Main results and conclusions of the OL3 Level 1 and Level 2 PSAs for the operating license in connection with the fulfillment of the regulatory requirements

Heiko Kollasko [a], Gerben Dirksen [a], Roman Grygoruk [b], Jari Pesonen [c]
Lasse Tunturivuori[c] and Antti Tarkiainen[c]
[a] Framatome GmbH, Erlangen, Germany
[b] AREVA GmbH, Erlangen, Germany
[c] TVO, Olkiluoto, Finland

Abstract: The EPR plant in Olkiluoto (OL3) in Finland has been designed to comply with current international safety principles, Finnish regulatory requirements and the European Utility Requirements, including a management strategy for core melt accidents.
The operating license application for the Olkiluoto EPR in Finland requires plant-specific full-scope Level 1 and Level 2 PSAs which need to fulfil the Finnish regulatory requirements.
Apart from demonstrating that the probabilistic design objectives set by the Finnish regulatory requirements are met, the PSA was used for specific applications during the design and construction phases of the project. The PSA was applied in several areas during the design and construction of OL3, e.g. to support the detailed design of systems, structures and components (SSCs), evaluate plant modifications (DCRs), define pre-service inspection programs (RI-PSI), and evaluate the safety classification of SSCs. It was also used in the definition of risk-informed in-service inspection programs (RI-ISI), the evaluation of allowed outage times and periodic testing frequencies for technical specifications, providing input for reliability centered maintenance (RCM), the optimization of proposals for online maintenance packages, the development of operating procedures and the simulator training program for operating personnel, and the evaluation of commissioning tests.
The scope of initiating events and plant operating states analyzed in the PSA is presented including the special treatment of dependencies of support system functions and specific issues concerning modeling the digital I&C in the PSA.
The FMEA approach was used as a link between system design and fault tree modeling.
The PSA scope of initiating events not only contains internal events such as transients and LOCA but also internal hazards such as internal fire and flooding and external events including a seismic PSA. Specific issues concerning the modeling principles of hazards are provided. The fire PSA is an essential part of a full-scope PSA. Although a fire PSA was performed as early as during the design phase to provide probabilistic insights for the design, not all information usually needed for a detailed fire PSA was available at this stage. In particular, the cable routing information. Therefore, a two-stage approach was applied to the modeling of the event internal fire.
The PSA includes all plant operating states in power and shutdown operation. Specific issues relating to shutdown operation modes are presented.
The Level 2 PSA was performed with a non-integrated approach for which the PSA model consists of the three parts: Level 1 PSA model, Level 1 – Level 2 PSA interface model and an accident progression event tree model. The Level 1 PSA event tree model is expanded by the event tree modeling of the Level 2 PSA interface, whereas the accident progression event tree model is created in a dedicated Level 2 PSA event tree program. Some of the advantages of this process are: it is possible to use the special features of the dedicated Level 2 PSA event tree model, and it is possible to calculate path-dependent source terms within the event tree model using this process.
Finally the main results and conclusions for the Level 1 and Level 2 PSAs are presented.

Keywords: PSA, Risk application, Licensing

1. INTRODUCTION

A third nuclear power plant Olkiluoto 3 (OL3) is under construction at the Olkiluoto site in Finland, and currently, it is in the commissioning phase.
The OL3 NPP is of a European Pressurized Reactor (EPR) type, which is designed to comply with the current international safety principles, the Finnish regulatory requirements as well the European Utility Requirements. The design of EPR type of plant also includes the management strategy for severe accidents. In Finland, the operating license application requires a plant-specific full-scope Level 1 and Level 2 PSA, which shall fulfil the Finnish regulatory requirements. The Level 1 and Level 2 PSA were performed during the construction phase and submitted for operating license application after detail design.
This PSA has been developed based on an early design phase PSA required for a construction license and has been updated continuously during the detailed design phase of the project in order to get the insights from PSA results and to ensure that the design is kept in line with probabilistic requirements. The PSA insights then have been used to support the detailed design by evaluating alternatives.

The OL3 PSA meets the Finish regulatory requirements set in the YVL guides. In addition to the assessment of design solutions, the PSA has been utilized, in accordance with the YVL guides, for the assessment of the Technical Specifications, the supporting the determination of the safety classification of structures, systems and equipment, the preparation of the in-service inspection program for piping, the preparation of periodic testing and preventive maintenance programs for systems and equipment, the preparation of procedures for emergency and abnormal conditions and as inputs to simulator training for operators, etc.

This paper describes the main results and conclusions of the Level 1 and Level 2 PSA which was updated at the end of 2017. The results show that the numerical design objectives for OL3 NPP are met as defined by the Finnish regulatory guides.
The scope of initiating events and the analyzed plant operating states is described and an overview of the applied methodology in Level 2 PSA is presented. Finally, the use of the PSA in several applications during the licensing, construction and commissioning phases is explained.

2. MAIN RESULTS AND CONCLUSIONS OF THE LEVEL 1 AND LEVEL 2 PSA

The OL3 PSA has comprehensively dealt with various initiating events in all plant operating states, including annual outages, i.e. full scope PSA. The analysis also includes events occurring in the fuel building with the potential to result in damage of the spent fuel.
Probabilistic design objectives to be applied are addressed in YVL 2.8 [1][*]. According to the Government Resolution (395/1991) [13], accidents leading to large releases of radioactive materials shall be very unlikely. Accordingly, in YVL 2.8 [1] the following numerical design objectives for the whole nuclear power plant are given:

- The mean value of the probability of core damage is less than 1E-5/a.
- The mean value of the probability of a release exceeding the target value defined in section 12 of the Government Resolution (395/1991) must be smaller than 5E-7/a.

The calculated core damage frequency of 1.7E-6/a (mean value) is well below the regulatory limit of 1E-5/a demonstrating good compliance with the requirements. The same applies to large releases. According to OL3 Level 2 PSA analyses, the expected value of the large release frequency is 7.7E-8/a, including both reactor and fuel pool events, well below the regulatory limit of 5E-7/a. In addition, the share of early (<6 hours) releases is only in the order of 1% of all releases, which can be considered to be sufficiently small and to demonstrate the functionality of the severe accident management strategy.
Finally, it is concluded that the OL3 plant fulfils the probabilistic design objectives given in YVL 2.8.

[*] YVL 2.8 has been applied for OL3 design. New YVL A.7 has been released during OL3 construction and it replaces former YVL 2.8. The numerical design objectives are kept same in YVL A.7 [2].

2.1. Main results of the Level 1 PSA

The core damage frequency resulting from all initiating events during power and shutdown states is calculated with 1.4E-06/a, as point estimate, respectively with 1.7E-06/a as expected value.
The following grouping of initiating events is defined for the detailed design phase PSA of OL3:

- Internal events like Transients, Secondary side breaks, LOCA, VLOCA, SGTR and Common cause initiators;
- Internal hazards like Internal fire / explosion, Internal flooding / steaming Secondary effects from pipe whip / missiles; Load drop, etc.
- External hazards like Seismic events and Other external events impacting the plant operation by effecting structures, ventilation, ultimate heat sink and offsite power.
- Events affecting the heat removal from the spent fuel stored in the spent fuel pool.

The OL3 PSA core damage frequency is divided for initiating event groups as follows:

Internal events	65%
Internal hazards	27%
External hazards	8%

The relative contribution of initiating event categories to the overall CDF at power and shutdown states are as follows (Figure 1):

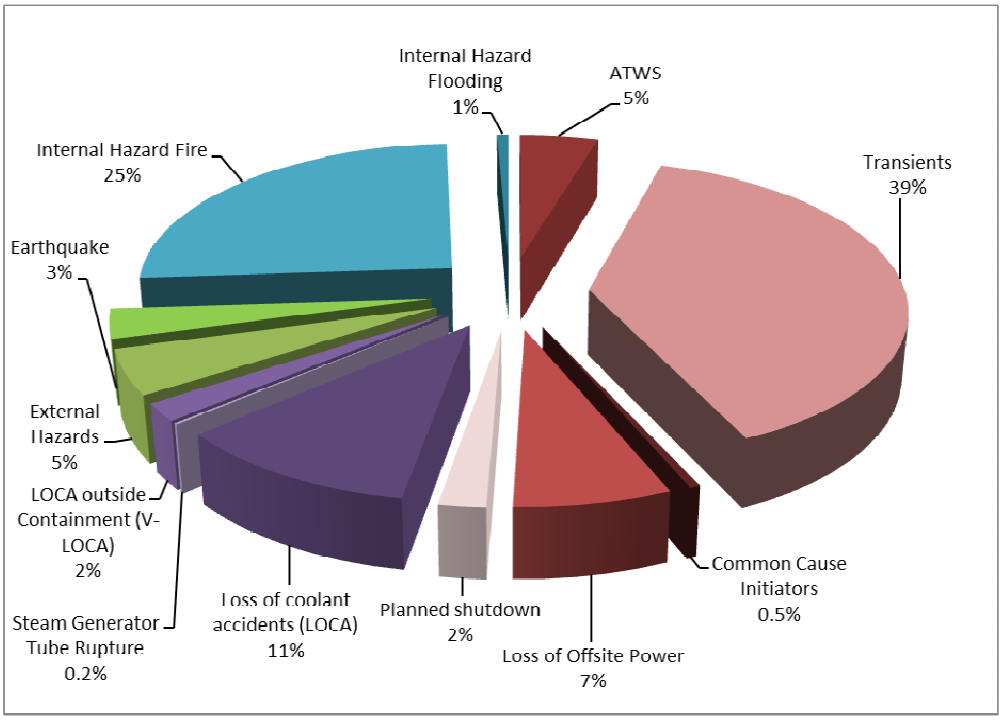

Figure 1: Relative contribution of initiating event categories to the overall CDF at power and shutdown states

Power operation contributes 60%, shutdown states with RPV closed contribute 13%, and shutdown states with RPV open contribute 27% to the core damage frequency.

Both quantitative and qualitative uncertainty analyses were conducted for the Level 1 PSA results evaluation. A quantitative uncertainty analysis has been performed using Monte Carlo Simulations to assess the expected (mean) value of core damage frequency and its distribution.

Modeling assumptions and modeling simplifications have been evaluated qualitatively with regard to their potential impact on the overall core damage frequency, on the frequency of steaming in the fuel

pool and on the frequency of damage of the fuel elements in the fuel pool caused by a loss of fuel pool cooling.
Based on the qualitative analysis of uncertainties due to modeling assumptions and modeling simplifications it is concluded that neither the core damage frequency nor the frequency of steaming from the fuel pool or even the frequency of damage of the fuel elements in the fuel pool have been underestimated.

2.2. Main results of the Level 2 PSA

The expected value of a large release (over 100 TBq of Cs-137) frequency is 7.7E-08/a, of which the proportion of reactor core is approximately 72% and that of the fuel building fuel pools is approximately 28%.

The cumulative distribution of the OL3 Cs-137 release fraction is presented in Figure 2. The prohibited zone is restricted by the YVL 2.8 guide, where the frequency of releases exceeding 100 TBq must be less than 5E-7 /a. A release of 100 TBq corresponds to a release fraction of 1.9E-4 of the core inventory.

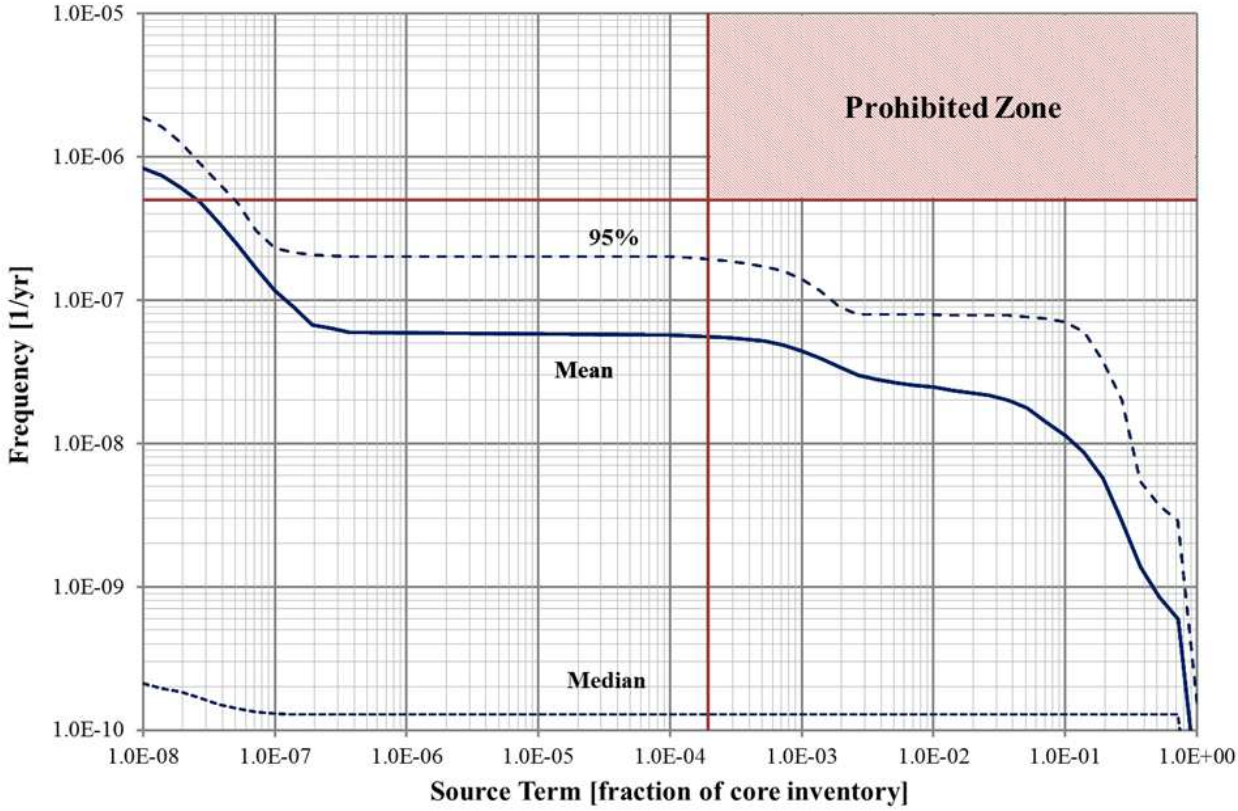

Figure 2: Cs release from reactor core calculated in the OL3 Level 2 PSA. The X axis shows the release fraction and the Y axis shows the frequency at which the release fraction is exceeded (in units of 1/a).

According to Figure 2, plant unit OL3's severe accident release is clearly lower than required in the YVL 2.8 guide. Because the distribution is almost horizontal at the release limit (100 TBq corresponds to 1.9E-4 Cs release fraction), the uncertainties of the release calculation do not significantly affect the margin between the obtained large release frequency and the required large release frequency.

3. SCOPE OF THE PSA FOR OL3

3.1. Plant operating states

The OL3 PSA deals with initiating events in all operating states. The operating states modeled in the PSA are based on the Technical Specifications. In the analysis, transitioning periods from the shutdown to the fuel replacement modes and further to the startup modes have been added to the operating states. A total of 11 shutdown operating states have been defined in PSA which split between modes C and F depending on plant parameters and systems configurations and power operation state which comprises two modes (A, B). The plant modes have been defined in Technical Specifications as following:

A – Power operation;
B – Shutdown with secondary side heat removal;
C - Shutdown with primary side heat removal;
D – Refueling low level;
E – Refueling high level;
F – Core offloaded.

In addition to the nuclear fuel in the reactor pressure vessel, the OL3 PSA also covers any damage of the fuel in the fuel building pools.

3.2. Initiating events

The selection of initiating events is a crucial step in the PSA. After all initiators have been identified and aggregated into initiating event categories, the event sequences are developed. The purpose of the definition and grouping of initiating events is to develop a set of initiating events, which is as complete as possible. Initiating events are characterized by a disturbance of the balance of heat production in the core (respectively the fuel pool) and heat removal from the core (or from the fuel pool) in such a way that countermeasures are required to prevent core (respectively fuel) damage. An initiating event can be caused by equipment failure, human actions, threatening events inside the plant or external events.

The OL3 plant unit is of a new design, and it has no plant-specific reliability data to be used based on operating experiences. In the recognition of initiating events and the estimation of their frequencies, operating experience data from reference plants (German Konvoi and French N4 pressurized water reactors), information from their PSA models and the PSA models of other EPR plant units under construction have been used. In addition, generic data on pressurized water reactors and their possible initiating events have been used. Effort has also been made to systematically recognize possible initiating events using the Master Logic Diagram (MLD). Similarly to accident analyses, events that could lead to disturbances in the reactor power control, water inventory or residual heat removal have been analyzed in MLD. Technical Specifications and the operating manual have also been used, in particular, for shutdown initiating events. In order to ensure the completeness of initiating events, accident analyses, I&C failure analyses and failure and effect analyses (FMEA) have been used after.
The grouping of initiating events is based on the fact that for events in the same group, the progress of the accident and the required safety functions are essentially similar.

According to the above-mentioned principle, the initiating events in the OL3 PSA have been divided into the following groups of initiating events:

- loss of coolant accidents (LOCA)
- operational occurrences (transients such as the loss of feed water, heat sink, off-site power or residual heat removal)
- primary-secondary leaks (e.g. steam generator tube rupture)
- leaks on the secondary side (e.g. steam pipe break)
- anticipated operational occurrence in which reactor trip fails (ATWS)
- common-cause-failure initiating events (CCI, e.g. loss of intermediate cooling chain)

- planned shut down
- internal hazards (e.g. fires, explosions, floods, load drops, impacts of missiles)
- external hazards (e.g. exceptional weather conditions, earthquakes)

The major internal hazards are internal fire and internal flooding for which specific methodologies have been provided. Fire PSA is an essential part of a full scope Level 1 PSA. Cable fires play an important role in fire PSA and therefore cable routing is considered in detail. During the design of new nuclear power plants the information on cable routing is not yet available. However, for the use of probabilistic safety insights during the design and for licensing purposes a fire PSA is requested. Therefore, the fire PSA for OL3 was conducted in two stages. The methodology, which has been developed for the first stage, makes use of the strictly divisional separation of redundancies in the design of modern nuclear power plants. Within one such strictly separated division the exact information on cable routing is not needed and is therefore replaced by the conservative assumption that all the equipment in the concerned division fails due to a fire; critical fire areas are defined where components belonging to different divisions may be affected by a fire [9]. During the second stage, the conservative modeling of the early phase fire PSA has been replaced by the integration of cable routing information in the detailed design phase PSA. With respect to flooding hazards, the PSA modeling takes credit from the general EPR concept regarding protection against internal flooding in the divisionally-separated buildings, which is based on the principle of restricting the effects of flooding to one safety division. This explains the low contribution of flooding events to overall CDF (less than 1%).

External hazards, defined as events originated from outside the plant, but with the potential to create an initiating event in the plant, are distinguished as seismic events or other external hazards.

The seismic PSA uses the state of the art methodology as described in Appendix B of ANSI/ANS 58.21 “External-events PRA methodology”. The key elements of the seismic PSA are:

- A seismic hazard analysis, which develops frequencies of occurrence of different peak ground accelerations at the site. The seismic hazard for the site is available from the seismic PSA performed for OL3 Nuclear Power Site.
- A seismic fragility evaluation which estimates the conditional probability of failure of important structures and equipment whose failure may lead to unacceptable damage to the plant (e.g., core damage). Seismic walkdown was performed to check the assumptions and validity of fragility analyses used in risk quantification and resulted in updates of some of the fragility analyses.
- A systems/accident sequence analysis which models the various combinations of structural and equipment failures that could initiate and propagate a seismic core damage sequence.
- Risk quantification which presents the results of a seismic hazard, fragility and system analyses to estimate the frequencies of core damage and plant damage states.

External events other than seismic events are analyzed using a screening analysis based on [10].
Single phenomena have been eliminated based on the following criteria:
– severity
– occurrence frequency
– distance
– inclusion in other events
– warning time
– occurrence at the plant location

In addition to single natural events, multiple external events have been examined. Multiple external events may be important for safety, because different phenomena may simultaneously threaten diverse ways to implement safety functions. In the elimination of multiple external events, the following elimination criteria were used in addition to the elimination criteria for single phenomena:
– independence and low probability of simultaneous occurrence,
– inclusion in the definition of a single phenomenon to be examined,

– effect on the plant not greater than the effect of a single part of a multiple external event.

As a result of the elimination, one multiple external event was selected for PSA modeling: strong wind combined with simultaneous snowfall.

Events affecting the fuel pool cooling function have also been analyzed. Consequences (Damage States) of events leading to a loss of fuel pool cooling system are:

Steaming: Steam goes to the fuel building atmosphere after loss of fuel pool cooling function while sufficient water level in the Spent Fuel Pool is ensured by a make-up system, thus preventing fuel damage; and

Fuel damage: Fuel assemblies in the Spent Fuel Pool are uncovered during an extended period of time.

3.4. Specific issues related to initiating events during shutdown states

In the OL3 shutdown PSA, the initiating event probabilities are calculated per refueling outage (equivalent to "per calendar year with a refueling outage" when considering one outage per year). In other words, the initiating event probability (frequency) assigned to a particular POS takes into account both the expected hourly rate of occurrence of the initiator while in a particular POS and the duration of the POS.

Two different models are applied to the initiating events probability (frequency) calculation in the OL3 shutdown PSA, in order to generate per refueling outage probabilities (or "per calendar year" frequencies):

- Model (1) is suitable for initiating events which may occur randomly at any time in a POS. In this case, the initiating event probability (frequency) is proportional to the time spent in the POS. This model is useful when initiating event probabilities (frequencies) are estimated directly from operational experience or when data is available on the occurrence of precursors, but not on the occurrence of the initiating event itself.
- Model (2) is relevant for situations in which the initiating event probability (frequency) is not dependent on the duration of the POS.
  In this case, initiating events arise due to errors or failures following an event, which occurs a fixed number of times in the POS. For example, to model the probability of an Uncontrolled Level Drop or an Heavy Load Drop,

The possibility of an initiating event being caused by a human error is usually included in the frequency estimate of the initiating event based on operating experience data from similar plants. In the OL3 PSA, the estimation of the frequencies of the following initiating events also includes an explicit analysis of the probability of a human error:

- An uncontrolled decrease of the water surface level (shutdown states Cbd and Du),
- homogenous boron dilution (shutdown states),
- incorrect cooling water discharge from residual heat removal system (RHR) 1 and 4, (shutdown states Cad1 and Cad2),
- common-cause-failure initiating events (loss of cooling chain and loss of safe-guard building ventilation/cooling).

3.5. Systems modeling

A separate system analysis is performed for each front line system performing the safety functions modeled in the event trees, and for each support system to the front line systems. The system analysis is used to analyze the undesirable states of the plant systems in order to determine all the credible ways in which the undesirable state can occur.
A Failure Mode and Effects Analysis (FMEA) is required in YVL 2.0 [3]. The system analyses are based on respective system FMEA as the FMEA provides an efficient interface between the plant system documentation and the fault tree modeling.

The fault tree model considers:

- failures of the components itself in their specific failure modes,
- failures of the power supply of the component (electrical power supply, compressed air),
- failures of the signals for actuation as well as undesired (spurious) emission of signals,
- failures of auxiliary systems (e.g. cooling water, room cooling, lubrication oil supply) as far as those not included in the component boundary,
- scheduled test and maintenance unavailability of the component
- common cause failures
- human errors (pre-accident and post-accident)
- specific conditions, e.g. adjustment of a safety function to a specific event, by switching on or off fault tree branches,
- unavailability of components due to hazards (e.g. fire, flooding).

In the OL3 PSA the functional system dependencies are considered in the fault tree (FT) model while the necessary safety functions are defined as success criteria in the event tree (ET) modeling.

3.6 Component reliability data

Since the EPR is a new reactor design no reactor specific operating experience is available. Thus, the main goal of the reliability data assessment is the identification of components used in Framatome and Siemens/KWU plants that are similar to the OL3 components with respect to component task, operating conditions and design. Reliability data for these similar components are reported in the databases ZEDB [4] and EIReDA [5]. If no similar components have been identified or no reliability data are given in the ZEDB and EIReDA other data sources are used, especially the T-Book [6] and sources on equipment performance in U.S. plants (Generic component failure data base for light water and liquid sodium reactor PRAs (EG&G) [7], NUREG/CR-6928 [8]).

Equipment failure modes identified in the failure mode and effect analyses as relevant for PSA are directly linked with one of the two basic reliability models in FinPSA:

- “Standby” model to describe the unavailability of periodically tested equipment not in operation before the initiating event
- “Operating” model to describe
    - A failure of equipment during a specified mission time or
    - A failure of operating equipment that failed before the initiating event and that is still unavailable (repair not finished yet).

Uncertainty distributions for all component reliability data are defined in order to perform quantitative uncertainty analyses using the Monte-Carlo-Analysis with 10000 Simulation runs. The FinPSA parameter “Population” is used to define groups of basic events whose reliability data are based on the same data source. The FinPSA tool allows to define the accuracy as an optional termination criterion for the results in percentage. To ensure sufficient convergence the accuracy is set to “default” in FinPSA tool. In addition the maximum relative change of the estimates compared to previous estimates is calculated and reported by the FinPSA tool.

Uncertainties due to modeling assumptions and modeling simplifications are evaluated qualitatively concerning their potential impact on the overall core damage frequency in a qualitative uncertainty analysis.

3.7 Human reliability analysis

Experiences with other PSAs have shown that human errors may have a significant importance with respect to the total CDF and LERF. A multidisciplinary HRA team has been established to identify relevant operator actions and to quantify the probability of human error.
The following types of human action are considered in the PSA:

- Tasks performed after an initiating event (post-IE):
  The design of the OL3 plant aims to provide enough automatic protection to preclude any need of operator action within the first 30 minutes after accident initiation. However, post-IE operator failure has to be considered in all cases where
  - the plant has to be brought into a safe shutdown condition in the longer term,
  - beyond design conditions occur due to loss of safety systems,
  - activation of safety systems is necessary to mitigate the consequences of severe accidents as backup to automatic actuation (in case of its failure).
- Pre-IE errors during maintenance and repair can decrease the reliability of safety functions. Typical examples of this type of errors are valves left in wrong position after a test and mis-calibrated instruments
- Inadvertent plant personnel performance may lead to initiating events, additionally. Errors of this type (leading to IE) is of interest especially in the shutdown PSA.

THERP (Technique of Human Error Rate Prediction) method is used to predict human error probabilities for the PSA. THERP is a very detailed analysis method using the decomposition of actions. It is recommended for NPP applications in the European Utility Requirements Ref. [15] as well as in the PRA Guidelines published from the German Federal Ministry for Environment, Nature Protection and Nuclear Safety Ref. [16].

3.8 Modeling specifics for instrumentation and control systems

The modeling of instrumentation and control I&C systems in the OL3 PSA uses a so-called super-components approach, where failures of I&C signals are presented as aggregates of I&C modules with a specific functionality. The modeling is based on the detailed modeling of the I&C reliability analyses for the respective I&C systems.
In the OL3 PSA the malfunctions in I&C systems are analyzed and modeled in details for both as failures or faults leading to components unavailability (no signal, output “0”) and to undesired spurious actuation (spurious signal, output “1”) of functions. The faults originated in systems hardware and software are considered. Potential software related common cause failures (CCF) of computerized I&C systems are taken into account explicitly in the modeling process.

3.9 Level 2 PSA aspects

In the OL3 plant’s Level 2 PSA, the durability of the containment has been analyzed in associated separate analyses. Containment durability or bypass has been examined with regard to the loads of the following phenomena occurring during severe accidents:

- early and late hydrogen fire/explosion
- steam explosion inside and outside the pressure vessel
- rupture or melt-through of steam generator tubes
- pressure vessel melt-through
- missiles, including high-pressure shattering of pressure vessel
- direct containment heating (DCH)
- molten core control failure, molten core–concrete interaction
- slow containment over-pressurization.

In addition to these, the Level 2 PSA includes containment isolation failure analysis, containment bypass leakage recognition and examination of filtered containment depressurization.

The Level 2 PSA was performed with a non-integrated approach (see [11]), shown in figure 3, for which the PSA model consists of three parts: Level 1 PSA model, Level 1 – Level 2 PSA interface model and accident progression event tree model. The Level 1 PSA event tree model was expanded by the event tree modeling of the Level 2 PSA interface, whereas the accident progression event tree model was created in a dedicated Level 2 PSA event tree program. Some of the advantages of this process are: the possibility to make use of the special features of the dedicated Level 2 PSA event tree model, including integrated modelling of the substantial uncertainties related to many severe accident phenomena, and the possibility to calculate path-dependent source terms within the event tree model.

A dedicated Level 2 PSA program also allows the exact quantification of the accident progression event tree, taking into account the possibility of large branch probabilities, whereas the extended Level 1 model can be calculated using minimal cut sets (MCS), a method that is mathematically designed to deal with small branch probabilities and the assumption that the probability of success is one.
Another advantage of the dedicated Level 2 PSA program is the possibility to assign variables to the different branches and to calculate path-dependent source terms, together with related uncertainties, within the event tree model.

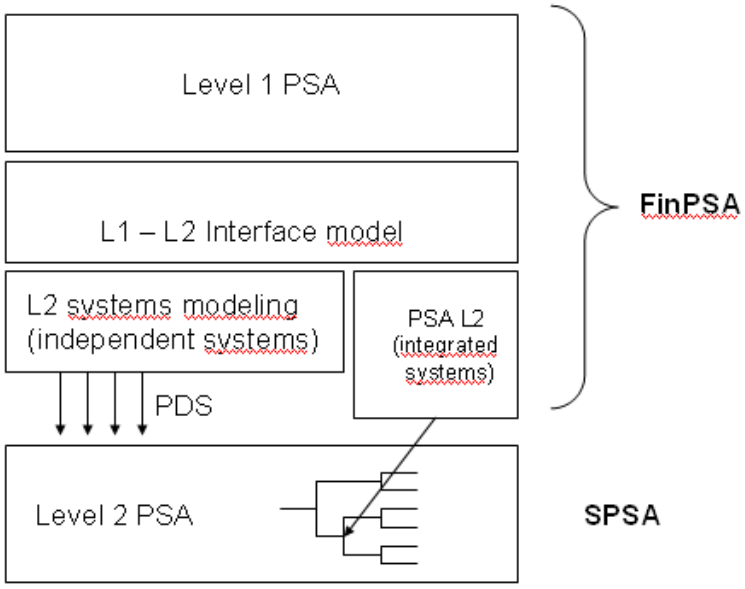

Figure 3: Level 2 PSA using a non-integrated approach

In order to transfer input from the Level 1 PSA modeling to the Level 2 PSA a separate interface model is provided with FinPSA which includes the modeling of relevant severe accident mitigation functions (which are not modeled in the Level 2 PSA modeling) either by an expansion of the event tree or by separate fault tree modeling, such as:

- Prevention of high pressure core melt scenarios by opening primary depressurization valves / pressurizer safety valves
- Containment isolation
- System functions to prevent a containment failure (Containment heat removal system, Containment venting).

The core damage sequences (consequence CD) are grouped into plant damage states (PDS) comprising 18 non-bypass PDS, ten of which are at-power PDS, 15 bypass PDS, one PDS representing gap release and one PDS dedicated to direct large release due to an initially ruptured containment.

Level 2 calculation produces almost 3.5 million source terms, which are classified into 13 source term categories (release categories). The source term model is of type XSOR [12], which models three volumes (containment, annulus and safeguard building/fuel building) and the environment. The flows between them have been modeled as a function of accident conditions. The flow speeds are based on values received from the MAAP and COCOSYS models. Timings connected to accident progression, and their uncertainties, are based on the MAAP calculations done for the PSA and on COCOSYS calculations done for the deterministic severe accidents source term.

Releases are calculated for at least 100 hours starting from the moment that fission products start being released from the core. The calculation model produces an estimate of the amount, quality, timing and probability with uncertainties of the radionuclides released into the environment. The initial height of the release is not included in the model, but it can be determined based on the containment failure point or bypass point.
The source term model considers the release and transfer of noble gases and nine different aerosol categories.

The distributions of the reactor core release fractions are specified for five main cases (the pressure refers to pressure at the moment the pressure vessel breaks):
– high-pressure transient or minor LOCA
– low-pressure transient or major LOCA
– small containment bypass leak, no depressurization
– large containment bypass leak or small bypass leak with depressurization
– molten core outside the pressure vessel; includes molten core–concrete interaction.

4. PSA APPLICATIONS

Based on the regulatory requirements set in the YVL [1] the PSA modeling and results were used for specific applications during the design and construction phases of the project. The PSA was applied in several areas during the design and construction of OL3, e.g.

- to support the detailed design of systems, structures and components (SSCs),
- evaluate plant modifications documented by design change requests (DCRs),
- define pre-service inspection programs (RI-PSI) and
- evaluate the safety classification of SSCs.

The PSA was further used in the definition of risk-informed in-service inspection programs (RI-ISI), the evaluation of allowed outage times and periodic testing frequencies for the Technical Specifications, providing input for reliability centered maintenance (RCM), the optimization of proposals for online maintenance packages, the development of operating procedures and the simulator training program for operating personnel, and the evaluation of commissioning tests.

The experience in implementing Risk-Informed Applications (RIA) on advanced PWR i.e. the EPR is presented in [14].

5. CONCLUSION

Starting with the preparation of a design phase PSA for nuclear power plant unit Olkiluoto 3, which was a part of the construction license application, the PSA has been continuously updated and issued several times to correspond with the progression of the detailed design. The results obtained have been used further to verify the plant design as well as verify/optimize operating and maintenance procedures.
The latest PSA update was submitted to the regulatory body (STUK) as part of the operating license application.
The OL3 PSA has been used to demonstrate that the nuclear power plant has been designed, constructed and commissioned in a way that meets the safety requirements.

The OL3 PSA has comprehensively dealt with various initiating events in all plant operating states, including annual outages. The analysis also includes events occurring in the fuel building with the potential to result in damage of the spent fuel.

By comparing the results obtained with the numerical design objectives on the

- mean value of the frequency of core damage to be less than 1E-05/a
  and
- the mean value of the probability of a release exceeding the target value defined in section 12 of the Government Resolution (395/1991) to be smaller than 5E-7/a,

with,

- the calculated core damage frequency of 1.7E-06/a (mean value of the uncertainty analysis for the overall core damage frequency) being well below the design objective
  and
- the expected value of the large release frequency of 7.7E-8/a, together with a very small share of early (<6 hours) emissions,

it is concluded that the OL3 plant fulfils the probabilistic design objectives. The results also demonstrate the effectivity of the implemented accident management features and strategies.
Finally, OL3 PSA is used for different Risk-Informed Applications supporting a safety management of the plant as described above.

References

[1] Guide YVL 2.8, *Probabilistic Safety Analysis in Safety Management of Nuclear Power Plants*, STUK (2003)
[2] Guide YVL A.7, *Nuclear Power Plant Risk Management*, STUK (2011)
[3] Guide YVL 2.0, *Systems Design for Nuclear Power Plants*, STUK (2002)
[4] Centralized Reliability and Events Database, Reliability Data for Nuclear Power Plant Components, TW 805e-13 – Volume 1 and Volume 2, December 2012, ISSN 1439-7498
[5] EIReDA 1998, European Industry Reliability Data Bank, Joint Research Centre of the European Commission, 1998
[6] T-Book, Reliability Data of Components in Nordic Nuclear Power Plants, 7th edition 2010, ISBN 978-91-633-6144-9
[7] EGG-SSRE-8875, Generic component failure data base for light water and liquid sodium reactor PRAs, February 1990
[8] NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, January 2007
[9] J. Blombach and H. Kollasko, *Methodology for Fire PSA during design process*, Independent journal for nuclear engineering (Kerntechnik) Vol. 74 No3 May 2009.
[10] SKI Report 02:27, *Guidance for external events analysis*,.
[11] H. Kollasko, E.-M, Pauli, G. Dirksen, R. Grygoruk, "*Integrated versus non-integrated Level 1 – Level 2 model, sharing experience with both approaches*," PSAM11, 2012, Helsinki.
[12] NUREG-1150, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, U.S Nuclear Regulatory Commission (1990)
[13] Government Decree on the Safety of Nuclear Power Plants 395/1991
[14] Pierre LACAILLE, Jean-Yves BRANDELET, Hervé BRUNELIERE, *"Framatome's lessons learned on Risk-Informed Applications", PSAM 14, September 2018, Los Angeles*
[15] European Utility Requirements VOLUME 2; GENERIC NUCLEAR ISLAND REQUIREMENTS, CHAPTER 17 PSA METHODOLOGY Revision D October 2012
[16] Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke Facharbeitskreis probabilistische Sicherheitsanalyse für Kernkraftwerke BFS-Schr-37/05 Bundesamt für Strahlenschutz, 2005