Olkiluoto 3 EPR
PSA Main results and conclusions – fulfillment of the regulatory requirements for operating license

Presented by: Heiko Kollasko – Framatome

Co-Authors:
Roman Grygoruk – AREVA
Gerben Dirksen – Framatome GmbH
Jari Pesonen, Lasse Tunturivuori, Antti Tarkiainen – TVO

Probabilistic Safety Assessment and Management PSAM
September 20, 2018, UCLA, Los Angeles, CA
Content

(1) OL3 EPR Main features
(2) Regulatory framework
(3) Project performance
(4) Targets
(5) Scope and Modelling
(6) Results
(7) Conclusions
OLKILUOTO 3 EPR MAIN FEATURES
4 loop Pressurized Water Reactor 1600 MWe, supplied by consortium of AREVA and Siemens to TVO

Safety approach consists of

- improved preventive measures against accidents
- Mitigation features to cope with severe accident

Accident Prevention enforced by:

- Four redundant and geographically separated safeguard system trains (divisions)
- Diversity in system design and safety functions including back-ups to eliminate common mode failures
- Physical separation against internal & external hazards
- Increased grace periods for operator actions by large water inventories
- Optimized man-machine interface by digital instrumentation and control systems
- Severe accidents are taken into account in the design
REGULATORY FRAMEWORK
Authority STUK supervises compliance with legislation and regulations

Regulatory Guides on nuclear safety and security (YVL)

YVL 2.8* - May 2003 – valid guideline for the operating license „PROBABILISTIC SAFETY ANALYSIS IN SAFETY MANAGEMENT OF NUCLEAR POWER PLANTS“

- Requirements on a “PSA DURING THE DESIGN AND CONSTRUCTION OF A NPP”
- Requirements on a “PSA DURING THE OPERATION OF NUCLEAR POWER PLANTS”
- CONTENT AND DOCUMENTATION OF PSA
- QUALITY MANAGEMENT

→ Provides basic requirements on the scope and application of a PSA

* Replaced Nov 2013 by YVL A.7
The Finnish YVL regulatory guide requires the use of the PSA during construction and commissioning by Risk-Informed application, e.g:

- **In-Service Inspection (RI-ISI)**
  “The PRA shall be used in the risk-informed development of the in-service inspection programmes of Safety Class 1, 2 and 3 as well as Class EYT system piping.”

- **Periodic Testing (RI-PT)**
  “The PRA shall be used in the risk-informed development of testing procedures for systems and components important to safety”

- **Technical Specification (RI-TS)**
  “The PRA shall be used in the risk-informed development of the Operational Limits and Conditions (OLC) to assess their coverage and balance.”

- **Classification/categorization (RI-SSC)**
  “The PRA shall be applied to determine the safety classification of structures, systems and components.”

- **Preventive Maintenance**
  “The PRA shall be used … to develop preventive maintenance programmes”.

Furthermore the PSA shall be used for:

- drawing up EOP and provide input for the staff training
- provide potential risk related insides to the commissioning test phase and program

* See paper #162 on Lessons learned on RIA
PROJECT EXECUTION

OL3 NPP Basic Design Phase (design phase)

1st PSA L1/L2 (safe and balanced design)

OL3 NPP Detailed Design Phase (construction phase)

Update #1 PSA L1/L2

Update #2 PSA L1/L2

As-built PSA L1/L2

1st round of RIA

Gap Analysis

Final round of RI applications

Construction License

Operating License

OL3 NPP Operating Phase
OL3 PSA
Project execution (1)

- **Design phase PSA**
  - A level 1 and 2 “Design phase PSA” is submitted for the application for construction license (CLA)

- **Detailed design phase**
  - Continuous update of the PSA
    - to support the detailed design
    - to form a basis for the “Construction phase PSA”
  - Intermediate FinPSA model releases for reference configurations (e.g. 2009, 2010, 2015)

- **Construction phase PSA**
  - A level 1 and 2 “Construction phase PSA” is submitted for the application for operating license (OLA)
  - Releases 2015 + 2016 with an Extended Fire PSA and a conservative and realistic model
  - Last release in 2018 (update concerning design reference configuration integration authority comments on OLA PSA)
Determination of methods on different topics in specific methodology reports

→ included a STUK Review + Approval

◆ PSA
  - internal flooding und internal fire
  - Common Cause Initiator
  - HRA
  - Seismic PSA plan
  - Developing of Seismic Fragilities
  - Consideration of spurious signals in PSA

◆ PSA based risk application
  - Probabilistic Review of Safety Classification
  - Risk-informed Periodic Testing
  - Risk-Informed Technical Specifications
  - Risk informed Pre-Service and In-Service Inspection Methodology

→ Securement of the progressing PSA work for the final license process
TARGETS
According to the Government Resolution (395/1991) referred in YVL 2.8, "accidents leading to large releases of radioactive materials shall be very unlikely"

- In YVL2.8 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 $5E-7/a$.
  - Definition of large release:
    - Atmospheric release of cesium-137 exceeding 100 TBq
SCOPE AND MODELLING
- Level 1 and Level 2 PSA
- Plant operating states: at-power and shutdown
- Spectrum of initiating events:
  - Internal events: (e.g. Transients; Secondary side breaks; LOCA)
  - Common cause initiators (based on screening analysis);
  - Internal hazards:
    - Internal Fire;
    - Internal Flooding;
    - Load drop;
  - External hazards:
    - Seismic events
    - other external events (based on a screening analysis)
  - Events affecting the heat removal from the spent fuel pool
System modeling is based Failure Mode and Effects Analysis (FMEA) which includes
- Component failures by their specific failure modes,
- Failure of dependencies
  - power supply of the component (electrical power supply, compressed air)
  - signals for actuation,
  - auxiliary systems (e.g. cooling water, room cooling, lubrication oil supply),

Additionally fault tree modeling includes:
- Scheduled test and maintenance unavailability of the component
- Common cause failures
- Human errors (pre-accident and post-accident)
- Unavailability of components due to the initiating event (e.g. CCI and Hazards like fire, flooding)
- undesired (spurious) emission of signals
Modeling of I&C

- Based on FMEA for I&C systems

I&C reliability analyses to verify unavailability targets:
  - Detailed FT-Modelling of I&C functions with basic events on hardware module level
  - Modelling of software failure modes
  - Provides the basis for the I&C modelling in the PSA

Compact modelling of I&C in the PSA:
  - Super components sub fault trees to create super-component basic events representing the failure of I&C system units
    - Not directly linked to the PSA model
    - Provide the failure probability for the I&C super-component basic events in the PSA
  - Super-components are then used for the I&C Fault tree modelling in the PSA (detected and undetected failures),
    - Signal conditioning
    - Processing units
    - Explicit modelling of dependencies on power supply, HVAC and indications in the control room for diagnosis tasks
Treatment of uncertainties

- Quantitative based on the uncertainty distributions of parameters
  - initiating event frequencies
  - component failure rates
  - Parameters on common cause failures
  - Human error probabilities

- Qualitative
  - Discussion of modeling uncertainties (assumptions and simplifications) → includes an evaluation of the impact on the result
  - Tracking of model modifications with the reasoning and evaluation of the impact on the result

- Sensitivity analyses for the major uncertainties on modeling assumptions, methods and data e.g:
  - CCF Modelling according to US NRC MGL parameters versus EUR
  - Consideration of multiple spurious operations due to software failures
  - Sensitivity studies on assumptions made for ATWS modeling
  - Sensitivity studies on assumption in Fire PSA
Level 2 PSA

Non-integrated approach consisting of 3 parts:

- Level 1 PSA model
- Level 1 – Level 2 PSA interface model
- Accident progression event tree model

Advantages:

- Modeling of the substantial uncertainties related to severe accident phenomena
- Possibility to calculate path-dependent source terms within the event tree model
- Exact quantification for large branch probabilities
RESULTS
Core damage frequency of the Level 1 PSA:

- Mean value: $1.7 \times 10^{-6}$/a
  (Percentiles: 5% $\rightarrow 5.4 \times 10^{-7}$, 50% $\rightarrow 1.1 \times 10^{-6}$, 95% $\rightarrow 3.5 \times 10^{-6}$)
- Point estimate: $1.4 \times 10^{-6}$/a

Fuel damage frequency (fuel pool events):

- Mean value – $2.2 \times 10^{-8}$/a

Large release frequency Level 2 PSA

- Mean value (includes core and spent fuel pool)
  
  (over 100 TBq of Cs-137) $7.7 \times 10^{-8}$/a,

- Core related ca 72%; spent fuel pool related ca 28%.

* 2018 Release
OL3 PSA
Main contributors to CDF

Internal events (Transients and LOCA) 66%
Internal Hazards 26%
External Hazards 8%

Power operation 60%,
Shutdown states with RPV closed 13%,
with RPV open 27%
Relative contribution of events leading to fuel damage

Power operation and non refueling outage 47%,
Refueling outage 53%,
The prohibited zone is restricted by Guide YVL 2.8, where the frequency of releases exceeding 100 TBq of Cs 137 must be less than 5E-7 /a.

*) Basis 2017
OL3 PSA
Conclusion

- Continuous update of PSA from the beginning of the Project to correspond to the progression during detailed design and provide insights to the design
- Results used to verify the plant design as well as verify/optimize operating and maintenance procedures and commissioning program by RI applications
- Latest PSA update was submitted to the regulatory body (STUK) in 2018 as part of the operating license application
  - Full scope PSA concerning spectrum of initiating events, plant operating states and modelling of systems (including dependencies)
  - Demonstration that the core damage frequency and the frequency of large releases is well below the target values required by finnisch regulation
Thank You

Heiko.Kollasko@framatome.com
Any reproduction, alteration, transmission to any third party or publication in whole or in part of this document and/or its content is prohibited unless AREVA NP has provided its prior and written consent.

This document and any information it contains shall not be used for any other purpose than the one for which they were provided. Legal action may be taken against any infringer and/or any person breaching the aforementioned obligations.
DISTRIBUTION OF LARGE RELEASE BINS

- Containment isolation failure: 34.9%
- Early containment rupture: 17.0%
- Non-isolated SGTR: 3.1%
- Interfacing system LOCA: 45.1%
FREQUENCY VERSUS SOURCE TERM, NON CUMULATIVE
FREQUENCY VERSUS TIME OF RELEASE, Early (first 20h)

- Intact containment (small)
- Early containment rupture (large)
- Containment isolation failure (large)
- Arrested core melt after passive rupture and injection (small)
- Induced SGTR (large)
- Early containment leak (small)
Component reliability data

- Reliability data assessment on failure rates including uncertainty distributions based on operating experience taken from reference plants N4 (France) / KONVOI (Germany)

If applicable for the respective equipment use of:
- Germany – ZEDB (centralized reliability data base)
- French data – EIReDA data base

Otherwise use of other data sources e.g:
- Nordic failure data provided in T-Book
- US operating experience
Modeling of Human actions

- Identification of relevant operator actions by a multidisciplinary HRA team

- Types of human action considered in the PSA:
  - Post IE errors on tasks required after an initiating event:
    - Automatic protection design precludes any need of operator action within the first 30 minutes after accident initiation
    - Post-IE operator failure relevant
      - the plant has to be brought into a safe shutdown condition in the longer term,
      - beyond design conditions due to failure of safety system functions,
  - Pre-IE errors during maintenance and repair (e.g. wrong position of valves; miscalibration of measurements)
  - Inadvertent plant personnel performance may lead to initiating events,
    - errors of this type are of interest especially in the shutdown PSA

- THERP (Technique of Human Error Rate Prediction) method used to predict human error probabilities
  - very detailed analysis method using the decomposition of task (diagnosis and action)
  - recommended for NPP applications in several guidance, e.g. European Utility Requirements and German PSA Guidelines