolant pump seal cooling system are also situated in the reactor building basement, there is a possibility that primary coolant pump seals start to leak and at the same time the emergency core cooling pumps are lost.

In the PSA, it is assumed that the rise of seawater above the +3.0 m level will lead to core damage. Conservatively, no credit is given, e.g., to the flood spreading time inside the buildings.

Plant response – Refuelling outage

During the refuelling outage the sea water cooling systems can be open for maintenance. Seawater flooding inside the plant from the intake side is prevented by the steel sluice gates installed at +2.5 m and the condensers installed at 3 m on the turbine hall. On the discharge side, the top level of the bulkhead gate preventing seawater from flowing backwards into the open seawater system is at 2.1 m. If the seawater level exceeds 2.1 m, water starts to flow into the turbine hall when the manholes of the sea water piping are open due to maintenance. When the turbine hall is filled over the level of −0.20 m, the usual connection at outage to the external power grid through the start-up transformer can be lost. It is possible to connect the power to the other main transformer. It is assumed that, if the countermeasures fail, the rise of the seawater level above +2.1 m will lead to core damage during cold or refuelling outage.

The flood levels described above have to last several hours because time delays related to filling up the plant compartments in these situations are long. Typically, the duration of flood maxima in the Gulf of Finland is a few hours and the analyses can be considered conservative.

Conclusions on the adequacy of protection against external flooding

The frequency estimate for the sea water level to rise above the critical 3 m is approximately $4 \cdot 10^{-7}$/a. During refuelling, the plant is more vulnerable to high seawater level. However, the annual refuelling outages are scheduled for late summer - autumn when the seawater levels are lower than during winter.

The core damage risk due to high seawater level is estimated to constitute 3 % of the current total risk. The risk due to high seawater can be considered small but it is not negligible. The potential vulnerabilities have been identified previously in probabilistic safety analyses and periodic safety reviews, and the topic has been included in the process of continuous safety improvement. The stress test did not reveal such new vulnerabilities that would require immediate measures.

Some improvements are under consideration as discussed in Section B.3.2.

B.3.1.2 Provisions to protect the plant against the design basis flood

The most critical target is the turbine building. During annual outage, the critical level is +2.1 m and during power operation +3.0 m. If the flooding water in the turbine building rises above the weir walls (+1.0 m), seawater will spread through the cable channels into the reactor and auxiliary building. In the reactor building, both emergency cooling pump rooms and the sealing water system of the main circulation pumps will become submerged under water. The weir walls in the cable tunnels between the turbine hall and the reactor building basement were built to limit flood spreading in the case of a rupture of seawater pipes. The weir wall crest elevation +1.0 m covers typical annual variation of seawater level but not the most extreme cases.

Seawater level +1.5 m

If the sea level rises above +1.5 m, seawater could, e.g. in the case of failures of drain check valves, flood backwards via the drainage piping into the basement drainage wells and further into different parts of the plant. Flooding via drainage piping is slow. It will take several hours for the level to rise to the turbine hall's –0.20 m level. It is highly improbable that seawater would rise higher inside the plant during the flood cresting period. However, an initiating event leading to reactor scram or the loss of main feed water can occur during the cresting of the flood.

From the reactor building's drainage water pumping plant, water can enter the reactor building's pipe tunnels via the drainage wells, but the rate of flow via this way into possibly high-risk spaces is so slow that there is plenty of time for countermeasures and the risk is considered insignificant.

Residual heat is removed during hot plant operating states by emergency feed water system or by backup emergency feed water system. Heat removal in cold plant operating states is not endangered. The risk related to the sea level rise over 1.5 m is negligible.

Seawater level +2.1 m

If the sea level rises above +2.1 m, the design basis is exceeded, and the plant units should be brought into a shutdown state. If either of the plant units is in annual outage (a cold or refuelling outage), water will flow over the discharge side's bulkhead gate in the main seawater piping and through hatches into the turbine hall, in addition to what was presented for seawater level +1.5 m. Water will spread into both units via the turbine hall's bottom floors. The flooding of the turbine building causes the main condensate and plant makeup water pumps and the conventional intermediate cooling circuit's pumps to be submerged under water. As a result of a complete loss of the conventional intermediate circuit, the supply of the main and emergency feed water pumps and the residual heat removal pumps will be lost. Also emergency core cooling systems and main circulation pump seal water system may be lost. The emergency feed water system will be lost once the feed to the plant makeup water stops. Residual heat is removed during hot plant operating states by auxiliary emergency feed water system and integrity of main circulation pump seals is ensured by closing seal water back pressure line isolation valves. If the primary circuit is opened, the residual heat removal capability is lost. The heat transfer from the containment to the ultimate heat sink is explained in Section B.1.1.2.

Even if the flood exceeded the turbine hall level +1.0 m during cold or refuelling outage, removal of residual heat is possible by feeding water into the open primary system by temporary arrangements and boiling it.

Seawater level +2.5 m

The maximum theoretical sea level maximum was estimated as +2.13 m. Should the sea level, however, rise above +2.5 m, the phenomenon would be associated with extremely strong wind that could cause a loss of offsite power and push waves of water into the yard area; the water would flow through doors and other hatches into the turbine hall. The flood could not be isolated. Otherwise, the consequences are equivalent to the sea level rise above +2.1 m. Spent fuel storage cooling system will also be lost if the service water system pressure transmitters installed above +1.0 m level of the turbine hall are submerged.

Seawater level +3.0 m

Should the sea level rise above +3.0 m, the yard would be flooded and the road would become submerged under water. Water would flow through doors and other hatches into the building with the same consequences as with the sea level rise above +2.1 m and +2.5 m. Additionally, it is estimated that the auxiliary emergency feed water and emergency diesel generators will be lost. Some uncertainty is related to the water level that would cause the unavailability of the auxiliary emergency feed water. Pump failure could be caused by submerging of the pumps (installed at +3.35 m), wetting of the control cabinet live parts (+3.2 m) or significant flooding in the fuel tank room (floor level of +2.5 m).

Provisions to prevent flood impact to the plant

Flood protection is implemented through the selection of the design basis against high seawater level and ordinary civil engineering and process design solutions. The design basis and the plant response to various levels of seawater are presented in Section B.3.1.1 and earlier in this section. Flood barriers (weir walls) have been built in the cable tunnels between the turbine hall and reactor building as described above. There are no external structures built especially to prevent flooding.

The plant has operator instructions for unusually high sea level. The following actions are triggered by increasing seawater level.
– Seawater level over +1.3 m: Inspection rounds to lower plant compartments are increased and flood alarms and basic water pumps are tested.
– Seawater level over +1.5 m: Lower plant areas and basic water pump houses are brought under continuous surveillance. STUK is informed of an unusually high sea level. If further sea level rise is forecast, the line organization is alerted.
– Seawater level over +1.75 m: Preparations for shutdown are started. Depending on the forecast, shutdown may be commenced. If the plant is already in cold shutdown, seawater pipes possibly open due to maintenance are sealed.
– Seawater level over +1.95 m or seawater level over +1.85 m and the wind speed exceeds 25 m/s: The plant is brought to a hot shutdown state. Further operating state changes are considered depending on the situation.

If it is expected that water flows over the discharge side's bulkhead gate during annual outage, flood can be prevented by closing opened sea water system hatches in advance.

Situation outside the plant

The Hästholmen Island is connected to the mainland with a 200 m causeway including a short bridge. The nearby islands and a breakwater partially prevent high waves from flooding the road. The elevation of the road is +2.9 m at the gate, +3.5 m in the middle of the strait and +3.8 m at the bank of the island. The bridge should be accessible even if the sea level would reach the critical level of +3.0 m. The road that leads to the Hästholmen Island is more vulnerable to flooding. A specific road section at a distance of 12 km from the plant is flooded if the water level rises to +2.0 m. The road would probably still be accessible to trucks but not to passenger cars. However, it is possible to go around the vulnerable parts of the road using a local inland road on much higher terrain.

Additionally, strong winds could temporarily cut the road leading to the plant by falling trees on it. Under normal conditions the road could probably be cleared quite quickly. Extreme flooding is in practice possible only in connection of unusually high winds possibly causing widespread damage, possibly also to the power transmission grid, and the rescue services might be overburdened. See also Section B.4 on the effects of extreme weather conditions.

B.3.1.3 Plant's compliance with its current licensing basis

The bulkhead gate is installed on the discharge side of the seawater system during annual outage to isolate pipeline sections and to prevent seawater from flowing backwards into the plant. The bulkhead gate can also be constructed to isolate a seawater system pipeline leakage. The condition of the bulkhead gates and related structures can be monitored visually during the installation of the gates.

The condition of seawater system pipes and other pipelines is inspected regularly according to piping inspection programs. Critical systems and components are tested according to test intervals defined in the Technical Specifications.

The use of mobile equipment during flooding is not planned by Loviisa NPP.

Deviations from the licensing basis have not been observed.

B.3.2 Evaluation of safety margins

B.3.2.1 Estimation of safety margin against flooding

The critical level of Loviisa NPP for flooding is +3.0 m during power operation. The maximum measured seawater level during the plant's operating history is +1.77 m (January 2005). An estimate by the Finnish Institute for Marine Research for the theoretical maximum level is +2.13 m.

The critical level +3.0 m is well above the observed maximum and the estimated theoretical maximum. The statistically estimated frequency for exceeding the critical level +3.0 m is quite small, $4 \cdot 10^{-7}$/a.

The plant is more vulnerable to high seawater level if either of the plant units is in cold shutdown and the seawater system has been opened for maintenance. In this situation, the critical height is +2.1 m. However, the refuelling outages are usually scheduled for period from August to October when the seawater levels are significantly lower than during winter. Additionally, the open hatches of the seawater system can be closed in advance if the seawater level is rising.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan and schedule to ensure plant safety in case of abnormal sea level at the Loviisa NPP site.

B.3.2.2 Measures which can be envisaged to increase robustness of the plant against flooding

Measures have been recently implemented to improve main transformer availability during cold and refuelling outages, and its recovery is now possible in 3 hours. The main transformer can be used to restore offsite power if the usual connection during outage (110 kV) is lost due to flooding of the turbine hall. To further improve possibilities to recover availability of the main transformer, the actions needed should be taken into account in procedures.

To respond to STUK's requirements after Fukushima accident, Licensee is studying the following improvements to reduce flooding risks.

- Modernization the bulkhead gates used to close the cooling water discharge openings. The concrete bulkhead beams would be replaced with steel sluice gates equipped with seals. In the same connection, the top level of the gates would be raised from the +2.1 m level to +2.45 m, which corresponds to the top level of the intake pipe's gates. This would decrease the risk related to flooding during annual outages by the order of magnitude.

- Flood banks and new check valves for rainwater drains could be installed to prevent seawater from flowing inside the plant.
- Higher flooding barriers in the tunnels between the turbine and reactor buildings would prevent, or at least delay, water spreading inside the plant.

In the recent years, the annual refuelling outage has been in August – October. Flood risk increases if the annual refuelling outage is done later and decreases if the outage is done earlier in the summer. On average, the seawater level is at the lowest in June.

B.4 Extreme weather conditions

B.4.1 Design basis

External phenomena other than earthquakes and external flooding considered as original design basis for Loviisa NPP are the following:

Maximum air temperature

Original design basis for the HVAC systems is +25°C. Original design basis for the HVAC systems of the new automation building is +33°C.

Minimum air temperature

General design basis for low external air temperature is –28°C.

High seawater temperature

The design basis for seawater temperature is +23°C for systems cooled by seawater. The emergency diesel generators are dimensioned for sea water temperature of +25°C, and the design basis for new automation buildings is +27°C.

According to the water permit under the Finnish water legislation, the temperature of the discharge water may not exceed +32°C, which determines that the temperature of the plant's intake cooling water should not exceed about +23°C when both units are operating at maximum capacity.

High winds and storms

The design specifications for the structures are based on the speeds of a 3-second gust at a 10-meter elevation and the design basis for strong winds for non-bearing structures is 36 m/s.

Load-bearing plant structures i.e. steel and reinforced concrete structures have been designed with respect to radiation and fire protection aspects and can withstand considerably higher wind speeds. The steel frames of the turbine building, control room buildings as well as the load-bearing steel frames of other buildings are presumed to withstand high wind loads.

The design basis of power line poles was 700 N/m^2 equivalent to 3-second wind gust speed of 33 m/s. Taking into account the safety factor of 1.4, this equals a wind speed of 39 m/s. When the wind speed exceeds 45.5 m/s, the design basis for non-load-bearing structures will be exceeded, even the safety factor of 1.6 taken into account.

Heavy rainfall

Original design basis for rain water runoff in the yard and on the roofs is 0.02 $(l/s)/m^2$ or 72 mm/h of rain. The roofs are originally designed to withstand 180 mm layer of water or a corresponding amount of snow (roughly 1800 mm).

Design basis derives from construction regulation in effect during the site construction. Since then, the site yard has been resurfaced a few times and additional buildings have been constructed. However, the original design basis is valid.

Lightning

The original design basis for Loviisa NPP is 0.02 lightning strikes/a for reactor buildings and less for ventilation stack and other buildings. Lightning protection systems of the site buildings are designed according to guide by Electrical Inspectorate.

B.4.1.1 Reassessment of weather conditions used as design basis

High and low air temperature

The air temperature, about +28°C may lead to an administrative power reduction through a potential alarm of high oil temperature of main transformer.

A high air temperature, about +35°C may lead to an administrative reactor shutdown if the alarm temperatures of flow through cooled room spaces are exceeded. The raise of air temperature up to +40°C will endanger safe shutdown.

High seawater temperature

A high seawater temperature alone does not cause initiating events in power operation and hot plant operating states, but it may hamper the cooling of the instrumentation rooms as well as the controlling of the initiating events requiring a residual heat removal chain. High seawater temperature has been taken into the consideration when evaluating the low pressure safety injection sump recirculation possibility after the loss of coolant accidents.

A rise in temperature is estimated to lead to a shutdown through power reductions before the temperature rises to the point causing a scram and the loss of control equipment. When the temperature of the seawater rises above 20°C at the intake side, the emergency heat transfer chain will be tested and the plant power limited, if needed. According to the licensee's studies, the HVAC system of the equipment rooms in the control room building operates normally even when the seawater temperature is about 30°C. The high-pressure tripping preventing the equipment to function requires the temperature of the seawater to rise above 35 °C. Thus, high seawater temperature does not impact the probability of losing the instrumentation room ventilation.

High winds and storms

The maximum speeds for wind gusts are higher than for sustained winds, and wind speeds at higher elevations are higher than at lower elevations. A 0.3-second wind gust is already adequate to damage structures, but short-term gusts don't have enough time to impact the plant's relatively low, massive concrete structures. The shortest duration gust selected for assessment in the intensity-frequency distribution assessments is 3 seconds.

The design basis of the structures and power grid has been determined in terms of wind load, as well as the safety factors related to the design and materials of the structure. The structure is expected to break when the wind speed exceeds the design basis and safety factor value. The breakage probability of a structure designed in compliance with the National Building Code of Finland, derived from the load and durability distributions of an ordinary structure at the design point, is about 10^{-3} when the safety factors have been taken into consideration. This design basis is also valid for the structures of Loviisa NPP.

The concern in evaluating a storm's impacts is the non-process facilities. The material thicknesses of structures such welding halls, warehouses, barracks, information building, revision cafeteria and simulator building has been minimised without using any safety factors. The concern will arise from the potential detaching and partial breaking of these structures due to strong storm, which may carry the detached parts to more vulnerable plant areas, such as the switchyard and seawater plant's intake openings.

Potential, hidden faults in the mounting of the claddings of plant structures, rainwater gutters and roof structures may also cause the above-mentioned problem. In the weather risk analysis of the Loviisa PSA, it is presumed that cladding and roofing panels are mounted in accordance with the manufacturer's instructions i.e. their design basis has been the same as for non-bearing plant structures (36 m/s), however, without the safety factors. The wind speed of 36 m/s corresponds to the pressure of 800 N/m^2. The uncertainties in this assumption are caused by hidden installation errors, corrosion and fatigue of the mountings. Additionally, structures like gutters and downspouts, for example, are not similarly designed. However, the forces on these during a storm are considered to be milder due to the smaller surface area.

When the wind speed exceeds the design basis of 45.5 m/s, a limited breakage of non-load-bearing plant structures with a safety factor of 1.6 is presumed. According to the strength analysis of the licensee, the turbine hall can withstand an air pressure exceeding the design basis. The turbine hall can better withstand the loads caused by ordinary winds than the pressure created by a tornado affecting simultaneously all surfaces. The pressure caused by a tornado is estimated to exceed the turbine hall's tolerance at the wind speed of 46.3 m/s, conservatively presuming that the cyclone encloses the entire turbine building. It is estimated that the turbine hall can withstand downbursts and unidirectional winds up to 65.5 m/s.

According to the licensee's estimations the ventilation stack withstands an average hourly wind of 25 m/s measured at the height of 10 m, which at Loviisa NPP equals a wind gust of 53 m/s for a time average of 1…3 s.

<u>Lightning</u>

The original design bases for lightning have been re-evaluated in the PSA analyses. It has been estimated that the strike frequency to the plant buildings is 0.03…0.14 /a based on the 30 kA strike. About 92% of the lightning strikes exceed 10 kA and roughly 1% exceeds 150 kA.

Risks that lightning can pose to Loviisa NPP include: loss of offsite power, grid disturbances, fire and disturbances or damaging of instruments and automation possibly leading to reactor trip.

During 1990's several additions were made to lightning protection systems. Lightning protection of site buildings is presumed adequate above the ground level after the modifications. Additionally, the lightning protection of buildings below ground level is nowadays in accordance with the modern guidelines such as German KTA 2206.

Low seawater level

An extreme low sea water level can prevent sea water pumps from operating. The main sea water pumps will trip and service water pumps will not to be operable when sea water level is around –2 m.

If oil, algae or frazil ice blocks the sea water intake, it is possible to get cooling water from the discharge side of the sea water circuit. If the sea water level is lower than –0.5 m, the weir at the discharge side hinders the use of the discharge as an intake. The probability that the seawater level is below –0.5 m is estimated to be 0.015 according to the licensee’s PSA studies.

Geomagnetic storms

A geomagnetic storm is caused by a solar wind shock wave that interacts with the Earth's atmosphere. This could cause damage to electric grid, if geomagnetic currents are induced in long transmission lines.

The effects of geomagnetic storms on Loviisa NPP have been studied. According to the Finnish electricity transmission system operator Fingrid, the transmission grid in Finland is well protected against geomagnetic storms due to the durability of the installed capacitors, transformers and relays, and due to the grounding principles used. The risk to Loviisa NPP is low, although strong geomagnetically induced currents could cause overheating of main transformers.

Verification of weather conditions used as design basis; frequencies

The distributions of the maximum annual wind speed, sea level, rain/snow events and temperatures used in the weather risk analyses were determined based on local or regional meteorological data collected by Loviisa NPP, Finnish Meteorological Institute and Finnish Institute of Marine Research. The frequency and amount of sea-vegetation was based on site experience (”precursor” events). The basic exceeding frequency of a phenomenon was multiplied by a relevant fraction (e.g. wind direction sector, or the fraction of a year for certain conditions, or relative target area for cyclones) to obtain the initiator frequency.

High air temperature

Exceptionally hot weather typically lasts for just a couple of days according to the past observations. Average temperatures are used due to short period of the daily high temperature and the large thermal capacity of the buildings and equipment. The spaces with flow-through cooling are an exception to this because the temperatures of these spaces correlate to outdoor temperatures.

Based on the measurements of the intake air temperature of the instrument room cooling device during in July-August 2003, and the additional data observed at the Kaisaniemi weather observation station from 1830…2002, the licensee has evaluated the frequency distributions of the maximum average temperatures for one hour, six hours, 24 hours, one week, 30 days and 60 days. The Weibull distributions were found to be consistent with the observed data. Also exponential tangent has been applied in the extrapolated part starting from the maximum observation value. Six hour values are used in PSA.

Low air temperature

Average 24 hour temperatures are used due to short period of the daily low temperature is brief (a few hours) and the large thermal capacity of the buildings and equipment.

High seawater temperature

The frequency assessments for the cooling water temperatures are based on the observed measurements using Weibull distributions for one hour, 24 h and one week. The hourly observations are from 1998–2003. The 24-hour and weekly average observations are from 1977–2003.

High winds and storms

The frequency distribution for 3-second wind gusts at Loviisa NPP based on the measurement data of Loviisa NPP's meteorological mast in 1977–2005. Previous estimates and other observations from Rankki and Olkiluoto measuring stations have also been utilised. Frequency distributions at three different locations are presented: the top of the ventilation stack and the rooftops of the reactor building and the turbine building (at the heights of 107.5 m, 64 m and 35 m above ground). The speed of a 3-second gust blowing at the elevation of the turbine building's rooftop is about 1.05 times higher than the wind at an elevation of 10 m.

At the turbine building rooftop, the frequency estimate for winds correlates with the exponential distribution of $f(v) = 1.231E6\ e^{-0.6413\ v}$ /a. The wind speeds of tornados and downbursts are not estimated to vary according to elevations. Their frequency estimates, however, are affected by surface area, and their occurrence would cause an initiating event. The impact area of the plant is estimated to be 0.25 km^2 and the grid's right-of-way area 2.2 km^2. Frequencies for downbursts and tornados have been estimated by the licensee with the following functions.

Downbursts: $f(v) = 0.02822\ e^{-0.1534\ v}$

Tornados: $f(v) = 4.326 \cdot 10^{-6}\ e^{-0.01044\ v}$

The wind speeds of 28 m/s are dominant for the frequency of high winds at the plant area.

Near-ground wind measurements performed at Rankki and also at Loviisa include mechanical turbulence caused by the uneven surface. The disturbances are smaller in measurements made at higher elevations. This disturbance effect is visible when comparing the observations at different elevations at the Loviisa weather mast and at Rankki. Wind speed estimates on the basis of higher elevations are the most reliable due to smaller disturbances at higher elevations.

The gusting of wind increases closer to the ground surface, even though the average speed decreases. For this reason, wind speed observations with a longer integration time, e.g. at a 10-m elevation, do not provide a reliable picture of the frequency of 3- second gusts.

During the storm that raged in Loviisa on 23 January 1995, the mountings of the containment buildings' sheet-metal wall panels became loose in the gutter area. Repairs were underway as soon as within two days of the event, but loose mountings were still being detected two years later. Repairs have been made to over 100 m^2 of the sheet-metal area.

In January 1992, storm winds separated 700 m^2 of sheet-metal wall panels on the boiler building at Pohjolan Voima Oy's Kristiinankaupunki heat plant; the sheet-metal panels flew into the switchyard, causing a loss of offsite power. At the time, the measured wind speeds at a 10-m height in 3-second gusts were about 28 m/s.

The frequency estimate of a storm possibly detaching building facade materials is 0.0196/a (28 m/s at the turbine building rooftop) and it would lead to loss of offsite power for an average of two hours with a probability of 0.5. In case the loss of offsite power, both 400 kV connections are presumed to be lost, a major grid disruption (average duration 0.8 h) might occur with a 3% probability, according to the licensee's studies. Furthermore, the loss of 110 kV connection is lost due to storm with a high probability (0.667). The probability of an unsuccessful coupling of the 110 kV bus bar is estimated 0.023. The frequency of an electricity outage of 1…4 h is thus estimated to be $3.2 \cdot 10^{-3}$/a. The risk related to this event is low.

The frequency estimate of a storm causing a loss of offsite power for over 4 h is $9.6 \cdot 10^{-4}$/a according to the licensee's studies. The share of tornados and downbursts is $5.7 \cdot 10^{-5}$/a. The total frequency for the loss of offsite power is $1.2 \cdot 10^{-3}$/a, which results in core damage with the frequency of $3.8 \cdot 10^{-8}$/a (less than 0.1 % of the total risk).

The frequency of turbine hall damage is estimated to be $5.7 \cdot 10^{-7}$/a (due to tornados) and the estimated frequency of the ventilation stack falling is $4.9 \cdot 10^{-7}$/a, resulting in a total core damage frequency $1.1 \cdot 10^{-6}$/a (2.4 % of the total risk).

<u>Heavy rainfall on unfrozen ground</u>

Due to low frequency of the measurements of the rain there are no official data on rain intensity. Maximum amount of 198.4 mm over the 24 hour period have been measured in Lahnus, Espoo in 1944. In 1986, exceptionally heavy rain flooded the low areas of land with meters of water and damaged several buildings, bridges and roads. Amount or intensity of that rain was not measured. Bardö, Åland experienced heavy rain in 1991, which according the unofficial records measured over 200 mm of rain. The meteorological institute of Finland measured the intensity with the meteorological radar to have reached levels of 100 mm/h averaged over the 30 minutes period. Rain continued about 4…5 hours. According to the Doppler-meteorological weather radar operated by Helsinki

University the intensity of the rain may reach levels of several hundred mm/h in rain shower.

Heavy rainfall on frozen ground

During the cold season there is less rain than during summer due to smaller water vapour content in a colder air, and additionally, less vapour evaporates from water bodies and plants.

Lightning

Based on the average lightning strike of 30 kA, the strike frequency to any building at Loviisa NPP site has been evaluated to be 0.03…0.14/a. Ventilation stack and reactor building shield other buildings partially from lightning strikes of over 10 kA. Shielding is better against high current lightning strikes, and the strikes of over 30 kA hit almost exclusively to ventilation stack and roofs that are on the edges of building complex. The fraction of over 30 kA lightning strikes is about 50% of all lightning strikes based on the licensee's studies.

Based on plant experience it is evaluated that a moderate interference in instrumentation can occur 0.05/a. The frequency estimate for an unnecessary reactor trip initiated by lightning is 0.0025…0.01/a, and the estimate for a moderate disturbance in grid connection is 0.05/a according to the evaluation of international data.

Low seawater level

Probability distributions for monthly minimum sea level of the whole year and average of winter months used in weather risk analysis are based on the observations by the Finnish Institute of Marine Research 2008.

Combinations of extreme weather phenomena

Because of correlations between phenomena, the probabilities of combinations can be larger than the products of individual probabilities e.g. a high wind from a certain direction can raise the sea level, loosen vegetation and metal sheets (roof or siding), and thereby increase the probabilities of seawater inlet or heat exchanger flow blockages and loss of power events. The probability of frazil ice blocking the cooling (sea-) water intakes is highest during cold weather but only accompanied by high wind, and when the sea surface is not yet covered with ice.

Wind and algae

A strong wind together with a heavy concentration of algae in the seawater can cause a loss of offsite power and the clogging of the intake of the seawater pumps and the intake screens of the diesels' cooling pumps. The licensee has estimated the probability of algae occurring simultaneously with storms to be 0.20.

The loss of offsite power can be caused by sheet-metal panels being detached by the wind (> 28 m/s) and blown into the switchyard. This power outage will be restored in a short time, 1…4 h. During the outage, seawater pumps will stop and the diesels will start up. The service water pumps are operable. Diesels can trip in about an hour due to the possible clogging of the cooling water pumps' intake opening. This would lead to a loss of the cooling of the main circulation pumps' sealing water and possibly, thirty minutes later, to the loss of the integrity of the seals, in case the back pressure line isolation valves fail to close.

A very strong wind (> 39 m/s) might topple the main grid power line poles, which causes a long-term power outage (> 4 h). The repair of a small leak that has possibly occurred will be unsuccessful due to the total loss of power. If the small leak does not occur, the primary circuit residual heat can be removed with the auxiliary emergency feed water system.

Wind and frazil ice

Strong wind together with frazil ice can pose a threat of a loss of offsite power. At the same time, frazil ice can clog the intake of the seawater pumps and the intake screens of the diesels' cooling pumps. However, the licensee has assessed the event to be highly improbable.

In order for frazil ice to enter the cooling water tunnel, a cold easterly wind must prevail and blow the wind-chilled water against the east-west oriented shoreline. The wind should turn to blow from southwest and carry the supercooled or icy water to the water intake channel opening.

The frequency estimate of a frazil ice occurrence is $2.2 \cdot 10^{-2}$/a according to the licensee's analysis. The wind speed of 5…10 m/s is strong enough to generate frazil ice. These wind speeds occur frequently. The share of the winds potentially causing a loss of offsite power is less than 0.01. Thus, the frazil ice frequency can be multiplied by a factor of 0.01. On the other hand, the stronger the wind blows, the stronger the frazil ice phenomenon can create.

Wind, high seawater level and debris

Strong winds are always associated with the high seawater levels, and debris entering the water doesn't cause any risks beyond those already presented.

Wind and low temperatures

During normal operation, low temperatures as an individual phenomenon are not deemed to jeopardise the availability of the plant's systems due to the big thermal loads. As a combined phenomenon, low temperatures together with strong wind may break windows and non-load-bearing structures, potentially resulting in the rapid cooling of premises. The implementation of corrective measures effectively might be difficult during the storm.

The localised detachment of insulation material is not deemed to impact the operation of process equipment inside the buildings because of the big thermal loads during operation, the large thermal capacity of the massive structures, and the slow cooling. There is ample time for restoring measures.

If a storm causes a loss of offsite power, the diesel back-upped premises start to cool. Temperature alarms will be received for low temperatures in safety-critical areas. Because of the process equipment's excess heat and the thermal capacity of the structures, the premises will cool slowly, which gives more time to arrange for a temporary heating.

The exposure of equipment located near doors or other openings to freezing temperatures is deemed to be so local, due to the thermal load of the operating plant, that the worst consequence of such an event would be a reactor scram, which is included in the reactor scram frequency in the PSA.

A low outdoor air temperature will not limit the use of the main transformers, internal transformers or 6/0.4 kV transformers during normal operation because the waste heat produced by the transformers is sufficient to keep the transformer oils warm enough. Nor are special measures required to take a cold transformer into use.

In terms of the battery arrays, a low temperature in the premises will reduce the capacity and discharge load of the battery arrays. The capacity of the battery arrays will decrease by about 1%/°C (0.6…1.7% depending on the discharge time) compared to the design rating of +20°C. In this case, the battery array's capacity will decrease to the half at the temperature of about –20… –25°C. This kind of situation could occur in a situation where the heat to the location of batteries is lost in winter as a result of a loss of offsite power. These battery arrays include e.g. the laboratory building's battery rooms, the emergency feed water pumping plant's start-up batteries and the injection diesels' start-up batteries. Due to the large mass of the battery arrays, their cooling is slow giving more time to arrange for an additional heating. The control room is alerted to the low temperatures in the battery rooms either directly through a temperature alarm, an HVAC shutdown alarm, or from the alarms of adjacent areas belonging to the same HVAC area. Due to these factors, low temperatures are not deemed to impact the availability of the battery arrays, according to the licensee's analysis.

The switchyard equipment can withstand low temperatures. Rotary engines and motors can withstand low temperatures because of the waste heat they generate during operation. The lubrication oils and greases of control and shut-off valves and regulating units may become less viscous in low temperatures and thereby hinder the operation of the equipment in question.

Test oscillators, power supply switchboards, transfer substations, level and pressure transmitters, and other electrical and instrumentation equipment can tolerate low temperatures and their operation is not deemed to be at risk in this conjunction. However, moisture condensing in the equipment during plant start-up and when the premises are being re-heated may cause a problem.

The consequences of heating ventilation failure were assessed also in situations where the blowing of cold air into the rooms still continues. The licensee has used the COCOSYS program in analysing the impacts that the loss of heating of ventilation intake air may have on the conditions of the rooms in the lower part of the containment building including safety related instrumentation. The results of the analysis indicate that the temperatures in the reactor building's instrumentation rooms (sheet-metal rooms) will not drop too low between the regular shift checking rounds.

<u>Wind and freezing conditions (snow storm)</u>

As a result of a storm leading to a loss of offsite power, diesels can also be lost due to the clogging of the intake-air openings, if freezing or clogging conditions prevail at the same time. Such conditions will include heavy snowfall, supercooled rain and wind-detached sheet-metal pieces or both or other obstructive materials. The auxiliary emergency feed water system's intake air openings are also at risk of clogging in the same conditions.

According to the licensee's analysis, the probability of freezing conditions occurring simultaneously with strong wind is 0.27.

<u>Wind, frazil ice and freezing conditions (snow storm)</u>

As a result of a storm leading to frazil ice and the loss of offsite power, diesels also can be lost due to the clogging of the intake-air openings, if the freezing conditions prevail: heavy snowfall, supercooled rain and wind-detached sheet-metal or both or other obstructive materials. The auxiliary emergency feed water system's intake air openings are also at risk of clogging in the same conditions.

If frazil ice occurs, there is a 0.01 probability that the wind is strong enough to result in a loss of offsite power. The probability of freezing conditions is 1/3 during the whole year.

<u>High sea and air temperature</u>

When the seawater temperature is high, there is a high probability that also the air temperature is high. Combination of high seawater and air temperature may hamper the cooling of the instrumentation rooms. According to the licensee's analysis the risk related to this event is however low, because the frequency estimates of the events are very low.

Conclusions on the adequacy of protection of weather conditions

The original design of the plant unit did not take into account all possible aspects of weather phenomena related to safe operation of plant or their combinations with other external conditions of natural origin. However, the plant preparedness and strength against external hazards has been improved due to the plant modifications performed using the principle of continuous improvement.

Operational experiences regarding the impact of extreme weather phenomena on plant operation have been taken into account in the design of preventive and corrective measures including technical modifications and plant procedures.

Weather phenomena and other extreme external conditions including the combinations of phenomena relevant at the plant units have been comprehensively analysed using the Weather PSA, which is part of the living PSA. The meteorological and hydrological data available from the local and national observations and records have been extensively utilised in analysing the duration, intensity and frequencies of external phenomena. The potential risks involved in the increasing oil transportation in the vicinity of plant have been assessed in the external hazard risk analysis as a part of PSA.

According to the results of PSA, the total core damage frequency resulting from extreme weather phenomena is $6.6 \cdot 10^{-6}$/a, which is roughly 14% of the total current risk. The analysis includes all plant operating states. The most significant risks related to external hazards, other than seismic or external flooding, found by the licensee, are related to algae combined with wind exceeding 39 m/s and wind exceeding 45 m/s. In addition, the licensee is asked by the regulatory body to reassess the present design basis and protection regarding the impacts of extreme high and cold air temperature on plant safety systems including their auxiliary systems.

Extreme weather conditions, including the impact of climate change and global warming, are studied within the EXWE project in the Finnish Research Programme on Nuclear Power Plant Safety [SAFIR2010, SAFIR2014]. The results of the programme might necessitate reconsiderations regarding design basis and safety margins for external phenomena, in particular air temperature, wind and rain. The licensee participates in the national programme above.

B.4.2 Evaluation of safety margins

B.4.2.1 Estimation of safety margin against extreme weather conditions

<u>High air temperature</u>

The air-condensed instrumentation rooms cooling device design basis outdoor temperature is +25°C, but the cooling device will trip from the condenser's pressure protection at an outdoor air temperature well over +40°C. The trip temperature frequency estimate is less than 10^{-8}/a.

Standard room temperatures (about +20°C) could be exceeded, if the design basis outdoor air temperature of the HVAC system is exceeded. Without exception, the cooling will continue and a new balanced condition will be found. Design basis for the instrumentation rooms indoor temperatures are +35…+40°C. Design basis for the new automation building indoor temperature is +40°C.

The temperatures of the flow-through or by free convection cooled spaces or devices correlate to outdoor temperatures. The gap between temperatures depends on the volume of cooling and generation of excess heat.

Outdoor air temperature tolerances for flow-through cooled spaces or devices are +40°C. According to the licensee's analysis, the frequency estimate for +40°C outdoor air temperature is less than 10^{-8}/a, thus tolerances could be considered to be adequate.

Instrumentation rooms which are normally cooled by the redundant HVAC can also be cooled by flow-through or by free convection. Outdoor temperature tolerances in these cases are conservatively assumed to be +25°C.

<u>Low air temperature</u>

As an individual phenomenon, low temperatures are not deemed to jeopardise the availability of the plant's system because of the big thermal loads during normal operation.

The consequences of low temperatures combined with strong winds are discussed in Section B.4.1.1 above.

High seawater temperature

According to the licensee's analysis, the risk related to high seawater temperature is low. The Technical Specifications define measures to be taken if the seawater temperature exceeds the design basis +23°C. Additionally, plant power must be reduced so that the discharge water temperature does not exceed the water permit upper limit +32°C. High seawater temperature leads to shutdown through power reductions before the temperature rises to the point that it could cause the loss of control equipment. In addition, the frequency estimates for extremely high seawater temperatures are low.

High winds and storms

Winds with speed below 28 m/s do not result in any significant consequences.

A wind speed exceeding 28 m/s could, in the worst case, cause the following initiating events with coincidental failure occurrence such a small loss of coolant accident, loss of main feed water, reactor scram, erroneous opening of safety valves, or loss of ventilation of instrumentation rooms.

A loss of offsite power might occur when sheet metal or other material is blown into the switchyard, resulting in short circuits and earth faults in the 400 kV and 110 kV yards. Consequently, connections to the main grid are lost when the circuit breakers disconnect the plant from the grid. Consequently, the loss of cooling of the primary circulation pumps' seals could be generated, in case the diesel generators are unavailable from any reason, potentially leading to a SLOCA through the loss of integrity of a PCP seal. This event is included in the SLOCA frequency estimate in the PSA.

A strong storm could detach a large amount of sheet metal from the plant structures, warehouse and welding halls as well as debris in the cooling seawater that carried by wind blowing toward the intake basin hindering the seawater flow to the plant. The possible shutdown of the main seawater pumps will lead to, at most, the loss of the main feed water. In the PSA, these sequences have been taken into consideration in conjunction with the loss of main feed water.

Structures, mainly pieces of sheet metal, detaching from the plant structures and carried by the wind mainly through windows into the process areas can cause failure of individual electricity and instrumentation cables or impulse pipes. This can lead to the loss of safety-critical equipment located at the feed water tank level of the turbine hall. Potential initiating events identified through cable or impulse pipe damages at the feed water tank level are reactor scram, erroneous opening of the pressurizer safety valve or the loss of instrumentation room cooling in the control room building. The frequencies of these events have been estimated according to operating history and the strong wind has no significant effect on them.

Objects entering the seawater pumping plant through the windows can cause a loss of the main seawater pumps primarily through damage to the nearest cable racks, e.g. through damage to the instrumentation cables that lead to the measuring of the temperature of the oil cooling for the motors. The cabling of the service water pumps is better protected (e.g. refractory insulation and routing), thus these pumps are presumed to remain operational. The hydrogen lines adjacent to the window and along the wall at the seawater pumping plant may be damaged in this conjunction and ignite a fire at the seawater plant.

The clogging of the special ventilation system filters through the auxiliary building's air intake opening during a storm requires a powerful storm, the right direction of offshore wind and snowfall/sleet/supercooled rain. The maximum consequence is a reactor scram.

The loss of the instrumentation room cooling device cooling air could cause a loss of instrumentation room ventilation if the redundant cooling device that is cooled by sea water does not start.

A storm might cause the clogging of the SAM diesel air intake openings, preventing the use of the diesels. This will lead to unavailability of the containment external spray system in a situation where a storm has resulted in a loss of offsite power and the emergency diesels are unavailable, and a leak in the primary circuit increases the pressure of the steel containment.

A wind speed exceeding 39 m/s is assumed to result in a loss of offsite power lasting an average of 15 h. Other possible initiating events correspond to those events resulting from the wind exceeding 28 m/s.

A wind speed exceeding 45 m/s could cause limited breakages of non-load-bearing structures. Additionally, a limited breakage of the turbine building, and the falling of the ventilation stack are anticipated. The breakages could lead to the following consequences: loss of offsite power, loss of emergency feed water, a steam leak, a small leak, loss of diesels and the secondary seawater circuit as a result of intake clogging, and a loss of instrumentation room ventilation. In the Loviisa PSA, this is conservatively assumed to lead to core damage.

A partial breakage of the turbine hall wall A and missiles blown by the storm into the turbine hall can cause a fire if they break the generators' hydrogen cooling lines or the turbines' lubricating oil lines. The consequences of a possible fire have been assessed in the fire risk analysis.

Limited failure in the upper part of the turbine hall C wall may lead to the same initiating events as assessed in conjunction with a wind speed of 28 m/s in Section B.4.1.1 above. The biggest risk for structural failure on the C wall is between the reactor building and the C wall due to flow acceleration, the nozzle effect. Based on the intensity of the phenomenon, the loss of the main and emergency feed water system is presumed due to damage of the cabling of regulating equipment at the feed water tank level. Additionally, a steam leak is presumed probable through the auxiliary steam system's control valves, main steam system's dump valves to atmosphere or the turbine by-pass system's valves as a result of the faulty operation of the corresponding control circuits.

The loss of instrumentation room ventilation of the control room building will follow the malfunction of the ventilation cooling device's automation and electric cables, as well as due to the loss of the ventilation cooling's control supply air and the cooling fan coil located on the exterior wall.

The direction of the fall of the ventilation stack, or the consequences to the buildings have not been separately assessed in the Loviisa PSA, instead, the falling of the ventilation stack is presumed to cause a core damage.

Heavy rainfall on unfrozen ground

Design basis for the draining in the yard and on the roofs is 0.02 (l/s)/m^2 or 72 mm/h of rain. The frequency of rain lasting 2 hours (equal to total rain of 144 mm/d) is about 10^{-4}/a.

The roof is designed to withstand 180 mm layer of water. Since the highest daily amounts of water will rain down on heavy showers which last only few hours it can presume the maximal daily amount to rain in less than one hour. Even in that situation the flat roof will withstand the rain of about 250 mm (design basis of 180 mm plus 72 mm removed by the draining) the frequency of which is $3 \cdot 10^{-8}$/a.

The yard is located lower than the surroundings and therefore water will leave the yard only via the draining to sea. The water from the surrounding areas does not flow to yard in any significant amount, thus, the water level in the yard will be equal to the level of rain. If the rain of 260 mm lasts one hour, the water level will not rise above 190 mm since draining removes 72 mm of rain in the same time frame. Since the yard has falls away from the sills the water level will be lower closer the doors. A possible flooding of rainwater into the turbine hall does not threaten safety-significant equipment. Diesel buildings' floors are at the height of 100…150 mm above the ground but even if the water level raises above that the problems will be minimal since only a small amount of water would seep to the floors.

Heavy rainfall on frozen ground

Roof is designed to withstand 180 mm layer of water, and ice layer on the roofs is not presumed to be heavy. Ice layer can also be removed from the roof if the layer starts to get thicker. Additionally, snow can be manually removed from the roofs, if necessary. Usually, there is no snow on the turbine hall roof because of the excess heat generated by the turbines and other equipment.

Problems on the ground level by the diesel buildings might be more significant but not concerning, since the floors are 100…150 mm above the ground level.

Lightning

In the Loviisa PSA, the loss of offsite power, a fire leading to the loss of one redundancy, reactor trips and the loss of main feed water are included in corresponding initiating events. Separate frequencies are determined to the loss of one or both redundancies due to lightning strike that hits control room building roof or ventilation stack resulting in the loss of critical systems.

It is assumed that low current lightning strike always hits and moderate current lightning strike can hit the control room building roof with probability of 0.1. Otherwise lightning strikes are captured by the ventilation stack, and only high voltage lightning strikes can induce serious potential differences to the grounding network that way. Fraction of low current (< 10 kA) lightning strikes is approximately 8%, moderate current (10…200 kA) around 92%, and high current (> 200 kA) less than 0.1% of all lightning strikes.

Lightning strike frequency used in the PSA is $1/km^2/a$. This value corresponds to average lightning strike frequency in Finland, and is conservative for Loviisa NPP. Area for lightning strikes is 100 m^2 for low and moderate current lightning strikes and 0.05 km^2 for high current strikes due to capturing effect of ventilation stack. The probability of lightning arrester evasion is assumed to be 0.5 for low current and 0.1 for moderate current lightning strikes. The probability of loosing one redundancy is assumed to be 1 for moderate current lightning strikes and 0.1 for low and high current lightning strikes. The probability of loosing both redundancies is assumed to be 10% of one redundancy loss. Initiating event frequency for the loss of one redundancy due to lightning strike on control building roof is $6.1 \cdot 10^{-6}/a$, and for loss of both redundancies $6.1 \cdot 10^{-7}/a$.

The lightning protection of the new automation buildings is based on both surface protection and internal equipotential bonding, and is designed according to KTA 2206 and national standards. Taking into account the modifications of lightning protection system in 90's, the overall level of lightning protection of the site is acceptable. The only significant deficiency and concern is the coarse grounding network. The modification work regarding the grounding network is ongoing.

<u>Low seawater level</u>

According to the licensee's assessment, the occurrence low sea water level preventing sea water pump operation is highly improbable ($<10^{-8}/a$). If oil, algae or frazil ice blocks sea water intake it is possible to get cooling water from discharge side of sea water circuit. If sea water level is lower than –0.5 m compared to average this isn't possible due to weir at discharge side. The probability that the seawater level is below –0.5 m is estimated to be 0.015.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan to secure decay heat removal to ultimate heat sink in extreme external events and to investigate the effect of extreme environmental temperatures to the plant safety.

B.4.2.2 Measures which can be envisaged to increase robustness of the plant against extreme weather conditions

The availability of main transformer during cold and refuelling outage has recently been improved by allowing the recovery of a main transformer in 3 hours after the demand. In addition, the licensee has plans to replace the main transformers with new ones. To further improve possibilities to recover availability of the main transformer, the actions needed should be taken into account in procedures.

The licensee has installed a backup diesel generator, common to both units in October 2011. This will decrease the risks related to the loss of off-site power connection. According to the licensee's preliminary analysis, the backup diesel generator will decrease the total core damage frequency roughly 5%.

Modernization of the grounding network of whole site according to KTA 2206 guidelines is ongoing and will be finished during 2012.

The improvements above are part of ongoing processes, and thus not initiated due to Fukushima accident.

To respond to STUK's requirements after Fukushima accident, Licensee is investigating the following issues.

- As an alternative ultimate heat sink, the possibility to install independent air-cooled cooling towers with no connections to seawater systems or emergency diesel generators. The cooling towers would take care of decay heat removal of reactors and fuel pools of both units and of spent fuel storage pools. Preliminary design on the solution is ongoing, and the basic design is estimated to be ready until summer 2012.
- The need for further improvements on the diesel driven auxiliary emergency feed water pumps. The investigation includes verifying the actual operation of each component of the system without AC power from the grid or diesel generators.
- The possibility to improve the diesel driven auxiliary emergency feed water pumping station protection against flooding above +3.0 m level.
- Securing the electrical power supply for the pumps that are used to refill the water reservoir of the auxiliary emergency feed water pumps.

Further improvements against extreme environmental temperatures are considered not necessary, as the related risks are estimated to be very low. STUK is evaluating this assessment.

B.5 Loss of electrical power and loss of ultimate heat sink

B.5.1 Loss of electrical power

LO1 main electric diagram is presented in Figure B-3. The diagram in shows only one of the two redundancies, and there are two similar sub-systems per unit for LO1 and LO2.

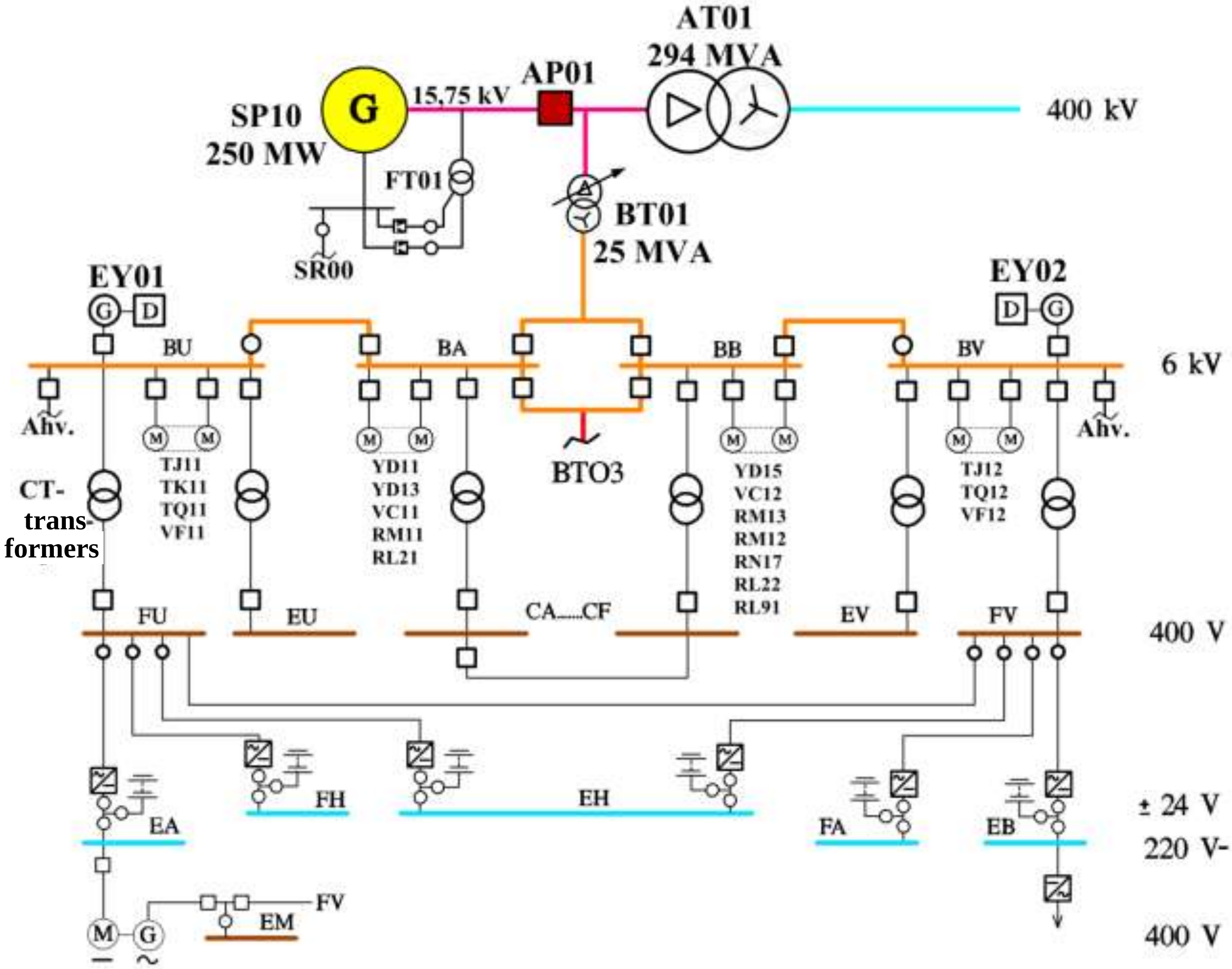


Figure B-3. Main electric diagram of LO1 (“Ahv.” refers to the hydropower plant nearby) [Fortum 2011]

B.5.1.1 Loss of off-site power

The connection of the LO1 and LO2 to the Nordic 400 kV power grid is implemented with two independent 400 kV overhead lines running from the Loviisa switchyard to different grid nodes. Damage of a single 400 kV overhead line will not cause the loss of 400 kV grid connection. In addition, both plant units are connected to the national 110 kV power grid. The connection is implemented with one separate transmission line.

House load operation is the first defence line against the losing of the 400 kV grid connection. If this automatic switchover is successful, the plant can continue the house load operation indefinitely. The units have two main generators each.

If the 400 kV grid connection is lost and the house load operation is not possible, the units can try to switch to the national 110 kV power grid. The switchover is automatic. If the 110 kV grid is available but the automatic switchover fails, operators can make the connection manually.

Switchgears (BA...BD) critical to the grid connections and house load operation are located at level +3.00 m in four fire compartments.

The main defence line against loss of AC power is emergency diesel generators (EDGs). LO1 and LO2 have four individual 2.8 MW EDGs and safety switchgear systems per plant. The capacity of the EDG-system is 4×100% with the exception of 2×100 % switchboards FU/FV and FW/FX. Each EDG is in its own diesel room that is an own fire compartment at +3.00 m level in one building. The switch gears of safety loads (BU...BX, EU...EX and FU...FX) are at +3.00 m level also divided in four fire compartments. The load shedding and control systems are installed in rooms located at +8.70 m and +13.80 m levels. The cooling of the EDGs is arranged by independent sea water cooling systems.

If the off-site power is lost, EDGs will start automatically and provide power to the safety systems within 15 s. If automatic start-up is not successful, EDGs can be started and connected manually, either from the main control room or locally.

Each EDG has a fuel tank (day tank) with fuel enough for 10 hours of operation. These day tanks are automatically filled from a storage tank. There is one storage tank per two diesels and one storage tank holds enough fuel for three days of EDG operation (both two EDGs running at full nominal power).

All situations mentioned above are instructed and the operating staff is capable of performing them. The LOOP situations are a part of the standard operator training and they are rehearsed frequently at the training simulator.

B.5.1.2 Loss of off-site power and loss of the ordinary back-up AC power sources

If the EDG operation is not successful, emergency back-up power can be provided from a diverse non-safety diesel power plant (EY07) or from a hydropower plant.

The EY07 plant has capacity of 9.7 MW and it is capable of providing the required emergency power to LO1 and LO2. The plant is located above +7.50 m level. The EY07 is separated from nuclear units and is air cooled. The diesel plant is currently connected via the 110 kV switchyard to the nuclear units, but dedicated cable connections to the 6 kV safety switchgears (BU...BX) are under construction. The EY07 plant has to be started and connected manually, but operators can perform all the required operations from the main control room of LO1. Also local operations are possible. If the diesel engine is run at its maximum power there is enough fuel for 50 hours of operation. In case the diesel engine is used to substitute two of the EDGs simultaneously the fuel last for 86 h of operation.

The hydropower plant is connected to Loviisa via dedicated 21 kV overhead cable. The designed function for this connection is that it can replace one EDG on both units if the diesel generator is out of operation. The connection has to be initiated using local actions in both the hydropower plant and nuclear units and the estimated time needed is 4 h. The switchgear of the connection (BY) is located at +3.00 m level and control relays at level –0.60 m.

It is also possible to provide power between LO1 and LO2 units. Even though there are no dedicated connections between the plant units, there are a number of ways to transfer power from one unit to the other. In case of offsite power is lost and only one of the units has managed to switch to house load operation, the power supply from one unit to the other can be arranged via 400 kV sub-station. The required switching actions can be made from the main control rooms or locally. If the connection through 400 kV substation is not possible the connection can also be made between 6 kV switchboards. In case the connection is done via 6 kV systems the capacity of the connection is limited by the allowed loading of auxiliary transformer (25 MVA) and allowed current through 6 kV circuit breakers (1600 A). There is enough capacity to supply power for safety systems. The required switching actions must be made partly locally and the estimated time needed is 1 h. The elevation of the connection busbar is –0.60 m.

In case offsite power is lost and neither of the units manages switch to house load operation, there are two possible ways of connecting the emergency diesel generators to support the power system of the neighbour unit. In both cases the connection is done between 6 kV systems. The first option is to use a tube busbar normally used for 110 kV connection. The second option is to utilize the hydropower plant connection switchgear (BY). The power capacity of the connections is limited by the EDG power. The required switching actions must be made partly locally and the estimated time needed is 4...6 h. The elevation of the connection busbar is –0.60 m and hydropower connection +3.00m.

In addition, there is a separate 24 kV utility line coming from local electrical company. The line serves normally Loviisa outdoor area as a reserve connection, but can, if required, be manually connected to provide electricity to some systems of LO1 and LO2 (mainly lighting, water treatment plant and firewater pumps). The line has very limited capacity. The start-up of the connection needs manual local operations.

Battery capacity issue is described in Section B.5.1.3.

At Loviisa NPP there is a separate power system for loads needed in severe accident management (SAM). SAM electrical system belongs to SC3. The SAM electrical system is independent from other electrical systems of the plant and off-site power systems. The SAM power supply and distribution system is divided into two trains and it fulfils the single-failure criterion. The SAM electrical system is common for LO1 and LO2 and has enough capacity to supply power even in case both units suffer from severe accident. It includes two diesel generators and one diesel generator alone is capable of feeding all SAM-loads on both units.

The electrical equipment is located in different fire compartments according to their train. The cabling belonging to different trains is placed in corresponding fire compartments, or if not possible fire barriers have been applied.

The SAM system is designed to be as independent as possible from buildings or areas that could be affected due to external hazards leading to severe accident. Electrical equipment is chosen so that they can withstand environmental conditions that may appear during severe accident. Diesel engines are air-cooled. Diesel engines exhaust gas systems and air inlets are designed in a way that exhaust gas can't return to the inlet and that the fire in the other diesel generator room can not endanger the functioning of the other diesel.

B.5.1.3 Loss of off-site power and loss of the ordinary back-up AC power sources, and loss of permanently installed diverse back-up AC power sources

Battery backed electrical systems are located in two separated redundancies 1 and 2. The capacity of the redundant safety systems is 2×100%. In some cases (e.g. EDG systems) the battery systems are divided to separated 4×100% parts. The batteries are diesel backed up (exceptions are mentioned separately).

The list below presents the capacities and loads supplied by each battery-backed system:

- FK, FL, FM and FN 220 VDC
  - 4 redundant systems
  - EDG control, safety switchboard controls
  - Discharge time 10 h
  - Mounting level is +3.00 m
- EA, EB, ED, EE, FA and FB 220 VDC
  - 2 redundant systems
    - battery backed-up 0.4 kV AC system for loads that don't tolerate interruption in power supply which is caused by diesel engine start-up time
    - reactor coolant pump seal water system
    - electrical steam generator blow-out and feed water valve control of diesel driven auxiliary emergency feed water system
    - DC power needed at SC4 6 kV switchboards (BA ... BD)
    - reactor protection system (not ESFAS)
    - control rod system
    - solenoid valves
    - main generator protection and generator circuit breaker
  - Discharge time 1 h
  - Mounting level +3.00 m in LO1 and +10.20 m (batteries) / +6.60 (rectifiers and switchboards) in LO2
- EH, EJ and in LO2 also ES and ET 24 VDC
  - 2 redundant systems
  - Safety instrumentation and control systems
  - Discharge time 1 h 15 min
  - Mounting level +8.70 m
- FH and FJ 24 VDC
  - 2 redundant systems
  - Instrumentation and control systems of auxiliary processes

  - Discharge time 1 h 15 min
  - Mounting level +17.40 m LO1 and +9.00 m LO2
- FS and FT 24 VDC
  - 2 redundant systems
  - SAM system instrumentation and control
  - Discharge time 2 h
  - Mounting level +3.00 m
- FC and FD 220VDC
  - two quite redundant systems
  - Control power for 400 kV and 110 kV connections
  - Discharge time 10 h, no diesel back-up
  - Mounting level +3.00 m (DC distribution)
- New automation system batteries (not in full use yet) 24 VDC
  - 2 redundant 4 canal systems
  - New modernized automation
  - Discharge time 7 h (safety functions) and 3 h (operational I&C)
  - Mounting level +8.70 m and +13.80 m

It is possible to charge the batteries using the power sources mentioned in sections B.5.1.1 and B.5.1.2. In a longer-standing fault scenario, it is also possible to charge the main batteries by diverse SAM diesel generators (EY05). The generators have a fuel tank capacity for 24 h of operation. Generators are located at level +3.00 m. The rectifiers of the batteries must be switched manually to the SAM system, but all connections are ready made using permanent cablings.

If all AC power is lost at the time of reactor scram (station blackout), It has been calculated that SGs could be used for 4…6 h after the event for heat removal, even if there were no countermeasures. After this time period there is still 0.5 m of water in SGs and auxiliary fill up is possible without any threat to SG tube integrity. If the SGs were not refilled, it would still take additional 3 h before the core heat-up.

SG mass inventory is maintained with the diesel driven auxiliary emergency feed water pumps and excess heat is removed with main steam header relief valves or SG relief valves (battery driven, nitrogen driven, or safety relief valve). Within this mode the plant can be kept in a hot shutdown for 78 h without any excess heat-up in the primary circuit. The limiting factor for this time frame is the exhaustion of demineralised water in SGs make-up tank.

After 78 h SGs and make-up tanks will be emptied and pressure and temperature in the primary circuit begin to increase. If a complete loss of feed water injection happens in full power, it takes approximately 3 h until core starts to uncover after loss of SGs water inventory. Hence it can be conservatively estimated (since large amount of decay heat has already been removed and heat generation in the core has decreased) that time between start of core uncovery and loss of SGs water inventory is over 3 h in this case.

Due to loss of off-site power and loss of emergency diesel generators the total time before loss of fuel cladding integrity is more than 81 hours. On-site equipment can be used to prolong this timeframe till about ten days by using independent diesel driven pumps from fire water system, which can fill up the SG make-up tanks. This system is independent from any electrical power. The fire water pumping system can be connected directly to SG make-up tank simply by fire hose. The tank has already connectors to hoses. Using all these secondary side water storages for decay heat removal, alternate heat sink is available for 240 h, i.e. ten days. These additional actions are not included in the current emergency operating procedures.

During the loss of all AC power, removal of the decay heat from the spent fuel elements in the reactor building fuel pools to the sea water is not possible. The limiting worst-case situation for the available time is the evacuation of the whole reactor core to the loading pool. The decay heat power is about 5.2 MW. If the pool cooling is lost in such a situation, the pool water will start boiling in about 3.4 h. About 34 h after the start of the boiling, radiation level will start to increase. About 9 h after that, the top of the fuel elements will be uncovered. To prevent the water-level drop in the pools, make-up water supply of about 2.3 kg/s would be needed to compensate for the boiling.

Normally, the decay heat generated by the spent fuel elements stored in the in-containment fuel pools is much less after outage, and the uncovery of the fuel elements would occur after about 6 d 10 h. Make-up water supply of about 0.7 kg/s would be enough to compensate for the boiling in the normal situation.

Normal heating power in the spent fuel storage 1 is 378 kW (maximum of 605 kW) and 330 kW in storage 2 per pool. The heating time to 100°C is about 99 h (minimum of 49 h) in storage 1 and 90 h in storage 2. Level decrease due to the boiling to the level where radiation level starts to increase significantly in the storage hall is around 25 days (minimum of 14 days) in storage 1 and 21 days in storage 2. Amount of make-up water to the pool needed to compensate for boiling is 0.17 kg/s in storage 1 and 0.49 kg/s in storage 2.

Make-up water can be delivered to the pools using the fire fighting water system and the fire fighting pumps, which are equipped with their own diesel engines and are therefore independent of the AC power supply. The use of the fire water systems requires access to containment and spent fuel storages for the hose installation. If required, make-up water can also be pumped using the transferable pumps from the fire brigade.

B.5.1.4 Conclusions on the adequacy of protection against loss of electrical power

The time margin for the recovery of the AC-power supply before fuel damage is quite long if a total loss of the AC-power occurs. Core heat-up would take place no earlier than 7…10 h after the start of the event, even if there were no countermeasures. Using the auxiliary emergency feed water pumps the total time before loss of fuel cladding integrity is more than 81 h, which can be significantly increased with the systems already available on site.

The battery capacity of battery backed-up systems must be analysed. The capacity can be too low when the usage of auxiliary emergency feed water pumps is concerned. The integrity of main reactor coolant pump seals must also be taken into account in the analyses, so that the water inventory on primary circuit can be secured in the loss of off-site power situation.

LO1 and LO2 have adequate autonomy of EDG fuel. The units have fuel at least for three days when all EDGs are working at LOCA power level. But the capacity of EY05 and auxiliary emergency feed water system tanks are smaller.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan and schedule to increase fuel reserve for emergency power at the site and to secure DC power for long time needs.

Furthermore, the Licensee is required to investigate the availability and operability of safety systems and their components in accidents of long duration and investigate needs and possibilities to use mobile power supply and mobile pumps in accidents.

B.5.1.5 Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power

The capacities of the batteries securing plant automation will be improved during the ongoing automation renewal project.

To respond to STUK's requirements after Fukushima accident, Licensee is planning several modifications that can provide extra protection:

- In order to secure long-term operation of the diesel engines, the usability of the widely available biodiesel on the plant's diesel engines will be evaluated.
- A movable tank for fuel transfers at site will be provided.
- Possibility to install an additional diesel fuel tank to supply fuel for different diesel engines will be evaluated.
- The diesel generator plant recently installed at the plant site is connected to the plant electrical system via the 110 kV switchyard. In future, it will be connected directly to NPP's electrical busbars.
- Licensee has evaluated adecuacy of the battery capacity, and that no improvements for the auxiliary emergency feed water pump engines or SAM systems are needed, as the batteries are dimensioned on conservative basis. The charging possibilities will be further enhanced. STUK will evaluate this assessment.
- Licensee has evaluated that further improvements on securing the long-term operability of the safety systems and equipment are not necessary. The risk studies carried out during the plant operation have shown the possibilities for significant safety improvements, and these have been made. STUK will evaluate this assessment.
- The Licensee will evaluate the need for applying mobile device in securing boron injection into the RCS, coolant inventory in the RCS, coolant inventory in the secondary circuit, water supply for the diesel driven auxiliary emergency feed water pumps, electricity supply for instrumentation needed in accidents, electricity supply for the RCS depressurisation valves, containment heat removal during severe accidents, decay heat removal from the spent fuel storage pools, operation of diesel engines and their support systems, control room lighting, and plant communication systems.

B.5.2 Loss of the decay heat removal capability/ultimate heat sink

B.5.2.1 Design provisions to prevent the loss of the primary ultimate heat sink

The primary ultimate heat sink in Loviisa NPP is the sea, the Gulf of Finland. There are several mechanisms how ultimate heat sink can be lost (e.g. due to frazil ice, algae or oil entering the sea water system) and several design provisions to prevent that. Loss of sea water system will threaten the plant safety because virtually all process systems and major HVAC systems use sea water system as the ultimate heat sink. However, atmosphere can be used as ultimate heat sink for the reactor.

The cooling water is taken from south-west side of Loviisa NPP. There are three parallel inlet flow ports each with capacity to supply 50% of cooling water need on a normal operation. In a shutdown mode the need of cooling water is essentially lower. Each inlet has a mechanical screen cleaning system to remove impurities. One coarse screen has an electricity heated section which can be heated with electricity for frazil ice situations. Inlet flow ports can be closed in flow direction with a sluice before the coarse screen. Hence it is possible to prevent e.g. oil from entering the flow channel.

After flow ports and coarse screens, sea water flows to both units in a 70 m^2 rock tunnel which later breaks up to individual tunnels for both units. In unit specific sea water systems, there are four parallel suction chambers in the circulating water treatment system. Each suction chamber including fine screen and basket filter can be isolated with sluice gates.

There is a pipeline from LO1 and LO2 sea water systems, which can be used to divert part of the warmed sea water back to the inlet sea chambers. This system is used if water temperature at the inlet is close to frazil ice formation.

In case the inlet is blocked for some reason, e.g. because of algae or oil slick, sea water is circulated between the two units with LO2 service water system pumps. This applies only for cooling safety related systems. It is also possible to use LO1 service water pumps for recirculation if LO2 service water pumps are not available. This method is applicable until water becomes too hot for cooling purposes. The time delays are discussed in the following section.

Loviisa NPP has also prepared for the blocking of fine screens or basket case filters. In this case, it is possible to take necessary cooling water for service water system through the outlet tunnel and discharge warmed water to surge chamber at the inlet. This applies for both units.

Plant Emergency Operating Procedures (EOPs) include an individual procedure with a clear strategy and detailed actions for the following events:

- Loss of primary sea water system (partial or total)
- Starting recirculation between sea water systems of LO1 and LO2, in case inlet or inlet and outlet are blocked

In addition, incident procedures for risk of clogging of seawater system screens due to e.g. frazil ice, algae, or oil slick, are available. Hence, it is likely that for the most probable loss of seawater system accidents, the operators will be able to react swiftly.

Respective EOPs and other procedures are readily available in the main control rooms of both units. EOPs are also available in the auxiliary control room and emergency preparedness organisation facilities both in Loviisa NPP site and in the licensee's Technical Support unit.

B.5.2.2 Loss of the primary ultimate heat sink

The availability of an alternate heat sink depends on the plant state and feed water availability. If primary circuit can be pressurized (i.e. reactor vessel head is in place), atmosphere can be used as an alternate heat sink as long as there is enough water available for steam venting. Otherwise heat cannot be safely removed to atmosphere. However, it is possible to move heat to spent fuel storage cooling system and hence to intermediate cooling system, giving time for restoring ultimate heat sink.

If primary heat sink is not lost instantly, it is possible to install reactor head in its place. Installing reactor head takes approximately one day with normal actions, the best-estimate for emergency situation is 12…18 hours.

Alternate heat sink can only remove heat from reactor. If sea water system is lost completely, cooling of ventilation, component cooling, and emergency diesel generators are also lost. Because of the remarkable water volumes in different systems, there are many different time delays before design limitations are exceeded.

Most important time constraint for the availability of an alternate heat sink is whether either unit has its reactor head removed. Roughly 7% of a year either LO1 or LO2 is in shutdown with reactor head removed.

Second critical time constraint comes from the availability of feed water for keeping plant in hot shutdown. There are many water tanks to consume when removing decay heat through boiling and venting. Water consumption depends on the decay heat power. When all systems are available, all tanks can be consumed and more process water produced in the water supply plant.

Minimum water requirements for different tanks depend on the plant state and are defined in OL&C (Operating Limits & Conditions). As OL&C sets the minimum requirement, the tanks have typically greater amount of water in them. Table B-4 shows the tank volumes and their minimum OL&C water volumes. In shutdown states OL&C requirements are less strict, because of the smaller decay heat.

The available heat transfer chains in loss of seawater event are:

- main steam system forced control + auxiliary emergency feed water pumps
- main steam line blow-down + auxiliary emergency feed water pumps
- main steam system forced control + normal make-up & SG blow-down systems

Table B-4. Plant site water tanks and their minimum water volume during power plant states

Tank	Volume (m^3)	OL&C minimun volume at power operation (m^3)
ECCS tanks	1000	900
Auxiliary ECCS tanks (shared between both units)	1000	900
Pressurized hydro accumulators	70/70/70/70	50/50/50/50
Feed water tanks		120/120
Clean condensate tanks (shared between the units)	500/500/500	212/ total 423
Demineralised water tanks (shared between the units)	4×1000	2×635
Fire water tank/process water tanks (shared between the units)	2×1500	1400
Fire water tank (shared between the units)	1500	1400
SAM spray tank	120/120	111/111
Total amount per unit	6810	4148

If the primary ultimate heat sink only is lost, all above mentioned methods and water sources mentioned in Table B-4 are available at least in the beginning. Method of "main steam system forced control + auxiliary emergency feed water pumps" is completely independent from ultimate heat sink. Tank combinations of over 2000 m^3 are sufficient to remove decay heat of one reactor for over ten days.

Loss of the primary ultimate heat sink has a deteriorating effect to safety related cooling systems. Direct consequences and hence time delays of the loss of sea depend on the initiative event. If the inlet sea water tunnels are closed in time, it gives 2.5 days for keeping the safety related components and spent fuel with sufficient cooling.

On the other hand, if the initiative event includes instant loss of all heat exchangers connected to the sea, there are still at least 15 h to keep the normal decontaminated intermediate cooling circuit operational. This applies even if either unit is in shutdown state regardless of reactor vessel head status.

Because emergency diesel generators are water-cooled, they are also connected to the sea water system. Diesel generators cannot function without water-cooling. In case of oil is blocking LO1 heat exchangers, it takes roughly 4 h before oil would reach emergency diesel generator heat exchangers, if all four diesels per unit are running.

Spent fuel storage

Sea water acts as an ultimate heat sink for fuel pool cooling system. Loss of sea water cooling leads to necessity to boil the water in the storages. Situation in this case is very similar with loss of power because loss of electrical power leads to loss of ultimate heat sink by permanently installed equipment. The only real differences related to decay heat removal from spent fuel storages are possible working conditions (lighting) and availability of systems used for containment heat removal.

B.5.2.3 Loss of the primary ultimate heat sink and the alternate heat sink

The licensee has analysed the situation, where in addition to the loss of sea, all possible means of injecting feed water to SGs are lost. If reactor is in shutdown and cooled in water-water phase, i.e. SGs function only as water-water heat exchangers, the loss of circulation in secondary circuit and capability of injecting feed water is presumed.

External actions to prevent fuel degradation would depend heavily on the accident and include restoration of feed water injection and primary heat sink.

If either unit's reactor vessel head was not installed, possibility of head installation among other counter-measures before onset of boiling in primary circuit would be considered. This would take some 12…18 h according to best-estimate. As a last resort, water injection to open reactor could be performed through fire protection system. This requires also manual actions inside the containment.

It is possible to bring more coolant water to the site by tank or fire trucks. Fire fighting systems are connectable to the boron water treatment plant tank, equipped with standard fire water hose. The fuel tanks of the auxiliary emergency feed water system and the SAM diesel generators can be refilled from outside so that tank truck can be parked near by.

Due to the relatively large water volumes in primary circuit, even after loss of heat sinks, there are time delays before water inventory of the primary circuit starts to decrease. For a reactor in full power, it will still take roughly 6 hours from the beginning of the event before primary circuit's relief valves start to open, if no countermeasures are taken. It is assumed that all SGs and the pipelines to secondary side relief valves are in action. After 3.5 hours, SGs water level is lower than 0.5 m level. EOPs allow a SG to be refilled, only if its water level is not below 0.5 m. Rationale is that if SG has been emptier, refilling a SG would cause stronger tensions for SG's tubing integrity. In very extraordinary situations refilling a SG would be considered, if all SGs were empty. Level of 0.5 meters also indicates that the heat transfer capacity of SG has been reduced significantly.

In case of station blackout, assuming that only the hydro-accumulators and SAM valves are operational, the core uncovers in about 9 hours according to the licensee’s analysis,. This case is similar with the most pessimistic scenario of loss of ultimate heat sink.

In a situation where a reactor is in shutdown, there is more time due to lower decay heat. If SGs have already been filled, primary circuit should slowly heat and relief valves of secondary side (in residual heat removal system) start to open when pressure in secondary side reaches 14.7 bars. No simulation has been made from this scenario, but the time delays can be assumed to be longer due to substantially lower decay heat.

If pressure vessel head is not installed, primary circuit and in-containment spent fuel storage can be connected. This allows using spent fuel storage cooling system to also cool down the reactor. The available recovery time is estimated to be the same order of magnitude as given in Section B.5.1.

B.5.2.4 Conclusions on the adequacy of protection against loss of ultimate heat sink

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan and schedule to secure alternative means of reactor cooling in case of loss of existing systems, and a plan and schedule to secure alternative means of decay heat removal from fuel storage pools located in the reactor building.

Furthermore, the Licensee is required to investigate possibilities to secure decay heat removal from fuel storage pools (outside containment) and to secure availability of demineralised water at the site in an accident of long duration.

B.5.2.5 Measures which can be envisaged to increase robustness of the plant in case of loss of ultimate heat sink

In case of loss of heat sink, there is a time span for countermeasures before a loss of fuel integrity. Using of diesel driven auxiliary emergency feed water system with some additional measures will lead to the time spans of days rather than hours before severe problems.

To respond to STUK's requirements after Fukushima accident, Licensee is planning several modifications that can provide extra protection:

The licensee considers a plant modification to ensure the decay heat removal in case of loss of seawater by taking in use a secondary heat sink. The modification consists of two air-cooled cooling towers per unit, one removing decay heat from the reactor and the other one assures the decay heat removal from in-containment spent fuel pool and from the spent fuel storage pools. The tower is connected to the intermediate cooling circuit, and it replaces the seawater cooled heat exchangers.

Design of the backup heat sink system is based on the most critical loss of ultimate heat sink situation, which occurs when the service water cooling circuits of the units are lost in addition to the heat sink. The extreme weather conditions are considered in the design. The power supply of the cooling towers and all the necessary pumps is provided by air cooled diesel generator (EY07). Additionally, the system is equipped with a power connection to the grid and emergency diesel generators.

The backup heat sink system under design will assure an independent heat sink for the power plant, and thus reduce significantly the core damage frequency of the power plant in long-term loss of ultimate seawater heat sink situation.

In case of combined station blackout and loss of ultimate heat sink, the possibility to operate cooling towers, and in addition the boron injection pumps with air-cooled diesel-generator, has also been investigated. These modifications would create a possibility to closed-loop operation also in case of combined station blackout and loss of ultimate heat sink.

Possibilities to increase plant robustness in the shut-down mode

Possibility to use hydro-accumulator during outage as water storage will be investigated by the licensee. This would prolong the time constraints during the most limiting condition without any major plant modifications.

The planned cooling towers would also affect on the time constraints in the shut down mode. It is possible to cool down the reactor and spent fuel storages in shut down mode, and thus, to enable fuel cooling without sea water in shutdown mode virtually as long as needed.

The actions described in Section B.1.1.2

External actions and transportable devices

The licensee will investigate possibilities to increase the robustness of the plant with transportable devices. However, the amount of water on the site is relatively high and a lot of systems have been installed to the site after construction of the power plant. Most of these systems are safety classified and meet the requirements from nuclear safety system standards. Therefore, the need of transportable systems has not been seen that critical by the licensee.

Decay heat removal from the in-containment fuel pools

Licensee has evaluated that water injection into the pool and boiling of the pool water could be used as an alternative means to remove decay heat from the in-containment pools. Water injection could be provided from the containment sump or from external connection to a fixed system or through mobile water injection systems.

Availability of demineralised water

Licensee has evaluated that there are adequate reservoirs of demineralised water at the plant site. STUK will evaluate this assessment.

B.5.3 Loss of the primary ultimate heat sink, combined with station blackout

In addition to the assumptions in sections B.5.1.2 and B.5.2.3, it is assumed that only batteries and SAM diesels are available as power supply.

B.5.3.1 Time of autonomy of the site before loss of normal cooling condition of the reactor core and spent fuel pool

According to the licensee’s calculations with conservative assumptions, the clean condensate tanks are sufficient for removing the decay heat for at least 8 h from both units operating in full power only through the auxiliary emergency feed water pumps. More detailed SBO-analyses showed that one unit is capable to withstand SBO with auxiliary emergency feed water pumps at least for 24 h. After 8 h, the SG inventory starts to decrease and it will take at least 6 more hours before primary circuit inventory starts to decrease. In total 14 hours is available to refill clean condensate tanks from demineralised water tanks. Refilling is possible with the force of gravity. However, it has been estimated that hydrostatic pressure difference is not high enough i.e. the flow from the demineralised water tank to clean condensate tanks would be equal to the capacity of the auxiliary emergency feed water pumps. The demineralised water tank is equipped with a firewater connection enabling the pumping of water from the demineralised water tank to the clean condensate tank by a fire truck. This operation is instructed by a written procedure. The refilling of the clean condensate tank from the demineralised water tank prolongs the time till about 78 h, when both units are affected at the same time. This estimate is rather conservative, since the available water volumes are according to OL&C, and in most cases, the available water volume is double to OL&C requirement.

This time can be further extended if sufficient supply of feed water and fuel for auxiliary emergency feed water pumps can be provided. There are many tanks at the site which contain either diesel fuel or process water. Moving the fuel or water within the 78 hours could be possible with e.g. fire engines and containers on site. The clean condensate tanks equipped with fireplugs right outside can be supplied with three diesel-driven fire fighting pumps from fire water system. According to the OL&C, the service water and fire fighting sub-system has at least 1400 m^3 of water. This will remarkably increase the plant autonomy, till about seven days.

Loss of electricity prevents operator from borating the primary circuit or injecting water to the primary circuit. This poses a challenge to the integrity of the primary circuit, since seal water of primary coolant pumps (PCP) can no longer be injected. It has been estimated that if the seals will not be cooled, it would take at least 10 hours until a small leak from primary circuit trough the PCP seals to the containment is possible. Leakage would occur due to the postulated loss of integrity of seal material after temperature increase. However, this temperature limit is considered to be conservative value and there is an experimental study going on, which will confirm the real temperature resistance of seal material.

Station blackout poses two other problems for cooling primary circuit. Firstly, cooling too much will empty the pressurizer due to the higher density of cooler water. Secondly, the sub-criticality margin after all xenon has decayed is too low to allow cooling the primary circuit more than a few dozen degrees (when all rods are in). The exact limit will depend on the point of fuel cycle and whether all control rods are inserted or not.

If reactor is in cold or in hot shutdown, and SGs are operating in water-water phase, auxiliary emergency feed water pumps have only a limited use. The rough time of autonomy estimates are the same as in Section B.5.2.2.

If reactor head is not installed, the primary circuit's water inventory starts quickly to decrease. Natural circulation will dwindle and the primary circuit will start to heat-up. Even with a low decay heat power, in the most pessimistic case, it would take 28 minutes before the onset of boiling in the reactor. In a more typical refuelling shutdown, it would take 2 h 14 minutes for the onset of boiling. In emergency the only available action would in this case be to use the diesel-driven fire water pumps to inject water to the reactor shaft trough fire water hoses.

In the short term, the control of normal reactor coolant inventory can be restored when power is available, and in the long term when primary heat sink is available. Short term refers to at least 15 h of available time as mentioned in Section B.5.2.2.

B.5.3.2 External actions foreseen to prevent fuel degradation

External actions to prevent fuel degradation would depend remarkably on the accident, and include the restoration of feed water injection and primary heat sink. As a last resort for an open reactor, water injection to the reactor could be performed through the fire protection system. This would require manual actions inside the containment. The licensee will also investigate the possibility to use the hydro-accumulators as water storage for shut-down conditions. Using of hydro-accumulators could increase the time span for the onset of boiling from 28 minutes to approximately 1 hour, if two hydro-accumulators were available. At the same time two hydro-accumulators would increase the time span for core uncover about 8 hours (boiling would occur in the reactor shaft).

B.5.3.3 Measures, which can be envisaged to increase robustness of the plant in case of loss of primary ultimate heat sink, combined with station blackout

The item is discussed in sections B.5.1.5 and B.5.2.5.

In case of combined station blackout and loss of ultimate heat sink, the possibility to operate the air-cooled cooling towers and in addition boron injection pumps with air-cooled diesel-generator is also investigated by the licensee. The modifications in consideration would create a possibility to closed-loop operation also in case of combined station blackout and loss of ultimate heat sink.

Spent fuel storage

Water addition from external sources could be modified not to require an access to the containment and spent fuel storages. One possibility is a back-up electricity supply for water feed into the spent fuel storages by the SAM electrical systems and SAM I&C.

The new air-cooled heat sink i.e. cooling towers would remove the decay heat from all spent fuel storages.

B.6 Severe accident management

B.6.1 Organization and arrangements of the licensee to manage accidents

B.6.1.1 Organisation of the licensee to manage the accident

<u>Organization during normal operation and accidents</u>

The operating shift personnel (control room operators and field operators), plant's fire brigade, and the security personnel are working continuously 24/7. Additionally, the power plant's manager in charge and the on-duty safety engineer are on-call outside daytime working hours.

During normal office time the managers, the experts and maintenance personnel at plant as well as the Technical Support unit in the company headquarters may assist operating shifts in the normal operation. In addition to the personnel mentioned above, there are extra personnel at the power plant during the annual outages.

During a plant disturbance, the shift supervisor must lead the activities of the shift, monitor plant unit status and supervise that all necessary measures are carried out without delay. The power plant on-duty safety engineer assists the shift supervisor. During non-working hours the on-duty safety engineer shall arrive on site within 40 minutes of notification. Plans for strengthening the site organization in case of emergency include formation of emergency preparedness organization at the site and at the Technical Support unit.

The emergency organisation is headed by an emergency manager who shall be responsible for the emergency response on the site of a nuclear power plant and liaison with the authorities. Once the plant unit's shift manager declares a state of emergency, he also becomes the emergency manager. The shift manager acts as the emergency manager, and heads the rescue efforts at the plant until one of the managers in charge arrives at the emergency centre and takes leadership responsibility for the situation from the shift manager, thus becomes the emergency manager. The emergency manager is in charge of the on-site emergency response activities until the rescue authority notifies that it assumes command over the rescue operations. It should be noted that the shift personnel (i.e. the operators and on-duty safety engineer) deal with the severe accident situation according to SAM Guidelines, until further notice from the emergency manager.

In emergency preparedness plan there are detailed instructions how the emergency preparedness organization work is arranged and what is the composition of the organization. Based on practical experience the emergency preparedness organization is estimated to initiate activities at the emergency centre 20 minutes after receiving the alarm during daytime work hours and 45 minutes after of receiving the alarm outside daytime work hours. The emergency preparedness organization is estimated to be in full operational readiness 1.5 h after receiving the alarm.

Based on the advance planning, the regional rescue service participates in the power plant's rescue operations. Additionally, they have heavy duty clearing equipment. In an accident situation, based on their resources, they can prioritise their duties to provide assistance to Loviisa NPP and to clear access routes in and around the plant. Based on legislation, they have the option to present an official request for help from any authority to clear roads and to arrange alternative modes of transportation, such as boat and air transportation. In an accident situation, the rescue authority also has the right to requisition of private equipment.

When compiling the emergency preparedness organization and emergency preparedness instructions, the aim has been to take into consideration the shift changes of the emergency preparedness organization personnel in long-lasting transient and accident situations by assigning more than one person to the different positions in the emergency preparedness organization. Additionally, the matter has been addressed in the position-specific guidelines of the emergency preparedness organization by mentioning the shift change or the allocation of resources.

Radiation protection gears

Personal radiation protection gears are stored e.g. in the SAM control room, at the boundaries of the controlled area and in the warehouse in the service building. The protective gears and measuring instruments for the radiation measuring patrols is readily available at the emergency centre. Iodine pills are stored e.g. in the emergency centre and in the SAM control room.

Control rooms and Emergency Centre

The original design basis for the external radiation shielding of the MCR, without the need to evacuate the room, is a severe reactor accident after the LOCA. Analyses for main control room confirm the original design basis of habitability. In case the main control room is unavailable e.g. due to fire the main control room of the neighbouring unit can be used as an emergency control room to operate the unit in question to safe state. If both of the main control rooms are lost at the same time, the shifts of the both units will be evacuated into the SAM control room.

Severe accident management actions can be executed from the MCR or a separate SAM control room. This SAM control room is common to both plant units. The SAM control room has been designed for a severe accident in one reactor, but there are no significant technical constraints to manage severe accidents from SAM control room for both units simultaneously. The massive concrete structure of the SAM building and the possibility to use underground pathways ensure the SAM control room being accessible and operable during the severe accident.

The emergency centre is located in a shelter. The emergency centre has its own emergency diesel generator that provides the required energy if the electricity cannot be provided in the normal ways. The amount of diesel fuel is estimated to be enough for approximately 300 h without refuelling. The emergency centre is shielded against direct radiation by thick concrete walls ensuring long time habitability in the centre during potential radioactive release and outdoor fallout during a severe accident. If for some reason the emergency centre loses its ability to operate, the emergency preparedness organization can operate to the appropriate extent in the SAM control room.

<u>Procedures, training and exercises</u>

SAM Guidelines are based on the SAM safety functions (see Section B.6.3). Immediate SAM measures are carried out within the Emergency Operation Procedures (EOP). After carrying out immediate actions successfully, the operators concentrate on monitoring the SAM safety functions. The SAM guidance focuses on monitoring the leak tightness of the containment barrier, and on the long-term issues. The transition to SAM Guidelines takes place when the reactor core is damaged or is close to doing so, and there is no return to EOPs thereafter.

The SAM-handbook contains background material for better understanding of the SAM safety functions and accident phenomenology related to these safety functions, fuel storages, criticality issues and radiation protection during a severe accident. Relevant severe accident analysis results, experimental results, and thorough description of the SAM systems have been included. The handbook is used primarily by the emergency preparedness organization during the accident, and more generally also for training purposes.

Power plant operators are required to participate in the simulator training every year. Transient and emergency instructions are evaluated as a part of these simulator trainings. In addition to the revision of the instructions during training, all the instructions are assessed regularly.

All individuals working at the power plant receive basic emergency preparedness training. Evacuation exercises for personnel are arranged annually at the power plant. Individuals assigned to the emergency preparedness organization receive task-specific basic training before being assigned to the task. Those in the emergency preparedness organization receive annual refresher training and advanced training. Individuals working in the emergency centre receive training on emergency centre activities.

Training to emergency centre personnel of STUK, Rescue Service and Police Department of district Eastern Uusimaa, and power plant emergency centre personnel is organized annually in accordance with a separate plan.

Official emergency exercises are held annually. Every third year a nation wide emergency exercise of the plant is held. The training simulator is used when practicing the accidents, but the simulator is not capable of extending the simulation into the severe accident domain at the moment. When there is need to practice severe accidents then table top training is used together with the training simulator.

B.6.1.2 Possibility to use existing equipment

Possible means to prevent the accident to proceed to core damage and related actions are to a large extent already included in the EOPs, which can be executed by the personnel available on-site all the time.

Fixed severe accident management systems have been installed at Loviisa NPP as explained in Section B.6.3. Use of mobile devices is not assumed during severe accidents, except for supplementary water that must be provided for containment external spray system after 3 days of operation. In addition, this system can be operated through the external fire truck connection in case of loss of its pumps or heat exchangers. The use of this fire truck connection in a severe accident situation is considered possible due to the long time delay to the demand.

The situation is different for spent fuel pools. Actions not given in the EOPs might be required and the fire brigade needed to utilize either fire truck or fire water systems. Temporary electrical connections and valve operations might be required as well. However, the time delays are long (see Table B-2), except for specific outage conditions where the core is unloaded. In this one distinct outage condition the prevention of fuel damage is the easiest and can be made by utilizing fire water systems. Although time to bring these means and systems into use has not been evaluated, the time delays are considered sufficient to gain control over the situation.

The SAM safety functions defined in Section B.6.3 do not call for feeding water into the reactor, but it is necessary in the long term to finally terminate the accident.

Addition of diesel fuel is needed for SAM diesels after 24 h and for emergency centre diesel after 300 h of operation (see Section B.6.1.1). At the site there is no tank truck, but in future fuel can be transported in a small tank moved by a forklift available at the site.

Radioactive releases in severe accident are mitigated by containment isolation achieved by closing any containment penetrating routes and by ensuring the containment integrity. SAM strategy is developed to ensure containment isolation and integrity as discussed in detail in Section B.6.3. The applied SAM measures keep the releases at relatively low level.

As an additional measure the containment internal spray, if available, can be used to wash the fission products from the containment atmosphere. This action would minimize minor releases from containment design leakage and lower the skyshine radiation dose rates.

When all power supplies function as planned, all phone and telecommunications connections are also functioning.

In a situation where only emergency diesel generators are functioning, there are still several different communication systems available including external telecommunication and internet connections, as well as internal phone systems and VIRVE (Finnish authorities' secured radio network) phones.

In a total loss of power situation (emergency diesels are not in use) the emergency preparedness personnel at the plant can communicate externally using a satellite phone and internally via the direct channels of the VIRVE terminals to other teams at the plant, to e.g. the main control rooms of the plant units, the alarm centre, and the fire brigade and security. Also this communication will work as long as the batteries of the VIRVE and satellite phone have power. VIRVE terminals and satellite phone can be charged manually in the emergency centre and from SAM-diesel secured network.

B.6.1.3 Evaluation of factors that may impede accident management and respective contingencies

External destruction of infrastructure around the power plant area as a result of some natural disaster could result in the delay or prevention of additional personnel arriving to the plant. In this case, the personnel who are at the plant when the event occurs, has to manage the accident. Depending on weather conditions coastal guard boats or helicopters might be used for transportation instead of the road connections. Depending on the accident sequence some external actions might be required. In the long term diesel fuel is needed, and in case of the loss of the ultimate heat sink significant amount of spray water is needed for containment external spray system.

If the external communications connections are not available, the only external device left for communication is the emergency centre's satellite phone.

The actions needed to support the SAM strategy presented in Section B.6.3 can be carried out even when large amounts of radioactive fission products are present inside the containment. Design basis for local operations includes radiation protection aspects and the locations are shielded against radiation present in a severe accident.

The steel containment is designed to withstand the forces and thermal energy caused by the design basis accident and to prevent large radioactive releases. The outer concrete containment is thick enough to shield the other rooms and the plant yard from the potential high radiation source term inside the containment. The exceptions are main and auxiliary entrance pathway openings into the containment. The affected areas in front of the openings do not prevent the potential repair operations during or after the accident at the plant. Because of the reactor building roof configuration, the activity in the upper part of the containment or loss of the water from the in-containment spent fuel pool would cause sky-shine radiation at the plant yard, which is taken into account in the emergency operation plan.

In case of uncovered fuel in the spent fuel storages, the concrete ceiling prevents the skyshine to the plant yard, and the thick walls of the fuel pools and the storage building act as shielding against direct radiation. Radiation from the partly or totally dried spent fuel pools in the containment or in the spent fuel storages can be managed by injecting water into these pools. Radiation does not prevent the actions needed, except those requiring access to the containment or spent fuel storages.

Release and deposition of radioactive material may cause complex and severe situations in the plant and outdoors. Fallout at the plant yard and access routes to the plant would affect to the actions of countermeasures and material and workforce transport. However, skyshine may disturb detection of contamination.

If the main and emergency control rooms are lost, there is a specific SAM control room common for both units at Loviisa NPP. In the SAM control room the units can be brought to safe shutdown or SAM actions can be executed. In addition containment isolation can be performed from the local control centres using the SAM power supply.

The local control centres are normally located in the vicinity of high radioactivity (e.g. emergency cooling systems). Due to thick protective walls in these areas, the radiation levels are significantly reduced, which ensures tolerable conditions to carry out operations in the local control centres. In most cases, the accessibility of the local control centres is not threatened, but in the situation where large amount of radioactive water has flown into the material hatch, there may be elevated radiation levels along the access path. Spreading of radioactivity outside the containment depends on the availability and use of ventilation systems. Individual doses can be reduced by using personal protective equipment.

The basis for the SAM strategy is that all necessary accident management measures can be actuated from the main control room or SAM control room. Emergency centre is also needed for the severe accident management. If both units face the accident situation at the same time, skyshine won't make these places unavailable for the accident management.

Loviisa SAM safety functions rely on equipment that is located at plant yard level. Flooding exceeding the plant yard elevation would have impact also to the systems fulfilling the safety functions. Severe accident as a result of a flooding event necessitates use of containment external spray by external equipment (fire truck or other external pump utilizing sea water or other water at site).

The SAM systems are not designed to withstand earthquakes. Seismic analyses of these systems are not included in level 2 PSA and therefore there is no confirmation of the operability of these systems after an earthquake.

Possibilities to ensure SAM safety functions are considered in Section B.6.3. In a situation of total loss of power, managing the accident becomes more difficult. This has effect on all of the accident management aspects. To support immediate actions, the emergency preparedness organization has handheld lights available at the emergency centre and the fire brigade has a small generator unit on the fire truck. Additionally, the plant has a slightly larger, tractor-pulled generator unit. These two pieces of equipment enable a very limited supply of electricity, however.

B.6.1.4 Conclusions on the adequacy of organisational issues for accident management

It has been stated above that "depending on weather conditions coastal guard boats or helicopters could be used for transportation instead of the road connections". This might be possible, but this kind of operations may be difficult, and it could be beneficial to have a more detailed investigation on the possibilities for this kind of support in extreme situations in order to have realistic expectations. There is only one road connection to the site, and therefore equipment to restore the lost transport connection, e.g. after extreme weather situations, would be beneficial. Licensee's aim is to update EOPs and make modifications to enable all actions needed with the personnel available at the site 24/7.

The radiation doses possibly arising from the measures to be carried out during the course of a severe accident have been considered reasonable.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan and schedule to

– increase fuel reserve for emergency power at the site, and
– secure DC power for long time needs;

as well as to investigate the following issues for Loviisa NPP:

– availability (and operability) of safety systems and their components in accidents of long duration;
– needs and possibilities to use mobile power supply and mobile pumps in accidents;
– possibilities to secure availability of demineralised water at the site in an accident of long duration; and
– review of the applicability of procedures and availability of personnel in case of accident in multiple units.

According to the licensee, the skyshine issue above has not been considered as a problem that could make the accident management too difficult. STUK will review this assessment after receiving more detailed description of the situation considered. However, the simultaneous accident in both of the units would not make a significant difference in radiation levels at the locations where possible actions would be needed, as these locations are protected from the radiation from both of the units more or less in the same way. Thus, this is not seen as a major issue.

B.6.1.5 Measures which can be envisaged to enhance accident management capabilities

To respond to STUK's requirements after Fukushima accident, Licensee has proposed the following measures to enhance the accident management capabilities of the organization at Loviisa NPP:

– to take in consideration in the emergency instructions a case where an accident is considering both units and all fuel pools;
– improvement of the accident management training;
– to arrange emergency exercises in a date not informed to participants beforehand; and
– ensure availability of sufficient communication systems from electrical systems available in severe accidents.

The number of people in the technical support emergency organization was recently increased for better preparedness and support against accident situations. As the current organisation is based on assumption that the severe accident is ongoing at one unit only, further consideration on number of vacancies of radiation monitoring and laboratory personnel and contact persons between the emergency centre and technical support, will be reviewed.

B.6.2 Accident management measures in place at the various stages of a scenario of loss of the core cooling function

B.6.2.1 Before occurrence of fuel damage in the reactor pressure vessel

The safety systems supporting core cooling and their usage during accidents are described in Section B.1.1.2. As an ultimate measure, RCS feed & bleed is utilized to depressurise the RCS and to provide possibility for consequent ECC injection to enable core cooling as the last resort (see Section B.6.3.1).

Within the EOPs RCS depressurisation and other immediate actions supporting the SAM are carried out, when core exit temperatures permanently exceed 450°C thus showing that the core is uncovering. These are lowering the thermal shield of the RPV lower head and forcing open the ice condenser doors, to provide adequate flow paths around the RPV outer wall and ensure efficient mixing of the containment atmosphere, respectively. These are discussed in more detail in Section B.6.3.

B.6.2.2 After occurrence of fuel damage in the reactor pressure vessel

Severe accident management is discussed in detail in Section B.6.3. The main goal is to protect the containment function with different systems and measures.

B.6.2.3 After failure of the reactor pressure vessel

Loviisa NPP SAM strategy relies on retaining corium inside the pressure vessel, as described in Section B.6.3.5. The consequences in case of failure of in-vessel retention are discussed, as well.

B.6.3 Maintaining the containment integrity after occurrence of significant fuel damage in the reactor core

In Finland, the introduction of severe accident management has been required as a design extension also of the operating units. Consequently, a comprehensive SAM strategy has been developed for Loviisa NPP to mitigate the consequences of severe accidents. This strategy is based on SAM safety functions whose purpose is to ensure containment integrity and isolation. To ensure containment integrity energetic events like direct containment heating, steam explosion and hydrogen explosions must be avoided. Direct containment heating and steam explosions can be prevented by ensuring in-vessel retention of corium by reactor pressure vessel external cooling and primary circuit depressurisation. Hydrogen management is a separate safety function. Mitigation of slow processes, like prevention of a slow containment over-pressurisation has to be ensured as well.

The SAM safety functions are
- containment isolation,
- RCS depressurisation,
- in-vessel retention (IVR) of corium by reactor pressure vessel external cooling,
- hydrogen management, and
- management of containment pressure by containment external spray.

Containment isolation is discussed in more detail later in this Section. Other SAM safety functions are discussed in sections B.6.3.1, B.6.3.2, B.6.3.3 and B.6.3.5. In addition to the above SAM safety functions, sub-criticality and fuel pool cooling have to be ensured during a severe accident. These are discussed in more detail in Sections B.6.3.4 and B.6.3.2. All these issues are part of the SAM Guidelines and SAM handbook.

The design basis for all SAM safety functions is that the actions can be done, when the other supplies have been lost, with dedicated independent SAM electrical systems (see Section B.6.3.6) and dedicated independent SAM automation (see Section B.6.3.7) from SAM control room or main control room.

The SAM strategy has led to a number of hardware changes at the plant. Also the SAM Guidelines and SAM handbook were prepared (see Section B.6.1.1).

The main goal of severe accident management is to ensure that the radioactive substances released from the damaged fuel can be confined in the containment. Therefore, it is crucial to ensure that containment isolation is successful. In most cases, the containment is isolated automatically through a plant protection signal much before the transition into the severe accident regime. However, isolation of the containment and/or confirming isolation status is also part of the SAM Guidelines, due to the crucial importance of successful containment isolation before releasing radioactive substances from the core.

Containment isolation signals may be actuated manually by the operator through a key switch. The system was modified to enable locking the isolation status after verification that the containment was successfully isolated. Selected isolation valves have been modified so that closure is possible manually at a local control centres in case of loss of power or control systems. Significant modifications have been made to reduce the probability of by-pass sequences, e.g. steam generator modifications to reduce probability of large primary-to-secondary leakage accidents (PRISE). The containment leak-tightness monitoring system has also been significantly improved within the SAM project. There are indications of status of the isolation valves. The positions of the material lock and personal hatches and the containment vacuum breakers can be monitored. There are also water level and pressure measurements outside the containment in compartments where water leakages could be expected in case containment isolation had failed.

The containment isolation is in most SBO cases ensured by fail-safe valves or check valves. In those lines where two motor operated valves are needed to be closed, the electrical feed is ensured by batteries, emergency diesels and SAM-diesels. Isolation in SBO is not needed for some valves, but all these valves have hand-wheels for manual closure.

The SAM approach was developed and the SAM systems were designed to cope with the accidents starting from power operation states. More recently the severe accidents initiating during shutdown have been studied and the applicability of the SAM strategy for shutdown states has been evaluated. The basic requirements for severe accident management during shutdown are the same as for power operating states. In order to successfully mitigate the severe accident starting in shutdown states, some actions are needed to recover the functionality of containment and severe accident management systems.

Conditions in the containment and initial core conditions are also different from power operating states and these conditions will change during shutdown. In some cases this means that success criteria will be not only different from power operating states but also different depending on the outage stage. Extensive work has been done for Loviisa NPP in order to analyse the state of containment and the state of severe accident management systems during shutdown. Each of the SAM safety functions has been evaluated. The success criteria have been re-assessed and the state of hardware implemented for the SAM purposes have been studied during different stages of outage. The aim has been to study the applicability of the SAM strategy and to recognize possible actions and procedures in order to improve the applicability of the SAM strategy. The work has included large amount of observation work done in Loviisa NPP during several consecutive plant outages, background studies and code calculations.

In order to mitigate the consequences of severe accident initiated during shutdown, active recovery actions are needed in order to recover the operability of severe accident management systems. In Loviisa NPP, based on the work, guidance for SAM system recovery actions has been made as well as many procedural improvements. At the moment guidance is going through validation and verification. It has to be noted that guidance mentioned above, is guidance for recovering the SAM systems operability. These actions have to be started already before the core damage and before the conditions in the containment will make the containment compartments inaccessible. The goal of this guidance is to ensure that the SAM systems, which are needed in order to successfully mitigate the consequences if the accident would proceed to core damage, are available when needed. Difference has to be made between SAM Guidelines which guides the execution of the mitigation actions.

Recovery actions in order to resume containment tightness and the operability of the SAM systems will be needed in accidents starting during shutdown. One of the main challenges in the shutdown states in Loviisa NPP is that the containment function might be impaired and some recovery actions are needed. Also a lot of system maintenance, performance tests and inspections are done in shutdown states.

B.6.3.1 Elimination of fuel damage / meltdown at high pressure

The RCS depressurisation is an interface action between the preventive and mitigative parts of the severe accident management. If the RCS feed function is operable, the depressurisation may prevent the core damage. If not, the mitigative actions and measures to protect the containment integrity and mitigate large releases are started. New manually actuated depressurisation capability has been designed and implemented for severe accident management through motor-operated relief valves (two parallel lines with two similar valves in each line). Depressurisation capacity will be sufficient for feed & bleed operation with high-pressure safety injection pumps and hydro accumulators (in some cases even with low pressure safety injection pumps), and for reducing the RCS pressure before the molten corium degrades the reactor vessel strength. The new pressurizer severe accident relief valves were installed at the same time with the replacement of the existing pressurizer safety valves in 1996. The capacity of one pressurizer severe accident relief line is roughly 90% of the capacity of one pressurizer relief line.

With regards to mitigation of severe accidents, it is crucial to ensure low pressure conditions. High RCS pressure might lead to failure of the in-vessel melt retention and consequently, to a failure of the reactor pressure vessel. This could lead to a significant pressure increase in the reactor cavity due to direct containment heating, flashing of water and melt-water interaction. All these may jeopardize the containment integrity and to avoid this, the RCS pressure is lowered. Additionally, low RCS pressure is helpful for the prevention of induced SG tube ruptures during molten core conditions with hot gas and steam flowing to the SGs. Depressurisation is done before corium relocates into the lower head of the RPV to ensure in-vessel retention of corium.

As the depressurisation is designed solely for severe accident purposes, there are no special operational provisions required in addition to normal maintenance operations. Depressurisation is included in SAM Guidelines and EOPs, which direct the depressurisation valves (all four valves) to be opened when the core exit temperatures permanently exceed 450°C.

B.6.3.2 Management of hydrogen risks inside the containment

Loviisa NPP containments are equipped with ice-condenser containments, which are relatively large in size but have a low design pressure of 1.7 bar (abs). The ultimate failure pressure has been estimated to be above 3 bar (abs). An intermediate deck divides the containment in the upper and lower compartments. All the nuclear steam supply system components are located in the lower compartment and, therefore, any release of hydrogen into the containment will be directed into the lower compartment. The main route for hydrogen and steam to reach the upper compartment, which is significantly larger in volume, is through the ice-condensers.

Because of the relatively low design pressure of the containment, the hydrogen burns that can create a potential threat include not only detonations, but all large-scale combustion events that are rapid enough to yield an essentially adiabatic behaviour. The hydrogen issue was brought up for Loviisa NPP soon after the TMI-2 accident, and glow-plug igniters were installed in Loviisa NPP containments in 1982.

In the early 1990's an extensive research program was initiated at Fortum to assess the reliability and adequacy of the existing igniters. The studies were completed and the hydrogen management strategy for Loviisa NPP was formulated and implemented. The hydrogen management scheme concentrates on two functions: ensuring containment atmosphere mixing to decrease the hydrogen concentrations and controlled removal of hydrogen.

Hydrogen management is based on plant-specific features, and as in-vessel retention of corium is utilised, the only real concern regarding potential energetic phenomena is due to hydrogen combustion events. Plant modifications included a dedicated system for opening the ice-condenser doors to ensure adequate flow paths for efficient mixing of the containment atmosphere, passive autocatalytic recombiners (PARs), and a new glow plug system. Design bases of the PARs and ice-condenser door opening mechanism consider full oxidation of zirconium within the fuel bundles with analysed hydrogen generation rates. The glow plugs take care of reflooding situations where rapid hydrogen generation may occur. Both units have 154 PARs in the containment; 84 in the steam generator space, 66 in the dome, and 4 in some dead-end spaces.

The two redundant system to force open the ice condenser doors was installed in 2001 (LO1) and in 2002 (LO2). The doors of the two ice condensers at each unit can be forced open with pressurized nitrogen operated pneumatic cylinders. The nitrogen systems are located outside of the containment, except the nitrogen piping to the cylinders. After opening, the doors are locked into place requiring no nitrogen pressure. The doors can be opened by operator action or without electricity and automation by manual operations of nitrogen valves, which are accessible during a severe accident.

The PARs installed in 2003 are fully passive components and do not require any operator or local actions apart from shutdown state recovery actions. The arrangement of the PARs ensures hydrogen concentrations low enough not to cause a threat to the containment.

The new glow plug system was installed in 2003, and the old system has been disconnected and is to be dismantled. The glow plugs are powered by SAM diesel generators, and they are arranged based on DDT criteria in an optimal way to prevent flame acceleration. The glow plugs and their cabling are designed to survive in harsh environmental conditions of a severe accident. The glow plug system is qualified for LBLOCA, SLB and consecutive deflagrations.

Opening of ice-condenser doors and activation of glow plug system are included in SAM Guidelines and EOPs.

During the power operation PAR plates are constantly tested to ensure that plate poisoning doesn't endanger the start-up parameters, and a criterion is defined for plate replacement. During the shutdown states containment atmosphere may contain harmful fumes from maintenance work at the plant. For this reason PARs are protected for outage against and are therefore not functional. Furthermore, in order to prevent ice melting during shutdown states, mechanical wedges are placed to prevent opening of the lower inlet doors of the ice-condensers. Also some intermediate deck doors are made inoperable for maintenance actions by removing the opening wires.

It has been evaluated that in severe accidents during refuelling outages when the whole upper compartment of Loviisa NPP containment may participate in the hydrogen mixing, the hydrogen concentrations in the upper compartment remain low enough when at least 40% of the upper compartment PARs are available. If 60% of the upper compartment PARs are available, the hydrogen concentrations remain below the specified limit with a wide margin. The PARs in the lower compartment do not necessary need to be available in severe accidents during refuelling outages, although they may increase the margin to remain below the specified hydrogen concentration limit in the upper compartment. If no PARs are available in the lower compartment, the glow plugs can ignite the hydrogen in the lower compartment. In these concentrations hydrogen burns do not pose a threat to the containment integrity.

Based on the work, to ensure minimum capacity of the PARs during the shutdown states, the guidance for their recovery has been made. In addition, recovery actions defined for shutdown state severe accident management include removal of the wedges and reconnecting the opening wires.

B.6.3.3 Prevention of the containment overpressure

The studies on prevention of long-term over-pressurisation at Loviisa NPP started by considering the concept of filtered venting, as was done for many European NPPs after the Chernobyl accident. However, the capability of the steel shell containment to resist sub-atmospheric pressures is poor. By using filtered venting, it is possible that the amount of non-condensable gases after the venting is significantly less than initially, which after cool down of the containment atmosphere may lead to sub-atmospheric pressures and possibly collapse of the containment. Therefore, alternative solutions were sought for.

The concrete used in the reactor cavity of Loviisa NPP does not contain any CO_2, the amount of non-condensable gases (except for hydrogen) generated during core-concrete interaction would be negligible. Therefore, the overpressure protection of containment could be limited to condensing the steam produced. An obvious way of doing this is to spray the exterior of the containment steel shell. Later on, the concept of in-vessel retention was introduced to Loviisa NPP, which excludes core-concrete interactions altogether and thus finally ensures that no non-condensable gases apart from hydrogen need to be considered.

The containment external spray system is designed to remove the heat from the containment in a severe accident when other means of decay heat removal from the containment are not operable. Due to the ice condenser containment, the time delay from the onset of the accident to the start of the external spray system is long (16…36 hours from the initiating event taking no credit from actions to transfer heat to the ultimate heat sink). Thus the required heat removal capacity is also low, only 3 MW because a fraction of decay power is absorbed by thick concrete walls of reactor building and moved from the outer surface of the wall to the environment. Sufficient capacity has been validated by large-scale experiment in the German HDR containment near Frankfurt am Main.

The system is started manually when the containment pressure reaches the design pressure of 1.7 bar (abs). The single failure criterion is applied. The active parts of the system are independent from all other containment decay heat removal systems. All active parts are accessible during a severe accident as they are located outside the containment in protected areas. The containment external spray was implemented at the two units in 1990 and 1991. The both units LO1 and LO2 have their own external spraying circuits and spray water storage tanks. The cooling circuit of the spraying system and the dedicated SAM diesel generators are common for both units. The ultimate heat sink is sea water.

There is a possibility to use the external spray system without dedicated cooling system by water injection from external sources, e.g. a fire truck or other external pump. This can be done even without any electricity from skyshine radiation protected connection point (see Section B.6.1.3). Lack of cooling system requires that new cooling water (some other water supply at site or water transported by trucks) must be injected into the system and finally this water enters through intermediate tank to make-up water tank and from there through overflow into the plant yard. Alternative possibility is to inject additional water into the cooling circuit and recirculate the spray water between the tank and spray nozzles while cooling the recirculating water with cooling circuit. Recirculation can be achieved by fire truck or external spray system pumps if electrical power is available. If not, two external pumps are needed operating the external spray system this way. Water injected to the cooling circuit would flow into the plant yard after passing through the heat exchanger.

In case of LUHS, measures could be taken by fire fighters to restore a small water intake area from the sea for example for fire truck water intake. This would allow in some weather based LUHS cases the operation of containment external spray by sea water. Other possibility is to bring water to the site.

Other possibilities to remove decay heat from the containment are by the LPSI and containment internal spray system heat exchangers through the intermediate cooling system. However, as malfunction of these systems may be the ultimate reason for the severe accident situation, their availability in severe accidents is not ensured at the same confidence level as the availability of the dedicated external spray.

As the containment external spray is designed for severe accident purposes, there are no special operational provisions required in addition to normal maintenance operations. Activation of containment external spray, as well as alternative systems, is included in SAM Guidelines.

B.6.3.4 Prevention of re-criticality

Controlling core sub-criticality is one of the main accident management objectives. One particular example of the importance of the sub-criticality issue is a safety injection recovery situation if water could be injected into a core with an essentially intact geometry. In such a case the starting point should be that only borated water reaches the core, since unborated water could lead to re-criticality. Boron concentration of containment sump is discussed separately in Section B.1.1.2.

When the original core geometry is lost and a molten pool has been formed in the vessel, re-criticality should not be of concern, even if unborated water is used. However, diagnosing the state of the core geometry in a severe accident may be a challenging task. The risk of misdiagnose is therefore significant. Use of unborated water outside of the RPV, in the reactor cavity, may be problematic as well, even if it has no impact on the sub-criticality of corium inside the reactor pressure vessel. If the reactor pressure vessel failed, the sub-criticality of the debris in the cavity could not be ensured. The debris may become critical if it forms a rubble bed and this bed contains right amount of water acting as a moderator.

Thus, only borated water should be used in severe accident, and this is considered in the SAM Guidelines. No special operational provisions are required.

B.6.3.5 Prevention of basemat melt through

Some of the design features of Loviisa NPP make it most amenable for using the concept of in-vessel retention of corium by external cooling of the RPV as the principal means of arresting the progress of a core melt accident. Such features include the low power density of the core, large water volumes both in the primary and in the secondary side (long time delays, water for cavity flooding), no penetrations in the lower head of the RPV, and finally, ice condensers ensure a flooded cavity in most severe accident scenarios. On the other hand, if in-vessel retention was not attempted, showing resistance to energetic steam generation, steam explosions and coolability of corium in the reactor cavity could be difficult for Loviisa NPP, because of the small, water filled cavity with small floor area and tight venting paths for the steam out of the cavity.

After the concept of in-vessel retention (IVR) of corium was first proposed for Loviisa NPP, an extensive research program was carried out by Fortum. The work included both experimental and analytical studies on heat transfer in a molten pool with volumetric heat generation and on heat transfer and flow behaviour at the RPV outer surface. The IVR concept for Loviisa NPP was finalized in April 1994. The concept included plant modifications at four locations. The most laborious one was the modification of the lower neutron and thermal shield such that it can be lowered down in case of an accident to allow free passage of water in contact with the RPV bottom. Lowering mechanism is based on water-hydraulic cylinder that lowers the neutron and thermal shield as hydraulic pressure is relieved.

Other two modifications included slight changes of thermal insulations and ventilation channels in order to ensure effective natural circulation of water in the channel surrounding the RPV upwards and from the lower compartment back into the reactor cavity. Finally a strainer facility was constructed in the reactor cavity in order to screen out possible impurities from the coolant flow and thereby prevent clogging of the narrow flow paths around the RPV. The backfittings were implemented in 2000 (LO1) and 2002 (LO2).

In-vessel retention is mostly ensured by passive means, such as flap valves at inlet and outlet of reactor cavity and strainers. Active operations are required only to lower neutron and thermal shield. After the initial lowering no electricity is needed. Cylinder lowering can also be executed without electricity by manual operations of hydraulic valves.

Loviisa NPP SAM strategy strongly relies on retaining corium inside the pressure vessel, as described above. However, if all means to cool corium inside the pressure vessel are supposed to fail it is possible to enter in a situation where bottom part of the reactor pressure vessel is damaged and molten corium falls to reactor cavity. Primary circuit depressurisation prevents high pressure scenarios and vessel failure itself should not jeopardize the containment integrity in case the reactor cavity is dry. If there is water in the reactor cavity in this case the reactor cavity is pressurized by interaction between molten corium and water. Analyses show that this could break the reactor cavity cylindrical wall. In situation where molten corium is in the reactor cavity, all effort to supply water into reactor cavity must be done to get situation under control. In practise this is done by supplying water to primary circuit or containment. It is also speculated that if pressure in primary circuit is low, the pressure vessel may break relatively small surface area. Hence molten corium could be partly left in the pressure vessel and partly fall into reactor cavity. This configuration should make corium cooling easier. In this case, as above, every effort to supply water in reactor pressure vessel and containment must be done.

Issues impeding in-vessel retention of corium

For successful execution of SAM strategy some actions need to be executed in certain timeframe. Early actions are included in the EOPs and they are checked when entering the SAM Guidelines. In power states the actions are needed only after elevated core exit temperatures are detected.

Recovery of SAM systems and containment leak-tightness in shutdown states can also be considered as a cliff edge. If the recovery fails, also the SAM strategy might fail. When SAM strategy is working as planned, no cliff edge effects can be recognized when purely time delays are considered. Unexpected phenomena (RPV failure despite successful submerging of RPV, unexpected powerful hydrogen burns) could be considered as cliff edge. Phenomenological uncertainties are included in PSA level 2.

In some by-pass LOCA scenarios ice melting may not be sufficient to flood the reactor cavity. In this case IVR concept might fail leading to core melt in the bottom of the reactor cavity and possibly to containment failure. By-pass scenarios are included and recognised in level 2 PSA.

B.6.3.6 Need for and supply of electrical AC and DC power and compressed air to equipment used for protecting containment integrity

SAM strategy plan included creation of a dedicated AC power system to provide power supply from an independent source for all essential SAM instruments and equipment and a dedicated SAM control room (see Section B.5.1). Failure of power leads to failure of instrumentation. Accident management in this case is discussed in Section B.6.1.3.

The following SAM safety functions can be executed without electricity:

– Containment isolation can be executed without electricity by fail-safe valves or hand wheel operated valves (see Section B.6.3).
– Management of containment pressure by containment external spray. Containment external spray can be operated without electricity by a fire truck (see Section B.6.3.3).
– In-vessel retention of corium by reactor pressure vessel external cooling. Hydraulic cylinder can be lowered by hand operation of hydraulic system (see Section B.6.3.5).
– Hydrogen management: PARs do not need electricity, ice condenser doors can be operated manually (see Section B.6.3.2). Demand of glow plug system is questionable because absence of power makes core reflooding unlikely, although different electrical systems feed the safety injections and glow plugs.

Thus, RCS depressurisation only is dependent on the availability of actuation power, which can be supplied from mobile power source, as well.

Currently the SAM handbook and SAM Guidelines do not consider operation of SAM systems without electricity. Local control centres are considered, but in many cases the guidance considers local operation of valves with electricity.

Filling the day tank of SAM diesels is needed after 24 hours of operation in order to secure the availability of dedicated SAM electricity and SAM automation. Lubrication oil in the engine is estimated to last for 14 h of operation, and refilling from the storage tanks is needed thereafter. The storage tank provides extra capacity for 32 h, thus resulting in total operation time of 46 h without additional external supply.

B.6.3.7 Measuring and control instrumentation needed for protecting containment integrity

SAM strategy plan included creation of a dedicated independent SAM automation. In particular, new measurements for monitoring containment conditions and thus the status of the SAM safety functions have been added. In some cases, pre-existing instrumentation has been modified and qualified for severe accident conditions. The only measurements that are essential for correct actuation of SAM measures are the core exit temperatures (with supporting information from hot leg temperatures), radiation levels, containment pressure. The core exit measurements were pre-existing, but have been modified for SAM purposes. The hot leg temperature measurements are new. New pressure measurements were also installed in the upper compartment. Also the plant normal instrumentation can be useful in severe accident. There are also measurements for monitoring the success of all attempted SAM measures, e.g. position indicators of the ice condenser doors and the neutron shield, measurements for monitoring containment isolation function. Also dose rates and releases of radioactive materials are measured in several locations. Several SAM measurements are not required for carrying out any specific actions. They are needed for monitoring containment conditions in a more general sense, and they have been designed to provide useful information on the status of the SAM safety functions.

Important task was the modification of cabling in order to survive the harsh environmental condition of a severe accident. The severe accident conditions inside the containment have been evaluated to be much harder than in other kind of accidents. New qualification criteria were introduced for the equipment inside the containment fulfilling SAM safety functions. These criteria include depending on the equipment large break LOCA and main steam line break and severe accident temperatures and pressures, qualification against high radiation doses and for selected equipment also the pressure and temperature loads due to hydrogen deflagrations. Depending on the equipment the qualification criterion are defined based on demand for 72 h or for one year. Some equipment is not qualified for severe accidents. These include mostly support information but also and some essential equipment. For essential equipment the demand is prior to severe accident conditions (e.g. primary circuit depressurisation).

B.6.3.8 Capability for severe accident management in case of simultaneous core melt/fuel damage accidents at different units on the same site

Both units (LO1 and LO2) have their own dedicated SAM systems with the exception of the containment external spray system cooling circuit (see Section B.6.3.3). However, the cooling system is designed to for demand at both units simultaneously and the systems have also possibility to support the containment cooling function with external mobile device.

B.6.3.9 Conclusions on the adequacy of severe accident management systems for protection of containment integrity

The SAM strategy and its implementation at Loviisa NPP follows the requirements set in the Government Decree on the Safety of Nuclear Power Plants [733/2008] and the Regulatory Guides referred to in Section A.6. The approach and the plant modifications have been approved by STUK. The requirement for containment to withstand core melt ejection at high pressure has been considered to be taken into account by eliminating this phenomenon by reliable RCS depressurisation and IVR of core melt with adequate safety margins. Furthermore, the containment filtered venting system has not been required, as containment integrity is ensured by removing the heat through the containment dome by applying the containment external spray system.

The effectiveness of the SAM is further evaluated by the level 2 PSA studies, which show the possibility to carry out and the success of SAM measures in spectrum of initiating events and severe accident sequences. The frequency limits set for severe accidents and large releases are higher than those set in Guide YVL 2.8. The frequencies as such, apply for new NPP units to be built in Finland, and for old units the principle of continuous improvement of nuclear safety is applied.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to investigate the need to secure containment heat removal without the sea water systems (the present method).

B.6.3.10 Measures which can be envisaged to enhance capability to maintain containment integrity after occurrence of severe fuel damage

Loviisa NPP SAM strategy has been developed to ensure that large releases are avoided and containment integrity ensured. In shutdown conditions some of the severe accident management systems are taken out of use. Recovery of these systems is explained in detail in Section B.6.3. Efforts to further improve and optimise these procedures will continue in the future as well.

The SAM safety functions need electricity to function and therefore SAM diesels have been constructed. Failure of SAM electrical systems of SAM automation is highly unlikely for most of the initiating events. Guidance for severe accident management without electricity or possibility to perform RCS depressurisation with external equipment would further enhance the effectiveness of severe accident management in these situations.

Flooding events would probably lead to loss of AC power sources, which is discussed in Section B.6.3.6.

Containment bypass sequences (for example primary-secondary leakages) are also problematic, because the coolant can escape from the containment through the leak and there is not enough water to flood the reactor cavity and ensure the pressure vessel external cooling. Also ice condensers will not produce water by melting because the energy of coolant is directed outside of the containment. The overall SAM approach at Loviisa NPP was the prevention of core melt sequences which leads to an imminent threat of large releases. Continuous efforts have been made to reduce frequencies of bypass sequences and this work will continue in the future as well.

To respond to STUK's requirements after Fukushima accident, Licensee has studied the possibilities to implement additional injection points for mobile pumps to provide more flexibility to the external spray water supply. These connections could provide capability to inject enough water for both units with one pump. The different possibilities will be analysed in more detail in 2012.

B.6.4 Accident management measures to restrict the radioactive releases

B.6.4.1 Radioactive releases after loss of containment integrity

Radioactive releases from the containment are discussed in Section B.6.1.2. The actions required for restricting radioactive releases are included in SAM Guidelines and in the SAM handbook.

B.6.4.2 Accident management after uncovering of the top of fuel in the fuel pool

The accident management measures after protective water layer for radiation protection is lost and fuel starts to uncover are basically the same as explained in Section B.1.1.2, i.e. feeding water into the spent fuel pools and decay heat removal from the containment or venting the spent fuel storages. The only difference is that accident management measures in Table B-1 requiring access into the containment or spent fuel storages cannot be utilised. Decay heat generation in fuel pools is fairly low and for a quite significant time the steam from pool boiling is able to cool the fuel (see Section B.1.1.2). Therefore a wide time window still exists for effective actions before uncovering of the fuel.

In-containment spent fuel pools are normally covered during power operation by steel covers, which prevent circulation of air into the pools and assure steam environment during fuel oxidation. During the outages and fuel transport the covers are removed and oxidation of fuel cladding in air environment is possible. High heat load from oxidation in air increases the containment temperature and pressure. It is unclear how fast and how large the oxidation would be as there are no analyses and not a good knowledge of this phenomenon. As the heat loads to containment is unknown it is also difficult to estimate the capabilities of containment heat removal systems in this case.

Partly below the in-containment fuel pool bottom there is a room not part of the containment. There are no analyses of consequences in case of molten core-concrete-interaction in the bottom of the pool. Containment failure in this case is possible, but especially with low decay heat power it is also possible that the containment integrity is not threatened. The time delay to containment failure is, however, considered long as the concrete structure thickness below the pool bottom is 2.6 m.

Spent fuel storages are built on bedrock, and they do not have a containment building. The pools may be covered by steel covers at all plant operating conditions. Losing the fuel integrity increases the radiation levels in auxiliary building enough to prevent access to this building and thereby prevent the accident management measures. As the systems needed to feed water into spent fuel storages and the storages themselves are all located in the same building, loosing the fuel integrity in one of the storages probably prevents accident management measures for the other storage as well.

Fuel bundle overheating leads to hydrogen generation and at first hydrogen accumulates in the room where the spent fuel pool is located. In some containment bypass sequences hydrogen could be discharged into rooms that are not part of containment and are not vented. Bypass sequences from the in-containment pools can be practically excluded as the makeup water into the pools operate at low pressure, and no drainage connections exist. Also the spent fuel storages are operated at low pressure and bypass sequences are therefore unlikely.

To provide adequate shielding against radiation the top of the fuel needs to be 2.5 m below water, which is enough to keep the dose rates at the pool edge below 1 mSv/h. Systems for ensuring this are given in more detail in Section B.1.1.2.

The primary means to restrict releases from the damaged reactor is to ensure the containment integrity through the approach presented in Section B.6.3, which apply to fuel damage in the in-containment pools, as well. The only specific question is the hydrogen management and molten core-concrete-interaction, which were discussed separately above.

In the spent fuel storages the only possibility is to ensure submergence of fuel to limit the release from the fuel and to scrub part of fission products in water. Steam spreading into the auxiliary building of LO2 helps by utilising the structures as heat sinks for steam condensing and fission product deposition. There are no analyses how efficient this is. In theory the auxiliary building ventilation system with some filters could be used to vent the storages rooms, but this would also lead to large releases. Also the availability of this system is questionable as it is located in the same building unreachable for repair actions.

The SAM strategy for fuel pools and instrumentation used for this strategy currently will follow the principles in SAM Guidelines. This means that existing equipment is used for SAM with guidance to use them. Improvements to guidance are under development.

The in-containment fuel pool status can be determined by water level and temperature, and containment radiation level measurements of the normal automation measurements, and by outer annulus radiation level, containment temperature and pressure, and hydrogen concentration of SAM automation. Some of these measurements are influenced by accident in the reactor as well and it might be difficult to distinguish the effect of the fuel storage to these parameters. These measurements will be included in SAM Guidelines and SAM handbook.

SAM measurements are qualified for severe accident conditions as explained in Section B.6.3.7, but this is not the case for other measurements. Furthermore, these other measurements are connected to plant's normal or safety automation and thus their availability during severe accidents cannot be guaranteed. In spent fuel storages there are no SAM measurements, but the measurements of the normal plant automation (water level and temperature, dose rate, and air temperature) can be used to monitor their status.

Water addition into the different fuel pools is explained in Section B.1.1.2. These means make possible to prevent fuel damage. Temporary connections can be made outside the containment for most systems and they are not exposed to high pressures, temperatures or radiation levels. Therefore the systems can be assumed to be operational by temporary connections in most cases even in severe accident conditions. Inoperability may arise if the steam can not be vented out from the spent fuel storages or in case of containment bypass. Fire water systems remain operational also in this case and can be used to feed water into the fuel pools.

Habitability of main control rooms, emergency centre and SAM control room are discussed in Section B.6.1.1.

B.6.4.3 Conclusions on the adequacy of measures to restrict the radioactive releases

The approach for spent fuel pools is to "practically eliminate" the possibility of fuel damage, which can be considered acceptable. To support this, based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee

- to provide a plan to secure decay heat removal to ultimate heat sink in extreme external events,
- to provide a plan and schedule to secure alternative means of decay heat removal from in-containment fuel pools, and
- to investigate securing decay heat removal from the spent fuel storage pools.

These issues consider avoiding fuel damage, and thus they are dealt also in Section B.5.

The availability of support organisation might be threatened in case of extreme external event. Thus the actions foreseen to cope with the situation at the plant should be included in the instructions or procedures, although the time for corrective actions is considered long. The external event may also affect the possibility to carry out the preplanned actions, thus resulting in longer duration of the operations.

B.6.4.4 Measures which can be envisaged to enhance capability to restrict radioactive releases

A comprehensive SAM strategy with ultimate goal to ensure containment integrity has been implemented in Loviisa NPP. Ensuring the containment integrity shall be the priority as is already required in national requirements. Enhancements to ensure SAM safety functions are discussed separately in Section B.6.3.10.

Limitation of radioactive releases from spent fuel storages can be done best preventing fuel damage in the first place. EOPs, SAM Guidelines and SAM handbook will consider observation of water level and temperature in the containment fuel pool and the spent fuel storages. This has already been implemented in EOPs. When necessary, operators and/or emergency preparedness organization will initiate actions given in these documents. Temporary connections are not given in detail in these documents. The time delays are relatively long, and therefore it is possible to perform the required preparations. Ready made instructions, if available, help the accident management and prevention of fuel damage in the spent fuel storages. Improvements in guidance are under development.

Ready made connections to SAM I&C and SAM diesel generators would further improve the reliability of decay heat removal from the fuel spent fuel storages. This would also free the operators and plant personnel to other tasks when actions could be made from the main control room, emergency control room or SAM control room.

The strategy to manage accident situations in spent fuel storages should be decided and corresponding plant modifications done. The possibilities are to ensure prevention of fuel uncovery with steam discharge into the atmosphere, to implement new cooling systems or to manage damaged fuel.

In all spent fuel pools improvements in instrumentation is foreseen. Also current reactor building outer annulus radiation monitors could be moved into better places for better direct view into the containment storages to enhance the capability of these measurements to detect fuel uncovery.

B.7 General conclusions

B.7.1 Key provisions enhancing robustness (already implemented)

Principle for continuous improvement of nuclear safety has been the driving force for enhancing nuclear safety in Loviisa NPP since the start-up of its operation. The issues raised within the "Stress Tests" have been a part of the Loviisa PSA studies since 1990's, and risk-based improvements have been carried out by plant modifications and through revising and updating the emergency operating procedures. Furthermore, these issues have been a part of periodical safety reviews carried out at intervals of ten years.

The requirements for severe accident management (SAM) were included in the Finnish nuclear safety regulations in 1982 when the YVL Guide on safety principles in NPP design was issued. After the accident at Chernobyl NPP in 1986, it was required that these principles had to be applied also to plants already in operation. Requirements include dedicated, single-failure tolerant SAM systems and measurements, as well as procedures and guidelines for the organisation to manage the severe accident situation. Major safety systems upgrades in LO1 and LO2 have been made to fulfil the requirements. The respective WENRA reference levels [WENRA 2008] are fulfilled by these safety upgrades.

The following issues can be considered as advantages when assessing the safety of Loviisa NPP against hazards that contributed the accident at Fukushima Dai-ichi NPP.

- Against earthquakes and flooding, a big advantage is the seismic stability of the Loviisa NPP site and moderate seawater level changes anticipated in the Baltic Sea.
- Diesel driven auxiliary emergency feed water pumps and dedicated water storage tanks that provide decay heat removal capability during a total loss of electricity and loss of ultimate heat sink.
- Diesel driven fire water pumping station that gives the possibility to supply water for cooling also in cases without AC power supply.
- High capacity air-cooled diesel generator plant as a diverse on-site AC power source (in addition to the original EDGs)
- Dedicated SAM valves for RCS depressurisation in case of immediate risk of core meltdown
- Hydraulic system to lower the thermal shield of the reactor pressure vessel, for providing external cooling of the vessel in case of a core meltdown accident
- Autocatalytic hydrogen recombiners and hydrogen igniters powered by the SAM diesel generators
- Containment external spray (dedicated SAM system), also operational by mobile equipment in case of loss of its own pumping capability
- Independent SAM diesel generators equipped with the diversified cooling facility(not depending on EDGs)

B.7.2 Safety issues

The following safety issues need attention in future, when enhancing the safety of LO1 and LO2.

In bypass sequences, where the RCS water could leak outside of the containment through some interfacing system, the coolant is lost outside the containment and the ice in the ice-condensers does not melt. In these sequences the water is not accumulated in the bottom of the containment, and thus required RPV external cooling for in-vessel retention (IVR) is not possible. Significant risk reductions have been made, and the work still continues, to reduce the probability and safety significance of these sequences.

Shutdown states need additional safety assessment from the severe accident management point of view, as a part of the safety systems is not available and the containment is open in some situations during shutdown. Procedural changes to improve the availability of the safety systems have been made, and the work is on-going to make the accident management more reliable in shutdown states.

In case of loss of heat removal capability from the RCS, the primary coolant pump seal water system needs to be isolated in order to protect the seal from overheating. In case this failed , the initial situation with only loss of the heat sink may degenerate to a small-break LOCA.

B.7.3 Potential safety improvements and further work forecasted

The potential further improvements for enhancing the safety and robustness of the Loviisa plant against extreme external phenomena will be focused on the following issues:

- the strength of fire fighting systems, severe accident management systems, and fuel storage pools against earthquakes of beyond design basis;
- means to enhance safety margin against flooding caused by high sea water level;
- the sufficiency of on-site fuel reserves for diesel engines during a long lasting disturbance of electrical power supply
- the sufficiency of DC power during a long lasting disturbance of electrical power supply;
- the sufficiency of on-site demineralised water reserves during a long lasting disturbance of sea water cooling in extreme external conditions;
- additional means to remove decay heat from the in-containment fuel pools and spent fuel storage pools, or to supply additional water to those pools during a long lasting accident situation in extreme external conditions;
- installing additional temperature and water level monitoring instrumentation to all fuel pools;
- needs and possibilities for mobile power supply and pumps in accident situations
- the applicability of procedures and the availability of personnel and material resources in case of multi-unit accident situation in extreme external conditions

The above issues are discussed in more detail in sections above considering the measures which can be envisaged to enhance plant safety.

C. TVO – OLKILUOTO 1&2

C.1 General data about the site and nuclear power plant units

C.1.1 Brief description of the site characteristics

The Olkiluoto plant site is located on the coast of the Gulf of Bothnia in Eurajoki municipality about 13 km north of town of Rauma and about 34 km south-west of town of Pori. Olkiluoto island is separated from the mainland by sounds that are only a few tens of meters wide.

The license holder, Teollisuuden Voima Oyj (TVO), is a non-listed public company, established in 1969, producing electricity for its shareholders at cost price. The company owns and operates two nuclear power plant units, Olkiluoto 1 (OL1) and Olkiluoto 2 (OL2). TVO is also a shareholder in the Meri-Pori coal-fired power plant. A third nuclear power plant unit (OL3) is under construction at Olkiluoto.

An interim storage of spent fuel is in operation and spent fuel from OL1 and OL2 is stored there after adequate cooling time in reactor hall fuel pools. In future KPA-storage will be used to store spent fuel from OL3 also.

This chapter will cover the “stress tests” for OL1 and OL2, as well as for the KPA-storage. OL3 will be dealt with in the next chapter.

C.1.1.1 Main characteristics of the units

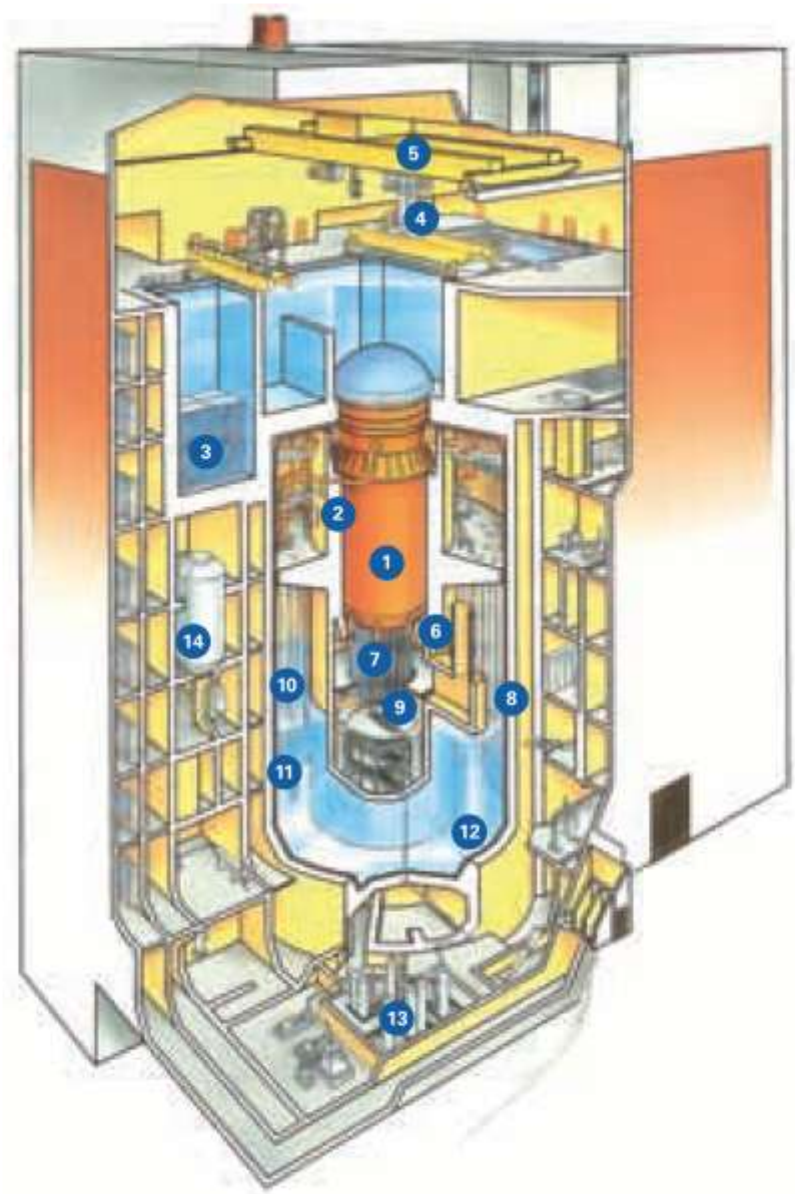
Operating units, OL1 and OL2, are BWRs with net electrical power of 880 MW. The units were supplied by the Swedish company AB Asea Atom (now Westinghouse Electric Sweden AB). First criticalities of OL1 and OL2 were achieved in July 1978 and October 1979, respectively. The thermal power of both units is 2500 MW. The operating pressure of the reactor is 70 bar.

Both units OL1 and OL1 have wet storage space for fuel elements. There are three water filled pools: a fuel service pool, a fuel transport container pool and a fuel storage pool. These are 12.265 m deep and the upper edge is 65 mm above the floor of the reactor hall. They are surrounded with concrete structures providing adequate radiation shielding. The walls and floors of the pools are covered with stainless steel sheet.

Interim storage for spent fuel is located at plant site and it provides storage capacity of total of 1800 tons of uranium for operating units OL1 and OL2. Presently there are three storage pools and one evacuation pool that has the capacity to store all spent fuel from any of the storage pools. The spent fuel storage was taken into use in 1987. Later the planned operational period of OL1 and OL2 has been increased from 40 up to 60 years. The fuel from OL3 will be stored in the interim storage, as well.

The capacity of the spent fuel storage is presently being increased by three more storage pools. The extended capacity will be in use in 2013. Usage of the storage for the purposes of OL3 will be taken into account in the operating license application process of OL3.

Cross section of OL1 and OL2 is shown in Figure C-1.



1. *Reactor pressure vessel*
2. *Main steam lines*
3. *Fuel pool*
4. *Reactor service bridge*
5. *Reactor hall crane*
6. *Recirculation pumps*
7. *Control rod drives*
8. *Containment*
9. *Control rod service platform*
10. *Blow-down pipes*
11. *Embedded steel liner*
12. *Condensation pool*
13. *Scram system tracks*
14. *SAM-scrubber*

Figure C-1. Cross-section of the reactor building and the containment [TVO 2008]

C.1.1.2 Description of the systems for conduction of main safety functions

Table C-1 below shows the system identifiers of OL1 and OL2 for the systems that are referred to when describing the plant safety features and operation. An overview of the emergency cooling systems of OL1&2 is shown in Figure C-2. Electrical systems are discussed in Section C.5.1 in more detail.

Table C-1. OL1&2 system identifiers

112	Cooling water channels	413	Turbine plant steam system
211	Reactor pressure vessel	431	Condenser and vacuum system
243	Fuel pools	434	Condenser cooling system
244	Reactor pools	461	Turbine control system
311	Main steam lines in reactor building	662	Diesel backed 660 V system
312	Feed water system	664	Battery backed 380 V AC system
314	Relief system	711	Cooling water screening plant
316	Condensation system	712	Shut-down service water system
321	Shut-down cooling system	713	Diesel-backed normal operation service water system
322	Containment spray system	714	Non-diesel-backed normal operation service water system
323	Core spray system	721	Shut-down secondary cooling system
324	Pool water system	723	Diesel-backed normal operation secondary cooling system
327	Auxiliary feed water system	731	Raw water treatment system
331	Reactor water clean-up system	732	Water demineralising system
342	Liquid waste system	733	Distribution system for demineralised water
361	Containment over-pressurization protection system	741	Containment treatment system
362	Containment filtered venting system	761	Tap water system
365	Containment water filling system	763	Heating system
		861	Fire fighting water system

<u>Sea water cooling systems</u>

The cooling water channel system (112) intake channel has debris screens, and thereafter the channel is divided into two lines and the sea water flows through a tunnel to the cooling water screening plant (711). The sea water screening plant building has four lines equipped with a fine screen and a basket filter. After the basket filters there is a pool space, which acts as a suction pool for the turbine main sea water pumps and generator cooling pumps.

There are hatches in the channel from the basket filters to the suction pool. Through these hatches water enters the channels that conduct cooling water to shutdown service water system (712) and non-diesel-backed normal operation service water system (714) in one of the auxiliary buildings and to system 712 and diesel-backed normal operation service water system (713) in the other. Both auxiliary buildings have discharge channels to the discharge side of the main channel.

Any clogs (collapse, waste, ice) in the intake channel prevent cooling water intake for the cooling systems. In this case the hatches in the channels to the auxiliary building can be reversed for water intake through the discharge channel.

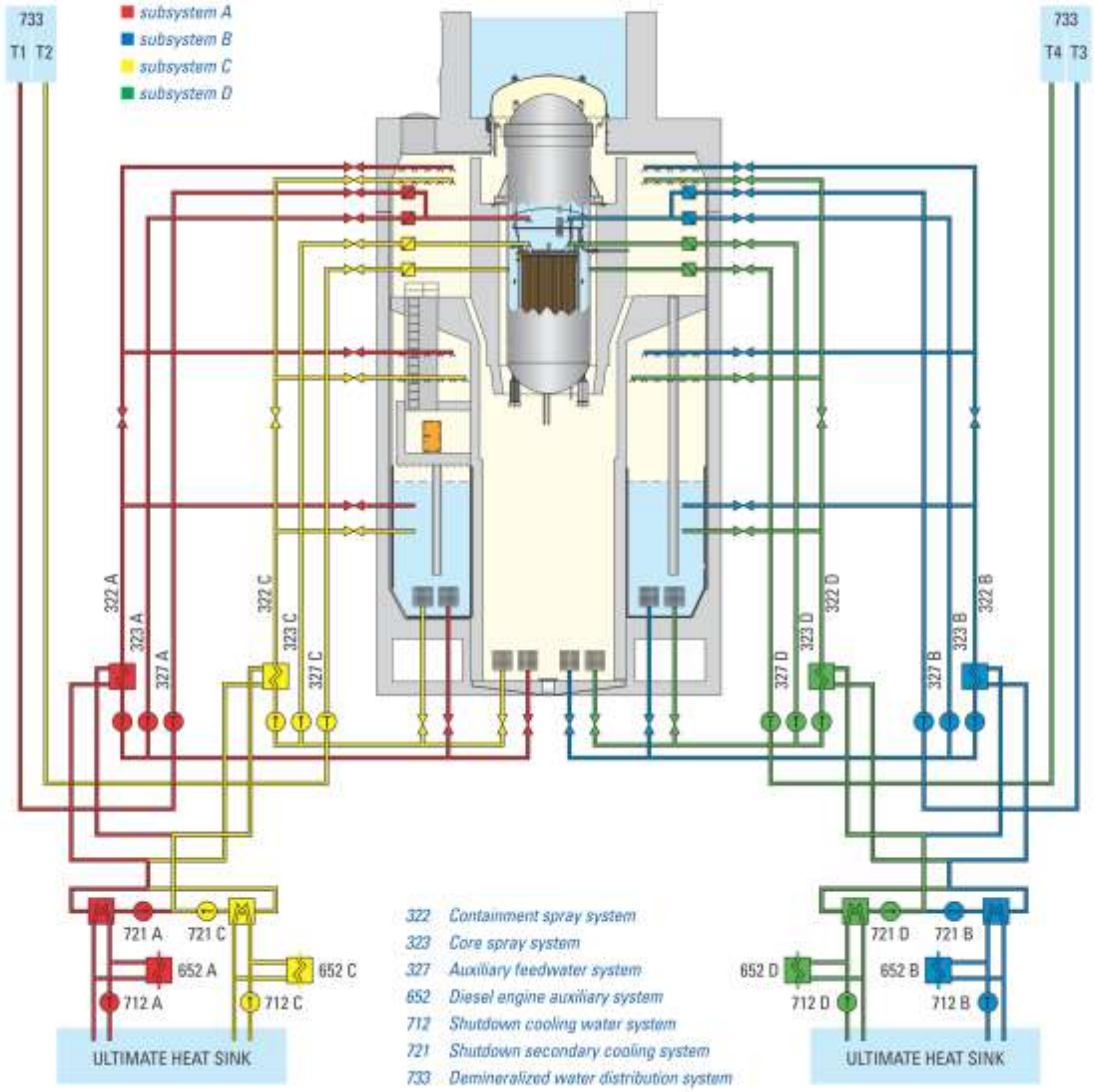


Figure C-2 – Emergency cooling systems of OL1 and OL2 [TVO 2008]

<u>Reactor pressure relief system (314)</u>

The steam lines in the reactor building (311) are connected to the relief system (314) valves inside the containment. The relief system includes 14 valves which are classified according to their purpose.

Eight of the valves are relief valves and four of them are safety valves. In addition, there are two fast opening valves, one in each reactor pressure control line. The relief valves receive electric opening signal in specific plant disturbances. The number of valves to be opened depends on the power level of the plant. When the reactor pressure decreases, the relief valves close at specified pressures. The relief valves are also equipped with spring-loaded impulse valves, which open the main valve in case reactor pressure exceeds 80 bar. The steam released through relief, safety and fast opening valves is led underwater in the condensation system (316) pool.

The safety valves open if the reactor pressure exceeds the design pressure (85 bar). An electronic control valve opens the main valve. The safety valves are also equipped with spring-loaded control valves. Two of the valves open at 85 bar and two at 88 bar.

Some disturbances require the reactor pressure to be decreased rapidly. In such case the automatic depressurisation function of the relief system opens eight valves in the system at 4.5 second intervals and decreases the reactor pressure to about 2 bar.

There are control valves in series with the fast opening valves of the system's control lines. The fast opening valves are opened according to the power level: the pre-selected valve open when the reactor power is below 56%, and when the reactor power exceeds 56%, both of the valves are opened and control valves start to control the reactor pressure. The control valves are supplied by the diesel and battery-backed network.

In case the reactor pressure is too low for the valves to remain open with the help of the medium pressure, the fast opening valves can be kept open to ensure low system pressure during severe accidents. To keep the valves open, they are equipped with piping, which can be used to supply water from the fire fighting system (861) or pressurized nitrogen (from system 754).

The plant can be kept at hot shutdown under normal operating pressure (70 bar), or the reactor pressure can be decreased to 12 bar with the control lines by relieving the the stem produced by residual power into the condensation system (316) pool.

<u>Condensation system (316)</u>

The system includes a condensation pool inside the containment. The condensation pool has 2,700 m^3 of water and its depth is 9.5 m. In addition, the pool has a gas space, which is called the wetwell gas space. From the upper containment drywell, 16 blowdown pipes with a diameter of 600 mm are led through the diaphragm floor and the wetwell gas space to the condensation pool. The blowdown pipe outlets are submerged 6.5 m below the water surface.

In case of an accident, the non-condensable gases in the drywell are transferred along with the steam to the condensation pool through the blowdown pipes and gathered in the wetwell gas space. From the wetwell gas space the gases can pass to back the upper drywell through check valves (so called vacuum breakers).

The pool temperature in normal conditions is below 20°C. When the turbine plant is not in use, the reactor residual power is removed by blowing steam to the condensation pool water space with the control lines of system 314. The heat is removed from the condensation pool with the containment spray system (322). In addition, the condensation pool acts as a water storage tank for systems 322 and 323.

Shut-down cooling system (321)

The primary function of the shut-down cooling system (321) is to cool the reactor to cold shutdown and to supply water to the spray system of the reactor pressure vessel lid during cooling. Its functions during normal operation include water supply to the reactor water clean-up system; some of the flow enters the reactor through the scram system (354) as crud removal flow. The rest of the water enters the feed water system (312). During refuelling, system 321 and the pool water system (324) together take care of cooling of the fuel pools, the reactor pool and storage pools for reactor tank internals.

System 321 forms a closed loop with the reactor pressure vessel. The circulation flow is normally maintained by one of two parallel pumps. After the pumps, there are two parallel heat exchangers, which are not in use during normal operation. The system receives its water from two parallel suction lines, which are connected to the reactor pressure vessel approximately 3 meters above the core level (more than one metre below the normal water surface).

The two parallel pumps of system 321 are identical, completely closed centrifugal pumps with a wet motor. The motor cooler is connected to the diesel-backed normal operation secondary cooling system (723). If necessary, the cooling can be switched manually to the shut-down secondary cooling system (721). The pumps are supplied by the diesel-backed network, and they are located in the reactor building at level –2 m.

For cooling the reactor and keeping it in a cold state, the pumps are used to circulate water through heat exchangers. The flow is adjusted manually with a control valve for maintaining a specific cooling speed or keeping the reactor temperature stable. The heat exchangers are cooled with system 721.

When the reactor is being cooled with system 321, both circuits of system 721 are needed for taking the plant to the cold shutdown state within a certain time.

Containment spray system (322)

The containment spray system (322) reduces the containment pressure in case of primary circuit leak inside the containment by condensing the steam in the drywell and wetwell and by cooling the condensation pool. Furthermore, it washes fission products from the containment gas space in case of an accident inside the containment and cools the condensation pool during reactor isolation or shutdown if steam is relieved from the reactor to the condensation pool through system 314. In addition, it provides cooling for the reactor water level measurement reference lines of the process measurements system (541).

During normal operation, system 322 is used for cooling the condensation pool, and also during reactor shutdown if steam is relieved from the reactor to the condensation pool through system 314.

The system comprises four nearly identical parallel circuits, 322-1, 322-2, 322-3 and 322-4. Each circuit consists of a pump, a heat exchanger and a half-circle shaped spray pipe in the containment drywell and a quarter-circle shaped spray pipe in the containment wetwell. Each circuit is located in a separate space, a so-called H bay.

The corresponding circuits of systems 322 and 323 that belong to the same electrical sub-division share an A300 suction pipe from the condensation pool. The shared suction pipe belongs to system 323. Each of these lines has its own suction filter in the lower drywell, and the pipes are led through the condensation pool via separate penetrations. After the pump and the heat exchanger, the lines branch, and depending on the situation the system can spray the containment drywell or the wetwell gas space, or cool the condensation pool by circulating water back to the condensation pool via a bypass line. Heat is transferred from the heat exchangers to the sea water with systems 721 and 712. The suction filters of the system can be cleaned by backflushing with pressurized nitrogen.

In case the containment has to be filled with water, fire fighting water from system 861 is injected into the containment through the containment water filling system (365) and containment spray system (322). As a provision for a complete loss of power, there are mobile diesel generators that can be connected to the power supply interface in the outer wall of the reactor building. The power of these generators allows opening valves in system 322 for injecting the fire fighting water inside the containment.

Reactor core spray system (323)

The reactor core spray system (323) protects the reactor core from overheating in case of a primary circuit pipe rupture inside the containment together with the auxiliary feed water system (327) and the relief system (314). It has no functions during the normal plant operation.

System 323 comprises four separate and independent trains. Each train includes a pump which sucks water from the condensation pool (316) in the reactor containment. The system shares the portion of the suction lines in the condensation pool with system 322. The suction lines are equipped with filters in the immediate vicinity of the condensation pool wall. At a low reactor pressure, the pumping capacity per circuit is over 115 kg/s.

The pumps of system 323 are in separate H bays, and they are supplied through different busbars by the diesel-backed 660 V network (662). The penetrations of system 323 in the reactor pressure vessel are located above the top edge of the reactor core.

Pool water system (324)

The primary function of the pool water system (324) is to remove the residual power released by the fuel in the fuel pools. In addition, the system cleans the pool water by filtering out particles and dissolved impurities. System 324 is used during refuelling outages for draining and filling the reactor pool.

The system comprises a level adjustment tank, two parallel-connected pumps, a precoat filter and two parallel heat exchangers. The level adjustment tank is connected through overflow chutes to all pools in systems 243 and 244. The pipes from the overflow chutes are connected to a common header pipe, which ends into a screen.

The screen is located in the level adjustment tank. The tank has a vent line, which is connected to the transfer cask pool above the water level. The level adjustment tank is connected via a pipeline to both pumps of the system as well as systems 321 and 352. The additional water required by the system is fed from system 733 through the level adjustment tank.

Both plate type heat exchangers are in use at the same time. The secondary side of the heat exchangers is connected to the diesel-backed normal operation secondary cooling system (723).

The system includes an additional circuit. The additional circuit comprises a heat exchanger and two centrifugal pumps. This equipment is used during annual outages when the reactor pressure vessel lid is removed and the tanks are filled with water. When the additional circuit is taken into operation, the shut-down cooling system 321 can be stopped after a sufficient time has passed from the reactor shutdown. The heat exchanger of the additional circuit is cooled by one of the two circuits of the shut-down secondary cooling system (721).

Auxiliary feed water system (327)

Auxiliary feed water system (327) maintains the amount of water in the reactor pressure vessel when the feed water system (312) is not in operation but the operating status is otherwise normal.

During accident situations, the system maintains the amount of water in the reactor pressure vessel until system 323 takes over. In addition, system 327 cools the reactor core together with system 323 in case of RCS pipe ruptures.

System 327 has four separate and independent circuits. Two of the circuits are connected to the feed water line inside the reactor containment, and the two other to the circuits of the core spray system 323 inside the reactor containment. Each circuit of system 327 includes a piston type auxiliary feed water pump with the capacity of 22.5 kg/s. The electricity to the pump motors is supplied by the diesel-backed 660 V busbar of system 662.

The suction of the pumps is connected with separate pipelines to the four demineralised water tanks. The tanks have 400 m^3 of water per circuit. System 327 connects to the tanks of 733 at the bottom so as to ensure that 225 m^3 of the water in the tank is dedicated to be used by the corresponding 327 circuit only.

Containment filtered venting system (362)

The containment filtered venting system (362) is designed to primarily operate in case of severe reactor accidents. The system allows controlled steam and gas release from the containment to the plant environment in case pressure increase may pose a threat to the integrity of the containment. The system must still be able to limit the levels of aerosol activity released to the environment with the emission so that no significant long-term soil contamination is possible. Also, the system must be able to effectively filter out gaseous elemental iodine. The system is presented in Section C.6.3.3 in more detail.

Shut-down service water system (712)

During operation, the shut-down service water system (712) provides the necessary cooling water flow for the heat exchangers of system 721. The safety-related functions of system 712 are to provide the necessary cooling water flow for the heat exchangers of the secondary cooling system 721 and the diesel motor coolers of system 652.

System 712 is an open sea water based cooling system, and it comprises four identical and independent subsystems, or circuits. Both auxiliary buildings have two circuits at level +3.5 m, which include a diesel-backed submersible pump. Each of the four circuits of system 712 receives the sea water coming from the 112 channels purified by the screening system 711 and discharges it forward to the 112 outlet tunnel. Each of the four circuits cools one heat exchanger of system 721 and one diesel motor cooler of system 652.

Each circuit includes a filter before the coolers. The filter can be rinsed with the system's own water flow as initiated by a filter pressure difference measurement or controlled by a time sequence as necessary. The rinsing water is conducted to the discharge pipe of the same circuit after the heat exchangers.

Diesel-backed normal operation service water system (713)

System 713 is an open sea water cooling system, and it provides the necessary cooling water flow for the sea water heat exchangers of system 723 and the turbine building ventilation coolers. In addition, the system keeps two of the circuits of system 712 filled with water when these are not in operation.

System 713 has a low-pressure and a high-pressure circuit. The low-pressure circuit has four parallel pumps, three of which are normally running. During wintertime, when the sea water temperature is low enough, the system can also run with only two pumps. In all conditions, two running low-pressure circuit pumps are enough to cool all safety-critical equipment. The two parallel pressure increase pumps are connected in series with the low-pressure pumps. One of the high-pressure circuit pumps is normally running while the other one is kept as a backup. All pumps of the system are located at level +3.5 m in one of the two auxiliary buildings. Water intake to the pumps is from the cooling water channel (112). The low-pressure circuit is connected to the heat exchangers of system 723 and two of the circuits of system 712. The high-pressure circuit is connected to the turbine building ventilation coolers.

Non-diesel-backed normal operation service water system (714)

The system is used for cooling the large pump motors, oil coolers and room coolers in the turbine plant. It also cools the reactor water clean-up system (331) in the nuclear island. Additionally, the system keeps two of the circuits of system 712 filled with water when these are not in operation.

Normally, three out of four low-pressure pumps are in operation, and they take the water from the intake water channel (112) at a flow rate of 600–650 kg/s. Only one of the two high-pressure pumps is running, and it takes its water from the low-pressure side at a flow rate of approx. 150 kg/s. The pumps are located at level +3.5 m in the other auxiliary building than those of system 713.

Shut-down secondary cooling system (721)

The shut-down secondary cooling system (721) provides cooling water to the heat exchangers of systems 321 and 322 to ensure the operation of these systems. Furthermore, system 721 provides cooling water to the air coolers of system 741, the pump motor air coolers of systems 322, 323 and 327 and the heat exchangers of system 327. When system 723 is not available, system 721 can also provide cooling water to the heat exchangers of system 324 and pump motors of system 321.

System 721 is a closed cooling system, which comprises two nearly identical and independent parallel circuits. Each circuit includes two diesel-backed pumps with a 50% nominal yield, and provides cooling water to one heat exchanger in system 321, two heat exchangers in system 322 and one air cooler in system 741. Of the pumps and heat exchangers of the system, two are located in one of the auxiliary buildings and two in the other one at level +3.5 m.

Both 721 circuits have two air coolers, which are located in different H bays. Each air cooler and two fans in series are used for cooling the pump motors of systems 322, 323 and 327 in one H bay. With each air cooler, there is a heat exchanger of system 327 in series. One of the circuits can also cool the pump motors of system 321 and the heat exchangers of system 324. Normally this equipment is cooled by system 723. In addition, both circuits include two heat exchangers, which are cooled by system 712.

If system 321 must be stopped during a refuelling outage, one of the circuits can be connected to cool the heat exchanger of the additional circuit of system 324.

Diesel-backed normal operation secondary cooling system (723)

System 723 is a closed cooling system, and it acts as a secondary cooling circuit between the service water system (713) and the equipment requiring cooling in the reactor, waste, auxiliary and turbine buildings. The system does not have its own nuclear safety-related functions, but it is used for cooling several safety-classified systems, equipment or rooms.

System 723 has two main circuits, whose water is circulated with four parallel pumps located in one of the auxiliary buildings at level +3.5 m. The circuits share four sea water heat exchangers also located in the same auxiliary building. Furthermore, the system includes sub-circuits, which are supplied either by the two main circuits or directly by the main line between the reactor building and auxiliary building. The pumps of the system are supplied by the diesel-backed busbar 662.

The cooled equipment in the upper and lower drywell of the containment is connected to different main circuits. The pumps of system 321 and the heat exchangers of system 324 can also be cooled with one of the circuits of system 721 through normally closed valves. The necessary valve operations must be performed manually.

The capacity of each pump is 33% of the designed cooling water flow. The heat exchangers are rated for 25% of the total required cooling capacity. The system is designed so as to achieve the required cooling capacity with three pumps and four heat exchangers, provided the sea water temperature remains below 18°C. In this case the water temperature at heat exchanger discharge is 25°C.

Fire fighting water system (861)

System 861 functions as the fire fighting water source for the water-based fire fighting systems in the power plant, and its purpose is to ensure the availability of fire fighting water at all fire fighting events for fixed water-based fire fighting equipment and operative fire fighting in the power plant area. The water tanks of the system also act as storage tanks for the tap water supplied to the units (731 and 761).

The plant area has two fire fighting water pump houses. Both pump rooms include an electric fire water pump and two diesel-operated pumps. The electric water pumps can be supplied by either plant unit, and they are started if the pressure in the piping becomes low. The diesel-operated pumps are started by batteries if the pressure in the piping becomes low. The water tanks have 2,000 m^3 + 2,000 m^3 of fire fighting water and 1,000 m^3 of tap water. Additionally, the plant area includes a 500 m^3 reserve water tank.

Two distribution lines are led from the fire fighting pumps to the plant unit piping loop. In case one line fails, it can be isolated with valves, while the other line ensures fire fighting water supply.

In case the containment has to be filled with water, systems 365 and 322 can be used to pump fire fighting water into the containment.

Fire fighting water can be supplied to the fuel pools with fire fighting hoses if normal water supply is not available. During outages, when the reactor pressure vessel lid has been removed, fire fighting water may also be supplied to the reactor. Fire fighting hoses can also be used for supplying water to the demineralised water (733) tanks.

The fire fighting water system can be used for pumping water to the plant units directly from Korvensuo raw water basin. The capacity of the raw water basin is above 130,000 m^3.

C.1.2 Significant differences between units

Main differences between unit OL1 and OL2 are the following.

- Process systems of the spent fuel interim storage (KPA storage) have a dependency on OL1: alarms from KPA storage are transferred to the main control room of OL1; in case of loss of off-site power electricity is provided for KPA-storage from diesel generator of OL1.
- A system to warm cooling water of both units OL1 and OL2 recirculates part of the cooling water from OL2 outlet back into the intake channels of OL1 and OL2.
- Gas turbine can be operated by both unit OL1 and OL2. However, if operator actions are needed locally at the gas turbine control room, the primary duty for this is set for OL2 staff.

Considering safety systems units OL1 and OL2 are identical.

C.1.3 Use of PSA as part of the safety assessment

The level 1 PSA for OL1 and OL2 is a full scope analysis including power operation, annual outages as well as planned shutdown and start-up of the plant. Due to the similarity of the units, level 1 PSA modelling is common to OL1 and OL2. The initiating events considered include internal initiating events such as component failures and human errors, internal hazards such as flooding and fires, and external hazards such as extreme weather phenomena, seismic phenomena and marine oil spills.

The dominating external hazard is the blocking of the sea water inlets due to a marine oil spill, which is estimated to correspond to about half of the risk contribution caused by weather related phenomena, and around 1/8 of the total CDF. The second most important weather related event is the blocking of the sea water inlets caused by either clams or algae, corresponding together to about third of the weather related risk contribution. The other weather phenomena included in the level 1 PSA model are lightning, high sea water temperatures, blocking of the sea water outlet due to clams, snow storms, low air temperatures, frost, and blocking of sea water inlets due to frazil ice. Also many other weather phenomena have been investigated but the risk significance has been estimated to be so low, or to be covered by other events, that they have been excluded from the actual level 1 PSA model. Seismic events have been analysed to contribute only 1% of the total CDF.

The high risk contribution of marine oil spills is partly explained by the conservative approach used in the analysis. The marine oil spills were introduced to the level 1 PSA model for the first time in April 2011 and the present level of analysis is quite conservative due to lack of detailed knowledge concerning e.g. the drifting of possible oil slicks in the nearby sea areas. A more detailed analysis is expected to reduce the risk contribution.

The accident progression analysis of level 2 PSA builds on the information received from level 1 PSA analysis. Level 2 analysis includes all level 1 core damage sequences, i.e. the analysis includes power operation, plant start-ups and shutdowns as well as refuelling outages. Level 2 analyses do not include events related to spent fuel storage. Due to the similarity of the units, level 2 modelling is common to OL1 and OL2.

C.2 Earthquakes

C.2.1 Design basis

C.2.1.1 Earthquake against which the plant is designed

Characteristics of the design basis earthquake (DBE)

Section A.2 describes the basis of DBE criteria. When the Olkiluoto NPP units 1 and 2 were built there were no regulatory requirements on seismic design, and earthquake loads were not considered separately in the design. The new systems, structures and components (SSC) critical to safety constructed after 1997 are designed and qualified to withstand the DBE. The DBE response spectrum is described in Section A.2, in Figure A-2. The corresponding horizontal PGA is 0.10 g.

Latest seismic PSA has been done 2008 as an update for original seismic PSA from 1997. Horizontal PGA value 0.082 g is estimated to take place on medium frequency of 10^{-5}/a, which is following the DBE frequency according to Guide YVL 2.6.

The PGA-value of 0.1 g has been applied in design of the spent fuel storage pools. Static method has been used in the original, first phase, pool design. Currently for the modification for extended capacity of the spent fuel storage, the seismic design for both pool structures and storage building structures has been done using dynamic analyses according to YVL 2.6. Seismic PSA for the interim storage for spent fuel has been started in fall 2011 and to be performed during year 2012 in order to take into account the modifications to enlarge pool capacity, which is currently at progress (see Section C.1.1.1).

Methodology used to evaluate the design basis earthquake

Section A.2 describes how DBE is based on statistical analysis of historical data with adjacent geological and tectonic information. Based on seismic PSA 2008 the horizontal PGA value 0.10 g is expected to take place at Olkiluoto NPP with median frequency less than $8 \cdot 10^{-6}$/a which is close from the safe side to the required frequency level of current design criterion of 10^{-5}/a.

Conclusions on the adequacy of the design basis for the earthquake

Due to the low seismicity of the Olkiluoto area, the fact that originally plant has not been designed against earthquakes does not post a major risk on the seismic safety of the plant. The seismic CDF is $1.7 \cdot 10^{-7}$/a which presents about 1% share of total CDF ($1.33 \cdot 10^{-5}$/a) indicate that there is no instant need for updating probability studies concerning DBE specification.

Ongoing efforts to develop and verify seismic design of NPPs in Finland are described in Section A.2. Final conclusions in detail level will be achieved later.

C.2.1.2 Provisions to protect the plant against the design basis earthquake

The high confidence of low probability of failure (HCLFP), 95% confidence of a less than 5% probability of failure, has been estimated for OL1 and OL2 to be about 0.12 g.

A total of approximately 800 components were placed on the seismic equipment list based on plant information and systems walkdown and guidance from IAEA, USNRC, and EPRI documents in identifying seismic initiators, plant safety functions, and associated plant equipment critical to seismic safety.

Most of the components including all buildings on the seismic equipment list were screened out based on the analysed HCLFP values which are above 0.3 g. Further on response analysis using models updated/refined starting from the 1997 models and 30 earthquake ground motions were generated to match the updated site hazard. Component fragility evaluations were updated as well.

Main operating contingencies in case of damage that could be caused by an earthquake and could threaten achieving safe shutdown state are studied in seismic PSA. The seismic event tree (SET) is used to delineate the potential successes and failures that could occur due to a seismic event, based on the fragility data of listed SSCs. Sensitivity studies were performed to identify potential areas to consider for the reduction of seismic risk.

Plant modifications that would most directly address the dominant seismic core damage sequences concern cabinets housing relays associated with the ATWS and isolation signals. By eliminating cabinet-to-cabinet impacts, the CDF contribution for seismic events can be lowered from $1.7 \cdot 10^{-7}$/a to less than $2 \cdot 10^{-8}$/a.

Protection against indirect effects of the earthquake to plant shutdown safety is included in seismic PSA of 2008. Potential flooding sources are large tanks. It was acknowledged that certain HCLPF (High Confidence of Low Probability of Failure) values would need to be shown higher values from about 0.06 g to 0.15 g, which is currently proven as the median seismic capacity. This can be done by corresponding structural analyses and if needed with modification of supporting structures.

Protection against loss of offsite power seismic capacity is driven by relay chatter, which median capacity is 0.127 g and HCLPF 0.05 g require also more efforts to prove out higher HCLPF capacity.

The road leading to the plant unit is not vulnerable to earthquake damage. The road has low, sturdy girder and plate bridges with short span lengths, which may be assumed to tolerate stress due to earthquakes well. In hypothetical damage situations, the connection may be assumed to be reopened to light traffic within one day, and to heavy traffic within three days after the earthquake. More details are given in Section C.6.1.

Fires or explosions are not identified as concern for OL1 and OL2 during plant walkdowns. Seismic capacity of diesel driven pumps at firewater building is high, HCLPF is 0.74 g.

C.2.1.3 Compliance of the plant with its current licensing basis

Due to the low seismicity of the site, no processes for ensuring seismic safety critical SSCs for achieving safe shutdown after earthquake, or limiting indirect effects are specified especially for earthquakes. Common maintenance, testing and monitoring of SSCs is considered to include also preparedness against seismic events.

Following transportable equipment are available: SAM generators (29 kVA), motor pumps (1600 l/min / 10 bar and 1900 l/min / 8 bar), generators (4.5 kVA and 7.5 kVA), and a fire engine with fire-fighting pump and generator. The equipment is used for severe accident mitigation (SAM generators and motor pumps) and for electrifying the reserve command centre (generators).

Earthquake was not demanded as a design basis for OL1 and OL2. Seismic requirements are taken into account in modifications and building of new systems and structures since 1997. Living seismic PSA is used to verify appropriate safety level for safe shut down after earthquake.

C.2.2 Evaluation of safety margins

C.2.2.1 Range of earthquake leading to severe fuel damage

Based on Seismic PSA the core damage risk due to earthquakes is estimated as $1.7 \cdot 10^{-7}$/a. The median PGA capacity of OL1 and OL2 is about 0.35 g. The HCLPF is estimated to be about 0.12 g.

The seismic event sequences associated with spurious ATWS and isolation signals are the most significant contributors to seismic risk, modification of the cabinets to reduce relay chatter would reduce the core damage risk by a factor of 10, to $1.7 \cdot 10^{-7}$/a. This modification proposal has been done to improve seismic capacity of OL1 and OL2.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a more detailed evaluation of the seismic stability of spent fuel pools and the fire fighting systems against earthquakes beyond the current DBE level at the Olkiluoto NPP site.

C.2.2.2 Range of earthquake leading to loss of containment integrity

Containment's HCLPF seismic capacity is above 0.3 g; inner wall 0.33 g and outer wall 0.43 g.

C.2.2.3 Earthquake exceeding the design basis earthquake for the plant and consequent flooding exceeding design basis flood

External floods due to an earthquake are not plausible in the Olkiluoto area. There are no nearby rivers or dams, and the probability of a tsunami in the Gulf of Finland is negligible.

C.2.2.4 Measures which can be envisaged to increase robustness of the plant against earthquakes

According to the seismic PSA of 2008, the share of the seismic core damage risk is 1% of the total risk of the plant. Licensee's strategy in decision making is applied to increase seismic capacity, when SSCs with seismic classification are replaced with the new ones.

Modification proposal has been done for the anchoring improvement of relay cabinets to prevent relay chatter (Note: in case of actuation, resetting is possible). Work is ongoing.

Steal racks for batteries which supports are not yet improved (only relevant for OL2, 672) will be modified when these batteries are replaced with new ones. At OL1 all supports of safety significant batteries in systems 664, 665, 672, 673, 678 and 679 have been changed to steel racks in order to improve seismic capacity.

Above mentioned modifications will decrease seismic CDF from $1.7 \cdot 10^{-7}$/a to less than $2 \cdot 10^{-8}$/a.

Already in ongoing modification works, where the seismic design is done according Guide YVL 2.6, are based on the strategy described above. Further improvement to seismic capacity has been done, especially for eliminating relay chatter: replacement of low voltage switchgears (systems 662, 664), one train in OL2 has been installed in 2011.

Planned work in future are: 2012 OL1 two trains; 2013 OL2 two train; 2014 OL1 two remaining trains; 2015 OL2 one remaining train.

To respond STUK's requirements after Fukushima accident, Licensee is studying seismic fragilities of pool structures of fuel storages in OL1 and OL2 during year 2012. Seismic capacity of fire water system will be completed to cover also the fragilities of piping and estimation of corresponding consequences also during year 2012.

C.3 Flooding

C.3.1 Design basis

C.3.1.1 Flooding against which the plant is designed

The Olkiluoto 1 and 2 NPP units have been designed against flooding up to the level +3.5 m in the N60 coordinate system. As the mean sea level is about –0.2 m in the N60 system, the units are protected against sea level rise to 3.7 m above mean water level.

The rate of water level rising has not been postulated and it is not considered important regarding flood protection at Olkiluoto. The rate of seawater rise can be up to a about 10 cm/h. Under special conditions, such as tornados or local air pressure fonts, the rate can be much higher.

The possible cause of flooding at the Olkiluoto site is the rise of seawater level. Due to the geography and topography of the site and its surroundings river flooding, dam breaks are not relevant hazards at the site.

The Baltic Sea is an enclosed sea with moderate variations of seawater level. Tidal effects are insignificant in the Baltic Sea. As the Baltic Sea is shallow (mean depth about 55 m) large tsunamis exceeding normal wave heights are not considered possible.

The variations of the sea water level in Olkiluoto are determined by the total quantity of water in the Baltic Sea, air pressure, wind and seiche (standing waves across the Baltic basin). In the long term (decades) the land uplifting and the possible ocean level rise due to global warming also affect the seawater level.

The total quantity of water in the Baltic is determined by the long term variations in weather conditions in the North Sea affecting the water flow though the Danish Straits.

The seawater flood height has been determined on the basis of available statistic using generalized extreme value distributions with conservative shape. Long-tern time series from near by mareographs has been used. In addition, the available historical data from the Baltic region has been reviewed.

Extreme value distributions for high and low seawater level are shown in Figure C-3. The use of an exponential extreme value distribution can be considered a conservative choice.

The extreme value distribution constitutes an extrapolation to return times several decades longer than the observation time. The low-frequency end of the distribution involves very large uncertainties. On the other hand, it is questionable if the highest seawater levels in the graphs are physically possible in the Olkiluoto region. According to the expert opinion of the Finnish Institute of Meteorology, it is higly improbable that the design level of +3.5 m would be exceeded in Olkiluoto. The frequency of exceeding seawater level + 3.5 m (N60) is estimated to be less than 10^{-9}/a (Figure C-3).

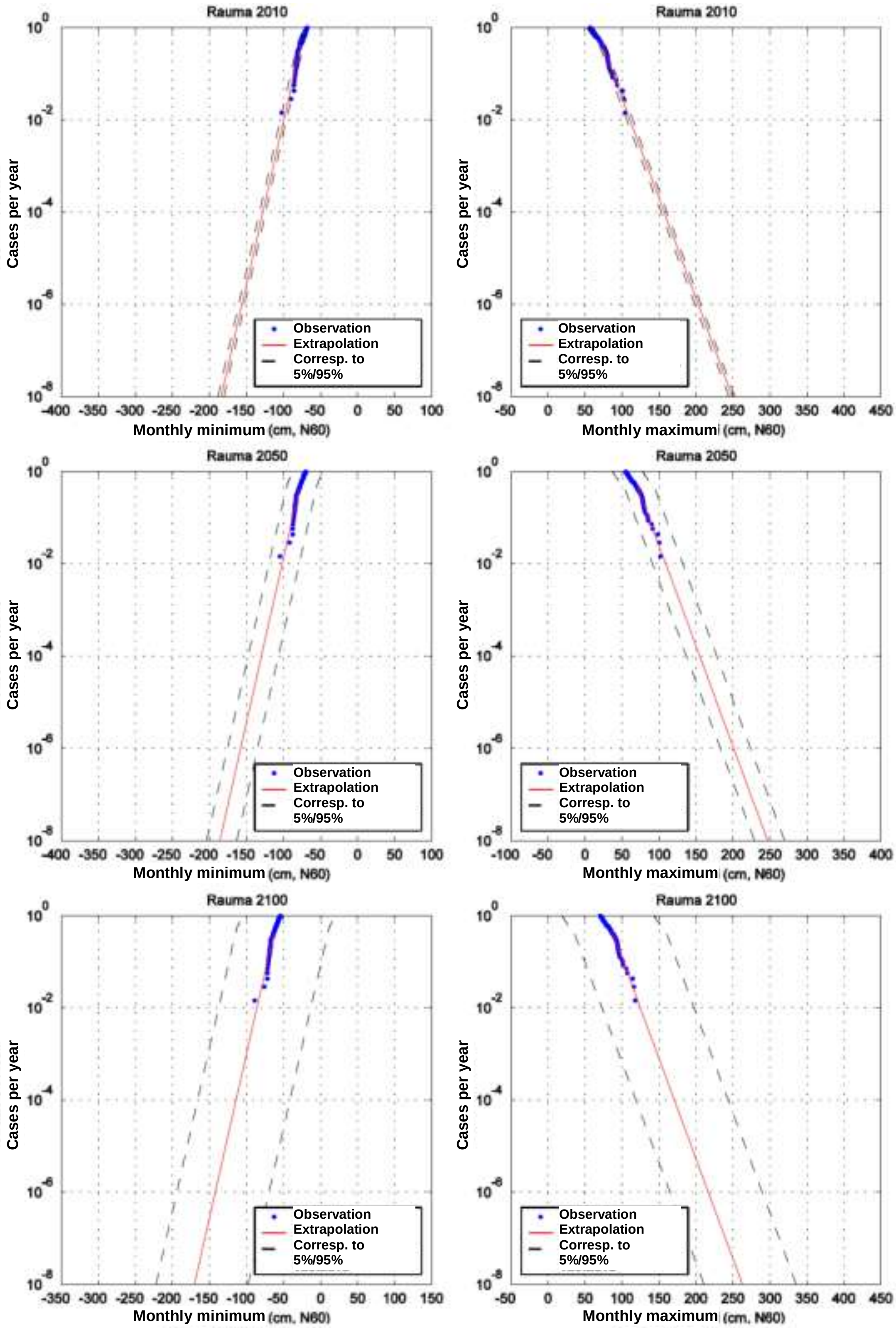


Figure C-3. Probability distributions for high and low seawater level extremes in the Rauma measuring station close to Olkiluoto with 5/95% uncertainty limits.

<u>Conclusions on the adequacy of protection against external flooding</u>

Based on the current understanding of meteorological and marine phenomena in the Baltic Sea region, the design basis +3.5 m (N60) of the OL1 and OL2 NPP units can be considered adequate.

The design basis +1.2 m (N60) of the KPA storage cannot be considered sufficient as such. According to the studies carried so far, the KPA storage can in practice withstand much higher seawater levels, as explained in the following sections.

C.3.1.2 Provisions to protect the plant against the design basis flood

The control rods and their drives are located inside the water-tight containment. The boron pumps are located at level +25.0 m (N60 system). The solenoid valves required for a hydraulic scram and their junction boxes are located at level –2.0 m. If the junction boxes of the solenoid valves are submerged, the solenoid valves open, which results in a scram. Flooding cannot endanger the automatic scram; instead, the water triggers the scram, shutting down the reactor. The boron pumps and control rod drives are supplied from the 662 busbars. They can be locally operated from the switchgears at levels +19.5 m (control rod drives) and +25.0 m (boron pumps).

Reactor pressure is controlled by means of the pressure relief system presented in Section C.1.1.2. The system may be used to transfer heat from the reactor into the containment condensation pool, reducing the water inventory in the reactor. The system is located inside the watertight containment. Relief valves prevent the over-pressurisation of the reactor. Reactor pressure is lowered by means of motor-operated pressure regulator valves. The valves are supplied from the relay rooms, where they are also controlled from. Electrical controls are required to lower reactor pressure.

Water may be supplied into the reactor by using feed water pumps, auxiliary feed water pumps, or the reactor core spray system, as described in Section C.1.1.2. The feed water pumps are located at level +3.5 m. Their electricity is supplied by the 642 busbar, the switchgears of which are located at level +3.5 m. The controls are implemented by the process control system, located at level +10.5 m. The pumps are cooled by using the non-diesel backed normal operation service water system. The auxiliary feed water pumps are located at level–2.0 m in H bays that are internally waterproof at least to a level of +10.0 m. The reactor core spray system pumps are located in the same rooms. Both are supplied by the 662 busbars, the switchgears of which are located at level +12.25 m; the necessary local controls may also be implemented here. The pumps are cooled using the shutdown secondary cooling system.

The condensation pool is cooled using the containment vessel spray system, from where heat is transferred to the shutdown secondary cooling system. The pumps of these systems are located at level –2.0m in H bays that are internally waterproof at least to the level of +10.0 m. The pumps are supplied by the 662 busbars, the switchgears of which are located at level +12.25 m; the necessary local controls may also be implemented here. The pumps are cooled using the shutdown secondary cooling system.

Residual heat from the reactor may be transferred to the shutdown secondary cooling system using the shutdown cooling system. The pumps of the system are located at level

+0.7 m. The reactor building is waterproof to the level of +3.5 m. The pumps are powered by the system 662 busbars. Local controls may be performed from the switchgears at level +12.25 m. The pumps are cooled using the diesel-backed normal operation secondary cooling system or the shutdown secondary cooling system.

In the extremely improbable event of a severe accident, the cooling of the fuel is ensured by flooding the containment. The lower drywell is flooded by routing water from the condensation pool into the lower drywell, until the water levels in the condensation pool and drywell are equalised. The required valve functions are powered by the SAM busbars located at level +19.5 m. The valves are located in rooms that are watertight to the level of +10.0 m.

The fuel pools are cooled using the pool water system. Heat is transferred into the diesel-backed normal operation secondary cooling system. Heat may also be transferred into the shut-down secondary cooling system. The pumps required for heat transfer into the diesel backed normal operation secondary cooling system are located at level +19.5 m. Their electricity is supplied by the 662 busbars, the switchgears of which are located at level +12.25 m. The pumps required for heat transfer into the shut-down secondary cooling system are located at level +9.0 m. Their electricity is supplied by the 662 busbars, the switchgears of which are located at level +25.0 m.

The emergency diesel generators are located at level +3.5 m. They are water-cooled; cooling is managed by using the shut-down service water system. Local controls may be performed from within the same fire compartment. The diesel oil day tanks are located in a separate fire compartment next to the emergency diesel room at level +6.5 m. The day tank has oil sufficient for 8 hours of continuous operation. Outside, there is a plant unit specific diesel oil storage tank, with oil sufficient for 1 week of continuous operation using all four diesel engines. From the storage tanks, oil is transferred to the day tanks using fuel transfer pumps, located outside at level +4.2 m.

The pumps for the diesel-backed normal operation secondary cooling system, the shut-down secondary cooling system and the non-dieselbacked normal operation service water system, diesel-backed normal operation service water system and shut-down service water systems are located at level +3.5 m. From the secondary cooling systems, heat is transferred into the corresponding service water system. The pumps are located on pedestals that are 30 cm high. The service water pumps are installed vertically, and the secondary cooling circuit pumps are horizontal. The pumps are estimated to be in service if the water level does not exceed +4.0 m. The non-diesel-backed pumps are supplied by the 643 busbars, and the diesel-backed pumps, including those of the shut-down cooling systems, are supplied by the 662 busbars. The switchgears of the power distribution systems are located at level +12.25 m.

The non-diesel-backed power distribution systems are fed from switchgears which are located at level +3.5 m.

The diesel-backed power distribution systems are fed from switchgears which are located at level +12.25 m. There may be sub-distribution systems at lower levels, but in case of short circuits, fuses will isolate the faulty group.

The battery-backed power distribution systems are fed from switchgears which are located at level +10.5 m. There may be sub-distribution systems at lower levels, but in case of short circuits, fuses will isolate the faulty group.

The SAM power distribution system is a battery-backed power distribution system for severe accidents. Normally, voltage is supplied from the battery-backed 664 busbars. If this voltage is disconnected, a portable diesel generator may be connected to the SAM busbar. The connection point for the transportable diesel generator is attached to the reactor building wall at level +4.8 m. There are separate batteries and busbars for the auxiliary voltage required by the containment monitoring system and the voltage required by the off-gas stack radiation monitoring at level +19.5 m.

Main safety-related controls are primarily done from the main control room. The controls pass through the relay rooms next to the control room. They are located at level +3.5 m.

<u>Plant response</u>

The theoretical mean sea level in 2011 was –0.20 m.

Plant unit response at different sea levels (N60 system):

- +1.3 m (+2.0 m in the outlet channel): The sea level probe in the auxiliary system building exhaust channel issues an alarm to the control room.
- +1.6 m (+2.3 m in the outlet channel): The turbine condenser's seawater pumps trip and cause a plant disturbance. Pressure in the condenser increases, which leads to a reactor scram. The reactor is shut down, and the mode is changed to hot or cold reactor shutdown. In hot reactor shutdown the temperature of the reactor is over 100°C and the pressure corresponds to the saturation pressure of the steam at the specific temperature.
- +3.5 m Design basis for plant safety systems and buildings, (see Section C.3.1.1).

If the flood exceeds +3.5 m, water may enter the floor level in all buildings. The buildings are divided into fire compartments, however, and doors slow down the spreading of water inside the plant units.

Water may rise freely in the seawater system pump rooms and service water pump rooms, and the flood would first spread into these rooms and the facilities below them. Underground rooms, with the exception of the reactor building and the waste building, will eventually be flooded as the floodgates give way. Closed outer doors and fire doors effectively prevent the spreading of flood water. The doors can be expected to rupture only when the flood reaches a level of +4.5 m. After the pump rooms, the flood can be expected to spread into the diesel rooms. If the seawater level has risen to above +3.5 m, the fire fighting water pump rooms may also be among the first rooms to become flooded. The other interior rooms listed below are behind several doors, which will effectively slow down the spreading of flood water.

The automatic control of important safety functions is lost. Local controls may be performed from the switchgears.

Flooding in the 6.6 kV switchgear building will lead to a loss of the subdivisions of the auxiliary power distribution system affected by the flood. One switchgear room contains switchgears of two subdivisions. For these subdivisions, the important safety related functions rely on diesel generators. The feed water pumps stop, which results in a scram. The functions important for safety are supplied from the diesel-backed power distribution system. If the flood spreads to both switchgear rooms, all safety functions rely on diesel generators. As mentioned above, it can be expected that the diesel generator rooms will also have flooded at this stage.

Flooding in the auxiliary cooling system pump rooms will inhibit the cooling of the condensation pool, water cooled pumps and diesel generators if the water level rises to +4.00 m.

If the flood spreads into a diesel generator room and the sea level rises to +3.60 m, the diesel generator in that room cannot be used anymore. If the subdivision of the auxiliary power distribution system is available, there is no consequence for the flood.

All power distribution systems are lost, except for the battery-backed power distribution systems. This affects all safety related functions, except the control of reactor criticality, including severe accident management.

<u>KPA Storage</u>

The most important functions of the KPA storage for achieving and maintaining a safe state are removing the flooded water from the storage building into the sea, and residual heat removal from the spent fuel by using the dedicated system or supplying additional water.

Flood water removal is achieved by using the submersible pumps (2×100%) that pump the accumulated water from the floor drains back into the sea. In a situation where the flood water cannot be removed from the storage building, a hydrostatic pressure of over 1 bar may be formed on the lower structures of the storage building. This pressure may damage the structures in the storage and create faults in the residual heat removal chain. However, it is more likely that the structures leak from the penetrations and seams to a degree where a large hydrostatic pressure can only be formed very locally.

The submersible pumps do not lose availability when coming into contact with flood water. The submersible pumps may be damaged due to faults related to electricity supply. The submersible pumps are supplied from the 380/220V busbar that is attached to the 660 V busbar via a 6.6 kV/400 V transformer. The 660 V busbar may be supplied from the outside area 6.6 kV switchgear, the 6.6 kV switchgear of OL1, and 660 V diesel busbar of OL1. The components critical for electricity supply are installed at level +3.5 m in the switchgear room of the KPA storage.

As regards the submersible pumps, the most important criteria for removing flood water is the rated flow, which is 4.5 kg/s for the ground submersible pumps. If the flood flow is larger than the rated flow of the ground submersible pumps, the water surface is able to rise inside the KPA storage.

It has been analysed that it takes over two days for the temperature of the water in the pools to rise to the boiling point. Adequate radiation shielding is provided until almost 11 days. As being conservative estimates, the analyses assume e.g. that the pool gates are closed, the thermal power of one pool is 1 MW, and the maximum burn-up is 45 MW/kgU. At present, there are three storage pools, with a total thermal power of approx. 1.3 MW.

According to analyses, the amount of additional water required to compensate the boil-off of water is 33.4 m^3/d. Additional water into the storage pools may be supplied from the demineralised water distribution system or by means of temporary arrangements by using the fire fighting water system.

In a flood extending to level +3.5 m, the pumps of the fuel pool cooling system and service water system will be submerged. The secondary cooling system pumps remain above the flood water; however, the distance from the surface of the flood water only equals the height of the pump platform. Thus, residual heat removal does not work as intended, if the sea level rises to +3.5 m.

The temperature and surface level of the pools are monitored by means of measurements with displays in the process control room. An alarm is received in the process control room and a group alarm is received in the MCR of OL1 from excessive pool water temperature and too high or too low surface level.

If the residual heat transfer chain is lost, more water is required into the storage pools to compensate for boiling and vaporisation of the pool water. Additional water is supplied into the KPA pools via the demineralised water distribution system from the storage tanks of OL1. The maximum flow into the KPA pools is 8 kg/s.

Instructions have been prepared for filling the storage pools using the demineralised water distribution system. The critical components that could be damaged in a flood due to an electrical fault, thus causing the additional water supply between the storage tanks and the KPA storage tank to fail, are the demineralised water distribution system pumps. The pumps are located at OL1 at level +3.5 m.

Furthermore, 22 fire hydrants have been installed in the KPA storage, some of which are located in the stairwells near the storage pools. The fire hydrants include 20 to 30 metres of hose on reel, fire brigade connections, and the necessary piping. From the fire hydrant, water can be channeled directly using the hydrant or by using the fire brigade connection. Water to the fire hydrant is received from the fire fighting water system of OL1, and the maximum flow is approximately 3 kg/s. By using the fire brigade connection, an estimated 15 kg/s of water is available to cool the KPA pools. Loss of electricity in the KPA storage does not affect the functionality of the fire fighting water system.

Successful use of the fire brigade connection requires that the fire brigade's hoses be connected to the fire brigade connection, the hoses be routed from the hydrant into the KPA storage pool, and the fire brigade connection be opened. Routing water into the KPA storage pools via the fire hydrants requires that the radiation level near the storage pool is low enough to perform the work safely. In terms of operation of the fire fighting water system, the most important components are the fire fighting water pumps, which pump water through the distribution piping into the fire fighting water system. There are two fire fighting water pump houses, both with three centrifugal pumps (two diesel-powered and one electrically powered). Normally, one pump house supplies water as required to OL1 and OL2 (and to the KPA storage via OL1), and the other supplies water to OL3. The capacity for one pump house has been defined so that the failure of one pump does not endanger the operation of the pump house. The pumps which normally supply water to OL1 and OL2 are at level +3.50 m.

Provisions to prevent flood impact to the plant

The grade level of the site is about +3.3 m (N60) and the reactor buildings have been designed watertight and to withstand hydrostatic pressure up to the level +3.5 m. No special structures or systems, such as levees are required for flood protection. The integrity of other buildings has been ensured by sufficient dimensioning or by equipping the structures with floodgates that limit the pressure differences, which the walls are subject to, at an acceptable level.

According to the design basis, the rise of outside water level to level +3.5 m (N60) does not create a risk to the safe shutdown of the plant unit or the radiation protection of the environment. To implement this principle, the following detailed design requirements have been followed:

- The reactor building is designed to withstand the pressure caused by the external water level rising to level +3.5 m.
- The integrity of other structures important to safety during external flooding has been ensured either by sufficient dimensioning or by equipping the structures with floodgates that limit the pressure differences, which walls are subjected to, at an acceptable level.
- The operation of systems and equipment required for a safe plant shutdown are not affected by external flooding up to a level of +3.5 m. Radioactive substances stored in the waste building are not affected by such floods, either. This requirement has been fulfilled by either designing the protective structures to be waterproof, or by placing the important equipment or stored radioactive substances above the level of +3.5 m.
- The H safety bays housing the emergency cooling pumps have been dimensioned to tolerate an internal pipe break. The dimensioning basis for the H safety bay is that the structures must withstand the pressure created by a water column up to level +10.0 m. The H safety bays are waterproof up to level +10.0 m.
- The reactor building has been designed to withstand internal flooding up to level +3.5 m. Water cannot leak into the transmitter rooms under the condensation pool.

For the KPA storage, structural design has been performed assuming a sea level +1.2 m. The structures of the storage have been designed based on this water surface level to be durable enough to prevent water from entering the interior of the storage. All connections from the KPA storage to the sea are located above sea level +1.2 m.

The pool structures and water gates have been dimensioned for the hydrostatic pressure that exists when the pools are full of water (in a normal scenario, the water is at level +8.70 m; in an overfill scenario, at level +9.70 m). When studying one pool, the adjacent pools may be either empty or full.

The pool surfaces are covered with a stainless steel liner, which acts as a leak tight barrier and ensures that the concrete structures do not come into contact with water. Water isolation has been constructed between the load-bearing bottom slab of the pools and the concrete base slab cast on top of bedrock. On the sides of the pools, the isolation has been extended up by 1 m. The aim of the water isolation is to ensure the water tightness of the base slab even in an accident scenario.

The structures of the pools have been dimensioned for a pool water temperature of +50°C under normal circumstances, and +100°C under exceptional circumstances. Adjacent pools may have different temperature, and some of the pools may be empty. In the dimensioning, a scenario where the water temperature is 100°C has been handled as an exceptional load scenario occurring once during the lifetime of the plant. The dimensioning of the pool bottom slabs takes into account the possibility of using a tighter rack layout and condensed fuel assemblies.

The measurements designed to indicate a blocked outlet channel trip the turbine condenser seawater pumps at a surface level of +2.3 m. This causes condenser loss and a reactor scram. At this point, seawater level is +1.6 m. The seawater level may rise by an additional 1.9 m past this point, before the design basis limit of +3.5 m is reached. The slower the water rises, the more time is available for cooling the reactor. The amount of heat transfer capacity needed for residual heat removal is reduced over time.

In a scenario where the ground water system submersible pump is not operational during a flood, the faulty submersible pump may be replaced by installing a new submersible pump in the ground water pump house. There are additional submersible pumps in stock, so additional pumps may be temporarily installed. If the residual heat removal chain for spent fuel is damaged due to flood, additional water may be supplied into the KPA storage pools by means of the demineralised water distribution system or the fire fighting water system. The need for additional water is small, so the capacity of the systems is quite enough to compensate for the vaporisation of pool water due to spent fuel residual heat. Supplying additional water requires successful operator actions.

<u>Situation outside the plant</u>

Olkiluodontie, the road which connects the Olkiluoto site to main road 8, is about 15 km long. The road runs a few hundred metres from the river Lapinjoki, the surroundings of which are low-lying areas.

The road surface level of Olkiluodontie is below +3.5 m at a few points. To the southeast from the bridge connecting Olkiluoto to the mainland, the road runs a few hundred metres at a level below +3.5 m. In the bridge area, the minimum level is +2.8 m. About two kilometres from the bridges towards main road 8, the road surface falls below +3.5 m for nearly two kilometers, with lowest point at about +2.0 m. Approximately three kilometres from main road 8, Olkiluodontie runs between +2.8 and +3.3 metres for a few hundred metres.

On the island of Olkiluoto, the level of Olkiluodontie falls below +3.5 m in the Flutanperä area. When the water level is at +3.5 m, water may flood the road at Rummintie. Based on the height readings from the island, the plant site, parking areas and the main gate area would be mostly covered by water when the seawater is at level +3.5 m. In some areas of the parking lot, there would be nearly 2 metres of water. In the yard areas, water depth would vary between a few centimetres and nearly one metre.

When the sea level exceeds +3.5 m, water will flood the road in places. Depending on the currents, the water may carry soil around so that the road or a bridge collapses, thus affecting entry into the plant area. In case of a long-standing elevated water level, entry into Olkiluoto via Olkiluodontie may be impossible in places.

TVO would work in cooperation with the police, border guard, the Defence Forces and the rescue services to restore road connections cut by individual natural phenomena or combinations thereof (see Section C.6.1.3). Emergency preparedness is described in Section C.6.1.1 in more detail.

C.3.1.3 Plant compliance with its current licensing basis

Flood protection has mainly been achieved passively. However, there are cables important to safety outside the reactor building at levels below +3.5 m. Their aging does not directly affect their tightness. The exception is their exposure to outside mechanical loads. Such mechanical loads may be caused, e.g., by the replacement of adjacent cables. The condition of the adjacent cables is visually checked during cable replacements.

The penetrations in the reactor building are pressure-proof. The condition of the penetrations is visually inspected regularly in connection with room inspections. If penetrations are opened for installation of cables, pipes, etc., their condition is verified before they are reinstalled.

The door from the control room building to the reactor building at level –2.0 m opens in the direction of the reactor building. It is unclear whether this door can withstand the pressure from the water (see also Section C.3.2.2).

The water level measurements in the outlet channel are checked twice a year according to the Technical Specifications.

No specific mobile equipment is planned to be used in the event of a flood rising to the ground level. However, Licensee has mobile equipment to be used to mitigate severe accidents.

Licensee's mobile equipment and its preventive maintenance is described in Sections C.2.1.3 and C.6.1.2. This equipment is used to ensure among others the electricity supply for the electric actuators of valves needed for flooding the containment drywell from the wetwell and filling the containment from the fire fighting water system in the event of a core melt accident. The mobile generator can be connected to the connection points on the reactor building wall. The transfer and connection are managed by the Olkiluoto onsite fire brigade. The generators are stored in the plant area at ground level. The generators may also be used to supply the reserve command centre and weather mast. The generators have an output of 23 kW.

The KPA storage has one submersible pump in reserve, stored in the ground water system well room, and there is a procedure for its connection. Furthermore, there are submersible pumps at the tool storage, but these pumps may be reserved elsewhere.

Based on recent periodic safety reviews (1997, 2008), PSA on external events and the national clarifications due to the Fukushima accident, OL1 and OL2 and the KPA storage comply with their current licensing basis.

C.3.2 Evaluation of safety margins

C.3.2.1 Estimation of safety margin against flooding

A definite maximum height of flooding cannot be derived on a physical basis for the Olkiluoto site. In some other connections, design vales against external events are chosen so that their exceedande frequency is less than 10^{-4}/a. The water level with exceedance frequency of 10^{-4}/a is about +1.5 m (N60). The margin of this value to the design basis is 2 metres. The frequency of exceeding seawater level +3.5 m (N60) is estimated to be less than 10^{-9}/a. Although the uncertainties associated with such low frequencies are very large, the margins can be considered adequate.

<u>NPP units OL1 and OL2</u>

If the design basis +3.5 m (N60) of OL1 and OL2 is exceeded, water starts to flow into the plant through doors which are not watertight. The flow rate is first very small and the spreading of water inside the plant is restricted by closed fire doors. Doors which are not designed to withstand hydrostatic pressure typically break when the hydrostatic pressure exceeds about 1 m water.

The flooding levels inside the plant which would cause the loss of certain safety systems and other important systems are presented in the previous sections. The most severe effec of flooding exceeding the design basis would be loss of connections to the off-site power transmission grid and the loss of emergency diesel generators, resulting in the loss of residual heat removal.

KPA storage

The maximum water level of +1.2 m used in the design basis of the KPA storage may be exceeded during the operating life of the storage. In a flooding scenario, the flood water is drained to the submersible pumps return water back into the sea.

Once the flood water flow exceeds the rated flow of the submersible pumps, the water level will rise in the KPA storage building. This poses a risk to the systems used for spent fuel residual heat removal. The time window for supplying additional water is several days. Additional water may be supplied to the storage pools by means of the demineralised water distribution system or via the fire fighting system, as explained in Section C.3.1.2.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a more detailed study on the effects to spent fuel storage pool heat removal systems and electrical supply in case of abnormal sea level at the Olkiluoto NPP site.

C.3.2.2 Measures which can be envisaged to increase robustness of the plant against flooding

NPP units OL1 and OL2

The event that the design basis flood would be exceeded is so improbable that measures to increase robustness of the plant specifically against flooding are not considered necessary. However, some topics could be studied for improving protection against flooding exceeding the design bases. In addition, some plant modifications and system renewals are studied for other reasons. In connection with them, it is possible to improve also the robustness against external flooding.

The door leading from the control room building to the reactor building at level –2.0 m opens in the direction of the reactor building. The water tightness and water pressure tolerance of doors leading to the basement of the reactor building and consequences of the eventual leakages will be investigated and, if needed, the water tightness and pressure tolerance will be improved.

In case of a renewal of the diesel generators, they could be designed to also allow for air cooling. In this case, they may also be used in a scenario where the possibility to cool them using the shutdown secondary cooling or service water systems has been lost.

The diesel generators are located in rooms which are separated into fire compartments, including a local control room. The water tightness of the diesel generator room and the local control room could be improved in parallel with the diesel generator renewal project. The improvement of the water tightness, for example raising the doorsteps, etc., would increase further the availability of diesel-backed electricity in the event of flooding at the ground level.

<u>KPA storage</u>

During the expansion of the KPA storage, a second ground water pump house will be built, and the underground drains to the south of the storage will be renewed. These procedures reduce the risk of water surface rising and flooding the building. The structures of the expansion are also dimensioned for water rising to the level of +1.2 m.

The flood tolerance of the KPA storage can be increased by increasing the rated flow of the submersible pumps. A proposal to increase the rated flow of the submersible pumps has been prepared. The plan is to increase the rated flow by the end of 2012.

A probabilistic risk analysis will be prepared for the KPA storage during its expansion. The risk analysis will contain the risks of internal and external initiating events, including flooding. Potential modifications improving nuclear safety will be analysed based on the results of the probabilistic risk analysis.

Even though the response times are long at the KPA storage, emergency procedures for external floods should be planned especially regarding loss of residual heat removal.

A procedure for additional submersible pumps would ensure that there is always a sufficient amount of submersible pumps in storage available for flooding situations.

Preventive maintenance package should be done for reserve submersible pump at the KPA storage. A preventive maintenance package would make the reserve submersible pump more reliable when it is required for service.

To respond to STUK’s requirements after Fukushima accident, Licensee has started analysing possibilities to diversify the residual heat removal of the KPA storage to allow for fuel pool cooling without water vaporisation even during a loss of off-site power and flooding scenario.

C.4 Extreme weather conditions

C.4.1 Design basis

Air temperature and humidity

The ventilation systems for the OL1 and OL2 plant units and the KPA storage have a lower design outside air temperature limit of –25°C, and an upper limit of +25°C.

For the operation of the electrical systems, the largest allowed interior temperature is +35°C, temporarily +40 °C.

For the diesel generators, the highest allowed ambient temperature is +40°C, with an outside air temperature of +25°C. According to the Technical Specifications, the cloud point for the diesel generator fuel shall be below –24°C.

The ventilation system 746 for the electrical facilities in the control room, switch gear plant and auxiliary buildings has a maximum outside air humidity of 50% in the summer. No design value for outside air humidity has been given for winter conditions.

Seawater temperature

In the original design of the plant units, +18°C had been used as the upper limit for the seawater temperature. This limit includes remarkable safety margin. According to the licensee's analyses from the VARMT project, it is assured that the OL1 and OL2 plant units may be operated at a seawater temperature of +27°C. However, this requires extended monitoring of the plant unit temperatures and cooling. Results of accident analyses and residual heat removal analyses and the cooling of H safety bay and emergency diesel generators are acceptable at a seawater temperature of +27°C.

The upper limit for the seawater temperature in the design of the diesel generator is +30°C. No lower limit for seawater temperature has been set in the design basis.

For the cooling of fuel pools, the upper limit of the design temperature for the KPA storage seawater circuit is +30°C.

According to the water permit for the plant unit, seawater temperature may not exceed +30°C as a weekly average in the discharge channel.

The Technical Specifications have a power nomogram for managing the temperature of the condensation pool. The nomogram sets limits for reactor power and the unavailability of the condensation pool cooling chains, when the temperature in the condensation pool and the seawater temperature are too high.

High winds and storms

The dimensioning of OL1 and OL2 in terms of wind loads is based on the Finnish national building codes RIL 59 and RIL 79. The buildings and stack are designed to tolerate wind speeds of 50 m/s; the lining sheet metal is designed to tolerate wind speeds of up to 28 m/s.

The consequences of exceptional wind loads have been taken into account by dimensioning the roofs of the reactor building and control room building to tolerate loads caused by the off-gas stack falling down.

For the KPA storage, the Finnish building code document “Structural safety and loads B1” has been applied. When calculating wind loads, a maximum value of 1.0 kN/m^2 has been used for the speed pressure.

The towers of the transmission lines in the national main grid are designed to withstand a gust wind load of 33.2 m/s. As safety factors are used for dimensioning the structures, the critical wind speed is clearly above the gust wind limit in question. In the weather risk analysis, it has been estimated that the high voltage transmission grid tolerates 39 m/s.

<u>Phenomena leading to seawater channel blockage</u>

Phenomena leading to seawater channel blockage have been taken into account in the design by installing a seawater screening system that mechanically removes impurities before seawater is routed into the cooling water channel. To prevent the collapse of the cooling water channel, structural requirements of the cooling water channel have been defined based on land use at ground level.

To prevent frazil ice caused by under-cooled water, a system has been installed to guide warm water from the outlet channel back to the intake side in order to warm the intake water.

Defences are developed for identified phenomena at the OL1 and OL2 plant units and the KPA storage. These include blockage caused by frazil ice, algae, bottom flora and fauna, mussels, bottom deposits and other loose material, and fish.

<u>External fires (wildfire, bushfire and forest fire)</u>

The fire protection design basis for the OL1 and OL2 plant units and KPA storage have been prepared with a view to internal fires.

Control room ventilation is designed so that no radioactive or otherwise harmful substances can enter the control room in a foreseeable accident situation. The same procedures can be applied to prevent combustion gases from entering the control room.

Transmission lines and switchyards are surrounded by zones in which the height of the vegetation is limited. At the plant site there is no high vegetation. The fire load of the underbrush at the plant site is low and eventual fires in the underbrush may be effectively confined and ultimately extinguished by the plant fire brigade and the regional rescue services. Furthermore, the plant units are surrounded by an asphalted yard, which effectively prevents spreading of an eventual fire to the plant unit buildings.

The plant site has a fire station, fire brigade, and fire fighting equipment. The fire brigade has a minimum staff of 1+3 and a response time of 5 min.

Rain

The roof drains of the OL1 and OL2 plant units have been designed withstand a rain of 72 mm/h, over-dimensioning the structures and components by 150…300 %.

Snow and ice

As regards snow loads, the dimensioning of the structures of OL1 and OL2, as well as of the KPA storage is based on the Finnish national building code. The design basis is the snow load of 1.4 kN/m^2, corresponding to a water layer of approximately 140 mm.

The roof of the reactor building has been dimensioned to withstand the stack falling on the roof, corresponding to approximately ten times the snow load.

C.4.1.1 Reassessment of weather conditions used as design basis

Lightning

A lightning protection system has been installed in the OL1 and OL2 plant units to protect the structures, equipment and personnel from overvoltage caused by lightning strikes. The design basis for the lightning protection is a lightning current of 100 kA and a maximum current rise rate of 80 kA/µs. The studied frequency range is 10 to 250 Hz.

For the KPA storage, preparations for overvoltage caused by lightning have been made by connecting the metal structures of the roofs and walls and the protruding metal parts to the earth of the building.

Expected frequency of originally postulated or defined design basis conditions

Outside air temperature and humidity

The observation stations having observations for the longest time series were used for analyses. The observation stations near Olkiluoto were Turku airport, Jokioinen, Pori airport and Kokemäki.

The probability to exceed the design basis temperature +25°C as a daily average in June is 0.01…0.02/a, in July about 0.05/a, and in August 0.01/a. The probability to go below the design basis temperature –25 °C as a daily average in winter time is about 0.1/a.

In order to induce any effects to the plant units, the hot or cold spell must last many consecutive days above or below the design basis temperature.

Climate change is expected to increase the probability of daily maximum temperatures and to increase the daily temperatures. Winters are expected to become warmer due to the climate change.

Seawater temperature

Seawater temperature is measured at the OL1 and OL2 plant units in the cooling water intake channel. During the studied period of 1998 to 2010, seawater temperature has never exceeded +25°C. The highest seawater temperature of +24.7°C was measured at the OL2 plant unit on 1 August 2003. The lowest seawater temperature of the studied period, –0.34°C, was measured on 20 January 2010.

High winds

The high wind speed has been studied at five observation stations. One of these is the coastal observation station at Hailuoto. The strongest wind gusts were observed at Bogskär.

Bogskär has an anemometer installed 27 m from the ground; at Hailuoto, it is located at a height of 46 m. Therefore, the above reoccurrence times can be used when studying wind speeds at a height of less than 60 m. Furthermore, the height of the mast most likely affects the large difference in reoccurrence times (probabilities) between the Bogskär and Hailuoto weather stations.

The highest average wind speed measured in Finland is 31 m/s. Taking into account a confidence interval of 95 %, a similar average wind speed probability is 0.02/a at Hailuoto. 50 m/s average wind speed is less probable than 0.002/a at these five observation stations. The probability of the design basis average wind speed 28 m/s is 0.002…0.01/a at Bogskär and 0.05…0.1/a at Hailuoto. When taking into account a confidence interval of 95%, the corresponding probabilities are 0.05…0.1/a and more than 0.1/a.

The highest gust wind speed measured in Finland is 39 m/s. The probability of such a gust at these five observation stations is less than 0.002/a. A gust of 28 m/s is more probable than 0.1/a at Bogkär and Hailuoto. A gust of 50 m/s is less probable than 0.002/a at these five observation stations.

A gust of 28 m/s occurs more than once per 10 years. In many of the storms in Finland, a storm gust can reach speeds of 25 to 30 m/s.

Climate change is expected to increase average wind speeds in winter by 5% by the end of the century.

Tornados

In Finland, the frequency for a significant whirlwind is less than 10^{-5}/a. For example, a total of six class F3 tornados have been observed. The strongest known tornado in Finland has been a F4 category tornado in northern Savo in 1934. The Finnish Meteorological Institute's tornado observation data from the years 1796…2007 was used. Consequences of tornados are limited to small areas.

Based on statistics from years 1930…2007, the probability of F2 or stronger tornado to occur inside an 80 × 80 km^2 area during one year is locally over 5% in southern part of Finland, in northern Savo and in Pohjanmaa. The surrounding areas of Olkiluoto have a lower annual geographic frequency for significant tornados. Olkiluoto may be considered an area with few tornados.

It is important to recall the uncertainties which are related to geographical probability of occurrence of tornados.

<u>Downbursts</u>

Downbursts are related to thunder and shower clouds. Their consequences are restricted to a local area. The most significant difference between a downburst and a whirlwind is that a downburst fells trees in one direction, whereas a whirlwind fells them in different directions. The most downbursts in Finland occur mainly during the summer months (June, July and August).

Estimating the effective area of a downburst, and therefore, the probability of their occurrence on certain area, is difficult. Estimating their effects has many uncertainty factors.

<u>Phenomena leading to seawater channel blockage</u>

Due to the location of the OL1 and OL2 plant units, it is possible that the travelling band screen may be blocked as a result of algae, mussels, or other sea debris, such as that released during a storm.

The risk of floating algae appearing is largest when the water temperature exceeds 16°C in spring, after a long warm season. This temperature is generally reached during the time from May to mid-June. A suitable wind direction will guide additional algae into the water intake. In the spring of 1992, seaweed caused a reactor scram at the OL2 plant unit.

According to TVO's experience, the water intake tunnels of the OL1 and OL2 plant units have collected a permanent layer of mussels, other sea flora and fauna, and sludge. A very powerful shake, such as an earthquake, or a strong storm can lead to loosen mussels in the intake channels.

In wind conditions promoting the formation of frazil ice, water undercools and undercooled or icy water enters the cooling water channel; this may quickly clog the screens and filters, endangering the cooling of the entire plant unit. TVO has had three frazil ice events that have caused an interruption of plant operation. In above-mentioned events, the amount of water flow to the safety-related systems has been sufficient. Plant modifications have been done to prevent frazil ice events.

<u>External fires (wildfires, bushfires and forest fires)</u>

The nearest forest is located in the areas in the vicinity of the plant site. It is highly unlikely that a fire could break out in this area that could be extensive enough for it to threaten the plant units by spreading into the plant site. The plant site, especially the nearby areas of the plant units, have very little vegetation and only shallow growths that the fire could spread along. The plant units are surrounded by areas covered by asphalt which will limit potential fires.

Rain

The largest measured amount of rain in one day in Finland was 198 mm (21 July 1944 Espoo, Lahnus).

The design basis rain of 72 mm/h occurs less than once every 100 years.

The climate models involving rain are more uncertain than those involving climate warming. With the climate change, the daily rain amounts are expected to increase during all seasons, and especially in the winter.

Snow and ice

The highest depth of snow in Finland, 190 cm, was measured in the village of Enontekiö in Kilpisjärvi on 19 April 1997. In Turku, the highest measured depth was 77 cm on 22 February 1966. The highest measured increase in snow depth during one day was 48 cm/day in Kilpisjärvi on 29 January 1981. The second highest value was 47 cm/day at Pori Airport on 22 November 1971. In south-western Finland, a snow depth of 65 cm is estimated to be reached once per decade or fewer. Once every 50 years, snow depth may increase to 75 cm. The water equivalent value states the amount of water in the snow, or the thickness of the water layer. Water equivalent value is usually reported in mm or kg/m^2. Snow load cannot be estimated based on the thickness of the snow layer, as the density of snow varies greatly. Freshly fallen snow has a density of approximately 100 kg/m^3, or approx. 10% of water density. Snow usually has the highest water equivalent value at the turn of March and April.

Snowstorms (average wind speed at least 21 m/s and snowfall at observation time/during last hour) account for less than 1% of all snowfall days.

On average, the coverage of snow is expected to become thinner, and snow is expected to have a lower water equivalent value. According to the simulations performed with climate models, the snowfall amounts are reduced by 20%. However, the largest amounts of daily snowfall in midwinter will increase by 20% in some simulations.

Lightning

Finland has lightning activity especially in the summertime. In the winter, thunderclouds mainly connect to thunder fronts above open water, such as sea. A typical lighting is negative, and the average strength is in the region of 10 to 20 kA. The peak current distribution for ground strikes extends from a few kiloamperes up to around 300 kA.

The Weather PSA estimates that, at Olkiluoto's latitude, the number of days with thunder is slightly below the average for the entire country. The annual density of lightning strikes per year in the Olkiluoto region is estimated at 0.3 strikes/km^2.

The percentage of strong ground strikes, from the annual lightning strike amounts, has been in the same region from year to year, approximately 0.02%.

Consideration of potential combination of weather conditions

Drought caused by a long-term high air temperature, high wind, and smoke due to forest fire

Long periods of extreme heat may occur in the summer, resulting in very low amounts of rain and very dry conditions. In periods like this, the probability of a forest fire is increased. A forest fire may be started by a lightning strike during a thunder storm, for example. The storm may cause a loss of off-site power and the forest fire may cause detrimental smoke effects in the plant area.

Wind and algae, bottom flora, bottom sediments and debris

A hard stormy wind may lead to a loss of off-site power and remove bottom sediments and debris from the seawater. This phenomenon is especially challenging for the operation of the intake channels, and it may deteriorate the functioning of the residual heat removal systems.

Stormy wind and lightning strikes

The combined effects of stormy winds and lightning are analysed in the PSA. The consequences are the same as for individual events.

High air and seawater temperature

A high air temperature does not cause problems for the plant units and the KPA storage in itself, if the ventilation systems are functioning as planned. However, a failure of the ventilation systems will raise the temperatures in the facilities to a few degrees above the outside spaces. If the seawater temperature rises too high, the thermal load cannot be transferred into the sea, either. The sea usually warms up at the end of a high temperature period, which makes a combined effect a real possibility.

Snowfall, wind and snow pile-up

Snow loads have been taken into account in the durability of the structures. However, a snow storm may clog the ventilation systems, which has not been taken into account in the design basis except for design of diesel generators.

Snowfall, wind and frazil ice

In scenarios where water in the cooling water channel cools unfavourably enough to create frazil ice, the wind speed is usually around 10 m/s. Wind at 39 m/s during a frazil ice scenario may cause a loss of off-site power, which will result in a need to use the diesel generators. If the storm includes snowfall, the snow may clog the air intakes of the diesel generators. In this case the air intake of the diesel is automatically be rerouted to the inside. In the case of a LOOP, electric power can be also provided from the gas turbine. Loss of off-site power in discussed in detail in Section C.5.1.

Conclusions on the adequacy of protection against extreme external conditions

The original design of the plant unit did not take into account all the possible weather phenomena or other natural conditions. However, the plant preparedness and strength against external hazards has been improved due to plant modifications performed using the principle of continuous improvement.

Operational experiences regarding the impact of extreme weather phenomena on plant operation have been taken into account in the design of preventive and corrective measures including technical modifications and plant procedures.

Weather phenomena and other external conditions of natural origin including combinations of phenomena relevant at the plant units have been comprehensively analysed using the Weather PSA, which is part of the living PSA. The historical meteorological and hydrological data available from the local and national observations and records have been extensively utilised in analysing the duration, intensity and frequencies of external phenomena.

Extreme weather conditions, including the impact of climate change and global warming and their effects on temperatures, wind speeds, rain and snowfall, are studied within the EXWE project in the Finnish Research Programme on Nuclear Power Plant Safety [SAFIR2010, SAFIR2014]. The programme may necessitate reconsiderations regarding design basis and safety margins for external phenomena, in particular, such air temperature, wind and rain. The licensee actively participates in the SAFIR programme.

C.4.2 Evaluation of safety margins

C.4.2.1 Estimation of safety margin against extreme weather conditions

<u>Outside air temperature and humidity</u>

If the outside air humidity exceeds 50% in summer, the inside air humidity cannot be maintained within the set limits. This has no nuclear safety significance, but it does affect the working conditions in the control room, for example. In cold weather, the moisture in the outside air may cause frost to collect on the surfaces of the ventilation grilles. Frost is removed from air conditioning equipment several times each winter. However, frost does not pose a nuclear safety hazard.

An average outside temperature of +25 °C has no effect on plant operability.

If the design temperature of the ventilation systems is exceeded, the room temperature inside the buildings may slightly increase. The air cooling systems are cooled with seawater so the interior temperature will not rise if the seawater remains sufficiently cool. An increase of the interior temperatures by a few degrees is of no consequence from plant operability or nuclear safety point of view. The diesel generators are cooled with seawater through the shut-down service water system. The temperature of the diesel rooms may be lowered by opening doors to the outside, if the cooling power of the air ventilation cooling system is not sufficient.

If the average outside temperature increases to +40°C for a long period (weeks), a reactor scram is possible. Based on the observations, such an event is highly improbable in Olkiluoto.

The oil storage tank of the diesel generator has a thermal insulation, and a decrease in diesel oil temperature requires a long period of cold weather. When the outside temperature falls below –25°C, the oil is circulated using the pumps of the diesel oil storage system to prevent settling. Therefore, the temperature of the diesel fuel falling to the cloud point is prevented.

Based on the consideration above, the nuclear safety hazard due to low or high air temperature is considered to be low at the present experience on the behaviour of outside air temperatures.

<u>High seawater temperature</u>

An operating procedure exists for an abnormal high seawater temperature, explaining the activities in such a situation. When the seawater temperature is between +25°C and +27°C, the operation of the plant units is continued at a separately defined power level that maintains sufficient margin for operational disturbances due to warm seawater. The sufficiency of the cooling capacity of systems and components are followed by using alarm information and rounds made at the plant unit. If necessary, the cooling is added to ensure the operability of systems. The shift manager informs the Operation staff of any cooling problems that might appear.

When seawater temperature exceeds +27°C, the operating mode of the plant unit is decided on separately. The safe state of the operating mode is evaluated on a per-case basis. Based on experience, the temperature peaks have been short, and a change in wind direction, for example, may quickly lower seawater temperature. If the temperature exceeds +30°C, the operating mode of the plant unit is changed to the hot or cold shutdown state.

Based on the experience, the electrical systems are able to operate at high ambient temperatures of over +50°C. The diesel generators can tolerate an ambient temperature of +45°C and a seawater temperature of +30°C.

<u>Low seawater temperature</u>

In winter, seawater temperature may fall below freezing point in certain conditions, and water may become subcooled. The subcooled water in a hard, turbulent flow may cause frazil ice, which may potentially clog the cooling water channels. The OL1 and OL2 plant units have had a few cases of calling water channel clogging due to frazil ice. These have resulted in the tripping of the condenser seawater system, and an interruption of plant operation. To prevent operational disturbances due to frazil ice, the pumps that allow water to be pumped from the discharge side to the intake side have been installed. The rate of this recirculation flow is 1 m^3/s at both plant units. The recirculation pumping is started as a precaution, when the temperature of the incoming seawater falls below +2°C.

As a second precaution against the clogging of the intake channel by frazil ice, the seawater intake of the left auxiliary building is rerouted to the outlet channel when the temperature of the incoming seawater falls below +2°C. This procedure ensures the uninterrupted seawater supply to all safety-related systems, even if the seawater intake channel is clogged.

At the KPA storage, active and passive measures have been taken to protect against the frazil ice phenomenon. As an active measure, discharge water may be redirected into the pump house water wells. As a passive measure, the pump house is located at a suitable distance from the coastline, at the end of an excavated water intake channel. A boom placed at the mouth of the channel moves frazil ice formation sufficiently far away from the water collection point. The section of the channel after the boom is the first to freeze, thus preventing frazil ice formation at the mouth of the pump house.

Preparations for high seawater temperature may be considered sufficient. The same applies to the frazil ice phenomenon.

Considering the behaviour of the phenomenon based on the present knowledge, the level of existing operating procedures for abnormal seawater temperature, the modifications already implemented on the basis of operating experience feedback and PSA, the plant precautions against abnormal seawater temperatures could be considered to be on the level of good safety practices.

<u>Wind</u>

Wind may cause damage as sudden gusts or long-term wind loads. Wind may directly damage the structures of the buildings, or it may throw debris onto the switchgear bay or cooling water channel. The off-site power may be lost if the poles fall over.

Winds with an average speed of over 28 m/s may appear at Olkiluoto. They may tear away the cladding sheet metal, which may cause damage at the switchgear plant or cooling water channel.

The licensee has assessed the consequences of extreme strong wind, in terms of nuclear safety, minor. However, the wind potentially combined with other external phenomena, and the potential impact of global climate change on those phenomena might cause unforeseen consequences to plant operation. Therefore, the phenomenon should be kept under monitoring, and reassessed, if necessary for instance when new results of the EXWE project [SAFIR2014] will be available.

<u>Blockage of the intake side sea water channel</u>

If the cooling water channel intake side is blocked, the water level decreases in the channel between the blockage and the cooling water pumps. This creates an alarm in the cooling water screening plant, which trips the cooling water pumps of the turbine condenser. At the same time, hatches will open in the cooling water channels causing a recirculation of water for the service water system pumps. Due to the rather small volume of recirculated water, the temperature of the water increases. Within one hour, the cooling water intake must be switched to the outlet channel.

During the recirculation with the intake blocked, water surface in the screening plant will rise, and the difference in level will work to remove the impurities that caused the blockage. If the impurities cannot be removed, water level will rise to a level of +3.5 m. This may cause flooding in the cooling water screening plant building, and further, in the auxiliary cooling water pump rooms. From here, the water can be discharged through the doors to the yard outside the plant unit. This will not damage the shut-down service water system pumps.

The water level will lower back to normal, and the normal flow direction in the channels can be restored after the blockage has been removed. After this, the operating state of the cooling water system is restored.

If the water rises to the pump rooms in the auxiliary system building, the water may spread elsewhere in the plant unit. The underground levels may be flooded. There is a small possibility that some water spreads into the diesel generator rooms, either from the inside or outside.

In 2009 the licensee started the planning of the yard modifications to take measures against the uncontrolled spreading of the water.

<u>Blockage of the discharge side sea water channel</u>

If a discharge channel is blocked (due to a wall collapsing, for example), an alarm is received in the auxiliary system building. The condenser cooling water pumps are stopped at a surface level of +2.35 m. After this, the surface level is restored to normal, and the temperature in the service water systems' recirculation water and the pump and discharge pits increases. The pumps of the non-diesel-backed service water system are stopped. A blockage on the discharge side is most likely not enough to completely block the flow from the safety-related seawater systems. If the water surface level continues to rise, water will flood to level +3.5 m in the auxiliary system buildings, from where it can be discharged into the yard. Water level on the discharge side is restored once the blockage has been removed.

The design of the plant unit has made appropriate preparations for the blockage of the intake and discharge channels separately. The simultaneous blockage of both channels can lead to the LUHS. This is discussed in detail in Section C.5.

The cooling of the fuel stored in the fuel pools is also normally performed by using the water in the cooling water channels. The fuel pools may be allowed to boil, removing the residual heat from the spent fuel as the cooling water vaporises. In this case, the vaporised water needs to be compensated by adding water from the distribution system for demineralised water pools or the fire fighting water system.

A loss of sea water as an ultimate heat sink is not a design basis event of the plant. Improved provision for the loss of sea water necessitates both plant modifications and a new EOP. Planning of plant modifications is underway.

Wildfire, bushfire and forest fire

Wildfires, bushfires and forest fires don't pose any danger to the plant beside the possible loss of off-site power. The licensee has shown in its analysis that the safety margins for the loss of off-site power are sufficient.

Rain

Drains have been installed on the roofs of buildings that route the rainwater off the roof. If the roof fails in the reactor building or turbine building, water may directly enter the facilities below. To prevent this, discharge pipes have been installed on the roofs of the reactor and turbine buildings; they route the rainwater out along the facade, if the drains are clogged. Large amounts of water cannot collect on the roofs of other buildings, even if the drains were clogged.

The rainwater survey for the OL1 and OL2 plant units completed in 2010 stated that the largest ponds in the areas near the plant units are caused by short, heavy rain with duration of 10 to 60 minutes. According to the survey, ponds start forming when the rain has an intensity of at least 1 mm/min and duration of at least 20 min, or if the intensity exceeds 2 mm/min, even a shorter rain is sufficient according to the licensee's analysis.

The most critical point is in front of the pump house for plant unit OL1. Water may enter the pump house and spread elsewhere onto the unit. Closed doors reduce the spread rate of water, and connections to the underground floor will lead most of the water there. Despite this, water may enter two diesel rooms from the inside and outside. According to the licensee's estimate, this is a very unlikely scenario.

However, the licensee should, further consider possible measures for increasing the safety margin against extreme rain, especially in respect of the potential impact of climate change on weather phenomena.

Snow and ice

Large snow loads may be prepared for in time by removing the snow.

Combustion air for the diesel generators is usually taken from the outside. If the grille on the air duct should be blocked due to snow, an alarm for the pressure difference across the grille would first be received in the control room. If the pressure difference were to increase further, the air intake of the diesel in the room would automatically be rerouted to the inside.

Snow pile up due to wind occurs against one plant unit wall at a time. As the diesel generators are located so that two are on the west side and two on the east side, pile-up will not occur on both diesel generator pairs at the same time. Thus, two diesel generators will be available even in a scenario such as this. Further, pile-up does not happen suddenly, which means there is time to react and remove the snow.

The separate location of the two sets of DG pairs can be considered to give a reasonable safety margin regarding snow loads taking into account the behaviour of wind and the span of accumulation of snow piles posing the threat in terms of safety.

Lightning

During the plant unit modernisation in 1996, a separate lightning strike risk evaluation was performed by the licensee. This evaluation determined that the risk of core damage caused by lightning strikes is low due to, among other things, the protection provided by structures and the distance between the devices.

Positively charged lightning strikes with a current of over 200 kA occur each year in Finland. The current design basis, however, is dimensioned against negative strikes. Their power seldom exceeds 100 kA. The equipment on the plant units can tolerate a short-term overvoltage of 3 kV.

Based on these results above, current preparations can be considered sufficient.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan to secure decay heat removal to ultimate heat sink in extreme external events and to investigate the effect of extreme environmental temperatures to the plant safety.

C.4.2.2 Measures which can be envisaged to increase robustness of the plant against extreme weather conditions

Attention will be paid to the cooling of ventilation in certain rooms containing electrical and I&C systems, if thermal loads will rise in future. It is evaluated that the temperature of the MCR, the computer room, and two of the relay rooms cannot be maintained at an acceptable level by using outside air for cooling. The subsystems responsible for the ventilation of these rooms, as well as the air in the electrical room air ventilation systems, are normally cooled using the brine system for air conditioning. The brine system is non-diesel-backed, which means that in a loss of external electricity scenario, the temperature in the relay rooms would rise above the outside air temperature. When the outside air temperature is high, the temperature in the relay rooms may rise to a level where the operability of electrical and I&C equipment, especially those representing modern technology, may be brought to question in future. For devices presently in use, a rise in operating temperature would mainly shorten the operating life, but not affect the instantaneous operability of the devices.

In case of a renewal of the diesel generators, they could be designed to also allow for air cooling. In this case, they may also be used in a scenario where the possibility to cool them using the shutdown secondary cooling or service water systems has been lost. The diesel generators are located in rooms which are separated into fire compartments, including a local control room. The water tightness of the diesel generator room and the local control room could be improved in parallel with the diesel generator renewal project. The improvement of the water tightness, for example the raising of doorsteps, etc., would increase further the availability of diesel-backed electricity in the event of flooding at the ground level.

The dependency of the auxiliary feed water system from seawater cooling could be reduced by modifying pump circulation so that water is returned into the auxiliary water tank. This would cause the heat from the auxiliary feed water pumps to be removed even when the secondary cooling system or service water systems are not available. Temperature increase in the water tank would be very slow in this case, and it would not be a limiting factor. Additional water may be supplied into the reactor via the auxiliary feed water system even when the secondary cooling and service water systems are not available.

The yard around the plant units will be shaped to ensure the passage of water from the pools formed during heavy rain or seawater in cases of seawater channel blockage away from the power plant units and further into the sea. The planning of the tilling has already started based on the rainwater survey completed in 2010. After the expansion of the KPA storage, the yard areas of the storage will be surveyed, and a rainwater analysis will be prepared based on the survey. Based on the survey, the yard area will be modified so that rainwater can be freely discharged into the sea.

In connection with the expansion, a probability-based risk analysis will be prepared for the KPA storage; it will also contain an analysis of the effects of extreme weather conditions on the KPA storage. Based on the risk analysis results, any needs for modifications (such as plant or disturbance procedure modifications) will be considered to ensure sufficient preparations for extreme weather conditions.

The improvements above are part of ongoing processes, and thus not initiated due to Fukushima accident.

To respond to STUK's requirements after Fukushima accident, Licensee is investigating the robustness of reactor, control room and auxiliary buildings against extremely high wind speeds.

Furthermore, Licensee has made a survey for rooms containing equipment susceptible to freezing temperatures (reactor pressure and water level reference pipes and e.g. I&C systems). After the survey, low-temperature alarms (+15°C) and manual ventilation channel closure flaps for the rooms containing reference pipes were installed. The procedures on actions in case of loss of heating at low temperatures were implemented and trained to operators.

The study of effects of extremely low temperatures on KPA storage is to be included in the PSA study of the storage as part of its extension project.

Licensee has stated that current procedures, including restrictions on power operation under extremely high sea water or outdoor temperatures are adequate. STUK is evaluating this assessment.

C.5 Loss of electrical power and loss of ultimate heat sink

C.5.1 Loss of electrical power

OL1 and OL2 electric main diagram is presented in Figure C-4 below.

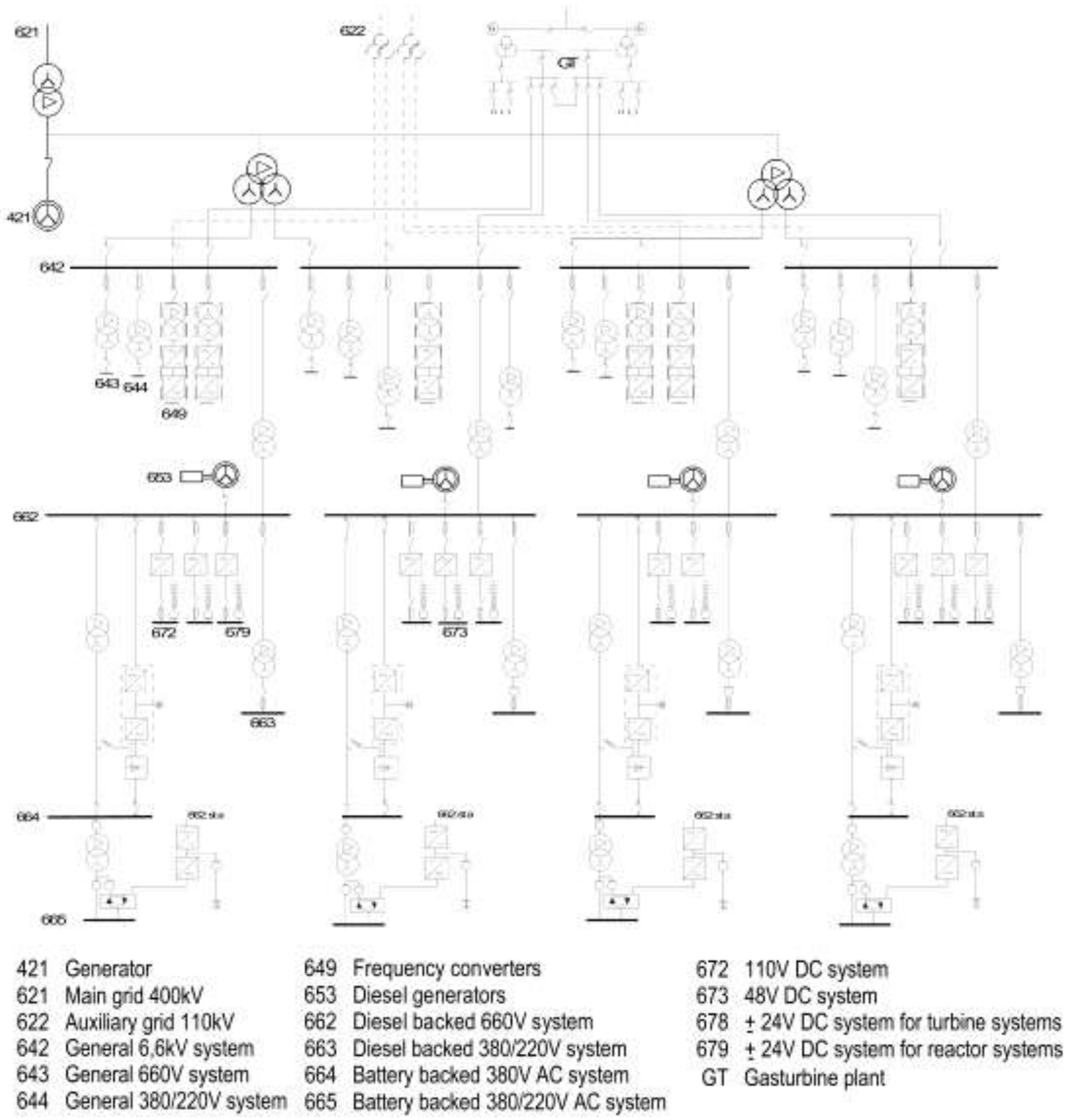


Figure C-4. OL1 and OL2 electric main diagram [TVO 2011]

C.5.1.1 Loss of off-site power

The connection of the OL1 and OL2 to the Nordic 400 kV power grid is implemented with several independent 400 kV overhead lines running from the Olkiluoto switchyard to different grid nodes. Damage of a single 400 kV overhead line will not cause the loss of 400 kV grid connection. In addition, both plant units are connected to the national 110 kV power grid. The connection is implemented with two separate transmission lines.

House load operation is the first defence line against the losing of the 400 kV grid connection. If this automatic switchover is successful, the plant can continue the house load operation indefinitely.

If the 400 kV grid connection is lost and the house load operation is not possible, the units will try to switch to the national 110 kV power grid. The switchover is automatic and can take place within 1…2 seconds. If the 110 kV grid is available but the automatic switchover fails, operators can make the connection manually.

Switchgears (642) critical to the grid connections and house load operation are located at level +3.5 m in two fire compartments.

The main defence line against loss of AC power is emergency diesel generators (EDGs). OL1 and OL2 have four individual EDGs per plant. The capacity of the EDG-system is 4×50% and the generators and the switchgear of safety loads are located in two separate safeguard buildings per plant. Each EDG is in its own diesel room that is an own fire compartment at +3.5 m level. The switch gears of safety loads (662) are at +12.25 m level also in their own fire compartments. The load shedding relay logics are installed two relay rooms located at +3.5 m level. The cooling of the EDGs is dependent on the operation of the service water system.

If the off-site power is lost, EDGs will start automatically within 10 s and provide power to the safety systems. If automatic start-up is not successful, EDGs can be started and connected manually, either from the main control room or locally.

Each EDG has a fuel tank (day tank) with fuel enough for 8 h of operation. These day tanks are automatically filled from an outdoors storage tank. There is one storage tank per plant and one storage tank holds enough fuel for one week of EDG operation (all four EDGs running at full nominal power).

All actions mentioned above are instructed and the operating staff is capable of performing them. The loss of off-site power situations are a part of the standard operator training and they are rehearsed frequently at the training simulator.

C.5.1.2 Loss of off-site power and loss of the ordinary back-up AC power sources

If the EDG operation is not successful, emergency back-up power can be provided from a gas turbine plant. The gas turbine plant has two 50 MW generator units, each with two gas turbines. Each gas turbine alone is capable of providing the required emergency power to all Olkiluoto units (OL1, OL2, OL3). The gas turbine plant is located above +3.5 m. The plant is separated from nuclear units and is air cooled.

The gas turbine plant has dedicated cable connections to the 6.6 kV bus bars of OL1 and OL2 but it can also be connected via the 110 kV switchyard. Switchgears (642) needed to the gas turbine connection are located at level +3.5 m (see Section C.5.1.1).

The gas turbine plant has to be started and connected manually, but operators can perform all the required operations from the main control rooms of OL1 and OL2. Also local operations are possible. Required main control room operations can be performed within 5-15 minutes. It is a normal operational procedure to start the gas turbine plant immediately after a loss of off-site power regardless of the operation of EDGs.

The gas turbine plant has storage tanks with combined fuel capacity of 48 hours of use at full nominal power. In emergency situations when the gas turbine plant is used to support OL1, OL2 and OL3 units, it is sufficient to use only one gas turbine providing 20 MW of power. This will limit the fuel consumption so that fuel will last for about 9 days.

It is also possible to provide EDG power between OL1 and OL2. At the most, two EDGs can be connected from one plant unit to another. Therefore, the four EDGs of one unit can be used to provide all the necessary emergency power to both units. The cable connections between the plant units are permanent and they travel below the ground, but the required manual switching operations have to be made locally. It is estimated that in a normal situation this can be done within 30…60 minutes, but in some cases the connections may require 1…3 hours.

If the 110 kV grid connection is physically intact but the power grid is lost due to a major grid disturbance, it is possible to serve the Olkiluoto units by establishing a dedicated connection to a nearby hydroelectric power plant. The capacity of this connection is estimated to be sufficient to supply power to support the safety functions of existing units OL1&2 and OL3 under construction. The connection can be build remotely from the control room of the national grid operator or using manual switch operations. If the connection succeeds automatically by sequence control, the connection time is approx. 10 minutes. If the connections require manual remote controls, the required time is approx. 30 minutes. If local controls are required, the connection time is approx. 2…3 hours.

In addition, there is a separate 20 kV utility line coming from local electrical company. The line serves normally Olkiluoto outdoor area but can, if required, be manually connected to provide electricity to OL1 and OL2. The line has very limited capacity. The required manual connection operations are instructed but they may require 3…6 hours of time. The switchgears of the 20 kV system are located at and under +3,5 m level.

All actions mentioned above are instructed and the operating staff is capable of performing them. Loss of off-site power situations are a part of the standard operator training and they are rehearsed frequently at the training simulator.

Battery capacity issue is described in Section C.5.1.3.

C.5.1.3 Loss of off-site power and loss of the ordinary back-up AC power sources, and loss of permanently installed diverse back-up AC power sources

Battery backed electrical systems are located in four separated redundancies A...D. The capacity of the redundant safety systems is 4×50% in all important (SC2) functions. Capacity is 2×100% in some lower class safety functions. Each redundancy is in its own fire compartment. The lowest equipment rooms are in level +10.50.

The list below presents the capacities and loads supplied by each battery-backed system:

- System 664 "Battery backed 380 V AC system (UPS)"
  - 4 redundant systems
  - Electric actuators, control room lighting, separate sub-switchgears (SAM-busbars) and reserve supply for system 665 if EDG-backed switch gear of safety loads (662) has a long-standing fault and the batteries for 665 are exhausted
  - Discharge time 16...63 h if not feeding 665
  - Discharge time 13...30 h if feeding 665 (normal connection)
- System 665 "Battery backed 220 and 380/220 V AC system (UPS)"
  - 4 redundant systems
  - Contactors, measurement transducers, computers, controllers, positioners, recorders, neutron flux measuring equipment, damper operating devices and auxiliary power for 649 main reactor coolant pump (RCP) frequency converters
  - Discharge time 3.8...9.5 h, but system 664 is feeding this system after the discharge of the batteries. For total discharge time see system 664.
- System 672 "110 V DC system"
  - 4 redundant systems
  - Circuit breaker motors, switches, solenoid valves, control circuits and relays of system 516 (Reactor protection system)
  - Discharge time 32...44 h
- System 673 "48 V DC system"
  - 2 redundant systems
  - Indicating lamps and certain automatic control cubicles of the turbine installation
  - Discharge time 100...110 h
- System 677 "24 V DC system"
  - 2 redundant systems (in different redundancies from 673)
  - System 548 (Containment monitoring system) additional containment instrumentation, SAM system radiation monitorings 553 (Stack radiation monitors)
  - Discharge time 32 h after a loss of power from UPS system 664 (see above)
- System 678 "+/– 24 V DC system for turbine systems"
  - Electronic equipments of the turbine
  - Discharge time 54 h (+ side) and 120 h (– side)
- System 679 "+/– 24 V DC system for reactor systems"
  - 4 redundant systems
  - Reactor island automation (Combimatic control system)
  - Discharge time 52...58 h (for + side; – side times are longer)

It is possible to charge the batteries using the power sources mentioned in sections C.5.1.1 and C.5.1.2. In a longer-standing fault scenario, the fixed rectifiers of direct current systems may be replaced by transportable rectifiers on wheels. There are transportable rectifiers for all DC voltage levels, and both plant units have their own. The transportable rectifiers are technically similar to the fixed ones. Supply for the transportable rectifiers may normally be taken from the diesel-backed power outlets (system 663) next to the battery rooms, or, if necessary, from any other power outlet, as long as the supply is brought in near the battery rooms. The transportable rectifiers are connected to the load test connectors on the direct current side.

DC-batteries feeding the severe accident handling systems (677) can be also charged by mobile generators. The generators are stored in the plant area and they can be connected to permanently wired sockets outside plant buildings at level +4.8 m. The connections for the diesel generators have been instructed. If needed, the transfer and connection of the generators are managed by the Olkiluoto fire brigade. There are at least 32 h discharging time before the charging of these batteries must be started.

If all AC power is lost at the time of reactor scram (station blackout), the top of the fuel elements will be uncovered in about 30…35 minutes. Core damage (fuel cladding temperature exceeding 1204°C) will commence about 25…30 minutes later, i.e. about one hour after the scram.

The time available to prevent core damage is increased the more time has passed since the reactor shutdown. If station blackout causes the loss of the core cooling 8 hours after the reactor shutdown, the top of the fuel elements will be uncovered in about 90…100 minutes and core damage will commence about 1…2.5 h later (i.e. about 2.5…4 h after the station blackout), depending when the depressurisation of the reactor has been performed.

If station blackout causes the loss of the core cooling 16 hours after the reactor shutdown, the top of the fuel elements will be uncovered in about 110…120 minutes and core damage will commence about 1…3 h later (i.e. about 3…5 h after the station blackout), depending when the depressurisation of the reactor has been performed.

If station blackout causes the loss of the core cooling 24 h after the reactor shutdown, the top of the fuel elements will be uncovered in about 130 minutes and core damage will commence about 1.5…3.5 h later (i.e. about 3.5…5.5 h after the station blackout), depending when the depressurisation of the reactor has been performed.

During the loss of all AC power, removal of the decay heat from the spent fuel elements in the reactor building fuel pools to the sea water is prevented. The limiting worst-case situation for the available time is the evacuation of the whole reactor core to the east pool with closed connection to the reactor pool. The decay heat power three days after the shutdown is about 10 MW. If the pool cooling is lost in such a situation, the pool water will start boiling in about six hours. About 20 h after the start of the boiling, radiation level will start to the increase rapidly as the water-level will be down to one meter above the top of the fuel elements. About 3.5 h after that, the top of the fuel elements will be uncovered. To prevent the water-level drop in the pools, make-up water supply of about 4.5 kg/s would be needed to compensate for the boiling.

Normally, the decay heat generated by the spent fuel elements stored in the reactor building fuel pools is much less. In this situation, the total loss of pool cooling would cause the pool water temperature to rise with the rate of about 1°C/h. That would mean that the uncovering of the fuel elements would take about two weeks. In this situation, make-up water supply of about 0.3…0.4 kg/s would be needed to compensate for the boiling.

Make-up water can be delivered to the pools using the fire fighting water system 861 and the fire fighting pumps, which are equipped with their own diesel engines and are therefore independent of the AC power supply. If required, make-up water can also be pumped using the transferable pumps from the fire brigade.

Maximum heating power in the spent fuel storage is 1 MW per pool. The heating time from 32°C to 100°C is about 59 h. Level decrease due the boiling to the level where radiation level starts to increase significantly in the storage hall is around 10 days. Amount of make-up water to the pool needed to compensate for boiling is 0.39 kg/s.

C.5.1.4 Conclusions on the adequacy of protection against loss of electrical power

The protection against the loss of electrical power is quite adequate. Both OL1 and OL2 units have several possibilities to recover from a loss of off-site power situation. The available means incorporate both redundancy and diversity, which makes the total loss of all electrical power an extremely unlikely event. The initiating events as well as system dependencies related to the supply of electric power have been carefully analysed in the probabilistic safety assessment and, even though loss of off-site power events have a significant risk contribution, the absolute risk has been analysed to be acceptable and to be in balance with the overall risk profile of the units.

However the time margin for the recovery of the AC-power supply before fuel damage is quite short if a total loss of the AC-power occurs. Core damage (fuel cladding temperature exceeding 1204°C) will commence about 55...65 min after the start of the blackout. After this the situation must be handled using severe accident management systems. The power company (TVO) is already planning plant modifications to enhance the situation (see Section C.5.1.5).

Limiting battery capacities are from 13 h to 30 h (664) depending of the redundancy. This is adequate compared to the time after which must be start to use the severe accident handling systems. Battery capacity of the severe accident management systems is described in Section C.6.

OL1 and OL2 have adequate autonomy of diesel fuel. The units have fuel at least for one week.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan and schedule to secure decay heat removal from OL1 and OL2 reactors in case of total loss of AC power sources, and to secure DC power for long time needs. Also Licensee was required to investigate the need, and to provide a plan and schedule if seen necessary, to secure fuel reserve for emergency power.

Furthermore, the Licensee is required to investigate the availability and operability of safety systems and their components in accidents of long duration and investigate needs and possibilities to use mobile power supply and mobile pumps in accidents.

C.5.1.5 Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power

At present the power company (TVO) is planning several modifications that can provide extra protection.

Already for several years, TVO has been preparing the possible renewal of all the eight emergency diesel generators (OL1 and OL2). Several plans, surveys and studies have been prepared for this project and TVO is at present considering it but so far no investment decision for the EDG renewal has been made. The proposed renewal plan includes several safety improvements. First of all, the new EDGs would be equipped with two diverse component cooling systems. The primary EDG cooling would be provided by the sea water based cooling system (712), similar to present EDGs units, but an alternative, automatically activated air based cooling system would be added to cope with the loss of sea water situations. This would provide extra protection against external hazards, internal hazards such as fires, as well as component failures.

Also, one extra EDG, a so-called 9th EDG, would be set up. This EDG would be located in a new, separate diesel building and, if needed, it could be connected to supply electric power to either OL1 or OL2. The 9th EDG could also be placed above ground level to improve protection against external flooding.

To respond to STUK's requirements after Fukushima accident, Licensee is studying the following issues.

An independent way of pumping water to the reactor pressure vessel is being considered. The present pipe connections would make it possible to pump water to the reactor from the fire fighting water system but the diesel driven fire fighting pumps available for the task do not have enough pumping head to overcome the counterpressure created by the containment filtered venting and the reactor pressure relief systems (systems 362 and 314). Therefore, a pressure booster would have to be added to the pumping route. As the time available for recovery actions may be quite limited, the booster pump would have to be fitted permanently and it would require a dedicated diesel engine or diesel generator for operating power supplied through a simple dedicated electric power system. Such a system would provide an independent way to supply water to the reactor and it would be available irrespective of the operation of the present backup power systems.

It is also possible to supply electrical power from the main generator of OL1 to OL2 or vice versa using the connections at the 400 kV switchyard. The instructions and procedures for these actions are being prepared at present. When OL3 unit starts operation, the main generator of each unit can be used to supply electrical power to the other units using the 400 kV switchyard connections.

To secure recharging of DC batteries, Licensee is investigating the possibilities for fixed connection points that would facilitate the use of transportable power generators and for recharging of the safety important batteries using transportable devices. The possible acquisition and use of transportable power generators for other supporting tasks, e.g. to recharge the batteries of the weather measurement instrumentation, is also under investigation.

Licensee has evaluated that the fuel reservoirs for diesel generators at the plant site are adequate. Furthermore, Licensee has secured long-term supply of the fuel with the supplier, which ensures that fuel requested by the Licensee is available. The fuel transportation to Olkiluoto NPP is dealt with a high priority.

Licensee has initiated an investigation to secure electrical power by mobile aggregates. Investigation includes also renewal of the present SAM diesel generators. Pre-planning of the arrangements is going to be ready in 2012 and possible installation are estimated to be carried out in 2013.

C.5.2 Loss of the decay heat removal capability/ultimate heat sink

C.5.2.1 Design provisions to prevent the loss of the primary ultimate heat sink

Sea water is the primary ultimate heat sink for OL1 and OL2. The sea water inlet is equipped with coarse and fine intake screens as well as travelling basket filters that will prevent fish and other foreign matter from being sucked into the water pumps and heat exchangers.

Oil booms are permanently stored in containers next to the inlet channels and can be installed with a short notice to protect the inlet channels from marine oil spills. More oil booms will soon be stored on the nearby islands on the inlet side.

If the inlet tunnel is blocked, it is possible to switch the water intake to the outlet side. In this case the water going to the auxiliary buildings is taken from the water outlet. This provides a sufficient water flow for the safety systems.

During winter time when the sea water temperature drops below +2°C, warm water is pumped from the outlet side to the inlet side in order to prevent the formation of frazil ice at the intake screens. In addition, as a precaution to minimise the consequences of possible frazil ice formation, the water intake of two safety trains will be switched to the outlet side.

The actions to be performed when either the inlet channel or the outlet channel is blocked are instructed and rehearsed.

C.5.2.2 Loss of the primary ultimate heat sink

At present, sea water is the primary ultimate heat sink for OL1 and OL2 and an alternate heat sink exists only partially. Both units can evaporate residual heat from the reactor core to atmosphere by conducting the steam produced inside the reactor pressure vessel to the condensation pool through the safety relief valves of the relief system 314, by letting the condensation pool to boil, and by venting the steam from the containment to atmosphere through the filtered venting system (362). However, the systems required to pump water into the reactor pressure vessel are either dependent on the sea water based component cooling systems (auxiliary feed water system 327, main feed water system 445) or on the condensation pool water (core spray system 323), which means that the complete loss of sea water as the ultimate heat sink will eventually prevent the supply of water to the reactor pressure vessel. System 323 will remain operational until the condensation pool water temperature reaches about 100°C, after which the pumps will fail due to cavitation.

The water in the condensation pool can act as a temporary heat sink but eventually the heat has to be transferred to either sea water or atmosphere, otherwise the structural integrity of the containment may be lost. Atmosphere could be used as an alternate heat sink indefinitely, but, at present, transferring residual heat to atmosphere is not a definitive solution as the lack of component cooling and the boiling of the condensation pool will eventually lead into the loss of water supply to the reactor. However, as system 323 is able to pump water to the reactor pressure vessel until the condensation pool water temperature reaches about 100°C, the time constraints related to the loss of the primary ultimate heat sink (sea water) are longer than those related to the station blackout situations.

C.5.2.3 Loss of the primary ultimate heat sink and the alternate heat sink

Reactors

According to the investigations by the licensee, the loss of atmosphere as an alternate heat sink does not affect the time estimates presented later in this section. The pressure inside the containment was in the studied cases so low that there was no need for venting. The need for containment pressure relief by the means of filtered venting would arise only later in time. Therefore, the condensation pool heat-up is at present the limiting time factor.

At present the only ways to prevent the eventual core degradation due to the loss of the primary ultimate heat sink would be to resolve the problems, e.g. component failures, blockage of the water tunnels or blinding of the intake screens, that originally caused the loss of use of sea water, or to organise some alternative cooling method that could be used to cool the auxiliary feed water pumps (327), which could then be able to supply water to the reactor from the demineralised water tanks (733), or to cool the containment spray system (322) heat exchangers, which could then be able to remove heat from the condensation pool and prevent the core spray pump (323) cavitation. Due to the difficulty to predict all the circumstances related to the possible loss of primary ultimate heat sink situations, there are no ready-made instructions or plans for all these conceivable actions.

If the use of the primary ultimate heat sink (sea water) is completely lost (LUHS) already at the time of reactor scram, the system 323 will be able to supply water to the reactor for approximately 4 h, after which the condensation pool water temperature will exceed 95°C and pump cavitation will soon become likely. Core uncovering (top of the fuel elements) will take place about one hour after the loss of the 323 pumping and core damage (maximum cladding temperature exceeds 1204°C) will commence about 2…2.5 h later, i.e. about 7…7.5 h after the LUHS.

If the use of the primary ultimate heat sink is lost 8 h after the reactor shutdown, system 323 will be able to supply water for about 6 h after that. Core uncovering will take place about 1.5 h after the loss of the 323 pumping and core damage will commence about 3 h later, i.e. about 10-11 h after the LUHS.

If the use of the primary ultimate heat sink is lost 16 h after the reactor shutdown, system 323 will be able to supply water for about 7…8 h after that. Core uncovering will take place about 1.5…2 h after the loss of the 323 pumping and core damage will commence about 3…4 h later, i.e. about 12…13 h after the LUHS.

If the use of the primary ultimate heat sink is lost 24 h after the reactor shutdown, system 323 will be able to supply water for about 8…9 h after that. Core uncovering will take place about 2 h after the loss of the 323 pumping and core damage will commence about 3…4 h later, i.e. about 14 h after the LUHS.

It is also possible to provide cool, extra water to the containment and containment pool and this way to extend the time span before the containment pool reaches cavitation temperature. One possibility to do this is to follow the severe accident management procedure for containment water filling. The containment water filling is implemented from the outside using the fire fighting water pumps and water reservoir. This operation is not dependent on the usability of the ultimate heat sink. If, for example, the primary ultimate heat sink is lost 24 h after the reactor shutdown and the containment water filling is started one hour after that, the system 323 will be able to supply water for 15…17 h after that. Core uncovering will take place about 2…2.5 h after the loss of the 323 pumping and core damage will commence about 4 h later, i.e. about 21…23 h after the LUHS.

The above mentioned times were calculated using MELCOR 1.8.6 and they were conservative by assuming that the heat distribution within the condensation pool is not even, i.e. the bottom layer of the pool water does not absorb any significant amount of heat but remains cool. Therefore, the whole condensation pool water volume (2700 m^3) was not taken into account but only about 2000 m^3 of water was used in the calculation of the heat-up times for the condensation pool. Recent temperature measurements made from the condensation pool suggest that the mixing of the pool water is effective when 323 pumping is active and, therefore, the real-life condensation pool heat-up times for situations, where electricity is available, are likely longer than those given by the above mentioned conservative MELCOR calculations. Another point of conservatism was the use of 95°C as the threshold temperature for the pump cavitation and the end time for 323 pumping. The exact cavitation temperature is not known and some estimates suggest that the pumps might remain operational even up to water temperatures close to 120°C.

According to the MELCOR-calculations using the full condensation pool water volume (2700 m^3), the effect of the pool volume is considerable. For example, if the use of the primary ultimate heat sink is completely lost already at the time of reactor scram, the system 323 will be able to supply water to the reactor for approximately 6…7 h, instead of the 4 hours calculated with the smaller 2000 m^3 water volume. Similarly, if the pump cavitation does not start until water temperature reaches, e.g., 110°C, pumping operation could be continued for 1…2 h longer. The conservative calculation features explained here relate also to the severe accident progression (Section C.6).

The amount of water (2700 m^3) inside the condensation pool cannot be increased permanently because the present balance between wetwell gas volume and water volume is important for the pressure suppression function needed e.g. in LOCA cases. External water supply to the pool may be useful in some cases, as shown above with the example concerning the containment water filling, but the drawback of this strategy is the decrease of the containment gas volume.

Spent fuel pools

Sea water is the primary ultimate heat sink for the decay heat generated by the spent fuel elements stored in the spent fuel pools. Both OL1 and OL2 have two storage pools for temporary storage of fuel elements that have been removed from the reactor. In addition, both units have a reactor pool, includes pools for steam separator and steam drier. Reactor pool is located between the two other pools. All three pools are located in the reactor hall, above the containment. The pools are connected to each others with gates that can be closed. The dimensions of the pools are given in Table C-2. The number of fuel elements that can be stored in the pools depends on the number of low density and high density spent fuel storage racks. The top of the fuel elements is 4.7 m from the bottom of the pool, i.e. there is about 7 m of water above the fuel elements. Here, it has been estimated that the fuel elements and racks occupy 10% of the pool volume.

Table C-2. Dimensions of the spent fuel pools at OL1 and OL2.

	Volume (m^3)	Water volume (m^3)	Surface area (m^2)	Max number of fuel elements OL1/OL2
West pool	910	820	78	840/480
East pool	630	570	570	680/1080
Reactor pool		ca. 2100	ca. 250	

The information given in Section C.5.1 concerning the loss of electrical power applies also to the loss of the ultimate heat sink with two exceptions. The gates connecting the reactor pool to the two spent fuel pools may readily be opened if electricity is available. If needed, this will help to ensure that the water volume in the pools is as large as possible in order to increase the time available to provide the required make-up water supply. The availability of AC power will also enable the utilisation of the reactor building ventilation system (742) and the vent gas filtering system (749).

The KPA storage has three pools of the volume of 750 m^3 each. Normal situation in the KPA storage is that all fuel pool doors are open. This increases the amount of water volume available for heat absorption and boiling. If electricity is lost from the spent fuel storage, heat removal from the pools is prevented.

When doors are closed between fuel pools and assumed heating power is maximum which is specified in the Technical Specifications (1 MW per pool), the heating time from 32°C to 100°C is about 59 h. Amount of make-up water to the pool needed to compensate for boiling is 0.39 kg/s, 33.4 m^3/d per pool in that case. Level decrease due the boiling to the level where radiation level starts to increase significantly in the hall is around 10 days.

According to the licensee's calculations, the total heat generation of KPA storage September 9th 2011 was 1225 kW. Considering a sudden loss of heat sink with this heat generation, the time before boiling starts in the KPA storage when fuel pool doors are open is around 8.5 days. Level decrease due the boiling to the level where radiation level starts to increase significantly in the hall is around 43 days.

C.5.2.4 Conclusions on the adequacy of protection against loss of ultimate heat sink

At present, both OL1 and OL2 are dependent on the use of sea water as the ultimate heat sink and the prevention of core degradation may be impossible if the use of sea water is lost for an extended period of time. Nevertheless, with the probabilistic analysis, the licensee has demonstrated that the level of plant protections and provisions implemented e.g. technical modifications and operating procedures against the loss of ultimate heat sink fulfil the requirements for the acceptable risk level of ultimate heat sink due to external phenomena taking into account the Olkiluoto site conditions and prevailing external conditions.

Considering the potential impact of the climate change and the recent experiences of the Fukushima accident, there are relevant plant modifications that could be implemented to further improve the level of protection against the complete loss of sea water as the ultimate heat sink, and accordingly, to improve the plant safety by facilitating the use of atmosphere as an alternate ultimate heat sink.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan and schedule to secure operation of the auxiliary feed water system for accidents involving loss of seawater as ultimate heat sink, and to secure decay heat removal from the fuel storage pools located in the reactor building in case of loss of existing systems.

Furthermore, the Licensee was required to investigate alternative methods to supply coolant to the fuel storage pools (including a potential need for new instrumentation) and possibilities to secure availability of demineralised water at the site in an accident of long duration.

C.5.2.5 Measures which can be envisaged to increase robustness of the plant in case of loss of ultimate heat sink

The licensee has considered some potential plant modifications, which can increase the robustness of the plant in case of the loss of the primary ultimate heat sink. Sea water is not necessarily needed as the ultimate heat sink for the residual heat from the reactor core, because the design of the containment and containment systems enables the transferring of residual heat from the reactor core to atmosphere by using the condensation pool as a temporary heat sink and by venting the steam from the boiling condensation pool to atmosphere through the filtered venting system of the containment. Because the venting system (362) is filtered and designed to work in severe accident conditions, the possible release of radioactivity to environment can be effectively limited even in the case of severe core degradation. If necessary, steam and other gases can be vented from the containment to atmosphere also by using the unfiltered containment venting system (361).

The use of this strategy is, however, at present hindered by the component cooling requirements of those safety systems that could be used to supply water to the reactor. The use of atmosphere as an efficient, alternate heat sink can be realised by removing the need for sea water based component cooling from the pumps of the auxiliary feed water system (327). If this system was not dependent on sea water based component cooling, it could remain operational even during the loss of the primary ultimate heat sink (sea water), and, as system 327 would use water from the 733 water tanks, boiling of the condensation pool would not affect the operation of the pumps. At present, Licensee is planning this kind of modification and Licensee's preliminary probabilistic risk analyses show that the suggested modification could result in a notable safety improvement.

The possible renewal of all emergency diesel generators could also provide extra protection against the loss of the primary ultimate heat sink and loss of off-site power situations. If the new emergency diesel generators would be equipped with double component cooling systems that could use sea water or atmosphere as heat sink, the robustness of the safety systems would be improved further (see also Section C.5.1.5).

To respond to STUK's requirements after Fukushima accident, Licensee is planning several modifications that can provide extra protection:

An additional arrangement for removing residual heat from the reactor and containment in the case of loss of the existing cooling systems or their power supply has been suggested by Licensee. The arrangement could be based on the fire fighting water system but additional booster pumps would be needed (see also Section C.5.1.5). The design basis of the new equipment has not been decided, but the need to consider extreme flooding will be assessed.

The licensee is also strengthening the protection against marine oil spills. In addition to the oil booms stored next to the water inlet channels, extra oil booms have been stored on the nearby islands. The instructions for taking them in use are under preparation, but the equipment would be available if needed, already.

The measures to increase the KPA storage robustness against the loss of electrical supply, applies to the loss of heat sink, as well.

Additionally, external junctions to the KPA storage pool water system will be added during the extension project of spent fuel storage. Feed of water to the fuel storage pools will be possible from fire-fighting vehicle via those junctions.

C.5.3 Loss of the primary ultimate heat sink, combined with station blackout

C.5.3.1 Time of autonomy of the site before loss of normal cooling condition of the reactor core and spent fuel pool

The station blackout (loss of all AC power) leads into core degradation more rapidly than the loss of the primary ultimate heat sink. Therefore, the information given in Section

C.5.1 is representative also of the combination of the loss of the primary ultimate heat sink with station blackout.

C.5.3.2 External actions foreseen to prevent fuel degradation

The conceivable, preventive actions are discussed in Sections B.5.1.2 and B.5.2.3 in context of the station blackout and the loss of the primary ultimate heat sink situations.

C.5.3.3 Measures, which can be envisaged to increase robustness of the plant in case of loss of primary ultimate heat sink, combined with station blackout

The potential measures are discussed in Sections C.5.1.5 and C.5.2.5 in context of the station blackout and the loss of the primary ultimate heat sink situations.

C.6 Severe accident management

C.6.1 Organization and arrangements of the licensee to manage accidents

C.6.1.1 Organisation of the licensee to manage the accident

<u>Organization during normal operation and accidents</u>

The shift personnel are divided into shifts, each consisting of shift supervisor, reactor operator, turbine operator, area work supervisor and two or three field operators. Additional licensed operators may be assigned to each shift for relief or staff augmentation as required during labour-intensive evolutions such as plant start-ups or shutdowns. The shift personnel, plant's fire brigade and security personnel are working continuously 24/7. Additionally, the power plant's manager in charge and the on-duty safety engineer are on-call outside daytime working hours.

During normal office time the managers, the specialists and maintenance personnel at plant assist operating shifts in the normal operation. In addition to the personnel mentioned above, there are extra personnel at the power plant during the annual outages.

During a plant disturbance, the shift supervisor must lead the activities of the shift, monitor plant unit status and supervise that all necessary measures are carried out without delay. The power plant on-duty safety engineer assists the shift supervisor. During non-working hours the on-duty safety engineer shall arrive on site within 40 minutes of notification.

Plans for strengthening the site organization include formation of emergency preparedness organization at the site. During the first stages of an emergency preparedness situation, the shift supervisor acts as emergency manager until one of the qualified emergency manager is present. Based on practical experience the emergency preparedness organization is estimated to be in operational readiness 15 minutes after receiving the alarm during normal working hours and one hour after receiving the alarm outside normal working hours. Emergency preparedness is taken into account in the company's Activity Based Management System, and Olkiluoto Emergency Plan (OEP) contains a description of the emergency arrangements at Olkiluoto power plant and instructions for the members of company's emergency organization and for the employees of the plant.

The emergency organization activities are arranged so that responsibilities and procedures remain as near normal as possible. The emergency organisation has been sized to allow operation also in a prolonged situation. At least five qualified persons are available to the most important positions.

Licensee's assessment is that the personnel of the operations organisation are adequate for prolonged accident conditions that concern several plant units. If emergency conditions emerge, more competent personnel are obtained from the emergency organisation. The staffing of radiation protection patrols and fire brigade in the OEP is based on an assumption of emergency in one power plant unit. Licensee's view is that there would be no need to increase the number of radiation protection patrols, although emergency situation would take place in more than one unit at the same time.

In all emergency situations TVO alarms or notifies STUK and the rescue service of Rauma district. The Rauma district fire chief of Satakunta rescue services is the director of all off-site activities. Through the district alarm centre he notifies and alerts other local authorities and rescue organizations at the communal, county and national levels. To recover and maintain normal operation of the site the help of police, rescue services, coast guard and military forces is available after request.

Radiation protection gears

Personal radiation protection gears are stored in several storages like at the boundaries of the controlled area. The protective gears and measuring instruments for the radiation measuring patrols is readily available at the shelter. In the fire station, in the laboratory and in the shelter there are protective masks with filters for use by these personnel. Iodine pills are stored in the shelter and in the emergency centres.

Control rooms and emergency centres

The main control rooms (MCR) are shielded against radiation and have filtered emergency ventilation systems. There are no secondary control rooms in OL1 and OL2 at the moment.

Each plant unit has an emergency centre, and there is a common sheltered reserve centre. The management of the emergency organization activates one emergency centre and normally the technical support group will occupy the reserve emergency centre. All emergency centres are shielded against radiation and have filtered emergency ventilation systems. Each emergency centre is provided with several communication systems and has access to process and weather parameters and to the readings of on-site and near-site radiation monitors.

In addition to the emergency centres at site, TVO has an opportunity to use air raid shelter facilities of town Rauma. The material needed in management of emergency situation has been gathered in these facilities.

Procedures, training and exercises

There are event-oriented operating procedures for events within design, ranging from insignificant disturbances to postulated design basis accidents. The reactor protection system and the engineered safety systems are automated to function so that no operator actions are needed during the first 30 minutes after an incident or an accident. It is assumed that the allowed operator response time of 30 minutes is enough for finding out what has happened and which procedure to follow.

If the reactor protection systems or some of the safety systems fail, a disturbance may develop into an emergency condition beyond design. The same may happen, if the initiating event is more severe than what has been postulated within the design basis. To cope with emergency conditions beyond design, a set of symptom-based emergency operating procedures (EOPs) is available. The actions included in the EOPs aim at restoring the operation of the normal safety systems.

The procedures contain guidance as to where the information required can be obtained and how the different operator actions can be performed. The availability of the information required by the procedures has been verified with control room walk-through exercises, where only the analogy display devices in the control room were credited. A computer-based safety parameter display system (SPDS) is also available. For each symptom-based procedure, the SPDS has a specific recipe which shows the information required by that procedure in a concentrated form as one or two display pages.

All persons working at the power plant receive basic emergency information during the induction course, written material is also available. Yearly emergency preparedness training sessions are conducted on general issues for all employees, and on specific respective roles and tasks within the emergency preparedness organization. Training is also arranged for rescue services, police and other municipal authorities.

Power plant operators are required to participate in the simulator training every year. Transient and emergency instructions are evaluated as a part of these training sessions. In addition to the revision of the instructions during training, all the instructions are assessed regularly. The simulator offers an authentic environment for carrying out operations during an emergency situation. Certain emergency exercises are also conducted with the aid of the simulator. In order to make operator training more effective, a PC-simulator has been developed to illustrate severe accident phenomena.

Official emergency exercises are held annually. Every third year a nation wide emergency exercise of the plant is held.

C.6.1.2 Possibility to use existing equipment

The severe accident approach with the specific systems to manage severe accidents is explained in more detail in Section C.6.3.

Mobile equipment plays a very limited part in the accident management schemes. There are two small (23 kW) mobile diesel generators, which can be used for two purposes:

- for recharging the batteries in a dedicated DC system (capacity for 24 hours), which in case all other sources of electricity have been lost, supplies power to dedicated instrumentation system for monitoring the conditions inside the reactor containment in connection with severe accidents; and
- for opening certain valves in order to allow water to be injected into the containment from the fire fighting system.

For both of these tasks, there is plenty of time (several hours) to start the operation. The mobile generators are stored and operated by the plant fire brigade. The instructions for switching in the generators have been written and verified.

There is enough fuel at the site for one week of continuous operation of the emergency diesel generators. For the gas turbine plant, fuel is also available at the site for one week of continuous operation at the minimum capacity required to supply power to all the safety related loads at the site. The amount of fuel available for the diesel motor driven fire water pumps ensures operation of one fire fighting pump for at least four days.

Some measurements in the dedicated instrumentation system utilize the bubble tube principle, and they need pressurized nitrogen for their operation. The system has pressurized nitrogen containers as a back-up source in case the normal distribution system is lost. The capacity of the containers is enough for 24 hours of operation. Replacement containers are readily available at the site.

At both OL1 and OL2, the amount of demineralised water available for feeding the reactor is at least 900 m^3, which is enough for cooling the core for about 1.5 days.

The final goal for severe accident management measures is to reach a safe stable state of the plant unit. In case of OL1 and OL2, this includes filling the containment with water up to the normal core upper level. For one unit, this would require about 5000 m^3 of water. The amount of fire fighting water available at the site is about 5500 m^3. The raw water basin, which is situated next to the plant site in Korvensuo, contains above 130,000 m^3 of raw water. Due to the higher elevation of the basin surface in relation to the plant site grade level, a gravity driven water flow from the basin to the water treatment plant at the site can be used to replenish the fire water reservoirs. This gravity driven flow has been verified to reach at least 50 kg/s with the normal basin level.

The main means to limit radioactive releases is to maintain the integrity of the containment even in a case of a severe accident. To support this, a containment filtered venting system has been installed, which is discussed in more detail in Section C.6.3.3.

In regard to communication systems, OL1 and OL2 have their own connection facilities, to support operation of the internal telephone connections within the units.

In case of loss of off-site power TVO's internal telephone connections will operate on battery backup for 24 h, and the external landline network and mobile telephone network are estimated to operate for a little less than 24 h. The battery backup arrangements of the mobile telephone network are dependent on the emergency response arrangements of the telephone operators. External communications can be maintained also through VIRVE network.

In addition to battery backup, a change-over switch can be used to obtain power supply from another unit to ensure data connections. Use of an external mobile power source is also possible.

C.6.1.3 Evaluation of factors that may impede accident management and respective contingencies

The number of employees that can be called to the site in postulated prolonged emergency conditions caused by natural phenomena obviously depends on the conditions and the access barriers possibly resulting from the conditions, as well as on the availability of required assistance from authorities. Depending on weather conditions coastal guard boats or helicopters could be used for transportation instead of the road connections. If a natural disaster would hinder access to the site, accident management at the site is possible at least for a week without material replenishment. E.g. inventory of fuel for the emergency diesels and gas turbine is adequate for one week of continuous operation at the capacity required for accident management.

TVO will co-operate with rescue organizations and authorities in order to restore the infrastructure required to support long term accident management. In case of massive destruction of infrastructure, management and administrative measures can be led from company's office facilities in Rauma and Helsinki. A dedicated room in command post facilities of Satakunta Rescue Services in Rauma is also available for such actions.

Power plant's communication facilities are described in Section C.6.1.2. In order to better recover in case of loss of all communication facilities/systems, TVO has decided to obtain satellite telephones to the emergency centres.

Conditions in the plant outside the containment are very important as regards successful accident management. Since local manual operator actions play an important part in the emergency procedures, it is essential that the components which need to be operated remain accessible. The operators have been protected against direct radiation for example by equipping the valves to be operated with remote hand wheels. No manual operations need to be performed in rooms directly adjoining the reactor containment either.

The systems in which manual operations are needed may contain different amounts of radioactive substances. In spite of protective measures elevated direct and scattered radiation levels may arise. Leakage of radioactive material through the containment walls increases radiation levels inside the reactor building, especially if the ventilation is out of operation. Basically the only actions that may be compulsory in almost every accident case are opening or closing the isolation valves of containment depressurisation systems. The hand wheels to open or to close the isolation valves are located behind a 60 cm concrete wall which provides a good shielding against radiation. The need for several manual actions in the reactor building within any short time period is very limited. Hence one person does not have to carry out more than one of the above mentioned operations.

The dose rates on the site may be very high under the radioactive release cloud. Under these conditions only the rescue operations will be carried out. However, in some accident cases and when the weather conditions are favourable, the dose rates on the site will stay at a relatively low level. So the impairment of work performance on the site is always case-specific and depends very much on the weather and the wind direction.

The isolation of control room and starting of the ventilation system for keeping the MCR over-pressurized are manual operations. According to analyses, the MCRs of OL1 and OL2 are habitable regarding also the radiation conditions.

Seismic events were included in the design basis of the systems implemented at the plant units as back fitting to provide possibilities for severe accident mitigation. Peak ground acceleration of 0.1 g was used as the design value (see also Chapter C.2).

If the plant site would be flooded above the grade level for an extended period of time, a severe reactor accident would be the most likely consequence (see also Chapter C.3).

Operability or accessibility of certain systems and components is essential for successful management and mitigation of severe accidents. These components are situated in rooms with floor elevation at the grade level or above. In case of flooding of the plant site, the accident management measures could be jeopardized only if the flood level reaches several tens of centimetres above the grade level.

Total loss of AC power sources would lead to a severe reactor accident. Core uncover would take place within 30 minutes, extensive fuel damage would be caused within an hour and RPV melt through would take 2 to 3 hours. However, the severe accident management measures are independent of the availability of AC power.

- Depressurisation of the reactor pressure vessel can be performed with the help of battery-backed power.
- Flooding of the lower drywell can be performed either with the help of battery-backed power or locally through manual operator actions.
- Water filling of the containment can be performed using diesel motor driven fire water pumps. The required valve operations can be performed partly manually and partly with the help of battery backed power. In case battery-backed power has already been depleted, the valve operations can be powered by mobile diesel generators operated by the fire brigade.
- The actuation of the containment filtered venting system takes place either in a passive manner by bursting of a rupture disk or through manual operator actions.
- The power for the dedicated SAM instrumentation system is provided by a dedicated battery backed system with a capacity for 24 hours of operation. The batteries can be recharged using one or the other available mobile 23 kW diesel generators.

Information on the conditions inside the reactor containment is a precondition for successful accident management. The normal in-containment instrumentation cannot be expected to withstand the environmental conditions during a severe reactor accident. Therefore a dedicated containment monitoring system has been installed as a back fitting measure in order to provide the operators with the information needed for the management of severe accidents.

The containment monitoring system has been designed to operate under the conditions created by a severe accident inside the containment. The system has no radiation or temperature sensitive components inside the containment, and the relevant parts have been protected against missile impacts. The system includes pressure, temperature and water level measurements inside the containment. The measurements have been doubled to achieve tolerance against single failure. In case of a total loss of AC power the system is powered by a dedicated system which can keep the instruments in operation for 24 hours without any external power supply.

An accident which has led to an environmental release in one of the units could also impede the accident management at another unit. For example, the dose rate in some locations at the site may be so high that it will restrict movement at the site. Yet, it has been analysed that the MCRs of other units still remain habitable in spite of the situation of the damaged unit.

C.6.1.4 Conclusions on the adequacy of organisational issues for accident management

It has been stated above that “depending on weather conditions coastal guard boats or helicopters could be used for transportation instead of the road connections”. This might be possible, but this kind of operations may be difficult, and it could be beneficial to have a more detailed investigation on the possibilities for this kind of support in extreme situations in order to have realistic expectations. There is only one road connection to the site, and therefore equipment to restore the lost transport connection, e.g. after extreme weather situations, would be beneficial.

The radiation doses possibly arising from the measures to be carried out during the course of a severe accident have been considered reasonable.

Furthermore, the need for not to increase the number of radiation protection patrols in caes of simultaneous accident in more than one unit will be evaluated by STUK.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee

- to provide a plan and schedule to secure DC power for long time needs;
- to investigate, and if needed to provide a plan to secure fuel reserve for emergency power at the site;
- to investigate the availability (and operability) of safety system and their components in accidents of long duration;
- to investigate the needs and possibilities to use mobile power supply and mobile pumps in accidents;
- to investigate possibilities to secure availability of demineralised water at the site in an accident of long duration; and
- to review the applicability of procedures and availability of personnel in case of accident in multiple units.

Plant improvements in order to provide better possibilities for dealing with station blackout or loss of ultimate heat sink are being planned. This means that EOPs will have to be updated.

C.6.1.5 Measures which can be envisaged to enhance accident management capabilities

Since backfitting measures have already been implemented at the plant units in order to provide possibilities for management and mitigation of severe accidents, no further measures can be envisaged in that respect.

However, in order to improve the possibilities for coping with loss of AC power or loss of main heat sink events, feasibility of certain plant modifications and introduction of new mobile equipment is being studied, as described in sections C.5.1.5 and C.5.2.5 above. Hereby, the aim is not so much to mitigate but to prevent severe accidents.

The survivability of the central building in connection with flooding is still an open question, and the need for further analyses has been recognized. One possible way to proceed could be the extension of the precipitation and ground water analysis concerning the plant yard of OL1 and OL2 to cover the office building, too.

In order to better recover in case of loss of all communication facilities/systems, TVO has decided to obtain satellite telephones to the emergency centres.

C.6.2 Accident management measures in place at the various stages of a scenario of loss of the core cooling function

Figure C-5 shows the overview of the containment of LO1 and OL2.

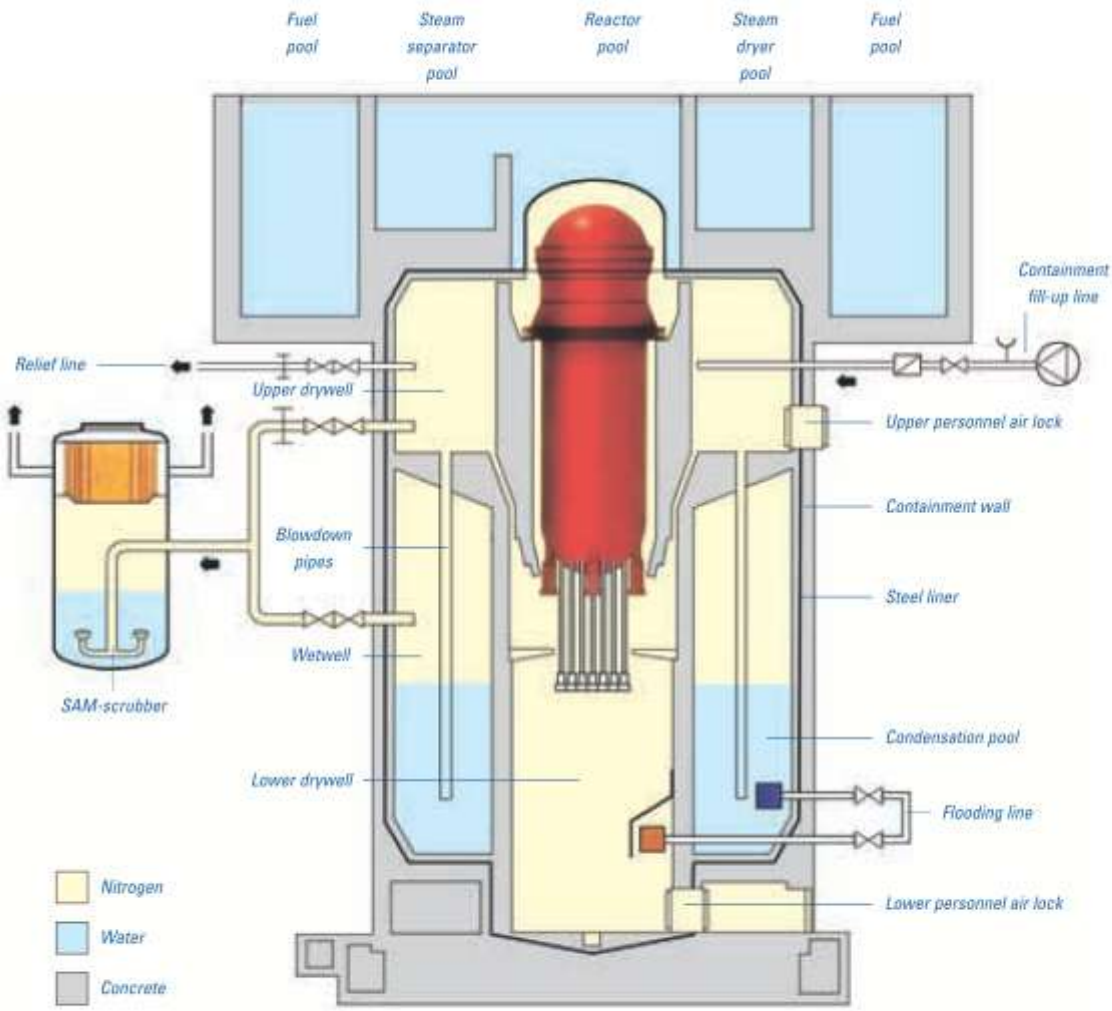


Figure C-5. Containment of OL1 and OL2 [TVO 2008]

General outline of the measures taken at various stages of the accident is given below.

C.6.2.1 Before occurrence of fuel damage in the reactor pressure vessel

The accident management measures included in the symptom based EOPs aim at restoring the operability of the normal safety systems in order to preserve the integrity of the fuel and the primary circuit.

C.6.2.2 After occurrence of fuel damage in the reactor pressure vessel

If it becomes obvious that a severe reactor accident is imminent (if the reactor cannot be made sub-critical or if the reactor water level cannot be restored within a certain time) the operators are guided to start the most time critical severe accident management measures (depressurisation of the reactor, flooding of the reactor cavity). However, the efforts to start core cooling are still continued, until there is a clear indication of pressure vessel melt-through.

C.6.2.3 After failure of the reactor pressure vessel

After failure of the reactor pressure vessel, it is clear that the only intact line of structural defence-in-depth is the reactor containment and that core coolability is no longer possible to restore. However, even at that stage, efforts to start the normal containment heat removal systems are still continued.

C.6.3 Maintaining the containment integrity after occurrence of significant fuel damage in the reactor core

Hardware modifications needed for the management and mitigation of severe accidents (up to core meltdown) were implemented in the plant units in the late 80's in the aftermath of the Chernobyl accident. The main goal for the accident mitigation is preservation of containment integrity and leak tightness, so that if releases from the containment become necessary, they can be performed in a controlled manner and the releases can be filtered. To this end, the following new systems were implemented:

- protection of the penetrations in the lower drywell against direct contact with the molten corium;
- containment filtered venting system;
- system for filling the containment with water from an external source (the fire water reservoir); and
- a dedicated instrumentation system for monitoring the conditions inside the reactor containment in connection with severe accidents.

Even though the management and mitigation of severe accidents was not included in the original design basis of OL1 and OL2, several original plant systems also play an important part in the severe accident management schemes, such as:

- reactor depressurisation system (to prevent pressure vessel melt-through under high pressure);
- devices for gravity driven flooding of the lower drywell (provision for core melt relocation into the compartment); and
- the fire fighting water systems (provides water for filling the containment in order to reach a safe stable state).

Severe accident management systems are introduced in more detail in following sections.

C.6.3.1 Elimination of fuel damage / meltdown at high pressure

Automatic depressurisation of the reactor pressure vessel will be actuated, if the water level in the reactor has been below the level of 0.7 m above the top of active fuel for more than 15 minutes. The depressurisation is performed by opening 8 valves of the reactor relief system. The valves can also be opened manually. To open these valves, battery backed power is needed.

If the automatic depressurisation is not actuated, the accident management procedures (part of the EOPs) will guide the operators to perform a manual depressurisation.

If the battery capacity is depleted, the depressurisation valves will close again. For these sequences, the reactor relief system has two so-called fast opening valves which will open and stay open in case the battery backed power for their control valves is lost. The capacity of these two valves is adequate to keep the reactor pressure at a low level after the depressurisation. Even these two valves have a tendency to close at very low pressures of the reactor (around 2 bar) due to the weight of the valve internals, but they can be locked in the open position using nitrogen from the pressurized nitrogen system or fluid from fire fighting water system. These actions are guided by the accident management procedures.

C.6.3.2 Management of hydrogen risks inside the containment

To prevent hydrogen burns or detonations the containments of OL1 and OL2 plant units are normally nitrogen inerted during power operation. Inerted containment is the main feature for hydrogen management. During power operation only for a short time before shut-down to refuelling outage and after start-up from refuelling outage the oxygen content of the containment atmosphere may be higher than 2%.

The pressure control of hydrogen, and also the control of other non-condensable gases, is based on the containment over-pressurisation protection systems described in Section C.6.3.3.

The limiting case for hydrogen generation assumes that that 100% oxidation of the core zirconium takes place in the lower drywell during 300 seconds after vessel breach. This will produce a total of 1800 kg of hydrogen. Geometry in pressure vessel lower head is assumed to prevent such in-vessel fuel-coolant interactions where large amounts of hydrogen could be generated. The case results in 5.67 bar maximum pressure of the containment. Due to inerted containment, no hydrogen is assumed to burn.

C.6.3.3 Prevention of the containment overpressure

The containment pressure can be decreased by following systems:

- containment vessel spray system (design basis accidents);
- containment over-pressurization protection system (design basis accidents); and
- containment filtered venting system (severe accidents)

Besides the depressurisation function, the spray system and the filtered venting system also remove radioactive substances.

Containment vessel spray system

The containment vessel spray system condenses steam in the containment atmosphere and thus decreases the containment pressure. The spray also washes radioactive particles from containment atmosphere. The system is not dedicated to severe accident management, but if available, it can be used for mitigating the consequences of a severe accident.

Containment over-pressurization protection system

The containment over-pressurisation protection is used if a loss of pressure suppression occurs during LOCA. The system is hence used in conditions beyond original containment design events. In situations indicative of major core damage, this system will be closed in order to eliminate the risk for unfiltered release of activity. The design basis accident for the containment over-pressurization protection system is a guillotine break of one main steam lines inside the containment in combination with a simultaneous 100% break of one RCS blowdown pipe. The system has been designed so that the maximum pressure inside the containment does not exceed 7.5 bar.

The over-pressurization protection system is a pipeline with a diameter of 600 mm, and the relief valve is a rupture disc with a bursting pressure of 7 bar. This provides sufficient margins with respect to the maximum pressure in design basis loss of coolant accident analyses (3.9 bar).

The system has been designed to blow from the upper drywell directly into the atmosphere. This is acceptable from the radiological point of view since a loss of coolant accident does not directly cause any fuel damage. The system is equipped with two normally open isolation valves, which will be closed manually after the system has fulfilled its safety relief function. After that the core cooling systems and containment spray system are assumed to be started and to keep the pressure below the original design pressure. In case of a slower pressure build-up and when core degradation is anticipated, the isolation valves must be closed before reaching the rupture disc burst pressure. This is indicated in the corresponding emergency operating procedures.

The rupture disc is equipped with a rupture indication and alarm in the central control room. This indication is based on temperature monitoring in the relief line downstream of the disc. In case an unintended rupture is indicated, the shut-off valves in the relief line have to be closed immediately.

Containment filtered venting system

The function of the filtered venting system is to enable release of steam and gases from the containment to the environment in a controlled way in cases where pressure rise may threaten the integrity of the containment. The system consists of pressure relief lines from wetwell and drywell, a two stage filter unit and an exhaust line to the environment.

The system can be actuated by opening the isolation valves in one of the venting lines. The drywell venting line penetrates the containment wall close to the ceiling, which makes water filling of the containment possible. If a release becomes necessary before containment water filling can be started, the wetwell venting line has to be used. In this way, the release of activity can be decreased by using the scrubbing efficiency of the condensation pool. Another pipeline is connected in parallel with the drywell venting line, bypassing the normally closed isolation valves. This line contains a rupture disc and two normally open isolation valves. The rupture disc has been designed to burst at a lower pressure than the disc in the containment over-pressurization protection system to eliminate the risk of an unfiltered release in accident situations, when large amounts of radioactive fission products may be present in the containment atmosphere.

The filter unit consists of a wet scrubber with venturi nozzles followed by a combined droplet separator and stainless steel fibre filter. The filter unit is housed in a pressure vessel containing 20 m^3 of dosed water. The venturi scrubber is operated at pressures close to the prevailing containment pressure levels due to the provision of a throttling orifice in the filter discharge line. The venting flow entering the scrubber is injected into a pool of water via 24 submerged venturi nozzles. The total decontamination factor for the filtering unit is 1000 for aerosol particles larger than 0.3 μm and 100 for molecular iodine.

Containment venting is started either manually or by bursting of the rupture disc in the drywell venting line. The rupture disc is designed to burst at a pressure of 5.5 bar. A throttling orifice installed downstream of the scrubber can provide for critical expansion of the cleaned gas as long as the containment pressure is kept above 2 bar. The critical flow conditions imply that the flow velocity inside the filter remains constant. The system has a relief capacity of saturated steam at 3.5 bar corresponding to the decay power generation 24 hours after reactor scram.

The cleaned gas is released to the environment through a separate discharge pipeline, which has been installed inside the plant stack and routed all the way up to the stack outlet. The discharge pipe outlet has been sealed with a rupture membrane with a bursting pressure of 0.5 bar above the atmospheric. The pipeline, as well as other gas filled parts of the system, is normally inerted with nitrogen to prevent burns or explosions if a large amount of hydrogen is vented during a severe accident.

Except for the passive rupture disc in the drywell venting line, the system for filtered venting has to be operated manually. The isolation valves have been equipped with mechanical devices for remote operation due to the high levels of contamination that the system may be subjected to. When the system has been activated during a severe accident, it does not require operator attention during the first 24 hours of the release. In the long run, makeup water has to be supplied into the system. Provisions for water addition into the filter vessel even under radiation conditions corresponding to a severe reactor accident are included in the system design.

C.6.3.4 Prevention of re-criticality

Re-criticality may occur, if the progression of a severe accident sequence is interrupted at a stage when the control rods have already melted but the core is still mainly intact. This kind of situation may happen in connection with so-called re-flooding sequences, when water injection into the uncovered and overheated reactor is started after a long interruption.

OL1 and OL2 have two diverse systems for shutting down the reactor. Beside the control rods, boron injection using enriched boron-10 is also an efficient means of rapidly reaching sub-criticality. The boron injection system will be automatically actuated in connection with ATWS event sequences, but not in connection with symptoms typical of severe accidents.

The SAM procedures guide the operators to start boron injection manually in case AC power supply is re-established after long interruption, e.g. if the depressurisation of the reactor has already been automatically actuated on low reactor water level due to loss of water injection. It will only take the boron system a few minutes to inject enough boron solution to assure sub-criticality of the core in all conceivable situations, as long as the pressure vessel is intact.

Since the risk for re-criticality is relevant only at the early stages of a severe accident sequence, when the pressure vessel is still intact, it is possible that the SIRM (Source and Intermediate Range Monitoring) system used for neutron flux monitoring could be still operable. This system could then provide possibilities for the detection of re-criticality. The accident management procedures always guide the operators to withdraw the SIRM-detectors from the core to a position about half a meter below the core as one of the first severe accident management measures. The aim is to avoid the detectors being damaged due to the high temperatures in connection with core uncovery.

C.6.3.5 Prevention of basemat melt through

In-vessel retention of the corium has not been considered a practical severe accident management scheme for OL1 and OL2. This is due to the fact that it would take too long to inject the amount of water needed to submerge the bottom of the reactor vessel (about 1300 m^3) into the containment.

To protect the basemat and the penetrations in the lower drywell, the compartment has to be flooded with water before the pressure vessel melt-through. This can be done using two pipelines that belong to the original containment spray system. There are two valves in each pipeline that must be opened to get the gravity driven flooding started. The valves can be opened either remotely from the main control room or locally through manual actions. Each pipeline has a flow capacity of about 0.15 m^3/s.

The amount of water available for flooding of the lower drywell corresponds to a water pool depth of approximately 9 meters in that compartment. In order to make sure that all the penetrations in the lower drywell are submerged before the molten corium enters that compartment, the flooding has to be started at least half-an-hour before pressure vessel melt-through (here, a single failure is assumed that would make one of the two flooding lines unavailable). This means that in connection with worst case scenarios, the flooding has to be started within 30 minutes from the onset of the accident. An example of such worst case scenarios is a rupture of a large primary system pipeline inside the containment, combined with a total loss of water injection into the reactor. In connection with accident scenarios with an intact primary circuit, the accident progression would be much slower. Flooding of the lower drywell is the most time critical operator action in the accident management schemes.

Since the floor area in the lower drywell is relatively large, over 60 m^2, the flooding also provides good possibilities for reaching a coolable state of the corium after pressure vessel melt-through. Corium concrete interactions would also be practically eliminated.

The containment penetrations in the lower drywell are protected against thermal and mechanical loads, including steam explosions due to molten material relocation into the flooded lower drywell.

It is assumed that the molten core is resolidified and fragmented when it slumps into the water pool in the lower drywell. It is estimated that the core fragments form a particle bed with a maximum thickness of 0.5 m. The penetrations below this level have shields of a special design intended to enhance the natural circulation of water in the vicinity of the shield wall and thus to assure the coolability of the shield and the corresponding penetration even when in direct contact to the core debris. The 0.5 m deep debris bed is estimated to be coolable for particles typically formed in a melt coolant interaction.

The penetrations which are located above the 0.5 meter level from the floor are protected only against missile impacts. The design basis missile is a falling control rod drive mechanism.

A special item to be protected is the drywell floor sump. It has been equipped with a cover to prevent excessive amounts of fragmented core material from being gathered into the sump, where the restricted geometry might threaten the coolability.

Typical time to pressure vessel melt-through is around 1 h in case of LBLOCA and consequent SBO, and around 2…3 h in case of SBO only. In connection with verification of the accident management procedures, special attention has been paid to the requirement that even the fastest conceivable progression of an accident shall be manageable by applying the procedures.

C.6.3.6 Need for and supply of electrical AC and DC power and compressed air to equipment used for protecting containment integrity

All the accident management actions can be performed without the need for AC power, either manually or by using battery backed power sources.

Pressurized air is not used for severe accident management, because intrusion of air into the containment might cause a risk for hydrogen burn or detonation.

Pressurized nitrogen can be used for keeping two primary circuit relief valves open after a successful depressurisation. Pressurized water from the fire fighting water system can also be used for this purpose.

The containment monitoring system dedicated for SAM purposes has some measurements which are based on the bubble-tube principle: containment pressure, pressure difference over the partition floor between drywell and wetwell, as well as water levels in the different compartments of the containment. These measurements use pressurized nitrogen. If the compressors of the pressurized nitrogen system cannot deliver the pressure needed, the containment monitoring system has back-up nitrogen containers, which can sustain operation of the system for 24 hours. Replacement containers are readily available at the site.

C.6.3.7 Measuring and control instrumentation needed for protecting containment integrity

The containment monitoring system serves to provide the operators with the information needed for accident management purposes. The system has been designed to operate under the conditions created by a severe accident inside the containment. The system has no radiation or temperature sensitive components inside the containment, and the relevant parts have been protected against missile impacts. The measurements include:

- pressure in the drywell
- drywell-wetwell differential pressure
- water level in the lower drywell, upper drywell and condensation pool
- temperature in the upper drywell and in the condensation pool.

All these measurements have been doubled to achieve tolerance against single failure.

In case of a total loss of AC power (SBO) the containment monitoring system is powered by a dedicated system, whose batteries ensure operation of the containment monitoring system without any external power supply for 24 hours.

C.6.3.8 Capability for severe accident management in case of simultaneous core melt / fuel damage accidents at different units on the same site

The operations needed for the management of severe accidents are described in emergency operating procedures. The actions needed are either automated or conducted by the operators in shift. Thus, in case of simultaneous accidents at different units immediate actions needed for severe accident management could be performed at each unit.

In the long-term, the containment water filling is needed. As there is only one fire brigade to carry out these operations, the possibility to the required operations should be ensured by proper manning and procedures.

C.6.3.9 Conclusions on the adequacy of severe accident management systems for protection of containment integrity

The SAM strategy and its implementation at OL1&2 follows the requirements set in the Government Decree on the Safety of Nuclear Power Plants [733/2008] and the Regulatory Guides referred to in Section A.6. The approach and the plant modifications have been approved by STUK. The requirement for containment to withstand core melt ejection at high pressure has been considered to be taken into account by eliminating this phenomenon by reliable RCS depressurisation. The drywell penetrations have been protected against ex-vessel steam explosions considered possible.

The effectiveness of the SAM is further evaluated by the level 2 PSA studies, which show the possibility to carry out and the success of SAM measures in spectrum of initiating events and severe accident sequences. The frequency limits set for severe accidents and large releases are higher than those set in Guide YVL 2.8. The frequencies as such, apply for new NPP units to be built in Finland, and for old units the principle of continuous improvement of nuclear safety is applied.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan and schedule to secure decay heat removal from reactor core and containment in case of total loss of AC power.

C.6.3.10 Measures which can be envisaged to enhance capability to maintain containment integrity after occurrence of severe fuel damage

Since the systems for management and mitigation of severe accidents have already been implemented at OL1 and OL2 and the corresponding procedures are in place, no further measures for this purpose are foreseen at the moment. However, the soundness and adequacy of the accident management schemes is being constantly assessed against the latest knowledge and experience obtained from different international sources.

To respond to STUK's requirements after Fukushima accident, Licensee is planning enhancements for heat removal as explained in sections C.5.1.5 and C.5.2.5.

C.6.4 Accident management measures to restrict the radioactive releases

C.6.4.1 Radioactive releases after loss of containment integrity

The severe accident management is based on maintaining the containment integrity. If the containment integrity is lost the means to control radioactive releases are very limited. There are no EOPs for these situations and the actions to restrict the radioactive releases would be based on the decisions that are made in the situation.

C.6.4.2 Accident management after uncovering of the top of fuel in the fuel pool

For monitoring the spent fuel state and supporting accident management, there are some water level switches in the fuel pools for monitoring the water level with respect to operability of the active cooling systems, which extract water from the pools using the "flow over a weir" principle. These switches also provide alarms to the main control room (from the spent fuel storage, the alarms are routed to the control room of OL1) in case of abnormal water level. However, due to the narrow measurement range, these level switches cannot provide the information needed to manage the cooling of the fuel in the pools using the "feed & boil" approach.

About 1 m of water above the top of the irradiated fuel assemblies is enough to provide sufficient shielding against radiation so that even poolside accident management actions can be performed if needed. Normally, the submergence of the irradiated fuel is about 7 m at OL1 and OL2 and about 7.7 meters at the spent fuel storage.

If the spent fuel within the pools is uncovered, metal water reaction or zirconium fire is possible only if the fuel has been cooled down for less than a year [Sailor et al. 1987]. This means that hydrogen generation from irradiated fuel would be an issue only at the plant units but not at the spent fuel storage.

No provisions have been implemented for dealing with the hydrogen generated from spent fuel in OL1 or OL2 fuel pools. The main goal is to keep the fuel always covered with water. If cooling by the closed systems is lost, ample time is available for establishing cooling in the "feed & boil" mode and the need for make-up water to the pools is very modest.

In case of fuel damage caused by handling accidents, the automatic switch-over to emergency ventilation will limit the releases from the reactor building at OL1 and OL2 or from the spent fuel storage. No special provisions are in place for restricting the releases in a hypothetical situation with extensive fuel damage due to uncovery and overheating (even the emergency ventilation is dependent on AC power).

The control rooms are far away from the fuel pools, so that even an uncovery of the stored fuel would not jeopardize the habitability of the control rooms.

The control room ventilation at OL1 and OL2 can be switched over to the emergency ventilation mode in case there would be airborne radioactivity present at the site. In that situation, the air intake into the ventilation system will take place from inside the control building, and the air is filtered before letting it into the control room. Moreover, the control room will be slightly over-pressurized with respect to its surroundings. The emergency ventilation system is dependent on diesel backed AC power.

As far as the spent fuel storage is concerned, the process may be supervised from the control room of OL1.

C.6.4.3 Conclusions on the adequacy of measures to restrict the radioactive releases

The approach for spent fuel pools is to "practically eliminate" the possibility of fuel damage, which can be considered acceptable. To support this STUK has requested the licensee to provide a plan and schedule to secure decay heat removal from fuel storage pools located in the reactor building in case of loss of existing systems, and to investigate alternative methods to supply coolant to fuel storage pools (including potential need for new instrumentation).

Licensee's evaluation that 1 m of water above the fuel elements in the pool would still provide adequate shielding against radiation to carry out poolside operations may be too optimistic. The radiation levels with water levels this low could be around 1 Sv/h, and although operations would take only few minutes, accident situation may slow down the operations. In practise, the water pool boiling might have made the area inaccessible much before the loss of radiation shielding.

C.6.4.4 Measures which can be envisaged to enhance capability to restrict radioactive releases

To support monitoring of the water level in the spent fuel pools, there is a plan to equip all the fuel pools with a level measurement system with a measurement range from the normal water level down to the top of the fuel assemblies.

No measures have been planned for enhancement of the capability to restrict radioactive releases from the fuel pools. Possibilities for adding makeup water from the fire fighting system to the pools from safe locations will be provided. The pool water level indications will also be routed to those locations.

C.7 General conclusions

C.7.1 Key provisions enhancing robustness (already implemented)

Continuous improvement of nuclear safety is the driving force for enhancing nuclear safety in Olkiluoto unit 1 and 2 since start-up of its operation. The issues raised within the "Stress Tests", have been a part of the Olkiluoto 1 and 2 PSA studies since 1990's, and risk-based improvements have been carried out by plant modifications and through revising and updating the emergency operating procedures. Furthermore, these issues have been a part of periodical safety reviews carried out at intervals of ten years.

The requirements for severe accident management (SAM) were included in the Finnish nuclear safety regulations in 1982 when a YVL Guide on safety principles in NPP design was issued. After the accident at Chernobyl NPP in 1986, it was required that these principles had to be applied also to plants already in operation. Requirements include dedicated, single-failure tolerant SAM systems and measurements, as well as procedures and guidelines for the organisation to manage the severe accident situation. Major safety systems upgrades in Olkiluoto1 and Olkiluoto 2 have been made to fulfil the requirements. The respective WENRA reference levels [WENRA 2008] are fulfilled by these safety upgrades.

The following issues can be considered as advantages when assessing safety of Olkiluoto NPP against hazards that contributed the accident at Fukushima Dai-ichi NPP:

- Against earthquakes and flooding, a big advantage is the seismic stability of the Olkiluoto NPP site and moderate seawater level changes anticipated in the Baltic Sea.
- High capacity gas turbine plant including two independent units as a diverse on-site AC power source
- Filtered venting system of the containment, designed to retain most of radioactive materials released to containment in connection with a severe reactor accident
- Possibility to fill the containment with water

A project is on-going to renew the existing Emergency Diesel Generators. The new EDGs will be both seawater- and air-cooled, which provides a possibility to cool the engines in connection with a variety of different external hazards.

C.7.2 Safety issues

Limited time of OL1 and OL2 to tolerate loss of all AC power sources before the core damage can be considered as a shortfall. There are, however, several AC power sources ensuring the power supply to the safety systems, and thus the power supply is very reliable. Nevertheless, it is prudent to consider new means for extending the time that decay heat removal from the reactor can be provided without relying on the existing AC power sources and distribution systems.

C.7.3 Potential safety improvements and further work forecasted

The potential further improvements for enhancing the safety and robustness of the operating Olkiluoto 1 and 2 units against extreme external phenomena will be focused on the following issues:

- ensuring decay heat removal from the reactor and the containment in case of a total loss of AC power for several days;
- the strength of the fire fighting systems, severe accident management systems, and spent fuel storage pools against beyond design basis earthquakes
- additional means to remove decay heat from the fuel pools in the reactor building and from the spent fuel storage pools, or to supply additional water to those pools during a long lasting accident situation in extreme external conditions;
- installing additional temperature and water level monitoring instrumentation to all fuel pools;
- the impacts of extreme sea water level of beyond design basis on spent fuel storage cooling systems and their power supply

The following issues related the Olkiluoto site and all units will be further investigated:

- the sufficiency of on-site fuel reserves for diesel engines and gas-turbines during a long lasting disturbance of electrical power supply;
- the sufficiency of DC power during a long lasting disturbance of electrical power supply;
- the sufficiency of on-site demineralised water reserves during a long lasting disturbance of sea water cooling in extreme external conditions;
- needs and possibilities for mobile power supply and pumps in severe accident situations
- the applicability of procedures and the availability of personnel and material resources in case of multi-unit accident situation in extreme external conditions

The above issues are discussed in more detail in sections above considering measures which can be envisaged to enhance plant safety.

D. TVO – OLKILUOTO 3

D.1 General data about the site and the nuclear power plant unit

D.1.1 Brief description of the site characteristics

For the site characteristics see Section C.1.1. This chapter covers the “stress test” issues for Olkiluoto 3 (OL3), whereas OL1 and OL2 are dealt with in the previous chapter.

D.1.1.1 Main characteristics of the units

OL3 unit is under construction. It is a four-loop PWR (European Pressurized Reactor, EPR) with electric output of 1600 MW and thermal power of 4300 MW. The reactor operating pressure is 155 bar. Operating license is required prior to fuel loading, but not submitted yet.

D.1.1.2 Description of the systems for conduction of main safety functions

General arrangement of the systems [TVO 2010]

The design of the safety systems is based on quadruple redundancy of systems. It means that the systems consist of four parallel trains, each capable of performing the required safety task on its own. The four trains are physically separated and located in different parts of the reactor building in independent divisions.

Each of the four safeguard building divisions contains a low and medium-pressure emergency cooling system with the closed cooling and essential service water circuits cooling them, the steam generator emergency feed water system, and the electrical equipment and instrumentation and control systems required for these systems. The emergency cooling systems take their water from the in-containment emergency cooling water storage tank. Examples of the safety features of OL3 are shown in Figure D-1.

Reactivity control

The plant is provided with two independent reactivity control systems which work on diverse operating principles: rod cluster control assemblies (RCCAs) and boron systems (chemical and volume control system, safety injection systems and emergency boration system). The RCCAs and the emergency boration system are separately capable of shutting down the reactor during normal operational and anticipated operational occurrences. Each of the boron systems alone is capable of maintaining the reactor in a shutdown state at any reactor temperature.

The control rod system is a part of the reactor power control system. The system is used for controlling the reactor power and for a reactor scram. The control rods enter the core through guide thimbles in the fuel assemblies.

The chemical control system, the volume control system and the reactor coolant pump seal injection and leak-off system respond to the actuation signals which are generated by the reactor control system or by operator action. In conjunction with the reactor boron and water make-up system they serve to adjust the boron concentration to the re-

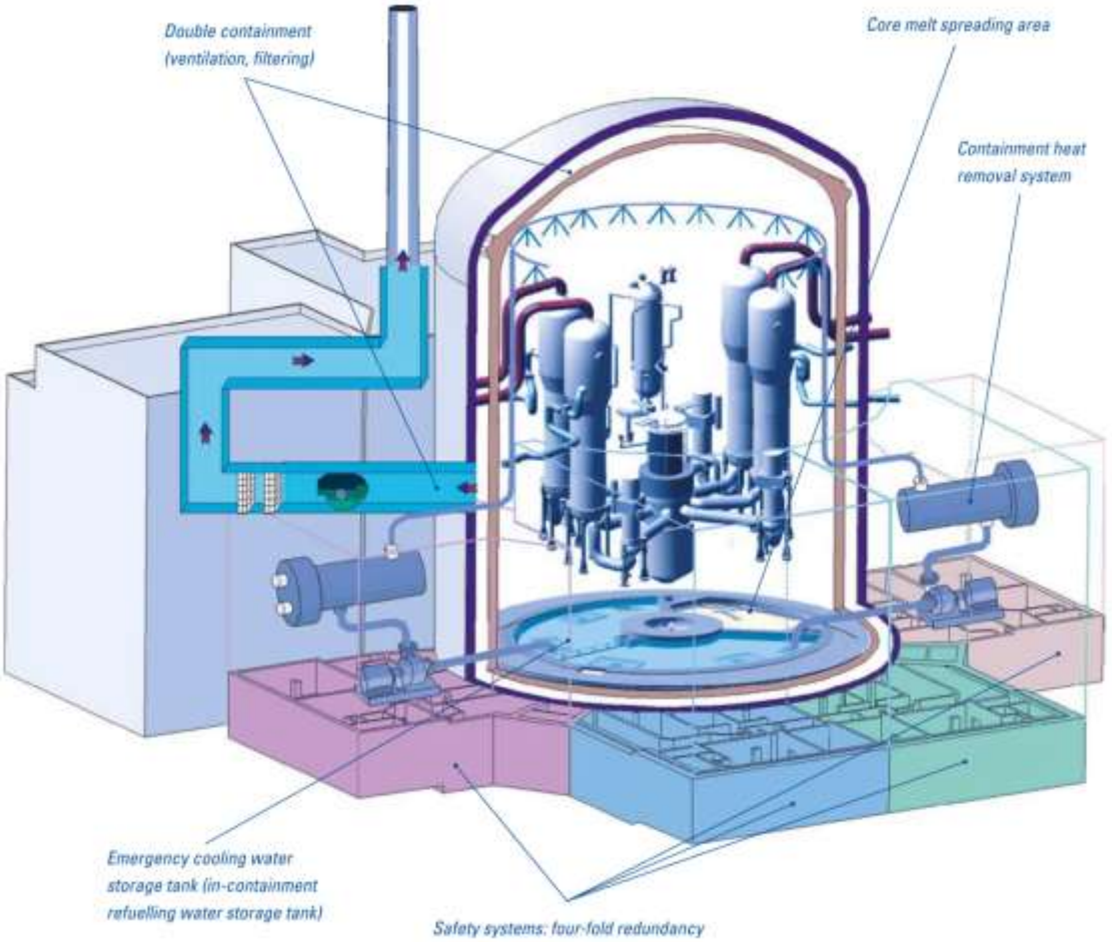


Figure D-1. Examples of principal safety features of OL3 [TVO 2010]

quired value in the core for the purpose of compensating reactivity equivalents of core parameters during power generation or to ensure sub-criticality by the required margin in shutdown states. As these systems are operational systems, their function with regard to reactivity control to reach to the controlled state after an accident is fulfilled by the extra borating system.

During normal plant operation, the extra borating system is on standby except for the periodic tests and for the hydrostatic pressure test of the reactor coolant pressure boundary. The system consists of two redundant trains and an additional third pump. Each main train is composed of its own boron tank containing high-concentration boric acid, a high-pressure reciprocating pump, a test line, containment penetration and injection line to the reactor coolant system cold legs. The injection line is divided into two inside the reactor building and is connected to the safety injection system lines.

A header interconnecting the bottom of the two boron tanks allows injection from both tanks using only one of the three extra borating pumps, each with a capacity of 100%. Although the pumps are 100% capacity each, the content of both tanks is required in the sizing case, which is to maintain the reactor in the shutdown state at any reactor temperature without control rods.

The third extra borating pump is used to replace one of the main train pumps, to perform tests (periodic or hydrostatic pressure test) or to inject refuelling water into the main injection lines inside the reactor building in order to prevent crystallization of the boric acid.

The extra borating system is designed to perform emergency boration of the reactor coolant system despite of a single failure and a simultaneous inoperability due to testing, maintenance or repairs. In addition, the two redundant trains are installed in separated divisions of the fuel building to prevent common cause failure as a consequence of an internal hazard in one division.

Heat transfer from reactor to the ultimate heat sink

During power operation, the heat generated in the reactor is transferred through the RCS to the secondary circuit via four steam generators (SGs). In the design of the OL3 SGs, particular attention was paid to the prevention of cross-flows in the secondary circuit and of the adverse effects caused by thermal layering due to the efficient heat exchange. The steam space has been enlarged, increasing the steam volume resulting in a long time to fill the SG with water from the primary circuit in case of a SG tube rupture (SGTR). High water volume of the SGs improves the safety margin and increases the grace period in a situation where all feed water systems malfunction and no cooling water is available for feeding into the steam generator.

During normal operation, three of the four motor-driven feed water pumps deliver feed water through the two high-pressure feed water heater trains to the steam generators. The fourth pump is on standby to be started in case of failure of one of the operating pumps. To fulfil the net positive suction head requirements, the feed water pumps are assisted by individual booster pumps. The pump sets are of single-shaft arrangement, which means that the booster and main pumps are installed at the same elevation, and each pump set is driven by the same electrical motor. The booster pump is directly connected to the motor and the main pump is connected via a gearbox.

The ultimate main heat sink is the sea water and the alternative heat sink is atmosphere.

The circulating water screening plant screens the circulating water and essential service water required for the plant and to keeps the circulating water and essential service water free of fouling during normal operation. The safety function of the system is to make water for the essential service water system available under all operating conditions as well as under accident conditions except in the case of loss of ultimate heat sink. The circulating water screening plant is located in the circulating water pump house and provides four screening lines for mechanical cleaning of the circulating water. Each screening line consists of one coarse screen unit with heating equipment and one fine screen unit with wash water equipment.

Safety injection and residual heat removal

The safety injection and residual heat removal system (SI&RHRS) takes care of the normal core residual heat removal, as well as the emergency core cooling for maintaining reactor core coolant inventory and for providing adequate core decay heat removal in accident conditions. Therefore it is also called emergency core cooling system (ECCS).

In the safety injection mode, SI&RHRS ensures the core reactivity control by supplying the core with water with high boron concentration, and in case of a core melt accident, sufficient margin to corium re-criticality is provided by flooding the corium with water from the in-containment refuelling water storage tank (IRWST).

In normal shutdown conditions, as soon as the steam generators are no longer effective, SI&RHRS is operated to bring the reactor to the cold shutdown condition and to ensure the core decay heat removal in the long term.

In postulated accident conditions, this system provides the emergency core cooling and, once the controlled state has been reached, long-term core decay heat removal. During core melt accidents, before forced corium cooling starts, passive corium cooling is ensured by flooding the corium spreading area and steaming.

In the residual heat removal (RHR) mode, design features are provided to limit radiological releases in case of a large RHR pipe break. In LOCA conditions, the system is designed to limit the containment pressure build-up so that the confinement of radioactive materials released into the containment is ensured supplied by the leaktightness of the IRWST anf SI&RHRS piping.

The RCS protection against cold overpressure protection is ensured both by pressurizer safety relief valves and by the RHRS safety valves. During normal plant shutdown, the SI&RHRS provides mixing of the reactor coolant when the reactor coolant pumps (RCPs) are stopped and filling of the refuelling cavities with water from the IRWST.

SI&RHRS comprises four identical and independent trains, each train consisting of the following main equipment: a medium head safety injection (MHSI) pump, a low-head safety injection (LHSI) / residual heat removal (RHR) pump, a hydro accumulator, a LHSI/RHR heat exchanger, valves (isolation, non-return, control), and piping. The IRWST is common to the four trains, equipped with sump strainers.

In the injection mode, the MHSI and LHSI pumps, located in the safeguard buildings inject water into the RCS from the IRWST.

The LHSI heat exchangers are located downstream of each LHSI pump. These heat exchangers are installed in the safeguard buildings and cooled by the safety-related component cooling water system (CCWS). The accumulators are located inside the containment and inject into the reactor coolant system cold legs when the reactor coolant system pressure falls below the accumulator pressure, using the same injection nozzles as the low head safety injection and medium head safety injection pumps.

In normal shutdown conditions, system SI&RHRS is operated in RHR mode. The RHR pumps take suction from the RSC hot leg piping and discharge through the RHR heat exchangers back to the RCS cold leg piping.

In LOCA conditions (injection mode), the MHSI and LHSI pumps are actuated by the reactor protection system. Core cooling is ensured by water circulation from the IRWST to the RCS loops. Decay heat is transferred from the IRWST to the cooling chain by the LHSI heat exchanger cooled by the safety-related CCWS. In case of a main steam line break (MSLB), only the MHSI pumps are actuated in order to supply the core with water with high boron concentration. After postulated accidents conditions, safe cooldown is performed by the SI&RHRS, which also ensures the long-term decay heat removal.

The SI system function is designed with sufficient capacity, diversity and independence to perform its required safety function also assuming a single failure in one train while a second train is out of service for preventive maintenance. To meet this purpose, the SI&RHRS is 4×100% redundant except for the accumulators which are 4×50%. Thus, in the case of a LOCA active components of one train are sufficient for core cooling. To perform the RHR safety function one train is adequate in all conditions.

In order to protect the SI&RHRS against internal and external hazards, the four redundant trains are installed in separate divisions of the safeguard buildings, and they are spatially separated in the reactor building. All four SI&RHRS trains are linked to separate I&C and electrical divisions.

To ensure its safety function in postulated accident conditions, the SI&RHRS components are emergency power supplied by the emergency diesel generators (EDGs). In case of loss of EDGs, an additional back-up is provided for two of the trains by the station blackout (SBO) diesel generators.

The RHR and inner containment isolation valves are also power supplied by 2-hour batteries. According to the general design principle for containment isolation, the LHSI&RHRS outer containment valves are emergency powered by the SBO diesel generators and by the 12-hour batteries.

Moreover, design provisions are taken to ensure LHSI in case of SBO, total loss of cooling chain and LUHS.

In case of large-break LOCAs with possible generation of debris in the reactor building, reliable operability of the MHSI and LHSI pumps is ensured by the sump filters. A backflushing system is provided to enable operators to remove clogging beyond design basis.

Emergency feed water system

The emergency feed water system (EFWS) supplies the required water to the SGs secondary side, if the main feed water system and the startup and shutdown system, contributing to normal water supply of the steam generators, are inoperable.

The EFWS consists of four redundant trains and has the following safety-classified functions: residual heat removal, cooldown to low-pressure conditions, fast cooldown to low-pressure conditions, partial cooldown, and SG isolation (in case of SGTR).

Water for the EFWS is supplied from the four storage pools, located in each safeguard building. Each pool is designed for 25% of the total required mass of water, and they can be connected through a suction header. Inoperability of one pool affects EFWS capability to cool down the RCS to low-pressure condition. Thus, the four EFWS pools are required available in any plant state, during which EFWS could be required. The water mass required is sufficient to reach hot standby and cooldown to RHR considering maximum mass of water to be lost to the feed water break before isolation at 0.5 hour delay.

The EFWS pump suction header interconnects the EFWS suction lines. Each division can be isolated from the header by a manual valve. The suction header is also connected in one of the safeguard buildings to the demineralised water distribution system to enable storage pool filling or makeup.

The water of the storage pools is injected into the SGs by four EFWS pumps, each designed to produce 50% of the required flow rate.

The pump discharge header interconnects the lines between the EFWS pumps and the SGs of the four identical trains. Each division can be connected to the header by the manual discharge header isolating valve, which enables each pump to inject into any of the SGs.

The SG level control and isolation equipment consist of level control valves, containment isolation valves and check valves. The control valves and the isolation valves enable full flow injection into each steam generator, control the steam generator level during post accident management and steam generator isolation.

The EFWS is connected to the demineralised water distribution system; the process drains collection and disposal system; the nuclear island vent and drain system; the mobile hydrazine injection system for NI; and to the containment heat removal system (CHRS). During periodic testing it might be necessary to inject hydrazine into the discharge line (using the mobile hydrazine injection system for NI) of the EFWS to condition the water to the water chemistry requirements.

The connection to the CHRS is done using a removable piping connection. In case of LUHS during refuelling outage, core cooling is ensured by the LHSI taking suction from the IRWST. The containment needs to be depressurised in the later phase of the transient in order not to exceed the design pressure. In this case the IRWST can be refilled by water from the EFWS storage pools.

Internal hazards such as pipe leaks and breaks, failure of vessels, tanks, pumps and valves, internal missiles, load drop, internal explosion, fire and flooding do not prevent the necessary safety functions from being performed.

The general layout provisions enable the EFWS to fulfil its safety functions despite the occurrence of external hazards. Protection against external hazards is provided by physical protection of two divisions of the safeguard buildings and by geographical separation of two other divisions. In case of LUHS, two trains of EFWS can operate without seawater cooling. The water content of the EFWS tanks is sufficient for 24 hours and there is a permanent water reservoir at the site for additional 48 hours.

Electrical power is supplied by independent trains. In case of loss of offsite power (LOOP), the EFWS is supplied by the EDGs. In case of SBO, two of the EFWS divisions are supplied by the SBO diesel generators.

Component cooling water system

The component cooling water system (CCWS) transfers heat from safety and operational process systems to the main heat sink via the essential service water system (ESWS). CCWS is subdivided into the operational and safety related parts. The safety related part consists of two subsystems, of which one is connected to the operational part and the other one is so called dedicated CCWS.

The operational part serves to cool the loads located inside the fuel building, reactor building, radioactive waste processing building and the nuclear auxiliary building during normal operation.

The safety related part, which consists of four separate safety classified trains, serves to cool and transfer heat from safety related systems during normal operation, transients and design basis accidents. The safety related part also contains two separate trains, which are part of the dedicated cooling chains and serve to cool and transfer heat from the CHRS. The main components of the safety related CCWS are pumps, heat exchangers and surge tanks.

The safety related trains of the CCWS correspond to the four layout divisions and the four electrical divisions. Each train includes a pumping facility, a heat exchanger, a surge tank¸ a sampling line connected to the sampling activity monitoring systems, a chemical additive supply line and a set of isolation valves. The corresponding main EDG supplies the CCWS pumps in case of a LOOP.

The dedicated safety related CCWS trains correspond to the divisions with CHRS. Each train includes a pump, a heat exchanger and a surge tank. In case of a LOOP, electrical power to the pumps of the two separate dedicated trains is supplied by the EDGs, and if these fail by the SBO diesel generators.

Essential service water system

The essential service water system (ESWS) provides cooling of the CCWS heat exchangers with water from the ultimate heat sink during normal plant operation and during accidents. The ESWS pumps, located in the ESWS pump buildings, draw cooling water from the circulating water pump building via the underground, divisionally separated water channels, and pump it through the CCWS heat exchangers located in one of the safeguard buildings back to the service water collecting pond.

The ESWS has four trains, each serving one train of the CCWS and each located in separate buildings. The trains are grouped in pairs in two pumping stations which are geographically separated. For the same reason all system piping is laid in tunnels.

The four ESWS pumps are powered by the emergency power supply. Two ESWS pumps are in operation at all times during normal plant operation. When challenged during a transient or accident, all four ESWS pumps are actuated by the safety injection signal issued by the protection system. Each of the four trains is provided with a fully automated tube cleaning system for the CCWS heat exchangers.

Raw water supply system

The raw water supply system is common to the plant units OL1&2 and OL3. The system is designed for the treatment of the raw water taken from river Eurajoki and for supplying the treated water to the ion exchange plant for production of process water to the power plant and for use as potable water and domestic water, for use in the cleaning of the power plant units and the plant components, and for use as fire water.

The water from the river Eurajoki is pumped through the raw water pre-treatment plant to the Korvensuo storage basin, and further to the water treatment plant in three parallel 100% lines whereby failure of one line will not influence the supply of raw water.

The treated water is led to two fresh water basins, and further through the pressure maintenance system to the water supply system of the power plant units. Fire water to OL3 is pumped with fire pumps to the technical ring and further to the fire water distribution systems of the plant. The treated water is pumped to the technical ring and further to OL3 (potable and sanitary water distribution system), and for production of process water to the demineralised water treatment plant.

In transient and failure situations that require shutdown of and repairs at the water treatment plant, the fresh water basins provide backup water supply to the power plant. If necessary, raw water can be supplied directly from the Korvensuo basin to the fresh water basins.

Water provided by the raw water supply can be used to partially fill the containment after certain accident conditions as a precondition for fuel removal.

Demineralised water distribution system

The demineralised water distribution system stores demineralised water in two storage tanks, supplies demineralised water by the transfer pumps to all loads inside the TI and the NI, and supplies additional demineralised water to the seal water supply system of the NI.

Fire water systems

The fire water systems consist of the fire water distribution system inside the TI and NI. During normal plant operation the systems are maintained at pressure and on standby. As a whole, the fire water systems consist of the pumping station with water supply, the ring main on site, the distribution systems and the connected fire extinguishing systems.

The fire water pumping stations are common for OL1&2 and OL3 (see Section C.1.1.2).

Spent fuel pools

The fuel pool cooling system and the purification system control that the boron concentration of the water in all pools corresponds to the refuelling concentration, although sub-criticality of the spent fuel assemblies stored in the spent fuel pool is ensured even without boron. Boron concentration is checked by sampling and ensured by adjusting the concentration of the makeup water.

The fuel pool cooling system removes the decay heat from the spent fuel pool during normal plant operation (power operation and outages) and during accidents. The purification system participates in heat removal by the SI&RHRS during LOCA, because dedicated lines of the system connect the instrumentation lance compartment to the SI&RHRS to provide back-flushing of the SI&RHRS screens.

The fuel pool cooling system is installed in the fuel building, which is protected by an outer shell against external hazards. The system consists of two separate trains, each composed of two pumps in parallel, one heat exchanger cooled by the operational CCWS, suction and discharge piping, and valves.

The main components of the fuel pool purification system are two purification pumps in parallel (one used for containment and the other one for fuel building purification; both capable of backing up each other), two purification chains (one in part of pool purification system and the other one is the coolant purification system purification chain), mechanical filters, mixed-bed filters, suction and discharge piping, and valves. The equipment is installed in the fuel building, the nuclear auxiliary building and the reactor building.

Internal hazards such as pipe leaks and breaks, failure of vessels, tanks, pumps and valves, internal missiles, load drop, internal explosion, fire and flooding do not prevent the necessary safety functions from being performed and do not initiate an accident.

In case of LOOP both cooling system trains remain operable as they are supplied by the EDG. Also cooling water is available as the four pumps of the operational CCWS are emergency power supplied.

In case of abnormal evaporation cooling in spent fuel pool, the steam is led from the fuel building hall to the stack chamber by a steel pipe. The rupture foil ensures its passive opening due to over-pressure in the fuel building hall.

The make-up system for water supply in case of fuel pool evaporation cooling is the fire water distribution system inside NI. Only few manual measures like installation of hoses or manual change of position of valves are required, and thereafter this make-up system is in stand-by position when evaporation starts.

Electrical systems [TVO 2010]

The electricity needed by the power plant itself is taken from the 400 kV grid through two auxiliary unit transformers, which are backed up by an auxiliary stand-by transformer connected to the 110 kV grid. These two power supplies are independent of one another.

The reactor plant electrical power system is divided into four parallel and physically separated sub-divisions. The power supply to equipment critical for the safety of each division is backed up with a 7.8 MVA diesel generator. The busbars of the diesel generators can also be supplied by the Olkiluoto gas turbine plant.

The systems are designed to ensure sufficient capacity for maintaining nuclear safety even if one division fails and another is simultaneously out of operation due to maintenance. Safety-critical systems are connected to backed-up electrical power systems. In case of the loss of all external power supplies, the malfunction of all four diesel generators at once, i.e. the complete loss of all AC power, the plant unit has two smaller diesel generators with an output of approximately 3 MVA each. These ensure power supply to safety-critical systems even in such a highly exceptional situation.

Electrical systems are discussed in Section D.5.1 in more detail.

D.1.2 Significant differences between units

OL3 is the only unit of its kind at the Olkiluoto site, and there are no shared safety related systems other than the fire fighting water supply system with OL1&2.

D.1.3 Use of PSA as part of the safety assessment

A level 1 detailed design phase PSA has been performed for power states and shutdown. The following grouping of initiating events is defined for the detailed design phase PSA of OL3: internal events (transients, secondary side breaks, LOCA); common cause initiators; internal hazards (internal fire/explosion, internal flooding/steaming, secondary effects from pipe whip/missiles, load drop, etc.); external hazards (seismic events; other external events impacting the plant operation by effects on structures, ventilation, ultimate heat sink and offsite power); events affecting the heat removal from the fuel pool.

During power operation external hazards have been estimated to contribute around 10% of the total CDF. The fraction of seismic events is less than 1% of the total CDF. During shutdown, external events are of less importance.

Level 1 analysis has been extended with level 2 PSA. Accident progression analysis has been carried out with a programme that computes the source term distribution for each release path in all CETs. Risk integration has been performed over all plant damage states using 8000 Monte Carlo simulation runs.

It must be noted that STUK has not yet approved the PSA analyses for OL3, and thus the results have to be considered as preliminary that will be updated.

D.2 Earthquakes

D.2.1 Design basis

D.2.1.1 Earthquake against which the plant is designed

Characteristics of the design basis earthquake (DBE)

Section A.2 describes the basis of DBE criteria. The DBE response spectrum is described in Section A.2, in Figure A-2. The corresponding horizontal PGA is 0.10 g.

The probabilistic seismic hazard assessment at Olkiluoto has been estimated in connection to the seismic PSA of the operating Olkiluoto plant units 1 and 2. Latest seismic PSA has been done 2008 as an update for original seismic PSA from 1997. Horizontal PGA value 0.082 g is estimated to take place on medium frequency of 10^{-5}/a, which is following the DBE frequency according to Guide YVL 2.6.

Methodology used to evaluate the design basis earthquake

Section A.2 describes how DBE is based on statistical analysis of historical data with adjacent geological and tectonic information. Based on seismic PSA 2008 the horizontal PGA value 0.10 g is expected to take place at Olkiluoto NPP with median frequency less than $8 \cdot 10^{-6}$/a which is close from the safe side to the required frequency level 10^{-5}/a of current design criteria.

Conclusions on the adequacy of the design basis for the earthquake

Olkiluoto is in the area of low seismicity. Horizontal PGA 0.10 g is expected to occur in median frequency less than $8 \cdot 10^{-6}$/a, which is less than 10^{-5}/a, as required for DBE frequency according YVL 2.6.

The seismic CDF is $1.3 \cdot 10^{-8}$/a which presents about 1% share of the total CDF ($1.58 \cdot 10^{-6}$/a) prove out that there is no instant need for updating probability studies concerning DBE specification.

Ongoing efforts to develop and verify seismic design of NPPs in Finland are described in Section A.2. Final conclusions in detail level will be achieved later.

D.2.1.2 Provisions to protect the plant against the design basis earthquake

The plant has been designed and the systems will be tested to meet DBE requirements. Failures of buildings and systems not qualified for the DBE are assumed conservatively. Following scenarios has been studied.

- If offsite power supply will be lost due to a failure of the 400 kV grid connection, a reactor trip may initiate.
- A turbine trip and the closure of all full load feed water lines can be initiated on reactor trip checkback.
- If turbine hall fail, it may lead to rupture of some/all main feed water and main steam lines outside the reactor building. Thus the thresholds for MS isolation may also be reached leading to a closure of all MSIV.

The following front-line systems are necessary to withstand the DBE: control rod drive system for reactor trip, extra borating system for RCS boration to transfer the plant to the cold shutdown state, pressurizer system for RCS overpressure protection, RHRS for the RCS, MFWS for SG isolation towards the turbine hall, EFWS for SG feeding, main steam system for SG isolation and secondary RHR via the MSRT. All these systems are seismically qualified.

Protection against indirect effects of the earthquake has been studied. Following global effects are analysed: adverse ambient conditions caused by failure of high-energy systems/components, consequential flooding.

All equipment in safety-classified buildings, except in nuclear auxiliary building and radioactive waste processing building is generally assigned to resist DBE. With respect to consequential failure of equipment inside these buildings it is ensured that unacceptable radiological releases from these buildings are prevented. Buildings are isolated from each other so that consequential failures between DBE protected buildings and nuclear auxiliary and radioactive waste processing buildings are prevented.

External power supply is not required for OL3 to reach the controlled state (hot shutdown state) or to reach the safe state (cold shutdown state).

The road leading to the plant unit is not vulnerable to earthquake damage. The road has low, sturdy girder and plate bridges with short span lengths, which may be assumed to tolerate stress due to earthquakes well. In hypothetical damage situations, the connection may be assumed to be reopened to light traffic within one day and to heavy traffic within three days of the earthquake. More details are in Section C.6.1.

Consequential failures are ruled out by defence in depth design by ensuring that SSC's failures can not lead to consequential fire or consequential explosion.

D.2.1.3 Compliance of the plant with its current licensing basis

After OL3 has been commissioned the operational instructions, maintenance procedures and plant modification handling processes ensure that plant safety is maintained. Seismic PSA effects are included in the modification safety assessments.

No mobile equipment and supplies are planned to be needed after an earthquake.

No deviations from licensing basis are identified. After commissioning living seismic PSA will be used to verify appropriate safety level of DBE with corresponding sensitivity studies.

D.2.2 Evaluation of safety margins

D.2.2.1 Range of earthquake leading to severe fuel damage

The lowest HCLPF capacities of SSCs important to seismic safety lay in the range of 0.2 g. Thus sufficient seismic margins are well beyond the European Utility Requirements [EUR], which are 40 % beyond the horizontal PGA of the DBE, i.e. HCLPF > 0.14 g.

The contribution of the Seismic initiating events is about 0.1 % of the design requirements based on YVL 2.8 (1E-5 1/a). The contribution of the different initiators to the overall seismic induced CDF is

- secondary side breaks following a failure of the turbine hall 44 %
- during power use the medium break LOCA 31 %
- loss of offsite power 17 %
- anticipated transient without scram (ATWS) 6 %
- during power use the loss of coolant accident outside containment (VLOCA) 2 %.

D.2.2.2 Range of earthquake leading to loss of containment integrity

HCLPF capacity against reactor containment integrity is 1.26 g.

D.2.2.3 Earthquake exceeding the design basis earthquake for the plant and consequent flooding exceeding design basis flood

Consequential flooding due to earthquake flooding exceeding the design basis flood is not relevant for the Olkiluoto site. There are no nearby rivers or dams, and the probability of a tsunami in the Gulf of Finland is negligible.

D.2.2.4 Measures which can be envisaged to increase robustness of the plant against earthquakes

Ongoing efforts to develop and verify seismic design of NPPs in Finland are described in Section A.2. Final conclusions in detail level will be achieved later.

D.3 Flooding

D.3.1 Design basis

D.3.1.1 Flooding against which the plant is designed

The operating design basis of OL3 against seawater flooding is still level of +1.3 m in the N60 system plus 0.5 m allowance for waves, altogether +1.8 m. In addition, it is assured that seawater level up to +3.5 (N60) does not endanger the systems, structures or components required to maintain critical safety functions. The level 3.5 m in the N60 system correspond to about 3.7 m above the current mean sea level.

The critical seawater level for safety systems is the same as for units OL1 and OL2. The characteristics of the site and design basis flood are explained in connection with OL1 and OL2 in Section C.3.1.1. The frequency of exceeding seawater level of +3.5 m (N60) is estimated to be less than 10^{-9}/a. The methodology used to evaluate the design basis is explained in section C.3.1.1.

<u>Conclusions on the adequacy of protection against external flooding</u>

The design basis flood and the design solutions for protection against the DBF are considered adequate. The OL3 unit is under construction. The adequacy of the technical implementation will be ensured during the review of the operating licence application and commissioning inspections.

D.3.1.2 Provisions to protect the plant against the design basis flood

Several pumps or other components required to maintain critical safety functions are situated in OL3 safety buildings below mean sea level, for example low head and medium head safety injection pumps and emergency feed water pumps. In the diesel building the diesel fuel, lubrication and cooling water pumps are situated below mean seawater level.

The safety of OL3 against seawater flooding is based on ensuring global stability of the building structures and by preventing water ingress into the buildings. In addition, spreading of flooding between safety divisions is prevented by reliable physical separation of the four safety divisions.

The issues considered in layout and structural design are increased buoyancy loads and hydrostatic pressure loads on outer structures including penetrations. The buoyancy loads and hydrostatic pressure loads on the outer structures including penetrations are considered for the building design for a seawater level of +3.50 m (N60).

The relevant penetrations below building level +0.00 m are tightened and building joints are tightened by Omega Water Stops. The Omega Water Stops are designed for a water height of +4 m or +25 m depending on the location. They prevent flooding from one division to another. The doors and openings in the Nuclear Island outer walls shall be kept closed.

The situation outside the NPP is explained in connection with units OL1 and OL2 in section C.3.1.2.

D.3.1.3 Plant's compliance with its current licensing basis

After OL3 has been commissioned the operational instructions, maintenance procedures and plant modification handling processes ensure that plant safety is maintained. Site flooding effects will be included in the modification safety assessments.

Use of mobile equipment is not planned for OL3.

No deviations from the licensing basis have been identified.

D.3.2 Evaluation of safety margins

D.3.2.1 Estimation of safety margin against flooding

A definite maximum height of seawater flooding cannot be derived on a physical basis for the Olkiluoto site. In some other connections, design vales against external events are chosen so that their exceedance frequency is less than 10^{-4}/a.The water level with estimated 10^{-4}/a frequency is about +1.5 m (N60). The margin of this value to the design basis is 2 m. The frequency of exceeding the design basis of +3.5 m is estimated to be less than 10^{-9}/a. Although the uncertainties associated with such low frequencies are very large, the frequency estimate can be considered very low.

No phenomena have been identified which would raise the seawater to the safety system design level +3.5 m. The long term climate change may result in the rise of seawater level, but in the Olkiluoto region the effect is predicted to be moderate during the operating life of OL3 due to postglacial land uplifting.

In addition, exceeding the seawater level +3.5 m would not immediately cause significant safety impacts. Although the outside doors do not have water tightness requirements, they have capacity to resist water ingress. Nuclear Island outer doors, including diesel buildings, have been tested and they have been found to be practically leak tight even with seawater levels of +15.5 m in the N60 system (12 m above threshold of the door, the leak less than 10 l/h).

Flooding would also be possible inside the essential service water pump building. If seawater rises above the +3.5 m level, the loss of the ultimate heat sink is assumed. However, the loss of the ultimate heat sink for 72 h is a design basis event for OL3 and it is treated in section D.5.1.2.

In summary, the safety margins of OL3 against seawater flooding can be considered adequate with regard to both the safety system design basis and the effects of exceeding the design basis.

D.3.2.2 Measures which can be envisaged to increase robustness of the plant against flooding

Based on current information on meteorological and oceanographic conditions in the Baltic Sea region, the design of the OL3 unit against high seawater level, as well against low seawater level, is adequate. The adequacy of the implementation of flood protection will be ensured in the review of the operating license application and in commissioning inspections.

D.4 Extreme weather conditions

D.4.1 Design basis

D.4.1.1 Reassessment of weather conditions used as design basis

The design values of weather conditions are presented in FSAR and the assessments of the weather conditions' frequencies are estimated in PSA. After 2007 the extreme weather conditions, weather phenomena and the area specific weather data have been researched in the research project EXWE within the national research programme SAFIR [SAFIR2010].

External air temperature and humidity

The following design values for maximum, minimum air temperatures and humidity conditions are considered in design:

Maximum air design temperatures
- Long-term base: +23°C for > 7 days
- Short-term base: +27°C for 6 h to 7 days
- Instantaneous: +36°C for 6 h

Minimum air design temperatures
- Long-term base: –29°C for > 7 days
- Short-term base: –32°C for 6 hours to 7 days
- Instantaneous: –39°C for 6 hours

Maximum external humidity conditions:
- Summer: 60% at +36°C (dry bulb)
- Winter: 100% at –29°C

The temperatures recorded at Olkiluoto between 2004…2007 have been used in assessing the behaviour of maximum and minimum temperatures in different months. Based on the cliff edge evaluation the important safety functions are ensured for extreme temperatures of –41°C and +40°C for duration of 6 h.

The provisions against high and low air temperature and the design values are considered sufficient by the licensee. High and low air temperature related events have been screened out in PSA based on severity criterion. The building layout is designed to accommodate the cooling systems capable of operating within the temperature ranges specified. The same applies to safety equipment, which is directly exposed to the wind. Values specified in the Finnish Code for Structural Loads and Effects (RIL 144) are used for structures.

Wind and wind-generated missiles

For the design basis conditions the design is adequate to the ranges of wind velocity based on basic wind speed in RIL 144 (Finnish Building Code), and extreme wind speed of 48 m/s. Structures housing for systems and equipment with safety function are designed to withstand loadings based on the extreme wind speed. Structures designed for extreme wind speed are designed to withstand wind-generated missiles.

Structures, systems and components without safety functions are designed to withstand the basic wind speed. If any failure of non-safety equipment would impair safety function, the equipment is designed against extreme wind. Ventilation systems are designed for extreme winds, as well.

Strong winds and tornados are included in the screening analysis in PSA. Tornados have been screened out of the detailed analysis using severity, frequency and inclusion criteria.

The frequency estimates are based on the observations from the monitoring station at site at 100 m's height during 1984…1989 and 1992…1999. Occurences for 3-second gust speed using POT method are: 2.73/a for 28 m/s; $1.16 \cdot 10^{-3}$/a for 39 m/s; and 10^{-8}/a for 43 m/s. Based on hourly observations measured at site weather station during 2001…2006, the maximum wind speed at 100 m height is 28.5 m/s.

The predominant wind direction is from southwest, and the most infrequent one from northeast. The winds blowing along the coastline are also common. Few times a year the sea breeze phenomenon occurs in coastal areas, potentially affecting atmospheric dispersion calculations.

Tornado intensity related strike frequencies have been calculated from the hit frequencies. The tornado area intensity distributions in NUREG/CR-4461, Rev. 2 have been used. Using data from the time period 1796…2007 in Finland, the estimated intensity related strike frequencies for tornados in Finland are: $3 \cdot 10^{-6}$/a for EF2; $2 \cdot 10^{-6}$/a for EF3; $6 \cdot 10^{-7}$/a for EF4; and $2 \cdot 10^{-7}$/a for EF5.

Extreme wind speed is not combined with other hazards in OL3 PSA studies.

Beyond design basis consideration:

Based on probabilistic consideration the tornado EF2 is considered regarding its effects on plant safety and the tornado EF3 is also taken into account regarding avoidance of cliff-edge effect. Licensee's studies show for tornado EF2 that the plant safety is assured because

- the safety relevant buildings can take the tornado load;
- the required safety systems are available due to their location inside the safety relevant buildings;
- the relevant ventilation systems can take the tornado loads; and
- the operability of the emergency diesel generator and the station blackout diesel is assured after tornado event.

The tornado loads are covered by plant design against external hazards. Downbursts are considered to have similar but less severe impacts on target areas than tornados, and therefore, it is not separately analysed in PSA of OL3.

<u>Cooling water temperatures</u>

For the design basis conditions the plant design is adequate to the following range of water temperatures at the intake for plant operation and safety functions:

– seawater: –0.4°C…+30°C

The temperature of the circulating water generally used in the design is +18°C. According to the licensee, the reactor operation at full power will be possible up to +25°C. Accordingly, high seawater temperatures of up to +30°C do not jeopardize the safe shutdown of the plant. A temperature of +30°C is specified in design for the component cooling and essential service water systems.

The minimum sea water temperature is based on the salinity of the sea water. The salinity is assumed to be 0.7% which is a conservative value in the Olkiluoto sea area. The freezing temperature is –0.4°C. The subcooling of water can be at the maximum 0.1°C and is generally significantly less. Thus the lowest sea water temperature can be –0.5°C at the Olkiluoto site. The subcooling and possible formation of frazil ice is discussed later in this section.

High seawater temperature related event has been screened out from the detailed analysis using the severity criterion and low seawater temperature using inclusion criterion, and is handled in connection of frazil ice. Frequency of annual high seawater temperature is based on Olkiluoto data from the period 1988…2003.

The seawater temperature is usually close to 0°C during December to February. In case of wind preventing the formation of surface ice, the water temperature may be below 0°C. In this case the relevant external event is frazil ice, which requires the seawater temperatures below zero as one of its preconditions.

Beyond design basis consideration:

The licensee's analyses on a best estimate basis in case of sea water temperatures beyond values above state that there is no cliff edge effect with respect to impact on the systems and equipment relevant for plant safety. The most important safety functions of the plant, i.e. heat removal from the core and fuel pool via primary side cooling chain, is ensured for a sea water temperature of 37°C.

In case of extremely low seawater temperatures and simultaneously the cooling water inlet hypothetically being blocked by ice, the operation of the essential service water system is performed according to mode "blocked inlet". The margins to the design basis in OL3 have an important role because the design basis of the maximum cooling water temperature might be exceeded during the plant life. The safety of the plant has been demonstrated even in this case. However, in connection with any plant modification adequate margins to design basis shall be maintained. Safety assessment and PSA will be made in connection to plant modifications to demonstrate acceptable design. During the period from 1998…2010 the seawater temperature has been in the range of +0.4…+25°C.

Based on the cliff edge evaluation the heat removal from the core and fuel pool via primary side cooling chain, is ensured for a sea water temperature of 37°C. The frequency of occurrence of such high sea water temperature is low.

Precipitation and external flooding

Seawater levels of −1.6…+1.3 m (N60), and maximum still level plus storm resulting in +1.7 m (N60) are specified for design basis conditions for OL3. The limiting design feature in OL3 with respect to low seawater level is the minimum still level N60−1.6 m and with respect to high sea water level the ground level for the plant at 3.2 m above mean sea level (N60). The basic elevation (0.0 m) for the plant buildings is at N60+3.5 m, i.e. there is a threshold level of 30 cm as an additional protection against external flooding.

Internal and external flooding routes and consequences of flooding are analysed, and it is assured that flooding up to N60+3.5 m does not endanger the systems, structures or components required to maintain critical safety functions. Flooding is discussed in Section D.3.

The annual minimum and maximum water levels at Rauma for the period of 1971…1995 have been analysed. Using the Gumbel distribution to the level data the estimates of extreme levels for different return periods were estimated as shown in Table D-1 below.

Table D-1. Annual minimum and maximum water levels at Rauma during 1971…1995

Return period (years)	Level (cm)
10	−65
100	−86
1,000	−106
10,000	−127
100,000	−148
1,000,000	−168
10,000,000	−189

The plant is designed to withstand design-basis rainfall depth of 100 mm in 1 h, and rainfall depth of 400 mm in 24 h concerning safety against external flooding. These values are considered for normal operation of the whole plant. The rain water system is designed according to the regulations and directions in the Finnish Building Code.

During the period 1959…1987, the maximum 24 hour amount of rain for the nearest observation stations was 83 mm (Rauma town). For the Olkiluoto weather station, the one-hour maximum (1992…1996) was 25 mm. The Finnish Meteorological Institute has estimated the expected maximum 24 h precipitation on the west coast of Finland to:

- 55…65 mm for return period of 50 years
- 65…75 mm for return period of 200 years

The snow loads are treated according to conventional Finnish construction standards. The whole plant is designed to withstand the basic snow and ice loads specified in Finnish Code for Structural Loads and Effects (RIL 144). The extreme snow and ice loads are specified by hazard curves and correspond to mean return period of 10000 years. The yearly snow load as equivalent to the water quantity for a frequency of 10^{-4}/a is 498 mm water, which is equivalent to 5 kN/m^2. This load is considered for the safe shutdown of the plant.

In the return values of critical weather events at nuclear power plant units the 24-hour snow depth increase at Olkiluoto was estimated on the basis of monitoring data using the GEV and POT method. The point estimate results of the GEV method are judged to be more feasible for return periods of up to about one million years (see Table D-2).

Table D-2. 24-hour snow depth increase frequencies from GEV method used in OL3 PSA

Frequency (1/a)	24-hour depth increase (cm)
10^{-1}	11
10^{-2}	21
10^{-3}	35
10^{-4}	55
10^{-5}	127
10^{-6}	189

Measures are taken to prevent blockage of intakes of heating, ventilation and air-conditioning, diesel generators or other systems, which rely on an air supply to maintain their function. Protection against intake snow is given by grids air intake and design of “concrete noses”. All air intake and outlet openings are heated so the air intake section is always the same. Coolers and fans are designed to be actuated during cold temperatures in the cooler rooms. Moreover, in order to avoid water condensing in the below level, the floor of cooler room has thermal insulation.

Rainfall has been screened out of from the detailed analysis using the severity criterion and snowfall using the severity and inclusion criteria.

<u>Lightning</u>

The design-basis lightning levels used for the protection of buildings are consistent with IEC 61024. The following values are taken into account:

– First Stroke (10/350 ms): peak current 200 kA; front time 10 ms; time to half value 350 ms; impulse charge 100 C; specific energy 10 MJ/W.
– Subsequent Stroke (0.25/100 ms): peak current 50 kA; front time 0.25 ms; time to half value 100 ms; average steepness 200 kA/ms.
– Long Duration Stroke: charge 200 C; duration 500 ms.

Peak currents of lightning have been measured by the FMI with lightning positioning equipment during the period 1987…1994. The frequency of occurrence of lightning stroke over 150 kVA is estimated to be $1.4 \cdot 10^{-3}$/year. The recent estimates indicate that the overall frequency of lightning with amplitude below 20 kA is higher than previously assumed. Generally, the overall frequency of lightning is about 0.3 stroke per km^2 and year; based on data from 1960…2001.

The lightning protection and earthing system of OL3 is based on the lightning protection level I (LPL I) according to the international standard IEC 62305-1:2006-01. Some further statements show that also an extreme lightning discharge considerably exceeding LPL I will not lead to unacceptable damages or effects on systems and components inside the plant.

The provisions for external and internal lightning protection have been considered in plant design for reducing the electrical and electromagnetic loads caused by external or internal electromagnetic interference to a level, which is acceptable for instrumentation and control. The external lightning protection system is installed to form a “Faraday cage” around each building. The internal lightning protection concept is based on the direct and short connection of all casings of I&C equipment (sensors, junction boxes, cubicles) and cable shields to the inner grounding system. Electrical equipment includes protection against surges resulting from lightning strikes on electrical transmission lines.

With respect to lightning protection the measures are realized in the complete plant (nuclear island, turbine island, balance of plant) to ensure sufficient level of immunity against electromagnetic interferences. Both the provision against lightning and the design values are considered sufficient. This event has been screened out from PSA due to severity screening criterion.

<u>Hazards with potential effects on cooling water intakes and air intakes</u>

Based on site-specific information to be verified, the hazards introduced in the following are considered in plant design.

<u>Intake water blockage</u>

Blockage of cooling water intakes by ice, frazil ice, debris, seaweed, and marine life, e.g. bivalves, jellyfish or fish

Frazil Ice. Frazil ice can be formed when cold wind is blowing over an open water surface the temperature of which is below the freezing point. The cold air and wind induced waves together cool down and agitate the surface water. Maximum sub-cooling in sea water can be about at 0.1 °C, and is generally much lower. The flocculation becomes active at some per mill concentration. When ice cover is formed on the surface of sea the frazil ice formation will be stopped. The frazil ice phenomenon has been investigated by the Licensee for OL1 and OL2 units, equipped with the anti-icing systems after phenomenon was detected. In OL3 in order to reduce the possibility of formation of frazil ice, the precautions include the heating of the coarse screen units, equipment of travelling screens with driving plates which will remove any frazil ice. Additionally, warm water is injected from the outlet tunnel by an anti-icing pump to the inlet structures.

Estimated frequency of clogging of water intake facilities due to frazil ice is 0.11/a on the basis of experience.

The cooling water intake is protected against floating objects by the trash racks in the intake structure, and additional mechanical cleaning equipment in the inlet of the circulating water pump building.

<u>Reduced flow due to algae and marine growth (e.g. bivalves)</u>

The OL1&2 experience on mussels, living and dying in the seawater tunnels has been considered in the design of OL3. Frequency of large amount of algae is 0.02/year based on OL1&2 experience. Algae can cause an initiating event only if precautionary actions such observation of the phenomena and algae nets fail or the band screens are blocked.

Prevention of oil slicks from entering cooling water intake

The determination of a frequency of oil spills entering the ESWS inlet channel has been estimated by the Finnish Technical Research Centre VTT. The calculation is based on an Event Tree taking into account the frequency of a tanker accident in the Gulf Bothnia and three countermeasures:

– Surrounding of the oil before the islands separating the Olkiluoto bay from the Gulf
– Installation of a temporary oil boom in the inlet channel
– Manual switchover of the ESWS pumps suction towards the outlet channel

Noxious, toxic gases: The control room personnel are protected against noxious or toxic gases and other airborne effluents from external sources.

Air Intakes

The safety related air intakes will be equipped with a heated physical protection grille to prevent ice formation. The air intakes are located above maximum predicted snow levels. Floor drains are provided in the air intake plenum floors to provide for water drainage.

The design of the SAC main air intake structures affords protection for the HEMP grille and intake dampers from wind and missile hazards.

In the supply air for buildings with sensitive electrical and I&C components, filters equipped with differential pressure measurements are provided for removal of atmospheric dust.

The filtration capability of the supply air filters will ensure that supply air is filtered to prevent the build up of dust and airborne biological agents (such as pollen).

The following external hazards that can impact on seawater cooling were screened out from the detailed study:

Under-water landslide has been screened out using the severity and applicability criteria. An under-water landslide may result in deteriorated quality of the intake water, which is assumed not to threaten the plant. Furthermore, any plant effects from bad intake water quality will be gradual. If any countermeasures are required, there according to the licensee will be time to plan and to implement them. The design of the intake water structures is such that no credible land-slide can occur, resulting in loss of the ultimate heat sink.

Surface ice has been screened out using the severity and warning criteria. The depth of the intake channel is about 6 m. The Finnish Institute for Marine Research presented in that the thickness of continuous fast ice is not several meters anywhere on the Finnish coast. Furthermore, any possible plant effects from a thick ice cover will be gradual. If any countermeasures are required there will be time to plan and to implement them. The warning time may also be used for a preventive shut-down of the plant, as the plant will be less vulnerable after a shut-down for this event.

Ice barriers have been screened out using the severity, warning and applicability criteria. Rocks and islands south-west of Olkiluoto prevent pack ice from entering the water intake area with a high probability.

Corrosion (from salt water) has been screened out using the severity criterion.

Chemical release to water has been screened out using the severity criterion. The event is defined as impact due to chemical releases to water. The focus is on reduction of water quality. The releases may be due to a ship accident, but may also originate from land. No credible effect can be defined, as plant is assumed to be non-sensitive to credible scenarios.

Consideration of potential combination of weather conditions

Through the external hazard screening analysis the licensee has covered the external hazards of natural origin or man-made relevant in the proximity of the site. The following multiple external events were identified in the licensee's screening analysis of multiple events:

- Strong wind (affecting external power supply) and snow (affecting ventilation)
- Strong wind (affecting external power supply) and frazil ice (affecting UHS)

  The strong wind is precondition for frazil ice. The main effect of a loss of off-site power is the loss of the main heat sink (loss of condenser), i.e. the same effect as for frazil ice. Frazil ice can be managed in case of loss of off-site power, as the cleaning lines of the Service Water intake (including the heating of the coarse screens) are connected to the emergency power supply.
- Strong wind (affecting external power supply) and organic material in water (affecting UHS)

  Organic material in seawater will be quantified as a single event. The multiple external events will not be quantified, as presumed that organic material already alone has caused the loss of ultimate heat sink.

Conclusions on the adequacy of protection of weather conditions

The present regulatory requirements and national building guidelines have been applied in the design of OL3. Additionally, the operational experience from OL1&2, and the good practices regarding the precautions against the impact of external phenomena implemented in OL1&2 have been well utilised in the design.

Weather phenomena and other external conditions of natural origin or man-made including combinations of phenomena relevant at the plant units have been comprehensively analysed using the external hazards PSA as part of the living PSA already at early stage of plant design. The meteorological and hydrological data available from the local and national observations has been extensively utilised in analysing the duration, intensity and frequencies of external phenomena.

During the licensee process of OL3, the regulatory body has required licensee's further investigations concerning plant design basis against unexpected extreme external phenomena such as extreme outside air temperature, exceptional wind speeds and other cliff edge events. The inspection of some details is still ongoing, for instance the diversity and design basis of SBO diesel generators regarding the safety impact of external temperature.

The emergency and disturbance procedures are still under preparation. The prerequisite is that the plant personnel are capable to manage accident management in exceptional situations including extreme external conditions.

Extreme weather conditions including the impact of climate change and global warming, are studied within the EXWE project in the Finnish Research Programme on Nuclear Power Plant Safety [SAFIR2010, SAFIR2014]. The results of the programme might necessitate reconsiderations regarding design basis and safety margins for external phenomena, in particular air temperature, wind and rain. The licensee actively participates in the national research programme.

D.4.2 Evaluation of safety margins

D.4.2.1 Estimation of safety margin against extreme weather conditions

Design basis conditions cover a wide range of air temperatures and humidity for plant operation and safety functions. In this section, beyond design basis is considered at specific external conditions.

<u>Outside air temperature</u>

On a best estimate basis, outside air temperatures beyond design do not result in cliff-edge effects with respect to impact on systems and equipment relevant for plant safety.

The most important safety functions of the plant are heat removal from the core and fuel pool via primary side cooling chain, secondary side cooling chain, safety relevant HVAC and chilled water, and emergency power supply. These are ensured for the extreme temperatures of –41°C and +40°C for 6 h. The margins to design basis in OL3 have an important role because the design basis of the maximum or minimum air temperature or the duration might be exceeded during the plant life.

The ventilation systems with relevance to the safety areas and potentially affected by extreme outdoor air temperatures are the main control room, electrical division of safeguard building, diesel building, station blackout diesel building, essential service water pump building, containment and fuel building. The ventilation systems for main control room, electrical division in safeguard building and essential service water building are to a large degree independent of the outside air temperatures and operable in recirculation mode. The building insulation according to the Finnish Building code reduces the impacts of the external phenomena.

The licensee has comprehensively assessed the functional ability and robustness of each ventilation system against extreme outside temperatures in ensuring the most important safety functions. These evaluations and calculations show that the design will to some extent ensure the function of ventilation systems in extreme external conditions of beyond design basis due to different items regarding diversity, redundancy, safety classification of equipment, back-upped electric supply, physical location of equipment, insulation of structures and buildings, air flow portion of outside air needed in recirculation mode, propagation of heat loads and plant configuration in exceptional conditions, and so on.

However, further studies are ongoing concerning the plant robustness against extreme high and low outside temperatures.

<u>Cooling water temperatures</u>

The most important safety function regarding temperature is to ensure the heat removal from the core and spent fuel pool in extreme seawater temperature i.e. the design basis +37°C.

In case of extreme temperatures for seawater (+37°C) and outdoor air (+40°C) the plant cool down as well fuel pool cooling can be performed without exceeding admissible system temperatures. The licensee's studies indicate that the cooling water supply can be kept below 45°C even when the temperature of seawater is +37°C.

According to licensee's analysis, the shutdown of the plant is possible with one residual heat removal system train under conservative conditions. With one RHR train, the heat is removed from the fuel pool, for which the water temperature of 53.3°C is evaluated under conservative conditions.

The fuel pool temperature has been calculated for full core discharge with two trains in operation. It is assumed, that there is no fuel pool cooling for the first two hours because of switch over measures in system PE. The fuel pool water temperature reaches a temperature of approx. 70.2°C two hours after failure of the spent fuel pool cooling. After two hours the fuel pool cooling is started again and the temperature decreases to 52.4°C (steady state conditions).

The minimum design temperature of the essential service water system is –0.4°C. The component cooling water system (safety related) is equipped with a bypass valve which maintains a minimum temperature of above 17°C. This means that it is ensured also in case of very low seawater temperatures that all the systems including chilled water system cooled by CCWS remain unaffected by this low seawater temperature.

In case of extremely low seawater temperatures, i.e. cooling water inlet hypothetically blocked by ice, the operation of the essential service water system is performed according to the mode "blocked inlet". This means suction will be taken from the cooling water seal pit. In this case the heated-up cooling water can be removed via anti-icing line. This mode can be performed for unlimited time. Only in case of even blocked anti-icing line the cooling water will be recirculated in closed loop, i.e. not being discharged via anti-icing line. The system design allows maintaining this mode up to cooling water temperatures of 37°C for a certain time, which allows performing measures to re-establish possibility to release via anti-icing line.

The available time depends on the operating mode. Two typical modes had been analysed:

- Plant in power operation, turbine and reactor trip after onset of the event. If after reactor trip the plant is maintained in condition "sub-critical, hot" with heat transfer via secondary side (EFWS and MS relief valves). The CCWS/ESWS removes heat from fuel pool cooling and component cooling (e.g. safety chillers). In this situation an operation for approx. 8…10 h can be guaranteed before reaching 37°C.
- Plant in primary side RHR mode, core in the RPV or unloaded in the spent fuel pool. The CCWS/ESWS removes heat from primary side, fuel pool cooling and component cooling (e.g. safety chillers). In this situation an operation for approx. 7…9 h can be guaranteed before reaching 37°C.

Further studies are ongoing concerning the plant robustness against extreme high and low seawater temperatures.

Wind and wind-generated missiles

The tornado loads are covered by plant design against external hazards; discussed in the previous section. Furthermore there is no cliff edge effect because the above given statements regarding tornado EF2 are also valid for a tornado EF3.

D.4.2.2 Measures which can be envisaged to increase robustness of the plant against extreme weather conditions

At this moment, no such design deficiencies have been identified regarding provisions against natural hazards that would lead to significant changes in the plant design. However, the further investigations requested by the regulatory body are ongoing regarding the plant robustness against extreme external phenomena.

To respond STUK's requirements after the Fukushima accident, the licensee is studying the following issues regarding exceptional extreme external conditions:

- the adequacy and availability of water supply for the cooling of reactor and spent fuel storage;
- the reliability of heat removal to ultimate heat sink;
- the impact of extreme high seawater level on the cooling systems of the spent fuel storage;
- the impact of beyond design basis high and low outside temperatures on the safety functions; and
- the applicability of procedures, and the adequacy of personnel, equipment and facilities.

D.5 Loss of electrical power and loss of ultimate heat sink

D.5.1 Loss of electrical power

A schematic of OL3 electric diagram is presented in Figure D-2 below.

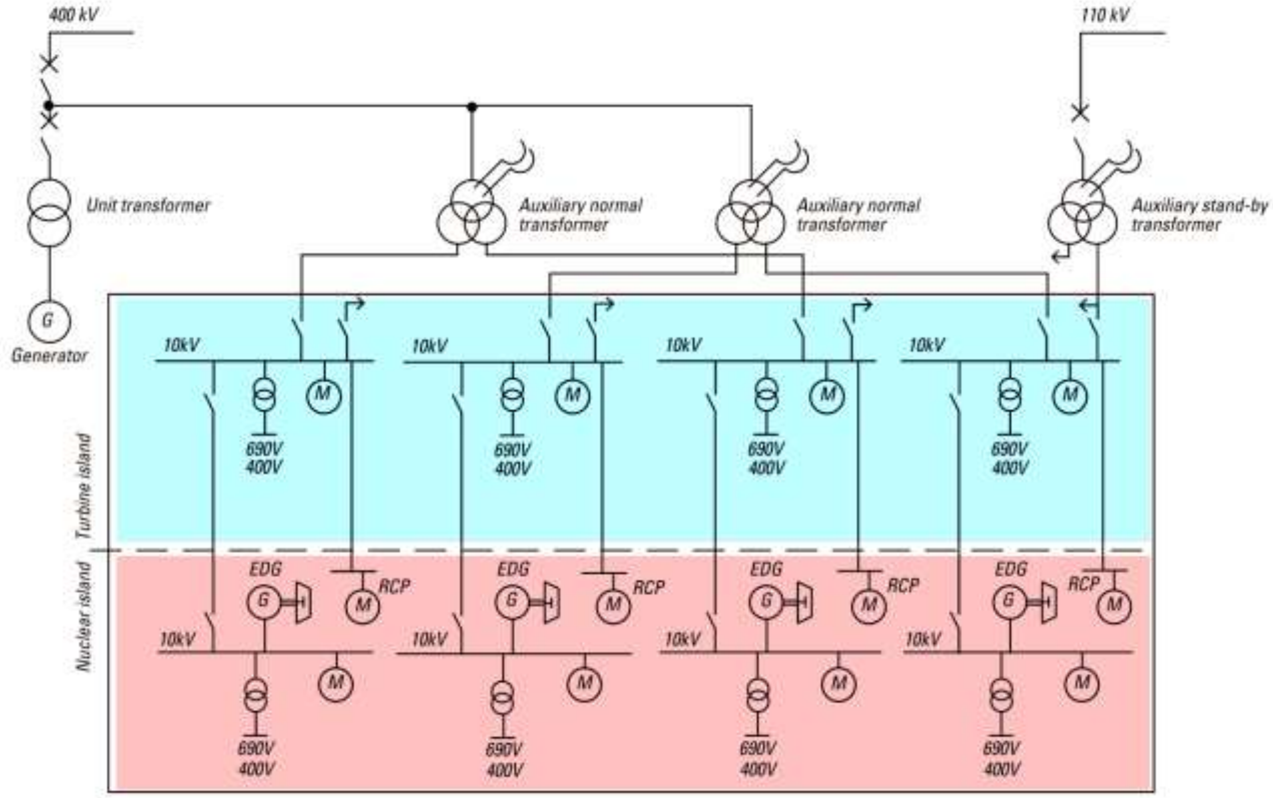


Figure D-2. Simplified schematic of OL3 electric diagram [TVO 2010]

D.5.1.1 Loss of off-site power

The connection of the OL3 plant to the Nordic 400 kV power grid is implemented with two independent 400 kV overhead lines running from the Olkiluoto switchyard to different grid nodes. Damage of a single 400 kV overhead line will not cause the loss of 400 kV grid connection. In addition, the plant is connected to the national 110 kV power grid. The connection is implemented with two separate transmission lines.

House load operation is the first defence line against the losing of the 400 kV grid connection. If this automatic switchover is successful, the plant can continue the house load operation indefinitely.

If the 400 kV grid connection is lost and the house load operation is not possible, plant will try to switch to the national 110 kV power grid. The switchover is automatic fast transfer. If the 110 kV grid is available but the automatic switchover fails, operators can make the connection manually.

Switchgears (BBA, BBB, BBC and BBD) critical to the grid connections and house load operation are located at level +3.5 m (from sea level) in two fire compartments.

The main defence line against loss of AC power is emergency diesel generators (EDGs). OL3 has four individual EDGs. The capacity of the EDG-system is 4×100% and the generators are located in two separate diesel buildings. Each EDG is in its own diesel room that is an own fire compartment at +3.5 m level. The switchgears of safety loads and required automation systems are at +11.65 m level in separate safety buildings. EDGs are air cooled. Each EDG is feeding its own safety division.

If the off-site power is lost, EDGs will start automatically within 15 s and provide power to the safety systems. If automatic start-up is not successful, EDGs can be started and connected manually, either from the main control room or locally.

Each EDG has a fuel tank (day tank) with fuel enough for 2 h of operation. These day tanks are automatically filled from storage tanks. There is one storage tank per EDG with enough fuel for 72 h of EDG operation.

D.5.1.2 Loss of off-site power and loss of the ordinary back-up AC power sources

If the EDG operation is not successful, emergency back-up power can be provided from a diverse station blackout (SBO) diesel generator systems. OL3 has two individual SBOs. There are two SBOs and they are dimensioned to handle anticipated transient and small LOCA accident situations. The generators are located in two separate diesel buildings. Each SBO is in its own diesel room that is an own fire compartment at +3.5 m level. The switchgears of safety loads and required automation systems are at +11.65 m level in separate safety buildings. SBOs are air cooled, and the supply two of the safety divisions.

If the on-site power is lost, SBOs must be started and connected manually from the main control room or locally. The start and operation of the SBO- diesel can be done with and without I&C power supply working (in case 2 h batteries are empty). SBO diesel start and connecting without auxiliary power supply (no battery power available) can be done only manually from local control panel (in the diesel building) and locally on the requested switchgear.

Each SBO has a fuel tank (day tank) with fuel enough for 2 h of operation. These day tanks are automatically filled from storage tanks. There is one storage tank per SBO with enough fuel for 24 h of SBO operation.

If the EDG or SBO operation is not successful, emergency back-up power can be provided from a gas turbine plant. The gas turbine plant has two 50 MW generator units, each with two gas turbines. Each gas turbine alone is capable of providing the required emergency power to all Olkiluoto units (OL1, OL2, OL3). The gas turbine plant is located above +3.5 m. The plant is separated from nuclear units and is air cooled.

The gas turbine plant has dedicated cable connections to the 10 kV EDG bus bars of OL3 units but it can also be connected via the 110 kV switchyard. Switchgears (642) needed to the gas turbine connection are located at level +11.65 m (see Section D.5.1.1).

The gas turbine plant has to be started and connected manually, but operators can perform all the required operations from the main control room of OL3. Also local operations are possible. Required main control room operations can be performed within 5…15 minutes.

The gas turbine plant has storage tanks with combined fuel capacity of 48 h of use at full nominal power. In emergency situations when the gas turbine plant is used to support OL1, OL2 and OL3 units, it is sufficient to use only one gas turbine providing 20 MW of power. This will limit the fuel consumption so that fuel will last for about 9 days.

It is also possible to supply electrical power from the main generator of OL1 to OL2 or from the main generator of OL2 to OL1 using the connections at the 400 kV switchyard. The instructions and procedures for these actions are being prepared at present. When OL3 unit starts operation, the main generator of OL3 can similarly be used to supply electrical power to the other plant units, and vice versa, using the 400 kV switchyard connections.

Battery capacity issue is described in Section D.5.1.3.

D.5.1.3 Loss of off-site power and loss of the ordinary back-up AC power sources, and loss of permanently installed diverse back-up AC power sources

Battery backed electrical systems are located in four separated divisions. The capacity of the redundant safety systems is 4×50% in all important (SC2) functions. Capacity is 2×100% in some lower class safety functions. Each redundancy is in its own safety building. The lowest equipment rooms are in level +11.65 m.

The list below presents the capacities and loads supplied by each battery-backed system:

- NI 2 h battery backed power supply
    - 4 redundant systems (in four separated divisions)
    - Feeds all electrical equipments which require uninterruptible power in the nuclear island
    - Discharge time 2 h
- NI 12 h battery backed power supply system
    - 2 redundant systems (in two division with the SBO diesel generator supply)
    - Feeds loads which are important in case of severe accident and require an uninterruptible power supply
    - Discharge time 12 h

Portable electric power sources for battery loading are not designed for the OL3.

The time in case of total loss of AC power is two hours without fuel overheating to prevent fuel cladding overheating and cladding failure. Opening of the pressurizer safety valves and loss of primary coolant would take place but fuel integrity would be ensured. The first opening of the first pressurizer safety valve would take place at 1h 20 min and there would periodic opening and closing of the first safety valve to 1 h 50 min. Pressurizer safety valves would remain open after 1 h 50 min into the accident when there would be no manual actions and the steam generators would have boiled dry. Until 1 h 50 min the coolant loss from the primary system would be small. Core uncover would take place within 3 hours, extensive fuel damage would be caused within 4 hours and pressure vessel melt-through would take 7 to 8 hours.

During the loss of all AC power, removal of the decay heat from the spent fuel elements in fuel pools is prevented. The limiting worst-case situation for the available time is the evacuation of the whole reactor core to the pool. The decay heat power after the unloading of the core is about 21 MW. If the pool cooling is lost in such a situation, the pool water will start boiling in about 4.5 h. About 25 h after the start of the event water level will be down to two meter above the top of the fuel elements. After 31.8 h the top of the fuel elements will be uncovered. To prevent the water-level drop in the pools, make-up water supply of about 9.3 kg/s would be needed to compensate for the boiling.

Normally, the decay heat generated by the spent fuel elements stored in the reactor building fuel pools is much less. That would mean that the boiling will start after 7.2 h in the beginning of cycle or after 22.4 h in the end of cycle (with separated fuel pools). To prevent the water-level drop in the pools at the start of the cycle, make-up water supply of about 2.7 kg/s would be needed to compensate for the boiling.

The make up system for water supply in case of fuel pool evaporation cooling is the fire water system which has both electric and diesel driven pumps. Only few manual measures like installation of hoses or manual change of position of valves are required.

D.5.1.4 Conclusions on the adequacy of protection against loss of electrical power

Based on various studies done for the OL3, design of the electrical power supply systems are assessed to be on the adequate level. There is no natural hazard identified, which could lead to total loss of the internal power sources.

However the time margin for the recovery of the AC-power supply before fuel damage is quite short if a total loss of the AC-power occurs. Core damage will start about 4 h after the start of the blackout. After this the situation must be handled using severe accident management systems.

Limiting battery capacities are 2 h. This is adequate in the current situation compared to the time after which one must start to use the severe accident handling systems. Battery capacity of the severe accident management systems is described in Section D.6.

The plant has adequate autonomy of EDG fuel (72 h) but the storage capacity of SBO fuel (24 h) is too limited in extreme external conditions. The power company (TVO) must develop means to refill SBO storage tanks from other fuel supplies in the site.

STUK is still evaluating the detailed design of OL3. At the moment there seem to be no such issues within the electricity supply that would require significant changes for preparation of the lincense application for operation.

D.5.1.5 Measures which can be envisaged to increase robustness of the plant in case of loss of electrical power

At present the licensee (TVO) is planning no modifications to OL3 plant but TVO must develop means to refill SBO storage tanks from other fuel supplies in the site.

D.5.2 Loss of the decay heat removal capability/ultimate heat sink

D.5.2.1 Design provisions to prevent the loss of the primary ultimate heat sink

Total loss of the ultimate heat sink (sea water) has been taken into account in the OL3 design and all safety functions are ensured in case of loss of the ultimate heat sink. The consequences of extreme external phenomena such low water level, freezing, frazil ice, blockages of cooling water intakes due to potential impurities in intake water or oil slicks have been considered at different plant operating states.

<u>Power operation</u>

The loss of ultimate heat sink during power operation is classified as a complex sequence (DEC-A case as an extension to postulated accidents). The consequences of the event are considered in the plant design and can be managed without violating the proper success criteria. The analysis performed for power operation according to the safety analysis rules shows that in case of a total loss of heat sink, the controlled state can be reached with the fulfilment of the acceptance criteria. The transition from the controlled state to the safe shutdown state with the RHR in operation can be performed by the operator following recovery of cooling chains. After 72 h the LUHS is assumed to be terminated and all the necessary systems for plant cool down and RHR connection are available. Reactor coolant system pressure and level measurements, core outlet temperature and SG pressure and level measurements are indicated in the MCR.

<u>Refuelling outage</u>

In case a total loss of ultimate heat sink during the plant refuelling outage the residual heat removal is ensured by the diverse cooling of the LHSI system pumps and the containment venting system. The reactor coolant system tightness is ensured by the actuation of the standstill seal system and by the closure of the coolant pumps seal leak-off lines. The containment can be closed before the steaming of the reactor coolant.

The analysis performed according to the safety analysis rules shows that in case of a total loss of heat sink during refuelling outage, the controlled state can be reached with the fulfilment of all the acceptance criteria. The core cooling is ensured by the LHSI pump with wide margins, and additionally, the heat removal from the containment is ensured by means of the containment venting for >72h. With the refill of the IRWST from the EFWS tanks the LUHS can be mitigated within the acceptance criteria for much more than 72 h. The containment venting would start at 12 h into the event.

In a shutdown state, the reactor vessel head still remaining closed, the opened man ways of the steam generator primary or secondary side can be closed in order to re-pressurize the reactor coolant system and the secondary side, and to remove the heat through the secondary side.

According to the licensee, all uncertainties involved are generally covered by enveloping boundary conditions and big margins to the acceptance criterion (i.e. the avoidance of recriticality and boron crystallization).

The loss of boron by venting is covered by the assumed 23000 ppm boron concentration in the core for the boron concentration analysis. Boron crystallization is excluded at any time of the transient.

Freezing

Cold weather protection is provided by ensuring the heat sink reliability (protection against freezing of the water intake) of the ESWS. This is accomplished by adequate heating (space heating), building structure inertia and heat sink water recirculation to the water intake.

Frazil ice

Criteria will be defined in the operating manual to identify the event. In this context experience from the existing units OL1 and OL2 will be taken into consideration. To prevent a blockage of the trash rack inside the inlet channel, a part of the preheated cooling water is re-injected into the cooling water stream. The recirculation flow is 3 m^3/s.

During power operation, a part of the main cooling water (heated up by the turbine condenser) is discharged back to the inlet rock tunnel via the anti-icing line. This will only be effective during power operation because heating up of the cooling water is provided by the condenser. The anti-icing pumps are not emergency powered and not safety classified. If the anti-icing line cannot ensure sufficient water supply for normal operation, the plant will be shut down in accordance with the operating manual, and only water supply for essential service water is needed. A consequential loss of offsite power in conjunction with frazil ice is not assumed because frazil ice has no effect on the offsite grid.

Emergency powered heating of all four cleaning lines (the coarse screens are heated) for assuring the supply for all redundancies of ESWS. In case of water intake blockage by frazil ice, a sufficient flow (800 kg/s per train) to the ESWS is ensured. Presuming all the countermeasures above failed, the features described under “blocked cooling water intake” are considered.

The OL3 cooling water intake is surrounded by islands, thus being protected against thick ice masses caused by ridged or hummock ice.

Marine life (e.g. seaweed, jellyfish, algae)

The plant will be provided against seaweed, jellyfish and algae in seawater:

- Manual cleaning of the intake screens in the circulating water intake structure
- Monitoring of circulating water screening plant equipment by differential pressure measurement
- Automatic cleaning of the screening plant in circulating water pump building; additional manual cleaning can be performed.

If the cleaning of the screens cannot ensure sufficient water supply for normal operation, the plant will be shut down in accordance with the operating manual. Consequential loss of offsite power in conjunction with marine life is not assumed because marine life has no effect on the offsite grid. Presuming that all countermeasures against biological impurities above will fail, the features described under "blocked cooling water intake" are considered.

Measures against bivalve fouling

Due to the slow flow velocity in circulating water intake rock tunnel, the loose shells from bivalves will mainly sink and accumulated in the rock tunnel. The larvae of the mussels will be transported. The cleaning plant in circulating water pump building will remove loose shells via the coarse and band screens. The larvae can pass through the cleaning plant. The cleaning of the circulating water pump building and its facilities with respect to mussels will be done depending on the amount of mussels.

Each of the four ducts from the UQA building to the service water pump buildings UQB can be isolated separately and manually cleaned.

The ESWS trains are protected against bio-fouling with the following countermeasures:

- selection of piping material which provide the smoothest surface roughness in order to reduce the attachment of mussels;
- selection of piping diameter in order to achieve a flow velocity of nearly 2.9 m/s which entrains the mussels and avoids attachment;
- upstream of the ESWS-CCWS heat exchanger a Taprogge debris filter is installed. The filtered mussels are back flashed to the downstream side of heat exchanger, and further transported to the outlet; and
- differential pressure measurements are provided for the pumps and the heat exchangers.

The dedicated ESWS trains are closed during normal plant operation, the part of the system including the heat exchanger and the debris filter are filled with demineralised water, which prevents organic (mussel) growth due to oxygen deficit and the smooth rubber surface in the pipes. The debris filter backflushing sequence will simultaneously be initiated when the pumps will function, thus preventing the clogging the filter.

Blocked cooling water intake

The cooling water intake is equipped with various screening facilities against algae, seaweed, marine life and debris, and other biological and organic material. If however, the sufficient water supply during normal plant operation cannot be ensured, the circulating water pumps will be switched off. After the trip of the circulating water pumps, a sufficient water supply for the ESWS pumps will remain. The required flow rate for all trains of the essential service water is lower than 8% of the required flow rate for all cooling water systems. The flow rate for all cooling water systems is even ensured in case of operation of 3 active cleaning lines (preventive maintenance of one screening plant). Due to this low required flow rate for essential service water, a sufficient free screen surface will be available for this water demand, even in case of the loss of the active cleaning function of the whole screening plant.

In case of frazil ice, the prevention of cooling water intake blockage will be done by warming the circulating water inlet by means of a conventional anti-icing system. Furthermore, the four cleaning facilities for circulating cooling water are emergency powered. In addition, the heating of the intake rack in circulating water pump building is secured by emergency power.

If the entire cooling water inlet is unavailable due to blocking, the ESWS pumps can be supplied with cooling water through the connection from the circulating water seal pit to the circulating water pump building supplying the essential service water pump buildings. The flow direction is reversed, from the circulating water outfall rock tunnel for at least two redundancies of service water. This connection needs to be opened manually.

The ESWS outlet lines will be switched over to the intake channel via an alternative outlet line (anti-icing line). This is established for all ESWS trains. The switchover can only be carried out when the anti-icing pumps are not in operation. The anti-icing line is designed for a flow of approx. 3000 kg/s (2 of 3 pumps in operation). According to the safety requirement only two lines are needed.

<u>Oil hazard</u>

The preventive measures against oil slicks are common with OL1&2 (see Section C.5.2).

After the detection of possible oil pollution in the cooling water intake protective measures are taken by the licensee's fire brigade at the plant site. The entry of oil pollution into the cooling water intake will be prevented by oil protection booms.

The oil can be collected into tank vehicles by suction. The oil pollution protection vessels of the Rauma, Pori and Eurajoki can be used if necessary. In case the entry of fine-grained submerged oil into the water intake cannot be prevented, the primary protection measure against oil pollution will be to change the ESWS water intake from the inlet side to the outlet side.

In the worst case if both the inlet side and outlet side have oil pollution and the entry of oil into the ESWS cannot be prevented, the ESWS will be unavailable. The event would thus lead to the loss of the ultimate heat sink (LUHS), which is taken into account in the plant design.

A summary of alternative possibilities for arranging the removal of reactor residual heat with the reactor in hot shutdown state

In hot shutdown state the decay heat will be removed through steam generators before the RHR connection.

The reactor will be tripped and all four main steam system trains are in operation, leading the steam generated in the steam generators to the condenser through the main steam bypass (MSB) or to the atmosphere.

When the MSB is not available, the steam generated in the steam generators will be released to the atmosphere by the MSRTs in an automatically controlled mode at 95.5 bar.

In an intermediate shutdown state the reactor can be under two different statuses: either the LHSI/RHRS system is connected or not. When the RHRS is not connected, core decay heat and RCS pumps power are evacuated by the MSB system to the condenser, and the feed water flow is supplied to the SGs by the start-up and shutdown system (SSS) or the emergency feed water pumps.

In case the unavailability of the condenser, the steam will be discharged to the atmosphere through the MSRTs, and feed water supplied by the SSS or the emergency feed water pumps, if the SSS is not operable.

Availability of competent personnel and existence of applicable operating instructions

The operating instructions are based on normal shift manning being adequate, and they will cover the postulated conditions. In severe accidents the emergency organisation will apply severe accident management guidance.

A summary of alternative possibilities for bringing the reactor from hot shutdown state to cold shutdown state

Alternative possibilities

Cooling by sea water is necessary for reaching the cold shutdown state.

The primary system pressure can be reduced either by transferring the heat through the secondary side or by opening of the pressurizer valves (safety valves or the dedicated valves). In both cases, the use of the safety injection system or emergency boration, or both is necessary for maintaining the primary system coolant inventory and core subcriticality.

The cold shutdown can be reached by transferring heat directly from the primary system through the cooling chain: the RHRS, CCWS and ESWS. In the normal cooling down procedure, the four LHSI trains in the RHR mode are needed to meet the cold shutdown in the optimum duration.

In case of one train is lost during the cooling phase, the impact will concern only the duration of this phase. Before the connection of the SIS trains in the RHR mode, the system is conditioned to limit the fatigue phenomena due to thermal solicitations especially regarding the LHSI pumps. This state is defined as intermediate shutdown with the RCS temperature above 120°C (or 135°C when MSB is not available) where the RHR is performed by the SGs. Above this temperature, the LHSI/RHR is not connected to the RCS.

In the first step, the two LHSI/RHR trains (in RHR mode) are involved to reduce the risk of a possible break when the LHSI line is aligned in residual heat removal mode outside the containment, directly associated with the pressure build-up in the room.

The RCS is closed and full (pressurizer level at zero load set point), and two RCPs are in operation. After reaching the RCS temperature of 100°C, the LHSI trains 2 and 3 are lined up. Thus, all the four LHSI trains in residual heat removal mode are involved as long as the reactor coolant system is full with respect to the cooling gradient requirements

(50°C/h). Two RCPs are in operation between 100°C and 70°C and one between 70°C and 55°C.

In parallel of the RCS cooling, the pressurizer level will increase. When the pressurizer level reaches the RCP spray lances, (at about 70°C) the RCS system is declared in solid state: the RCS pressure control is thus performed by the CVCS letdown line. One safety injection system accumulator (previously depressurised to 22 bar abs) will be connected to the RCS by opening its isolation valve. This connection is done in order to protect the RCP seal injection from damages in case of inadvertent depressurisation due for instance to a charging flow loss when PZR is in solid state.

All the RCPs will be stopped before dropping the RCS pressure below 27 bar. The automatic protection from the RCS loop level is only performed by the MHSI.

The accumulator, which was depressurised and connected to the RCS, will also be isolated before the dropping of the pressure and draining of the RCS. All the LHSI/RHR trains are involved to keep the RCS temperature below 55°C.

In case of LOOP the RCPs would not be in operation. In case the pressurizer spray (normal or auxiliary spray) is not operable, the reactor coolant system would depressurised and the pressurizer cooled by opening the pressurizer safety valves.

The RHR could be connected at 180°C in accident conditions.

The second possibility is to remove the decay heat from the containment by the cooling chain CHRS–CCWS–ESWS. The coolant would be recirculated to the reactor from the containment with the LHSI pumps in the divisions 1 and 4 where the pumps are cooled by the chilled water system with outside air as heat sink.

Total loss of the CCWS on the four trains would lead to the unavailability of the four SIS/RHR train except the two LHSI pumps (in trains with SBO diesels) which will be kept available by an emergency cooling using the safety chilled water system. These two pumps available will be used for the circulation of reactor water. The CHRS will transfer the residual heat from the IRWST to the ultimate heat sink via the intermediate dedicated cooling system. This will be achieved by cooling the IRWST water by the CHRS heat exchanger connected to the dedicated trains of the CCWS and ESWS.

Availability of competent personnel and existence of applicable operating instructions

The operating instructions are based on normal shift manning being adequate, and they will cover postulated conditions. In severe accidents the emergency organisation will apply severe accident management guidance.

A summary of alternative possibilities for the removal of residual heat from the reactor containment with containment pressure and temperature not exceeding design values

The use of active systems to remove the decay heat from the containment is connected to achievement of cold shutdown state. The use of the containment filtered venting system is connected with loss of ultimate heat sink during shutdown and severe accidents.

In severe accidents residual heat will be transferred into the containment atmosphere by water evaporation in the spreading compartment. In order to control the containment pressure, the CHRS transfers heat from the containment atmosphere to the IRWST by spraying the containment dome. The spray water condenses the steam in the containment atmosphere, and the water flows back to the IRWST, from where it is pumped through the heat exchangers further back to the spray nozzles.

D.5.2.2 Loss of the primary ultimate heat sink

Availability of an alternate heat sink

Sea water is the normal ultimate heat sink for decay heat removal.

The safety functions of the ESWS are to ensure
- heat transfer (decay heat mainly) from the CCWS during accidents;
- continued heat transfer from the fuel pool cooling ystem via the CCWS as long as any fuel assemblies are in the spent fuel storage pools located outside containment; and
- heat transfer during severe accidents by two dedicated ESWS pumps via dedicated CCWS trains; heat removal from containment shall ensure containment integrity.

In case of the total loss of sea water, the reactor core heat would be released to the atmosphere via the SG secondary side MSRTs. During refuelling outage the containment filtered venting would be used. The spent fuel pools would be cooled by evaporation.

Possibilities to remove heat to the atmosphere

<u>Steam generators and main steam relief trains</u>

In abnormal operation (if the MSB to the condenser is not available), the residual heat will be removed by the main steam supply system as a steam transfer to the MSRT from the hot shutdown conditions until RHRS connection conditions will be reached.Component cooling will be provided with the safety chilled water system air as heat sink.

The main steam supply system is able to discharge steam by the following means:
- 4 MSRTs, one per steam generator, each with a capacity of 50% of the full load steam generation at a set point of 95.5 bar.
- 4 main steam safety valves, one per steam generator, each with a capacity of 25% of the full load steam generation at a set point of 102 bar.
- 4 main steam safety valves, one per steam generator, each with a capacity of 25% of the full load steam generation at a set point of 105 bar.

Consequently each steam line can dump 100% of the steam generated in the SG of the associated loop to the atmosphere.

<u>Containment filtered venting system</u>

In case of reactor vessel is open and LUHS will occur, the nuclear cooling chain would not be efficient. The containment filtered venting system could be used for decay heat removal. The cooling of the core can be achieved by make-up water supply from the IRWST and coolant evaporating. The IRWST water replenishing can be performed via a water supply line. The generated steam can be routed through the containment filtered venting system to the stack.

In case of a severe accident situation, the containment filtered venting system is used to release the non-condensable gases in a later stage of the accident in order to depressurize the containment and minimize the possible uncontrolled release of radioactive substances into the environment. To restrict the releases along with the vent gas flow to the environment an efficient retention of airborne aerosols and iodine will be carried out. The filtered containment venting function is further utilised in PSA level 2 as an ultimate means to ensure containment integrity and limit the releases to the environment.

Possible time constraints for availability of alternate heat sink

Power operation

The water inventories of the emergency feed water storage tanks and demineralised water tanks of OL3 are designed for 72 h regarding plant operation at full power at the initiation of an event. At the site, there are two raw water storage tanks (about 2500 m^3 and 3000 m^3) and additional water can be supplied from the Korvensuo fresh water basin or Eurajoki river. Using sea water (conservative salinity 0.7%) would be the last option.

Refuelling outage

The analysis performed according to the safety analysis rules shows that in case of a total loss of heat sink during refuelling outage the controlled state can be reached with the fulfilment of the acceptance criteria. The core cooling is ensured by the LHSI pump with big margins and the heat removal from the containment is also ensured by means of the containment venting for longer than 72 h. With refill of the IRWST from the EFWS tanks the LUHS can be mitigated within the acceptance criteria for much more than 72 h.

D.5.2.3 Loss of the primary ultimate heat sink and the alternate heat sink

As described, the sea water and atmosphere are the diverse heat sinks and simultaneous loss of both excluded is considered very unlikely, and thus excluded from the analyses.

The quantification of external hazards has been done for following single and combination of multiple external events:

a) Single external events: frazil ice, organic material in water, oil spills, and strong wind
b) Combination of strong wind (affecting external power supply) and snow (affecting ventilation)

The Core damage frequency estimate from the external hazards other than external flooding and seismic events is $1.2 \cdot 10^{-7}$/a (point estimate), which is 1.2% of the design target of 10^{-5}/a set in Guide YVL 2.8.

D.5.2.4 Conclusions on the adequacy of protection against loss of ultimate heat sink

There is no natural hazard identified, which could lead to total loss of safety systems, fire water system and the internal power sources.

Based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK required the Licensee to provide a plan and schedule to ensure reactor heat removal in case of loss of existing systems. Furthermore the licensee was required to investigate possibilities to secure heat removal from the fuel pools in the fuel building of OL3 and heat removal into the ultimate heat sing in case of exceptional external events.

D.5.2.5 Measures which can be envisaged to increase robustness of the plant in case of loss of ultimate heat sink

To respond to STUK's requirements after Fukushima accident, Licensee further evaluated the robustness of EDG building doors against flooding (see Section D.3.2.1), and the results indicate that there is no threat to loss of EDGs due to flooding. Licensee also states that common cause failures are comprehensively taken into account in the design of OL3. STUK is evaluating this assessment and will take into consideration of causes other than flooding leading to loss of EDGs.

However, Licensee has evaluated the modifications needed to fulfil the requirement above, and possibilities to implement external feed water connections to the SG secondary side, connections to external AC power supply and external make-up water injection into the RCS during refuelling outages have been under consideration.

For the decay heat removal from the fuel pools in the fuel building of OL3 the possibility to use fire water systems and boiling of the pool water has been evaluated. Additional mobile pumps to provide water injection into the fire water system are to be acquired before the start of operation of OL3. The needed external connection points, as well as temperature and level measurements are included in the design of the fuel building systems.

Furthermore, licensing of OL3 is still underway, and STUK is evaluating fulfilment of the national resuirements set in YVL guides.

In order to reduce the threat of oil spills to the heat sink, the licensee is strengthening the protection against marine oil spills. In addition to the oil booms stored next to the water inlet channels, extra oil booms have been stored on the nearby islands. These can be used to close the sounds between the nearby islands on the inlet side of Olkiluoto site, which will provide additional protection. The instructions for taking the extra oil booms in use are under preparation, but the equipment would be available if needed, already.

D.5.3 Loss of the primary ultimate heat sink, combined with station blackout

D.5.3.1 Time of autonomy of the site before loss of normal cooling condition of the reactor core and spent fuel pool

According to the licensee's estimation, time constraints related to the station blackout apply with the loss of ultimate heat sink combined with station blackout. The time constraints are discussed in Section D.5.1.

The OL3 autonomy time in case of total loss of AC power is two hours without fuel overheating to prevent fuel cladding overheating and cladding failure. Opening of the pressurizer safety valves and loss of primary coolant would take place but fuel integrity would be ensured. The first opening of the first pressurizer safety valve would take place at 1 h 20 min and periodic opening and closing of the first safety valve would continue until 1 h 50 min. Pressurizer safety valves would remain open thereafter, if no manual actions were carried out and the steam generators would have boiled dry. Until this time the coolant loss from the primary system would be small.

D.5.3.2 External actions foreseen to prevent fuel degradation

There is no natural hazard identified, which could lead to total loss of safety systems, fire water system and the internal power sources.

D.5.3.3 Measures, which can be envisaged to increase robustness of the plant in case of loss of primary ultimate heat sink, combined with station blackout

Any design modifications to plant are not considered relevant at this moment.

D.6 Severe accident management

D.6.1 Organization and arrangements of the licensee to manage accidents

As the general organisational arrangements are common for the whole Olkiluoto site, only the issues for OL3 that are different from those described in Section C.6.1 are explained here.

D.6.1.1 Organisation of the licensee to manage the accident

Organization during normal operation and accidents

OL3 operation will be based on an assumed shift staffing of control room operators and field operators.

The Olkiluoto Emergency Plan (OEP) will contain the description of the emergency organization and instructions for OL3. The OEP is under preparation and it shall be approved by Regulatory Body before fuel loading.

Control rooms and emergency centres

The main control room and the secondary control room, as well as the emergency centre, are shielded against radiation and have filtered emergency ventilation systems.

Procedures, training and exercises

The Abnormal Operating Procedures (AOPs) have been defined so that the event sequences leading to the same kind of phenomena are handled in the same procedure. This means that procedures are defined globally and not for individual events. The event sequences assigned to an AOP are always considered in early phase where no reactor trip or hazard alarm is actuated. The actions concentrate on checking the plant state and the effectiveness of automatic functions, the state of operational systems, the stabilization of the plant at part load and the conditions for restart to full power or shut down to hot shutdown.

For emergency operation event-based and symptom-based procedures (EOPs) are used. An event-based procedure is, in general, a scenario dependent procedure. It is developed and optimised to respond to a specific family of events.

In case of a severe safety function challenge during emergency event diagnosis or event-based emergency operation, or if the initial event diagnosis proves impossible, the operators have to change over to symptom-based emergency operating procedures in order to ensure the safety of the plant. Symptom-based EOPs enable operator to respond to plant situations for which it is not possible to identify accurately the event that has occurred or where no specific event-based emergency procedure has been provided due to complexity of the event sequence or of its low probability of occurrence.

Safety function monitoring has to be applied during emergency operation starting from all operational conditions. Monitoring is performed initially by the Shift Supervisor and thereafter by the Safety Engineer, when available.

In case of severe accident separate severe accident management guidance document will be provided for the emergency organization management team to help assess the accident conditions and determine what coping strategies need to be implemented. Emergency organization will train these situations every year.

D.6.1.2 Possibility to use existing equipment

Use of mobile equipment is not planned for OL3. The mobile equipment of the fire brigade can be used, if necessary, in conditions that exceed the design bases.

Provisions are made to enable an event to be controlled and the reactor to be brought to a safe shutdown condition. For mitigation of severe accidents it is a required that the unit can be brought to a stable condition with regard to corium cooling and radioactivity confinement.

Sufficient provisions are specified such that:

- There is no need for operator action in the short term.
- Both the unit and the site are equipped for the operator to take the necessary actions on the time scales specified for the design without offsite support.

Operator action from the control room is not needed until 30 minutes after accident initiation. Consequently, automatic protection is provided for any event or internal hazard requiring actions within 30 minutes. The necessary operator actions and the times available are analysed for each event. Local operator actions on plant or equipment are not necessary earlier than 1 hour after accident initiation.

Portable equipment than can be credited after 6 hours from the start of an event is not permanently available at the unit but on site and easily accessible. The 6 hour period is provided to encompass the time scale for ascertaining the need for the equipment, location of competent personnel, installation, etc. Mobile equipment is not needed for the safety functions in the plant design.

OL3 is designed so that intervention requiring heavy equipment which can be transported to the site is not necessary until 3 days have elapsed. This grace period is ensured by the requirement to have on site storage of essential provisions sufficient for up to 3 days.

A grace period of 12 hours (after loss of heat removal from the core) is assumed before the containment heat removal system needs to be started. This time span is considered in the containment design.

The capacity of the fuel storage tanks allows an EDG to run for at least 72 hours and a SBO diesel generator for at least 24 hours without refuelling at full power. One EDG or one SBO diesel generator is sufficient to keep the plant in a controlled state, i.e. at hot shutdown. By reducing the loads the fuel is sufficient for at least three weeks to keep the plant in controlled state.

The battery discharge time is 2 hours assuming full design load. The batteries which support important safety functions in severe accidents are sized for discharge time of 12 hours without recharging.

HVAC systems participate in the function to contain radioactive substances; they participate in the reduction of radioactive releases into the environment for a specific DBC or DEC event. As supporting systems, the HVAC and cooling systems maintain ambient conditions for equipment and personnel within acceptable limits to ensure the correct operation of safety classified systems and habitability in the MCR.

The penetrations through the containment are each equipped with two quick-closing leak tight shut-off dampers mounted in series, one inside and one outside the reactor building. The dampers, which are open during plant operation, are of diverse construction, are fail-safe, and need no power supply for closing. The penetrations through the reactor building outer wall are each equipped with two motor-actuated leak tight dampers.

During a LOCA, the normal annulus ventilation is stopped, the supply and exhaust lines are closed by leak tight dampers and a specific annulus sub-pressure system collects all leakages from the containment and reduces the radioactive contaminants by filters before stack release. The release via a high stack is, even in the case of a severe accident and loss of all diesel generators, designed to maintain sub-pressure in the annulus by natural draft.

The safety functions of ventilation for the controlled areas except the reactor building are designed for:

– maintaining ambient temperatures and heat removal of safety mechanical equipment located in the safeguard building mechanical area and fuel building;
– confining the fuel pool room in case of a fuel handling accident;
– confining the safeguard building "hot" mechanical area in case of a LOCA; and
– confining the auxiliary building and waste buildings in case of release of radioactive substances inside the building.

Limitation of releases in severe accidents is described in Section D.6.3.

OL3 will have a range of equipment for plant communication to offsite locations by a telephone system including facsimile with a programmable central processing unit, and a local/external cable network (LAN/WAN) shall be provided.

The communication systems of OL3 enable communications inside buildings, between buildings and with offsite locations. Several independent communication subsystems are provided to ensure communication and additional alarm signalling during normal and emergency conditions. For safety reasons a system for voice communication between control rooms and local control stations and other important facilities is provided.

The communication systems inside OL3 are continuously supplied from the emergency power supply system. With exception of the combined telephone and LAN system each communication system is independent of the others, so that any failure in one will not cause problems in the others.

D.6.1.3 Evaluation of factors that may impede accident management and respective contingencies

The requirement of post-accident accessibility is stipulated by the necessity of post-accident management and by the necessity of repair of a failed component. The last point is mainly related to the safety-related pumps of the RHR and CHRS systems. Accessibility within the context of this report means ensuring that high radiation levels at work places are mitigated. The general approach to repair a pump is to provide sufficient radiation protected areas for work preparation and for actions like emptying and flushing the system piping including the failed pump in order to reach low dose rates inside the pumps rooms. It is demonstrated that the accidents are manageable, and the highest individual dose for a single task to be performed during the accidents is less than 10 mSv.

The process systems inside the nuclear auxiliary building and waste building are not seismically designed but the buildings are. In case of a radioactive leak, the HVAC systems would be isolated preventing releases to the environment.

Severe accidents are taken into account in the design of the main and secondary control rooms. HVAC systems can be used in recirculation mode to prevent contamination of the control room air. MCR post-accident accessibility may be influenced by radioactive release outside the containment from OL3 or by environmental releases from OL1 or OL2 during a severe accident. The releases from OL1 or OL2 may also have impact on accessibility of the outside areas of OL3.

Total loss of all AC power sources would lead to a severe reactor accident. Core uncovery would take place within 3 hours, extensive fuel damage would be caused within 4 hours and pressure vessel melt-through would take 7…8 hours. However, the severe accident management measures are independent of the availability of AC power.

- Depressurisation of the reactor pressure vessel can be performed with the help of battery-backed power.
- Flooding of the core melt takes place in a passive manner.
- The actuation of the containment filtered venting system takes place either by battery-packed power or through manual operator actions.
- The power for the dedicated severe accident management instrumentation system is provided by a dedicated battery backed system with a capacity for 12 hours of operation. The batteries can be recharged using the SBO diesel.

Dedicated severe accident (SA) instrumentation is required to manage and monitor the severe accident:

- Depressurisation of the RCS to reliably prevent high pressure vessel failure and induced steam generator tube rupture.
- Core degradation and coolability including re-criticality.
- Hydrogen control to prevent early containment failure and large fission product release.
- Melt retention to prevent basemat penetration.
- Containment heat removal to prevent late containment failure and increased fission product release.

- Overall plant behaviour (leak tightness), activity distribution within the containment, and releases to the environment.

Operator actions are needed only for RCS depressurisation and start of containment heat removal system. In case of failure of instrumentation, operator actions can also be based on time. If the instrumentation have failed, the operator actions might be performed too early which would lead to earlier core degradation as indicated above and earlier start of release, if containment filtered venting is used in case containment heat removal system is not operable. The containment integrity would be maintained and the release could be stopped.

D.6.1.4 Conclusions on the adequacy of organisational issues for accident management

STUK is still evaluating the design of OL3, and the final organisational issues are not provided. The accident situation in more than one unit of the Olkiluoto site will have to be taken into account when considering the acceptability of the final plans.

D.6.1.5 Measures which can be envisaged to enhance accident management capabilities

At the moment, modifications are not considered necessary.

D.6.2 Accident management measures in place at the various stages of a scenario of loss of the core cooling function

Severe accident management is taken into account in the EPR and OL3 design from the beginning of the EPR design. Consequently, the EPR and OL3 design incorporates features for core melt mitigation and the prevention of large releases. These are shortly described in the following sections, and in more detail in Section D.6.3.

D.6.2.1 Before occurrence of fuel damage in the reactor pressure vessel

Prevention of high-pressure core melt by high reliability of residual heat removal systems is complemented by dedicated severe accident depressurisation valves. Opening of these valves allow also feed & bleed operation as the last resort to maintain the reactor core integrity.

D.6.2.2 After occurrence of fuel damage in the reactor pressure vessel

Hydrogen combustion is prevented by reducing the hydrogen concentration in the containment at an early stage by mixing the containment atmosphere passively and removing hydrogen using passive autocatalytic recombiners (PARs).

D.6.2.3 After failure of the reactor pressure vessel

Molten core concrete interaction is limited by spreading the corium in a dedicated spreading compartment.

Containment pressure increase is controlled by a dedicated containment heat removal system which consists of a small capacity spray system and allows recirculation through the cooling structure of the core catcher, and heat exchangers to remove heat out of the containment.

A filtered containment venting system can be used to finally depressurize the containment in long-term by purging non-condensable gases to the exhaust stack via venturi scrubber. The system can also be used for decay heat removal by releasing steam from the containment.

Collection of leaks and prevention of confinement bypass is achieved by a double-wall containment.

D.6.3 Maintaining the containment integrity after occurrence of significant fuel damage in the reactor core

The OL3 containment is a double-wall structure founded on a basemat. This double-wall structure provides efficient environmental radiation protection under all events. The containment systems contribute to preventing unacceptable releases of radioactivity by containment isolation and the small leak rate of the containment (0.5%/day at design pressure).

The primary containment shell is a pre-stressed concrete structure with steel liner ensuring leak tightness implemented on the inner surface including a reinforced concrete basemat, thus forming a continuous surface. The containment's dimensions provide the necessary free volume of approximately 80,000 m^3 compatible with the design basis accidents (LOCA) and the severe accidents (i.e. hydrogen deflagration and pressure).

The design absolute pressure of the containment is 5.3 bar, and leaktightness is maintained up to the pressure level of twice the design overpressure. The ultimate pressure-bearing capacity of the pre-stressed containment structures, including singularities, is 2.5 times the design overpressure.

The basemat is a 3 m thick pre-stressed concrete structure. The interface between internal structures and the containment basemat is provided by a leak tight steel liner, which prevents any release of radioactivity into the groundwater.

The secondary containment shell is designed against external hazards. It stands on the common basemat and is formed by a reinforced concrete cylindrical wall topped by a reinforced concrete dome.

Severe accidents (SA) and their consequences are taken into account in the design of OL3. In order to avoid severe consequences in the environment, containment integrity and leak tightness must be maintained during the entire course of such an accident.

Processes which could occur during severe accidents and which could jeopardise containment integrity and lead to enhanced fission product release were identified in various risk studies. They include:

- failure of the reactor pressure vessel (RPV) at high pressure due to an attack of the core melt with a risk of corium dispersal and direct containment heating (DCH);
- energetic interaction of molten fuel and coolant: in-vessel and ex-vessel (MFCI);
- interaction of molten corium with the basemat with the possibility of basemat melt-through;
- fast hydrogen deflagration or detonation; and

– long-term pressure and temperature increase in the containment.

The design criteria used for the specific design measures for mitigation of individual phenomena are derived from the analysis of representative scenarios which are specified for the various phenomena and which are selected in a deterministic way.

Since the severe accident mitigation approach imposes special requirements on the confinement function of the containment, systems for isolation, retention and control of leakages are provided. Leakages through the inner containment wall are collected, filtered and released via the annulus ventilation system. Leakages via openings for personnel access or equipment supply are prevented during power operation by permanently closed hatches and by airlocks with double seals on both sides.

D.6.3.1 Elimination of fuel damage / meltdown in high pressure

RPV failure at high pressure is eliminated by deliberate depressurisation of the RCS to a pressure level below 20 bar. Depressurisation is be done by two parallel, independent depressurisation lines. Both lines have two highly reliable dedicated valves in series. The depressurisation system supplements the three pressurizer bleed valves. Valve opening is manually actuated.

The depressurisation also prevents early containment failure due to DCH, and containment bypass due to creep failure of the steam generator tubes. Different scenarios have been analysed in order to evaluate the pressure and temperature history within the reactor coolant system and the potential time window and criterion for activation of the depressurisation valves. The scenarios cover:

– total loss of AC power with unavailability for 12 hours of all diesels,
– total loss of feed water with unavailability of the primary feed & bleed,
– small break LOCA (SBLOCA) with unavailability of the safety injection.

At the very latest when the core outlet temperature reaches 650°C, the depressurisation of the RCS is performed via one of the two redundant dedicated severe accident bleed valve lines (primary depressurisation system, PDS). The position of the valves is to be monitored using the on/off switches in the electric actuator housing. The monitored RCS pressure serves as a redundant indicator for the PDS valve line having opened.

Both power and shutdown states are considered. The analyses show that depressurisation before 650°C core outlet temperature with the designed discharge valve capacity of 900 t/h enables delaying the core melting, owing to available accumulators' water injection, and reducing the reactor coolant system pressure at the time of RPV failure well below 20 bar, around 5 bar for many core melt scenarios. Sufficient time for activation is available and more than one hour grace period exists for the latest activation to avoid vessel failure above 20 bar and to prevent any risk of dispersal of corium debris, which could induce direct containment heating.

The vessel support and cavity structures are designed for the loads resulting from a vessel failure at 20 bar to supply a sufficient load bearing capability.

D.6.3.2 Management of hydrogen risks inside the containment

The large free volume provided by the large dry containment supplemented with efficient mixing and controlled removal of hydrogen enables avoidance of high hydrogen concentrations. The average hydrogen concentration in the containment remains below 10 vol-% in all cases.

Direct discharge of the RCS via a relief tank into the lower equipment compartments provides a large amount of steam at the time of hydrogen release, which improves mixing. Following an increase in pressure, temperature, or differential pressure the convection and rupture foils and mixing dampers passively/failsafe create flow paths to enable thorough mixing of the containment atmosphere. Around 50 PARs distributed mainly in the equipment rooms remove most of the hydrogen until RPV failure and support mixing of the atmosphere.

The justification of the hydrogen mitigation concept is based on representative scenarios (mainly SBLOCA scenarios with a break at different locations) and bounding scenarios with additional aggravation (e.g. with reflood of the hot core at the most penalising moment) selected to explore the limits of the concept and proceeds as follows:

- calculation of mass and energy input into the containment, leading to 500–800 kg hydrogen for representative scenarios and up to 1,000 kg with a peak rate of 6 kg/s for bounding scenarios;
- calculation of the gas and temperature distribution for the relevant phase (until mixing) with the CFD (computational fluid dynamics) method;
- assessment of the risk of fast deflagration or DDT with experimentally based criteria and the risk from slow deflagration via AICC (adiabatic isochoric complete combustion) pressure;
- calculation of the combustion process with a CFD code in case flame acceleration and fast combustion cannot be ruled out by the criteria; and
- assessment of thermal loads from recombination, short deflagration and long-lasting combustion ("standing flames").

The most important results are as follows:

- AICC pressure is always below the design pressure (5.3 bar) for representative scenarios and below the containment leak tightness pressure of 9.6 bar for bounding scenarios;
- flame acceleration occurs locally, mainly in the steam generators compartments, but flame is decelerated when it progresses in the three dimensional configuration of the dome; hence, no significant dynamic loads occur on the shell and slow pressure increase is enveloped by the AICC pressure, 6.5 bar;
- the recombination rate is largely independent of the arrangement of the PARs.

Temperature loads due to recombination on the internal walls are benign.

Hydrogen management systems are passive, and therefore need no SAM actions. Nevertheless, in order to monitor the threat of hydrogen combustion and to assess the proper functioning of the PARs, the hydrogen concentrations are monitored in the upper dome, as well as in steam generator, pressurizer and pressurizer valve compartments. The monitoring system consists of two redundant subsystems with four separate monitoring locations each. The system is based on sampling and it is designed to withstand severe accident conditions.

D.6.3.3 Prevention of the containment overpressure

Long-term pressurisation of the containment is avoided by a dedicated active two-train containment heat removal system (CHRS), whose operation is not required earlier than 12 hours from the beginning of the accident. The containment structures provide sufficient heat sinks so that the design pressure is not exceeded during this period. The external recirculation cooling loops are located in specific ventilated and shielded compartments with provisions for decontamination and repair of the components.

The system has two operation modes:

- spray within the containment dome for fast condensation of the steam and pressure reduction, and
- water recirculation through the cooling structure of the melt retention device for long-term prevention of steaming into the containment volume, which supports maintaining ambient pressure conditions in the containment.

Operation of CHRS and hydrogen recombination can reduce the containment pressure close to the atmospheric pressure. The two CHRS trains can be started via SA I&C, along with the required support systems. To carry out these operations, at least the SBO diesels need to be available.

In addition, filtered venting system is provided in order to release in the non-condensable gases in the long-term, if necessary. The venting is performed to finally depressurise the containment and terminate the releases. With proper functioning of the SAM systems, no need for use of the containment filtered venting system is anticipated. The design pressure of the system is 11 bar and the design temperature 200°C, and therefore it could be used as an ultimate resort to protect containment from overpressurisation.

The correct operation of the two CHRS trains is monitored by measuring the inlet and outlet temperatures in combination with the flow rate. Each of the two trains has redundant instrumentation: IRWST water temperature for the inlet temperature, CHRS pump inlet and outlet pressure difference for the flow rate. For leak detection, CHRS and support system compartment sump level gauges are provided. Assessment of remaining amount of water is carried out by monitoring the water level in the IRWST with sump level gauges, of which two, mutually redundant, are connected to SA I&C.

D.6.3.4 Prevention of re-criticality

For representative core melt scenarios, without reflooding, there is no risk of in-vessel recriticality due to the negative reactivity coefficient of UO_2 fuel voiding (which represents around 50000 pcm). The risk is studied for bounding scenarios in case of in-vessel late re-flooding (due to delayed RCS depressurisation or SI recovery).

Safety injection into the core from the IRWST ensures reactor shutdown due to high boron concentration.

For the later phases of core degradation, some phenomenological uncertainties exist on corium configurations (debris porosity, debris size, coolable mass). For these phases, relevant assumptions lead to grant no re-criticality risk for around 80 tons irradiated fuel at minimal average BU (20 GWd/t) in fragmented and cooled configuration. This mass is beyond the expected coolable limit and consequently re-criticality risk is not likely. However it is outlined that the fuel relocation is a non-uniform process: if mixture contains a large portion of fresh fuel it may cause a potential risk of re-criticality because critical mass may be sensibly smaller. It may not be assured that such configuration are not reached in core degradation progression, but they concern only limited masses and only in the first part of cycle when fresh fuel is available. When core degradation proceeds to form a large molten pool, re-criticality is not possible.

To cope with uncertainties regarding to the risk to reach criticality for these later phases, even though only low amount of corium could be involved, it is recommended to OSSA to inject water with higher boron concentration from available sources in parallel of water injection from IRWST.

During the ex-vessel phase, it has been evaluated that even in the very conservative case where water (at 3 bar and 70°C) penetrates the molten fragmented core, there still is margin to criticality (about 7500 pcm).

Since re-criticality is not considered possible, no specific or additional instrumentation is provided for this purpose. However, as re-criticality before RPV failure would be detected by the ex-core intermediate neutron flux measurement devices, of which at least two will be connected to the SA I&C and to the 12 h UPS batteries.

Corium re-criticality after RPV failure would be detected by a significantly faster containment pressure build-up than predicted assuming normal decay heat. Furthermore, the inlet and outlet temperatures combined with the volume flow rates of the two CHRS trains allow the amount of heat removed by the CHRS to be determined. This would also serve as an indicator of corium re-criticality outside the RPV.

D.6.3.5 Prevention of basemat melt through

Measures are provided to retain the melt within the containment to prevent penetration of the basemat by corium concrete interaction leading to release of fission products into the environment, including groundwater contamination.

The OL3 melt retention concept is based on ex-vessel melt retention, and in-vessel retention is not applied. The risk of ex-vessel FCI during failure is prevented by the provision of a dry reactor cavity and a dry spreading compartment.

The basic concept of OL3 for melt stabilisation is spreading the melt into a large lateral compartment, followed by flooding, quenching and cooling with water from the top and bottom drained passively from the IRWST. A characteristic feature of this concept is not discharging the corium directly into the spreading compartment as it is released from the RPV, but corium is temporarily retained in the reactor cavity. This feature results in a spatial separation of the functions:

- to withstand the thermal-mechanical loads during RPV failure where the robust concrete structures of the reactor cavity are only affected, and

– to transfer the melt to a coolable configuration and stabilise it where the structure of the core retention device is only affected.

This separation leads to a clear definition of loads for the involved structures and to better defined conditions for spreading and stabilisation of the corium.

The connection between the reactor cavity and the spreading compartment is normally closed by a plug, through which the corium will eventually melt. The wall of the reactor cavity is covered with a layer of sacrificial concrete which will be eroded by the corium. During the erosion time until the failure of the plug, there is time for corium to totally accumulate in the cavity. Thereafter, the melt will relocate into the adjacent spreading area of the core catcher under dry conditions.

The bottom and side structures of the spreading area are covered with sacrificial concrete to avoid transient thermal loads on the steel structure of the core catcher during spreading.

Underneath the sacrificial layer a cooling structure is provided consisting of an array of massive steel blocks which at the bottom form parallel channels for cooling. Water from the IRWST will pass through the cooling channels and then flood the melt from above. As a result, the melt is cooled from above and below. The generated steam is transferred into the containment via a specific steam exhaust channel. Heat removal from the corium to the containment atmosphere and the structures can be performed completely and continuously in a passive mode. The flooding is also carried out passively by the melt entering into the spreading area triggering the flooding valves from the IRWST to open. Thus the melt retention concept does not require any operator actions.

This passive mode is applied, however, only during the short-term of the accident. In the long-term, the containment heat removal system can perform active cooling by direct water injection into the cooling structure instead of spray injection into the containment atmosphere. Additional advantages are that the spreading compartment and the reactor cavity can be fully flooded, and the overflowing water which is still sub-cooled flows back into the IRWST.

Monitoring the corium position requires to detect threat of RPV failure, arrival of corium in the reactor pit and in the core catcher, and threat of basemat penetration.

Regarding cliff edge effects, the time delay between reactor shutdown and core meltdown is dependent on the time of RCS depressurisation. Too early RCS depressurisation will lead to early core degradation, whereas too late depressurisation may lead to high pressure melt ejection. These issues are included in the OL3 safety analyses and level 2 PSA.

In a light water reactor core melt accident, if the RPV fails at elevated RCS pressure, the expulsion of molten core debris may pressurise the containment beyond its failure pressure. The risk of containment overpressurisation due to DCH is treated together with vessel uplift movement. The melt that is deposited along the way in the equipment rooms and accumulated on the floor may form a non-coolable configuration in the equipment rooms.

D.6.3.6 Need for and supply of electrical AC and DC power and compressed air to equipment used for protecting containment integrity

In severe accidents AC power is supplied by the SBO diesels and DC power by the NI 12 h batteries (see Section D.5.1).

The minimum operator actions during the first 12 hours (in case of unavailability of SBO diesels and 2 h UPS) require closing the outer containment isolation valves via all four divisions, closing the CHRS compartment ventilation flaps and sump drain valves, and when exceeding the core outlet temperature criterion opening one of the two RCS depressurisation lines. These operations can be carried out without AC power.

After 12 hours, when at least one SBO diesel is available, opening of outer CHRS suction line and spraying line isolation valves (if closed) and actuation of CHRS / CCWS / ESWS pumps in divisions 1 and 4 in the two corresponding divisions is needed when the containment pressure is reaching the design pressure.

D.6.3.7 Measuring and control instrumentation needed for protecting containment integrity

For OL3 a specific SA I&C system will be provided to support measurement needs during severe accidents. All severe accident I&C functions are to be connected to SA I&C with the exception of aerosol and iodine samplers that are provided in a separate post-accident sampling system. The purpose of the measurements is explained in the sections above in more detail.

The following measurement sensors are dedicated to SA I&C:
- RCS pressure wide range,
- RCS depressurisation valve position,
- RPV lower head outside wall temperature,
- containment pressure,
- hydrogen monitoring of the containment atmosphere,
- position of the flaps providing flow paths for hydrogen mixing,
- post accident sampling system,
- temperature measurement in the venting chimney above the spreading area, and
- core catcher central cooling channel temperature.

Two out of four ex-core intermediate range neutron flux sensors, and core outlet temperature sensors are shared between SA I&C and protection systems.

The sensors for monitoring
- functioning of CHRS
- operation of cooling circuits in CHRS and component cooling water system
- IRWST water level and temperature, as well as clogging of CHRS sump screens
- dose rate in the containment
- dose rates and flow rates in the annulus ventilation, safeguard building ventilation and in the vent stack

- sub-pressure in the annulus
- operation of the containment filtered venting system

are shared with the safety automation system.

D.6.3.8 Capability for severe accident management in case of simultaneous core melt/fuel damage accidents at different units on the same site

OL3 has separate SAM systems from other units at the site. Therefore it can be considered that SAM measures can be carried out at OL3 although other units were undergoing a severe accident.

D.6.3.9 Conclusions on the adequacy of severe accident management systems for protection of containment integrity

The SAM strategy and its implementation at OL3 follows the requirements set in the Government Decree on the Safety of Nuclear Power Plants [733/2008] and the Regulatory Guides referred to in Section A.6. To OL3, as an EPR, the containment filtered venting system, and the single failure tolerance of SAM systems, including removing the radioactive material from the containment atmosphere and SAM measurements, have been applied.

STUK is still evaluating the design of OL3, but the overall SAM strategy and approach has been accepted. No such hazards or deficiencies that would require changes to this approach have been found, and based on studies responding to the letter from MEE after Fukushima accident (see Section A.7) STUK has not set any further requirements on the SAM approach of OL3.

D.6.3.10 Measures which can be envisaged to enhance capability to maintain containment integrity after occurrence of severe fuel damage

No changes to the approach described above are seen necessary.

Present analysis of TVO shows that hydrogen management is adequate in the containment but depending on Fukushima aftermath some additional review of accident management has become relevant. This issue concerns mainly the possible leak of hydrogen into the surrounding buildings and the associated hydrogen combustion phenomena. Taking into account the PARs for reduction of hydrogen concentration in the containment, containment volume and in severe accidents and capability to maintain containment leaktightness the risk of hydrogen combustion endangering containment integrity or the accident management actions is considered very low.

D.6.4 Accident management measures to restrict the radioactive releases

D.6.4.1 Radioactive releases after loss of containment integrity

Containment filtered venting can be used in case containment heat removal system is not operable. The containment integrity would be maintained and the release could be stopped after restoration of containment heat removal system. Manual operations are required to maintain long term containment integrity (see Section D.6.3.6).

Due to highly reliable SAM measures to maintain the containment integrity, no specific provisions to manage the releases in case of containment failure have been planned. If the containment leaks into the annulus, the same procedures to collect the releases with the annulus ventilation system apply. In large containment leakages, the capacity of the system may be exceeded.

D.6.4.2 Accident management after uncovering of the top of fuel in the fuel pool

Hydrogen management

If the irradiated fuel which is stored in the fuel pools is uncovered, metal water reaction or zirconium fire is possible only if the fuel has been cooled down for less than a year [Sailor et al. 1987]. This means that hydrogen generation from irradiated fuel would be an issue only at the plant units but not at the spent fuel storage.

No provisions have been implemented for dealing with the hydrogen generated from stored irradiated fuel at OL3. The main goal is to keep the fuel always covered with water. If cooling by the closed systems is lost, ample time is available for establishing cooling in the "feed-and-boil" mode and the need for make-up water to the pools is modest.

Providing adequate shielding against radiation

About 1 m of water above the top of the irradiated fuel assemblies is enough to provide sufficient shielding against radiation so that even poolside accident management actions can be performed if needed. Normally, the submergence of the irradiated fuel is about 8.5 meters at OL3.

Restricting releases after severe damage of spent fuel in the fuel storage pools

No special provisions are in place for restricting the releases in a hypothetical situation with extensive fuel damage due to uncovery and overheating (even the emergency ventilation is dependent on AC power).

Instrumentation needed to monitor the spent fuel state and to manage the accident

The spent fuel pools have level and temperature measurements which can be used for monitoring cooling function of spent fuel. The radiation monitoring devices indicate possible loss of water above the spent fuel (gamma detectors) and loss of cladding integrity (gamma detectors and air contamination detectors).

Availability and habitability of the control room

Severe accidents are taken into account in the design of the main and secondary room. HVAC systems can be used in recirculation mode preventing air contamination.

D.6.4.3 Conclusions on the adequacy of measures to restrict the radioactive releases

The approach for spent fuel pools is to "practically eliminate" the possibility of fuel damage. To support this STUK has requested the licensee to investigate securing decay heat removal from fuel storage pools in the fuel building of OL3.

Although not initially designed for this purpose, during shutdown states the containment filtered venting system can be used for removing heat from the containment without a threat to significant releases in to the environment.

Licensee's evaluation that 1 m of water above the fuel elements in the pool would still provide adequate shielding against radiation to carry out poolside operations may be too optimistic. The radiation levels with water levels this low could be around 1 Sv/h, and although operations would take only few minutes, accident situation may slow down the operations. In practise, the water pool boiling might have made the area inaccessible much before the loss of radiation shielding.

D.6.4.4 Measures which can be envisaged to enhance capability to restrict radioactive releases

To ensure fuel integrity in the fuel pools, the measures indicated in Section D.5.2.5 apply.

D.7 General conclusions

D.7.1 Key provisions enhancing robustness (already implemented)

The issues raised within the "Stress Tests", are required as a part of the designs bases of the Olkiluoto unit 3. External events are comprehensively taken into account in the design and the adequacy of the design has been demonstrated by PSA studies.

The safety systems of OL3 are well designed to tolerate external events by applying adequate physical separation and protection against dynamic loads. Earthquakes and flooding are included in the design to ensure safety functions to a high level of confidence.

Considering a loss of safety functions, OL3 is designed to survive 72 h without core damage in case of LUHS. By applying air-cooled EDGs, the AC power supply would be ensured, although the primary ultimate heat sink would be lost.

The requirements set in the Finnish legislation and regulatory guides (included in YVL guides since 1982) establish a good basis for severe accident management (SAM). Requirements include dedicated, single-failure tolerant SAM systems and measurements, as well as procedures and guidelines for the organisation to manage the severe accident situation. SAM systems have been included in the design of OL3.

- In addition, the filtered venting system designed to purge non-condensable gases out of the containment in a controlled manner in the recovery phase of a severe accident, could also serve diverse heat removal from the containment during shutdown states, in case other means of heat removal from the containment were lost.

The fuel pool cooling systems have capability for external water supply to the pools.

D.7.2 Safety issues

Licensing of OL3 under construction is still underway, and STUK is reviewing the design documents in order to confirm the fulfilment of Finnish requirements.

D.7.3 Potential safety improvements and further work forecasted

The further improvements for enhancing the safety of Olkiluoto 3 unit will focus on the following issues:

- the verification of the strength of SAM and fire fighting systems against earthquakes;
- possibilities to feed water to steam generator secondary side at normal operating pressure independently from the existing feed water systems;
- the sufficiency of on-site diesel fuel and water storages.

These issues are discussed in more detail in sections above considering measures which can be envisaged to enhance plant safety.

E. OVERALL CONCLUSIONS

The actions initiated in Finland right after the March 11, 2011 accident at Fukushima Dai-ichi NPP resulted in the national safety reviews of Finnish NPPs, which concentrated on the findings from the Fukushima accident. In those evaluations no hazards or deficiencies requiring immediate actions at the operating Finnish nuclear power plants were identified. Also, in the European stress tests no needs for immediate actions have come up.

Continuous improvement of safety is an important principle which has been implemented effectively during the operation of the existing NPP units in Finland. Although a license for operation of a NPP has once been granted, there is an explicit requirement to follow the national and international experiences, technological development and research related to nuclear safety issues, and to apply new knowledge for safety improvements.

Following the principle of continuous improvement, the licensees have long term programmes for plant ageing management, for modernisation of the plants, and for improving safety. Strategies and actions needed to cope with severe accidents have been implemented at the operating Finnish NPPs. Also in accordance with this principle, some actions will be implemented based on the stress tests, both at the operating NPP units and at Olkiluoto 3, to further enhance the safety of the units. These actions focus on the prevention of severe accidents in case of harsh environmental conditions and in case of loss of any of the three basic safety functions: reactivity control, decay heat removal, or containment of radioactive materials.

The experiences from the Fukushima accident will also be taken into consideration in the ongoing renewal of the Finnish Regulatory Guides called YVL Guides. A plan has been prepared which indicates the different issues to be considered and the corresponding affected Guides. A new Guide dealing with the design of NPPs is in the final draft stage and has been sent out for external comments. The draft already incorporates lessons from the Fukushima accident by requiring autonomous systems that enable the decay heat removal from the reactor and the containment and arrangements to ensure sufficient cooling of the fuel in fuel storages. Decay heat removal shall be possible for 72 hours without power supply from the plant's AC power distribution systems.

The YVL Guides need to be taken into account in the design of new NPPs as such (Fennovoima 1, Olkiluoto 4). A separate decision will be made concerning their application at the operating units (Loviisa 1 and 2, Olkiluoto 1 and 2) and also the unit under construction (Olkiluoto 3).

Furthermore, lessons from the Fukushima accident will be addressed in the National Research Programme on Nuclear Power Plant Safety 2011 – 2014.

References

Finnish regulation

[990/1987]
Nuclear Energy Act, 11.12.1987/990
http://www.edilex.fi/stuklex/en/lainsaadanto/19870990

[161/1988]
Nuclear Energy Decree, 12.2.1988/161
http://www.edilex.fi/stuklex/en/lainsaadanto/19880161

[733/2008]
Government Decree on the Safety of Nuclear Power Plants (733/2008)
http://www.edilex.fi/stuklex/en/lainsaadanto/20080733

YVL 1.0 – Safety criteria for design of nuclear power plants,
12 January 1996,
http://www.edilex.fi/stuklex/en/lainsaadanto/saannosto/YVL1-0

YVL 2.1 – Nuclear power plant systems, structures and components and their safety classification, 26 June 2000,
http://www.edilex.fi/stuklex/en/lainsaadanto/saannosto/YVL2-1

YVL 2.2 – Transient and accident analyses for justification of technical solutions at nuclear power plants, 26 August2003
http://www.edilex.fi/stuklex/en/lainsaadanto/saannosto/YVL2-2

YVL 2.6 – Seismic events and nuclear power plants, 19 December 2001
http://www.edilex.fi/stuklex/en/lainsaadanto/saannosto/YVL2-6

YVL 2.8 – Probabilistic safety analysis in safety management of nuclear power plants,
28 May 2003,
http://www.edilex.fi/stuklex/en/lainsaadanto/saannosto/YVL2-8

YVL 5.2 – Electrical power systems and components at nuclear facilities, 24 June 2004
http://www.edilex.fi/stuklex/en/lainsaadanto/saannosto/YVL5-2

YVL 5.5 – Instrumentation systems and components at nuclear facilities,
13 September 2002,
http://www.edilex.fi/stuklex/en/lainsaadanto/saannosto/YVL5-5

Other references

[Ahjos & Uski 1992]
Ahjos, T. and Uski, M. 1992. Earthquakes in northern Europe in 1375-1989. Tectonophysics, 207: 1-23.

[ENSREG 2011a]
ENSREG – EU "Stress tests" specifications, Annex I of the Declaration of ENSREG, Brussels 24 May 2011

[ENSREG 2011b]
Post-Fukushima "stress tests" of European nuclear power plants – Contents and format of national reports, 5 December 2011

[EUR]
European Utility Requirements
http://www.europeanutilityrequirements.org

[FENCAT]
Fennoscandian Earthquake Catalog
http://www.seismo.helsinki.fi/fi/bulletiinit/catalog_northeurope.html

[Fortum 2007]
Brochure: Fortumin Loviisan voimalaitos/Loviisa Power Plant

[Fortum 2011]
Loviisa NPP complementary safety assessment report – post-Fukushima "stress tests" of European nuclear power plants, 20 October 2011. LO1-K859-00771 (Versio 1.0)

[Mäntymieni et al. 1992]
Mäntyniemi, P. , Husebye, E.S., Kebeasy, T.R.M, Nikonov, A.A, Nikulin, V. and Pacesa, A. 2004. State-of-the-art of historical earthquake research in Fennoscandia and the Baltic Republics. Annals of Geophysics, Vol. 47, N. 2/3.

[NS-G-1.6]
Seismic Design and Qualification for Nuclear Power Plants,
IAEA Safety Standards Series, Safety Guide No. NS-G-1.6, November 2003

[NS-G-3.3]
Evaluation of Seismic Hazards for Nuclear Power Plants,
IAEA Safety Standards Series, Safety Guide No. NS-G-3.3, December 2002

[NUREG/CR-6372]
Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts,
U.S. Nuclear Regulatory Commission, NUREG/CR-6372, April 1997

[SAFIR2010]
The Finnish Research Programme on Nuclear Power Plant Safety 2007 – 2010
http://virtual.vtt.fi/virtual/safir2010/

[SAFIR2014]
The Finnish Research Programme on Nuclear Power Plant Safety 2011 – 2014
http://virtual.vtt.fi/virtual/safir2014

[Sailor et al. 1987]
V. L. Sailor, K.R. Perkins, J.R. Weeks, H.R. Connell. Severe Accidents in Spent Fuel Pools in Support of Generic Safety, Issue 82. NUREG/CR-4982. BNL-NUREG-52093.

[TVO 2008]
Nuclear power plant units, Olkiluoto 1 and Olkiluoto 2
http://www.tvo.fi/uploads/File/nuclear-power-plant-units.pdf

[TVO 2010]
Nuclear Power Plant Unit, Olkiluoto 3
http://www.tvo.fi/uploads/File/2010/OL3_esite_EN.pdf

[TVO 2011]
EU stress test for Olkiluoto NPP - Licencee report, 28 October 2011. 139778

[WENRA 2008]
WENRA Reactor Safety Reference Levels, January 2008