Probabilistic Risk Assessment of the Spent Fuel Pools of Olkiluoto 1 and 2 NPP Units

Simo Sihvola[a], Lasse Tunturivuori[*b]
[a] Platom Oy, Mikkeli, Finland
[b] Teollisuuden Voima Oyj, Eurajoki, Finland

Abstract: A probabilistic risk assessment (PRA) of the spent fuel pools (SFP) situated in the reactor halls of the Olkiluoto 1 and 2 NPP units has been performed in 2016. The PRA includes internal events, internal fires and floods and external hazards during power operation of the reactor of the NPP unit. During shutdown of the reactor, the spent fuel pool is included in the PRA of the reactor.

Internal initiating events are modeled by modeling component faults and manual recovery of faults due to lack of historical events. External and internal hazards have already been analyzed in the scope of the reactor PRA. Results from these have been incorporated into the SFP PRA. Internal hazards mutual to the reactor and SFP have been modeled separately.

The SFP PRA indicates an extremely low frequency of fuel uncovery due to good redundancy, diverse means of water supply, and very long recovery times. Initiating events mutual to the SFP and the reactor reveals, however, a possible benefit from using insights from multi-unit PRA initiatives.

Keywords: PRA, PSA, Spent fuel pool, SPAR-H.

1. INTRODUCTION

Olkiluoto NPP units 1 and 2 are boiling water reactors (BWR) built by ASEA-ATOM in the late 70's and early 80's. The NPP units have operated for nearly 40 years with excellent capacity factors. Both units' primary safety systems are divided into four redundant subsystems (divisions), each of which has a capacity of 50 %. The Olkiluoto NPP site is located on the remote island of Olkiluoto in Western Finland and is operated by Teollisuuden Voima Oyj, producing electricity to its owners at cost.

Spent fuel is stored for about five years in spent fuel pools (SFP) situated in the reactor hall before they are moved to a facility for interim storage of spent fuel, where all spent fuel in Olkiluoto is stored before final disposal. A final disposal facility, ONKALO, is being built in the Olkiluoto island bedrock, where all spent fuel from the Finnish Olkiluoto NPP units and Loviisa NPP units is to be disposed.

The first probabilistic risk assessment (PRA) of the Olkiluoto NPP units 1 and 2 was finished in late 1980's. It is continuously kept up-to-date in order to enable it to be used in risk-informed decision-making. Until recently, the PRA has only included at-power accident sequences linked to the reactor. The shutdown state accident sequences have included also accident states related to the spent fuel pools. Thus, the spent fuel pools have historically been included in the PRA only for reactor shutdown states. Inclusion of the SFP PRA is an increase in the scope of the PRA.

2. DESCRIPTION OF SPENT FUEL POOLS AND RELATED SYSTEMS

Spent fuel is stored for in average 5 years in two SFP's in the reactor hall. The amount of spent fuel bundles varies throughout the power cycle and also from one power cycle to another. Spent fuel is removed from the SFP during power operation of the reactor in order to allow for more space for fresh fuel. On the other hand, the spent fuel has to be cooled enough in order to allow safe transfer of the spent

[*] lasse.tunturivuori@tvo.fi

fuel to the interim spent fuel storage. Throughout the power cycle, the mean decay power of the spent fuel is 1 MW, varying between at most 1.3 MW in the beginning of the power cycle and below 0.9 MW after about five months.

Together with the reactor pool, the water inventory totals to about 3500 m^3. Its temperature in the FSAR is reported to be between 25 °C and 45 °C depending on the amount of spent fuel in the SFP and time elapsed since the last outage. In the beginning of the power cycle, the temperature is higher and it cools down quickly during the power cycle. Most of the time, the temperature is about 25 °C.

The SFP is cooled during normal operation by the diesel-backed reactor pool and SFP decay heat removal and purifying system (RHR system). One pump out of two is running and the other is in standby. The water in the SFP is cooled in two heat exchangers, both having a cooling capacity of 100 %. The heat exchangers are connected to a diesel-backed intermediate cooling system consisting of four pumps and heat exchangers, the capacity of each pump being 50 %. The intermediate cooling system is cooled in its turn by a diesel-backed service water system, also consisting of four pumps, each with a capacity of 50 %. The intermediate cooling system functions also as a component cooling system to safety-related components of the reactor. The RHR system is powered by two diesel-backed switchgears and the intermediate cooling system and service water system are powered by four diesel-backed switchgears, two of which two shared by the RHR system. Further, in the event of loss of the intermediate cooling system, the RHR system cooling can be switched by valve operations to one division of the diesel-backed reactor shutdown intermediate cooling and service water systems, having the capacity of two pumps and two heat exchangers, each with 50 % capacity. For cooling purposes during power outage of the reactor, the RHR system of the SFP has further a third heat exchanger and two extra pumps, each with a capacity of 100 %. The heat from this third heat exchanger is transferred to the reactor shutdown intermediate cooling system, the purpose of which is enable earlier maintenance of reactor decay heat removal systems and, thus, shorten reactor power outages.

In the situation in which the SFP needs added water, demineralized water from four tanks in the demineralized water distribution system may be pumped into the SFP. One diesel-backed pump with capacity of 5 kg/s is started automatically by pressure decrease in the demi water system allowing distribution of demi water to various consumers around the power plant, including the SFP. If the capacity of the pump cannot keep the pressure in the system, another non-diesel-backed pump with capacity of 60 kg/s is automatically started. Normally, there is at least 450 m^3 demineralized water available in the demi water tanks to fill the SFP. In addition, the demi water plant has a production capacity of about 8 kg/s if two out of three filter trains are operable. This capacity is sufficient to compensate for vaporized water in the SFP in the event of SFP boiling, the rate of which is 0.5 kg/s if the decay power is 1 MW. Furthermore, if the demineralized water distribution system is not available, water from the fire water system with a capacity of 100 kg/s may be pumped to the SFP in accident conditions.

3. EVENT TREE MODELING

3.1 Plant damage states

If the spent fuel cannot be cooled down by any means and the spent fuel is uncovered, the spent fuel will start to melt. Such a condition would lead to a severe accident in which a radioactive release is very likely, taking into account that the SFP is located outside of the containment in the reactor building and the reactor building itself is not designed to withstand pressure increase in connection with a severe accident. As long as the spent fuel is completely water covered, the spent fuel will remain intact. Thus for simplicity, the ultimate plant damage state is defined as uncovery of spent fuel. This is a very conservative definition of the ultimate plant damage state.

Further, for informational purposes, one plant damage state is defined as boiling of the SFP. This state prevents the use of the SFP cooling system due to the SFP water level decrease. Further, any operator actions in the reactor hall becomes impossible due to the steaming of the SFP and the reactor pool.

However, the plant has a strategy for recovering from the boiling of the SFP to normal SFP cooling. Thus, this state does not necessarily lead to fuel uncovery.

3.2 Initiating events

Spent fuel may be uncovered in the event of a SFP leak or a non-isolated leak in a connecting system or in the event that decay heat cannot be removed from the SFP.

The initiating event failure of SFP cooling is defined as the event that the SFP temperature exceeds 60 °C. Such a condition may occur if the water circulation in the RHR system fails or if the heat transfer to the primary ultimate heat sink, the sea, is blocked.

Due to the design of the SFP's, leaks leading to direct uncovery of the spent fuel are not possible, except due to very strong forces that could break the SFP. Such events have not been identified. Leaks that decrease the SFP water level by 1 m are possible, but due to the nature of the propagation of the initiating event, they are treated as loss of SFP cooling.

3.3 Actions to prevent or mitigate an initiating event

In order to prevent the initiating event from occurring, components in the RHR system backing up the failed components are started. Alternatively, RHR system loop normally used during reactor power outages may be taken into use. These actions are not possible if there has been a leak in the RHR system. Thus, leaks are always assumed to lead to an initiating event, but other hazards may be recovered from prior to the initiating event.

Due to the long time spans from the hazard, e.g., component failure, fire, etc, to eventual boiling of the SFP or uncover of the spent fuel, there is time to repair components or pipes in order to prevent a severe accident. In the SFP PRA, repair of components and pipes is taken into account. In the event that the repair of the failed components and start of the redundant components, heating of the SFP close to the boiling temperature cannot be prevented. Demineralized water from four demi water tanks can be pumped into the SFP or, if this means is not available, fire water can be pumped from the fire water system using hoses to connect to the SFP. The fire water regulating valves can be operated outside of the reactor hall.

4. INITIATING EVENTS

Both internal hazards, such as component failures, loss of power supply, fires, floods and heavy load drops; and external hazards, such as weather phenomena, nearby industrial human activity and seismic events; may lead to loss of SFP cooling. In the analysis, simultaneous abnormal operation or of the reactor or reactor accident is accounted for. This may have importance especially in the human response to the initiating event concerning the SFP, since the recovery or mitigation of loss of SFP cooling always requires operator interactions.

Taking conservatively into account the water volume of 570 m^3 in the smaller spent fuel pool, the temperature of the water increases at most 1.5 °C/h. Thus, there is at least 10 hours of reaction time from the hazard - the failure of the cooling of the SFP - until the initiating event occurs. Normally, this reaction time is about 24 hours. In most cases, the hazard only affects one cooling train, so starting the standby train prevents an initiating event. Further, if the initiating event occurs, there is another 26 hours grace time until boiling of the SFP starts and further 360 hours or 15 days until uncovery of spent fuel.

4.1. Failure of RHR pump

The RHR pump may fail either due to component failure of the pump or due failure in the power distribution. Failure in power distribution may be due to a component failure in the switchgears

supplying the pump. Manual start of the pump in standby before the SFP temperature rises to 60 °C prevents the initiating event.

4.2 Flooding events

Some flooding events analyzed in the reactor PRA also lead to loss of SFP cooling. These events are leaks in the RHR system or the diesel-backed intermediate cooling system or service water system. Unisolated leaks in the RHR system lead to water level drop of about 1 m in the SFP. The intermediate cooling system and the service water system are one-loop systems, so a leak lead to loss of the whole system, leading to a need to use the RHR system loop normally used during reactor power outages.

4.3 Fire events

Fires in cable rooms and intermediate cooling and service water system pump rooms are notable hazards both for the reactor and the SFP. The focus during such fires are on the reactor in the short term. Thus, resources for recovering the SFP cooling are only available after the first few hours after the fire.

4.4 External hazards

External hazards are identified from the reactor PRA. Weather events leading to loss of power supply and/or loss of ultimate heat sink (sea cooling) and oil spill events leading to loss of ultimate heat sink are identified as potential hazards. These lead to a reactor initiating event as well. Thus, resources for recovering the SFP cooling are only available after the first few hours after the fire. Seismic events have not been analyzed. Although the NPP units have not been designed against seismic events, the SFP and connected pipes are deemed to withstand seismic events more frequent than 10^{-7} a^{-1}. Seismic events will be analyzed in upcoming updates of the SFP PRA.

4.5. Human reliability analysis (HRA)

Restart of decay heat removal of the SFP and an eventual increase of SFP level requires always manual operations of the systems. Failure to perform manual operations is analyzed with HRA. These HRA's are mainly designed with reactor events in mind, especially methods prescribing human error probabilities (HEP). One main difference between a SFP PRA and a reactor PRA is the time available for diagnosis and manual operations, which are much longer in the SFP PRA. Furthermore, in events leading both to a reactor initiating event and a SFP initiating event, the focus is primarily (and rightfully) on the reactor.

For recovery tasks following the loss of SFP cooling or SFP leak prior to the initiating event, the SPAR-H [1] method is used. The HRA Worksheets included in the report are used.

Figure 1: Excerpt of HRA worksheet used in HEP evaluation

PART I. EVALUATE EACH PSF FOR DIAGNOSIS

A. Evaluate PSFs for the Diagnosis Portion of the Task.

PSFs	PSF Levels	Multiplier for Diagnosis	Please note specific reasons for PSF level selection in this column.
Available Time	Inadequate time	P(failure) = 1.0 ☐	
	Barely adequate time (≈ 2/3 x nominal)	10 ☐	
	Nominal time	1 ☐	
	Extra time (between 1and 2 x nominal and > 30 min)	0.1 ☐	
	Expansive time > 2 x nominal & > 30 min	0.1 to 0.01 ☐	
	Insufficient Information	1 ☐	
Stress/ Stressors	Extreme	5 ☐	
	High	2 ☐	
	Nominal	1 ☐	
	Insufficient Information	1 ☐	
Complexity	Highly complex	5 ☐	
	Moderately complex	2 ☐	
	Nominal	1 ☐	
	Obvious diagnosis	0.1 ☐	
	Insufficient Information	1 ☐	
Experience/	Low	10 ☐	

Tripping of the RHR pump does not induce any alarm to the main control room (MCR). High SFP temperature triggers an alarm to the MCR at 40 °C. This may take up to seven hours after the hazard event has occurred. The hazard may have induced other alarms which have resulted in actions taken by the operators. However, these actions may well be related to prevent a reactor-related accident. After the high SFP temperature alarm, there is about 13 h time available to restart SFP cooling and prevent the initiating event (SFP temperature over 60 °C).

If the restart of the SFP cooling fails and the initiating event occurs, there is further 26 h time available before the SFP starts to boil. After the initiating event, the possibility to repair failed equipment is accounted for. The probability to fail the reparation is assumed to be exponentially distributed:

$$P_{\text{repair fails}} = e^{-\frac{T_{\text{available}}}{\text{MTTR}}} \quad (1)$$

$P_{\text{repair fails}}$ is the probability that the repair fails in the available time after the initiating event, $T_{\text{available}}$. MTTR is the mean time to repair. In the above assumption it is assumed the maintenance team has had time to arrive to the site (if the event happens outside of normal working hours) and do necessary preparations before the repair during the time before the temperature of the SFP has increased to 60 °C. Further, it is assumed that finishing the repair is a Poisson process with parameter MTTR. Table 1 shows some examples of repair failure probabilities used in the SFP PRA.

Table 1: Examples of repair failure probabilities before SFP reaches 60 °C

Repair event	Available time to repair (h)	MTTR (h)	Faiure probability
Repair of large pipe failure	10	20	0.6
Repair of DG after severe lightning event	10	6	0.2
Cleanup of air intake after severe snow storm	10	2	0.007

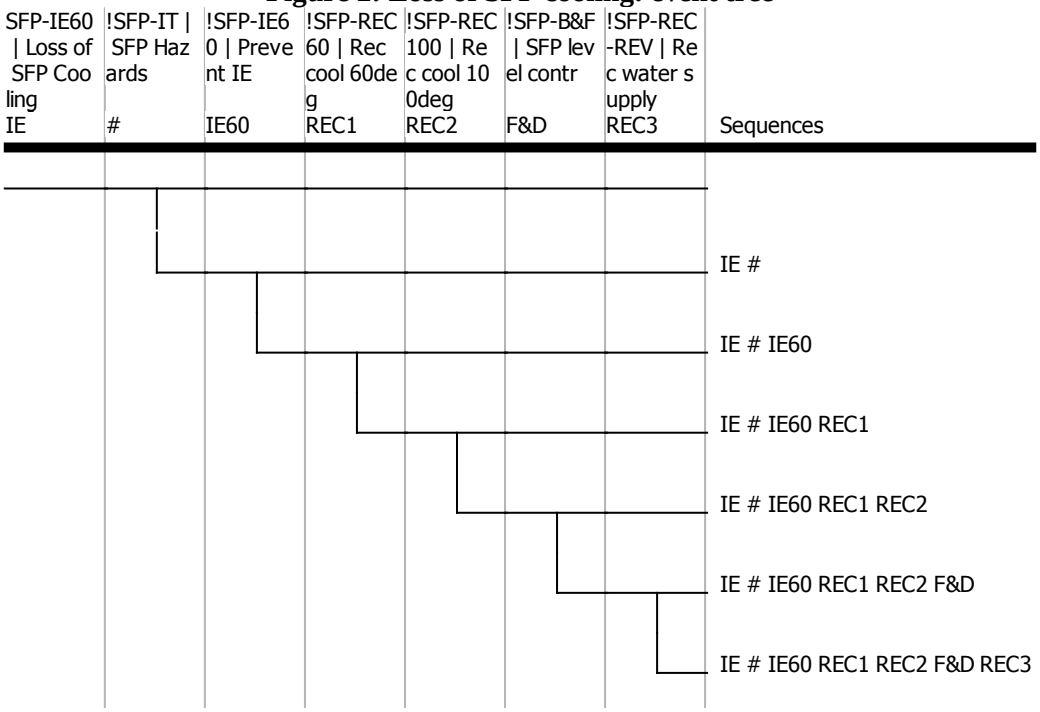
Due to the long time spans between the initial failure or hazard and eventual forthcoming events, such as SFP boiling or uncover of spent fuel, it is difficult to assess dependencies between different manual operation events, initial and forthcoming diagnosis events etc. All operations connected to the cooling

and water level management of the SFP are manual. Thus, manual events and dependencies between these are large sources of uncertainty in the results.

4.6. Event tree and fault tree modelling

Loss of SFP cooling is modelled with the following event tree:

Figure 2: Loss of SFP cooling: event tree



The hazards that may lead to the initiating event, i.e., component failures, fires, floods and weather phenomena, are modelled in a fault tree (!SFP-IT in the event tree in Figure 2). Failure to prevent the initiating event is in its turn modelled in another fault tree (!SFP-IE60, c.f. Figure 2). Failure to repair components or pipes in the RHR cooling chain fail before the SFP temperature increases to 60 °C is modelled in fault tree !SFP-REC60 (c.f. Figure 2). If all these three events occur, an initiating event occurs. Failure to repair failed components or pipes before SFP starts to boil is modelled in the fault tree !SFP-REC100 (c.f. Figure 2). Further, failure to initiate pumping of demineralized water or fire water is modelled in the fault tree !SFP-B&F. Finally, failure to repair components required for water pumping is modelled in the fault tree !SFP-REC-REV. Failure to pump demineralized or fire water into the SFP, with the condition that the SFP is boiling, leads to spent fuel uncovery.

5. RESULTS

Table 2 shows the proportion of the hazard frequency of modelled hazards in the SFP PRA. The major contributor is the failure of the running RHR system pump. Other important hazards are fire scenarios, where loss of house supply transformer leads to loss of offsite power supply to two divisions or fire in a pump room leads to loss of one RHR system division. The contribution to the initiating event frequency, the frequency of the temperature of the SFP rising to 60 °C, is rather low for the more common hazards, as seen in Table 3. For the initiating event, most important contributor is a leak in the SFP RHR system leading to a decrease of SFP water level by 1 m. Other hazards are not important contributors to the initiating event.

Table 2: Relative proportion of hazard frequency of modelled hazards

Hazard	Proportion
Failure of RHR system pump	90 %
Fire - loss of house supply transformer	3.3 %
Fire - loss of one division	1.8 %
Leak in RHR system filters	1.3 %
Leak in intermediate RHR cooling circuit	0.70 %
Fire - loss of both RHR cooling system divisions	0.59 %
Failure in diesel-backed 660 V switchgear	0.32 %
Fire - loss of running RHR pump	0.31 %
Leak in SFP RHR system	0.28 %
Mussels clog seawater channel - LUHS	0.28 %

Table 3: Relative proportion of initiating event frequency of modelled hazards

Hazard	Proportion
Leak in SFP RHR system	98 %
Frazil ice clogs seawater channels - LUHS	0.63 %
Fire in cable room, loss of two divisions	0.51 %
Algae clog seawater channels - LUHS	0.23 %
High wind and mussels - LOOP and LUHS	0.12 %
Oil spill accident at sea - LUHS	0.10 %
Failure of RHR system pump	0.10 %
Leak in intermediate RHR cooling circuit	0.08 %
Fire loss of both RHR cooling system divisions	0.05 %
Mussels clog seawater channel - LUHS	0.02 %

Table 4 shows the relative proportion of SFP boiling frequency due to the modelled hazards. The order of the hazards is almost the same as for the initiating event frequency, the differences in proportions only being more notable.

Table 4: Relative proportion of SFP boiling frequency of modelled hazards

Hazard	Proportion
Leak in SFP RHR system	0.997
Fire in cable room, loss of two divisions	2.1E-03
Frazil ice clogs seawater channels - LUHS	3.7E-04
Leak in intermediate RHR cooling circuit	1.9E-04
Algae clog seawater channels - LUHS	1.3E-04
High wind and mussels - LOOP and LUHS	7.1E-05
Oil spill accident at sea - LUHS	6.1E-05
Fire - loss of RHR system service water system	3.4E-05
Failure of RHR system pump	1.1E-05
Mussels clog seawater channel - LUHS	6.5E-06

Table 5 shows the SFP boiling Birnbaum measure (conditional probability of end state) of the most important hazards. It indicates that the most frequent hazard is also the most severe. The severity in a SFP RHR system leak lies in that it leads to total loss of decay heat removal. Boiling can only be avoided if the leak can be repaired before the SFP reaches the boiling point. The lesser severity of LUHS events

lies in that it is easier to clean the sea water channels from debris or oil and in that there is a certain degree of readiness to perform such measures. Such measures have written procedures and tools and chemicals are available for performing the measures.

Table 5: Conditional SFP boiling probability due to modelled hazards

Hazard	Proportion
Leak in SFP RHR system	0.091
High wind and mussels - LOOP and LUHS	2.5E-03
Algae clog seawater channels - LUHS	2.5E-03
Oil spill accident at sea - LUHS	2.5E-03
Frazil ice clogs seawater channels - LUHS	2.5E-03
Fire in cable room, loss of two divisions	2.9E-04
Leak in intermediate RHR cooling circuit	7.0E-06
Fire in service water pump room	7.0E-06
Service water system leak shower - fails reactor RHR system	6.6E-06
Algae clog seawater channels - partial LUHS	6.1E-07

Table 6 shows the most important basic events contributing to the SFP boiling frequency. It is noted that failure to repair the leak in the event of a SFP RHR system leak is the most contributing failure event. This is well in line with the SFP RHR system leak being the most important hazard contributor to the SFP boiling frequency. Other important basic events mainly involves repair of the systems failed in the hazard. Powering the RHR pumps from an intact electrical division after failure of the normal power supply is the third most important basic event. Other notable events are CCF events of involved pumps.

Table 6: Relative proportion of SFP boiling frequency of basic events

Basic event	Proportion
Repair of leak fails after leak in SFP RHR system	0.997
Reconnection of power to components fails after fire in cable room	2.1E-03
Power connection from other electrical division fails to RHR pumps	4.3E-04
Removal of frazil ice fails in frazil ice event	3.7E-04
4x CCF intermediate cooling pumps do not start	3.0E-04
3x CCF intermediate cooling pumps do not start	2.1E-04
3x CCF intermediate cooling pumps do not start	2.1E-04
Repair of leak fails after leak in intermediate cooling system or service water system	1.9E-04
2x CCF shutdown reactor intermediate cooling pumps do not start	1.5E-04
4x CCF service water pumps do not start	1.3E-04

6. CONCLUSION

SFP PRA is part of a full-scope PRA, extending the scope of the SFP events to reactor full-power events. SFP events progress much slower in comparison with reactor accident events. The ample time available for taking measures to recover from a hazard affecting the SFP makes the hazards less severe than hazards affecting the reactor.

In a SFP where no bottom leaks are deemed possible, events that may lead to boiling of the SFP of uncovery of the spent fuel act like loss of decay heat removal systems. Operations to switch to a redundant system are almost certain to succeed, since failure to perform the action can be recovered from multiple times. Also repairs can be undertaken during these time spans. However, dependency models for such long time spans are not readily available, which leads to quite a large degree of uncertainty in the final results. Also recovery or mitigation of a simultaneous reactor initiating event results in some degree of uncertainty in the final results. In total, however, the contribution of the spent fuel damage frequency to the total core damage and large release frequencies of the NPP units is very small.

References

[1] D. I. Gertman *et* al, "*The SPAR-H Human Reliability Analysis Method"*, NUREG/CR-6883, (2005).