“PSA applications and risk informed approaches. Introduction of risk monitor technology at the Leningrad NPP, challenges and experiences”

Sergei Kukhar, PSA laboratory head
Alexei Makushkin, Engineering Support Department, Deputy Head
(Leningrad NPP)
Grounds to perform the PSA work

1. “Programme of measures to improve effectiveness of PSA methods use when operating NPPs”

2. “Programme of the LNPP PSA development”

3. “Recommendation to perform PSA Level 1 for internal events”
Use of PSA results for operating tasks

- Periodic assessment (within scope of ISA) of NPP safety level to make a decision on the possibility to operate a Power Unit including operation beyond the design lifetime (obtaining of an Operating license)
- Development of measures aimed at improving the safety level and definition of priorities
- Assessment of upgrading measures effectiveness
- Assessment of safety-important system reliability, their stability to CCF and erroneous actions of operating personnel
Use of PSA results for operation

- Optimization of ageing management
- Optimization of Operating Instructions; improvement of personnel training
- Engineering support for technical decisions (based on systematic approach and practice of comprehensive safety assessment)
- Improvement of technical & economical indicators of NPP operation (including Capacity factor)
- Assurance of on-line safety level monitoring (safety monitoring)
LNPP PSA development background

Unit 1
1997-2002 – PSA Level 1 (within LISA Project) (before upgrading)
- Development of 5 measures aimed at safety improvement
2003 - PSA level 1 for the status as upgraded
- 29 areas were assessed and prioritized to support the current level and for subsequent safety improvement (including implementation of the alternative shutdown system)
- Significance analysis was done for 14 revealed deviations from the requirements of normative documents

2004 - updating of Level 1 PSA following implementation of MCPS-VSO (alternative shutdown system)
2004-2007 - LISA-C Project (PSA applications)
2007-2008 – pilot Risk Monitor model (based on Risk Watcher software), preliminary verification
2009- Level 2 PSA, pilot shutdown PSA
2010- implementation of Risk Monitor into trial operation, technical audit with SSM participation
LNPP PSA development background

Unit 2
- 1996-1988- P&DSA Project (analysis of upgrading effectiveness)

2001: PSA Level 1 for Power Unit current status (before upgrading completion)
- analysis and prioritization of 21 safety improvement measures were implemented including optimization of planned scope of upgrading
- Development of 8 short-term and low-cost safety improvement measures (implemented within 2001-2005)

2005: PSA Level 1 for the status as upgraded
- analysis and prioritization of 23 areas to maintain the current status and further safety improvement
- Significance analysis was done for 7 revealed deviations from the requirements of normative documents

2006: PSA Level 1 updating following implementation of IMCPS
- analysis of 2-steps Power Unit upgrading programme

Unit 3
2002- PSA Level 1 for Power Unit current status (before upgrading completion)
2008-2009- PSA Level 1 and pilot PSA Level 2 (status after upgrading completion)
  pilot shutdown PSA

Unit 4:
2008-2010 PSA Level 1 and pilot PSA level 2 after upgrading completion; pilot shutdown PSA
Assessment of upgrading effectiveness. Leningrad NPP PSA level 1 results.
Risk monitor technology system at the Leningrad NPP

• At the Leningrad NPP transfer of PSA-based decision making technology to technical management is performed by means of Risk monitor implementation.

• Risk Monitor (or safety monitor) is the tool to assess risk (CDF, LERF). Anytime Risk Monitor corresponds to the current configuration of the Power Unit in regard to any component under maintenance. Risk Monitor can be used by the NPP operating personnel to support the operating decisions.
The purpose of risk monitoring system:

- to assist the technical control operators to exclude hazardous maintenance configurations of the Power Unit;
- to support maintenance planning and checking the equipment availability taking into account the current risk information;
- to define and assess the accident precursor events;
- to assess AOTs in current configurations based on safety assurance conditions.
Unit 1 Risk Monitor trial operation

• In accordance with the Decision issued by Concern “Rosenergoatom” within the period 2007-2008, the scope of experimental work to implement the Risk Monitor based on Risk-Spectrum/Risk Watcher software by Scandpower AB (Sweden) at LNPP Unit 1 was completed.

• Several verification calculations to assess risk for different events during Unit 1 operation and technical audit of risk monitoring system (with SSM (Sweden), GAN SEC, LNPP local inspection of Rostechnadzor SEMTU and NIKIET participation).

• Risk Monitor is in trial operation at Unit 1 Main Control Room.
Arrangement of LNPP risk monitoring users working places

Server Computer with net key 1

Server Computer with net key 2

Server Computer with net key 3

Central server

Risk monitor model

4 Computers (Main Control Rooms)

4 Computers (PSA laboratory)

2 Computers (Training Centre)

10 Computers with individual keys

1 Computer (Local Regulatory Inspection)
Main screen of Risk Monitor output information, Risk Watcher software, (LNPP, Unit 1)

Operator’s screen: 1 – DiD window (Tech. Spec. requirements) 2 – Graphical display of risk changes (with time) 3 – System components taken out of service 4 – Level of current risk and AOT
Technical audit of risk monitoring system

• Consideration of validation & verification documentation on Risk Spectrum/Risk Watcher software, Version 1.22.00
• Checking (validation) the LNPP Risk Monitoring system arrangement.
• Risk Monitoring system testing on specific examples of application tasks.
• Assessment of risk monitoring compliance with domestic normative basis.
• Consideration of earlier developed methodical instructions to use Risk monitors and risk analysis of operating events.
The following justification was provided as a result of the performed Technical Audit:

- “Risk Spectrum/Risk Watcher” software provides the main probabilistic safety indicators (MPSI) of the Power Unit;
- Quantitative and qualitative assessment of main probabilistic safety indicators might be one of the main arguments when considering various Power Unit operating matters;
- Guideline documents how to use main probabilistic safety indicators calculated by means of Risk monitor are to be developed (with specification of recommended criteria) so that to be able to make risk-informed decisions.

The approach was confirmed as successful. It was recommended to implement Risk Monitor at LNPP Unit 1 and to extend its use to the other Power Units.
Several results of Risk Monitor testing

- Risk assessment for different violations of Unit 1 operation;
- Analysis of the AOT-related Tech. Spec. terms;
- Maintenance risk-informed planning.
Risk analysis of operating events

Risk monitor allows to perform off-line analysis of events (using the PSA methodology) based on the risk indicator and minimum cut-sets analysis aiming at revealing of deficiencies in risk barriers and their impact on safety.

The following questions could be answered by means of the performed analysis:

• What kind of risk barrier is assumed under postulated event?
• What kind of sequence would result in the situation degradation (hazardous state)?
• What kind of actions are considered to be the most acceptable over the situation so that to reduce the risk from the occurred event?
IE Risk Analysis method

- Scenario analysis
- Initiating event category and boundary conditions identification
- Data input into Risk Monitor
- Risk assessment, DiD analysis, importance analysis (RIF, RWF and MCS rate)
- Sequences analysis (situation degradation analysis)
- The most acceptable actions to reduce the risk
- Risk-informed event categorization
Event risk profile (example)

- **Зона высокого риска**
- **Зона приемлемого риска**
Risk Watcher for Event Risk Analysis

Defence-in-Depth

Plant Operating Modes

Components Out of Service

Risk Level

Risk Barrier

Boundary Conditions

PIE
Importance analysis

RIF and RWF
## Risk zones categories

<table>
<thead>
<tr>
<th>Zone of values of current risk indicator, 1/year</th>
<th>Risk zone category</th>
<th>Postulated event characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDF ≤ 1E-06</td>
<td>Small risk</td>
<td>Not hazardous event *1</td>
</tr>
<tr>
<td>1E-06 &lt; CDF ≤ 1E-04</td>
<td>Medium risk</td>
<td>Acceptable risk *1, 2</td>
</tr>
<tr>
<td>1E-04 &lt; CDF ≤ 1E-02</td>
<td>High risk</td>
<td>Hazardous event *1, 2, 3</td>
</tr>
<tr>
<td>CDF &gt; 1E-02</td>
<td>Very high risk</td>
<td>Extremely hazardous event, not acceptable risk</td>
</tr>
</tbody>
</table>

* Options of decisions made by an NPP and an operating utility based on the operational event risk monitoring:
  1 – Event cause analysis, preventive measures development.
  2 – Including the event to the programme of the personnel simulator training.
  3 – Compensatory actions developing and introduction.
Risk Watcher for Precursors Risk Analysis

Normal operation power mode

Precursor
Recommendations

Testing allowed to formulate several methodological particular features to perform risk analysis. Some of recommendations are stated below:

• When a demand for reactor protections actuation is generated, it is necessary to perform calculation of the whole model (for all initiating events with nominal values except postulated initiating event, which probability shall be set as 1 - "TRUE") and to perform calculation only for the postulated event (i.e. to compare average annual accumulated risk for specific IE with conditional probability).

• After reactor successful shutdown, to use the shutdown PSA model.

• PSA models for all possible operating states are to be developed.

• It is recommended to determine a maximum (over the monitored period) indicator of risk values difference. However, the conclusion on event significance should be done based on the risk level corresponding to Power Unit configuration and status in the endpoint of monitoring.
recommendations

• It is recommended to specify a period of monitoring starting from the initiating event origin up to the Power Unit power rising (return to initial state).

• It is recommended to recalculate the IE frequencies (groups) in the PSA model after risk analysis (caused by event-violation), so that at the time of return to the initial state, the current risk value would correspond to updated initial data in regard to the IE frequencies. At the same time, the updating of the risk diagram prior to the time of Power Unit return to initial state is not required.

conclusion

Application of risk monitor for the operating states analysis contributes into the PSA model improvement; as such a practice allows revealing events which are not included in the model. The accumulated operating experience will help to solve this task.
Analysis of the AOT-related Tech. Spec. terms

The following task was formulated:

• To assess AOT for several configurations by means of RiskWatcher and Unit 1 risk monitor model;

• To perform the comparative analysis of calculated AOT values with AOTs stated in the Tech. Spec. for Unit 1 for the appropriate configurations.
The AOT is the time period which is assessed under the condition that the annual accumulated risk should not exceed the target value 1E-5:

\[
\text{AOT} = \frac{1E-5 - \text{CR}_t}{\text{R}_{tk}}, \quad (1)
\]

Where

\text{CR}_t – actual accumulated risk for the time period t (evaluated by risk monitor at any given time point);

1E-5 – national target in regard to total accumulated risk during a year (as per OPB - 88/97, General Safety Rules);

\text{R}_{tk} – current risk (CDF) in configuration k (1/year).

\[
\text{AOT formula in RiskWatcher is a particular case of formula (1):}
\]

\[
\text{AOT} = \frac{1E-5}{\text{R}_{tk}}, \quad (2)
\]
The following configurations were selected as a result of comparative analysis:
A) those for which the Tech. Spec. requirements were obviously conservative;
B) those for which the Tech. Spec. requirements were obviously optimistic.

**Example of A type configurations (totally 14 from 106)**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
<th>AOT as per Tech. Spec. (h)</th>
<th>AOT as per (2) (h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPEN- 1 + MPEN -2</td>
<td>Two small feed water (MPEN) pumps of one group</td>
<td>2</td>
<td>4214</td>
</tr>
<tr>
<td>NB-1 + NB-2</td>
<td>Two pumps of reliable service water supply system</td>
<td>Immediate shutdown</td>
<td>2497</td>
</tr>
</tbody>
</table>
Example of **B** type configurations (totally 12 from 106)

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
<th>AOT as per Tech. Spec. (h)</th>
<th>AOT as per (2) (h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPEN-3 + DG-13</td>
<td>Small feed water pump and Diesel generator DG -13</td>
<td>While in Planned maintenance</td>
<td>457</td>
</tr>
<tr>
<td>DG-11 + APN-5</td>
<td>Emergency feed water pump APN-5 and DG -11</td>
<td>While in Planned maintainance</td>
<td>406</td>
</tr>
</tbody>
</table>

The obtained results indicate that there are configurations which are formed due to realization of significant events accident precursors, for which no AOT limitations are specified in the Tech. Spec. Note, that configurations of type **B** are individual for each Power Unit and their number is quite big, therefore all of them can’t be mentioned in the Tech. Spec. And at the same time Risk Monitor is capable to present all such configurations on demand.
Maintenance risk-informed planning

Option 1
- Events history is in compliance with planned test schedule for Unit 1 safety systems

Option 2
- Tests of APN-4 pump revealed a failure. The test schedule remains unchanged (corresponds to test schedule for Unit 1 safety systems)

Option 3
- Tests of APN-4 revealed a failure. Further testing is performed as per the amended schedule (APN-5 tests are shifted).
Analysis of changes in cumulative risk for test schedules
Conclusions from the analysis

• Option 2: the Tech. Spec. safe operation requirements are violated, but the routine safety systems testing schedule is not breached.

• Option 3: the Tech. Spec. safe operation requirements are met, but the tests schedule is violated.

• Option 3 is more preferable with cumulative risk taken into account.

• Both options (2 and 3) can be acceptable in regard to cumulative risk criteria (in this case a decision can be made based on the other factors, economic reasonability).
Audit about risk monitoring automation

“Risk Watcher” risk monitoring is easy to use and originate data for risk analysis. Data and a command to generate the analysis are entered by an operator, which has several advantages as well as disadvantages. Complete automation of risk monitoring might be useful for post-analysis but it is not applicable for pre-analysis when planning maintenance. It is expected that risk monitoring development would be performed so that to assure both manual and automatic data entry and processing.
Future plans

• Risk monitoring may be used to justify the amended safe operation conditions based on risk-informative methods (as soon as the appropriate normative documents are put in force). Economical benefits for NPPs can be justified as well.

• Introduction of approved industrial-branch methodologies and subsequent development of Rostechnadzor safety guidelines on risk monitoring technology implementation and use, are required.

• The approach success was proved. Risk monitor is recommended to be implemented at LNPP Unit 1 and extended to other Power Units. Access to LNPP experience in regard to risk monitor implementation and development is recommended to be available within the nuclear industry branch.
Proposals for cooperation

• To continue international cooperation for the period of trial operation of Risk monitor system at LNPP in regard to:
  - normative basis
  - Personnel training
  - Modelling and software issues for risk monitoring
  - Risk-follow-up analysis

To arrange experience exchange between LNPP and Scandinavian NPPs in PSA and Risk monitor use

Development and improvement of PSA models (PSA levels 2 and 3, shutdown/start-up PSA, area events, external events, etc) and their application when setting Projects priorities aimed at NPP safety improvement
THANK YOU FOR ATTENTION!