Key aspects in the development of PSA
Level 1
Aims of the Level 1 PSA

- Determine Core Damage Frequency (CDF)
- Compare with risk criteria/targets
- Identify weaknesses in design and operation
- Determine whether the risk is as low as reasonably practicable (ALARP)
- Provide an input into the Level 2 PSA
- Use for PSA applications
Core Damage Frequency (CDF)

- CDF for operating NPPs
- CDF for new NPPs

Large Release Frequency (LRF)

- LRF for operating NPPs
- Practical elimination of accident sequences that could lead to large early radioactive releases for new NPPs (NS-G-1.2)
• Definition of the objective
  ▪ To assess the level of safety of the plant and to identify the most effective areas for improvement
  ▪ To assess the level of safety and compare it with explicit or implicit standards
  ▪ To assess the level of safety to assist plant operation

• Definition of the scope of the PSA
  ▪ Potential sources of radioactive releases
  ▪ Core damage states
  ▪ Plant operational states
  ▪ Initiating events
Specific PSA project management issues

- Complex team composition
  - Many experts are needed in several areas of knowledge: human reliability, fire and seismic analyses, severe accident phenomena, thermohydraulic analysis, system analysis, data analysis, etc.
  - The NPP has to be technically involved in the development of the PSA, but lack of personnel or expertise normally requires to involve external organizations.
  - Limited availability of experts. Possible conflicts of interest between external organizations.
  - Need for a technology transfer to the utility. A reduced PSA team is needed to maintain the PSA / develop applications

- Clear needs for a set of procedures defining clearly responsibilities, tasks interfaces, information transfer, modelling criteria, etc.
Scope of the Level 1 PSA

Range of initiating events
• internal initiating events - transients, LOCA, ...
• internal hazards - fire, flood, ...
• external initiators - earthquake, extreme weather conditions, ...

Modes of operation
• full power, low power
• shutdown, refuelling

Sources of radioactivity on the plant
• reactor core
• irradiated fuel in transit/ storage
• radioactive waste

Modern practice is to carry out a full scope PSA that address all initiating events and hazards + all modes of operation + all sources of radioactivity
Familiarization with the plant

- Plant Familiarisation and Information Gathering can be one of the most difficult and time consuming activities with respect to producing a PSA.
- Main plant information
  - The safety analysis report for the plant;
  - Technical specifications for the plant;
  - Plant design information reflecting the normal and emergency configurations of the plant;
  - Plant operational information with regard to plant procedures and practices;
  - Plant test and maintenance procedures and practices;
  - Engineering aspects of the plant design;
  - Plant event data.
INITIATING EVENTS ANALYSIS

ACCIDENT SEQUENCE ANALYSIS

SYSTEM ANALYSIS (incl. passive systems and computer based systems)

ANALYSIS OF DEPENDENT FAILURES

INTEGRATION AND QUANTIFICATION OF PSA MODEL

ANALYSIS AND INTERPRETATION OF RESULTS: Importance, sensitivity and uncertainty
ANALYSIS
DOCUMENTATION

COMMON CAUSE FAILURE ANALYSIS

HUMAN RELIABILITY ANALYSIS

DATA REQUIRED FOR LEVEL 1 PSA (component reliability, unavailability parameters, IE frequencies)
Initiating event analysis

• Selection of initiating events (IEs)
  ▪ Internal IEs are hardware failures or faulty operations of plant hardware through human error or computer software deficiencies – LOCAs and Transients
  ▪ External IEs are events that create extreme environments common to several plant systems – earthquakes, floods, high winds, air crashes

• Determination of safety functions
  ▪ Control reactivity, remove core decay heat, maintain integrity of reactor coolant boundary, maintain coolant inventory, protect containment integrity
  • Assessment of functions/system relationships
  • Assessment of plant systems requirements
    ▪ Success criteria for front line systems

• Grouping of the Initiating Events
Selection of Initiating Events

- Generic IE lists
- FMEA
- Engineering evaluation
- Operating experience
- Deductive methods
- IE lists from other PSAs

PRELIMINARY LIST of IEs

Screening

FINAL LIST of IEs
Accident sequence modelling

• Impact of physical processes on the development of logic models
  ▪ Containment failure before core damage, blow down forces associated with LOCAs

• Classification of accident sequences into plant damage states
  ▪ Assign event tree sequences into groups to examine in-plant and ex-plant consequences of core damage
Accident sequences analysis

- An event tree is a graphical representation of sequences of events.
- Investigate, analyze and graphically document what sequences of events and its consequences your system may develop in case of an error or a disturbance in your day-to-day operations.

- We mostly use Small Event tree/Large Fault tree approach
System modelling

• System modelling is an attempt to evaluate the potential for failure or success of a system.
• The system boundary and the initial conditions of the system must be carefully defined.
• The analyst must understand how the system is designed to operate and how it can fail to meet the design requirement.
• The model of the system can be a success model, or a failure model; a graphical model, a tabular model, or a linguistic model.
• All the models study the relationship between CAUSE and EFFECT.
System analysis. Fault tree

- Fault tree analysis is the most widely used method for developing system models.
- Before such modelling to be applied, however, analysts require to have a very good understanding of the system and its operation, which can be enhanced by the use of quantitative techniques such as Failure Mode and Effects Analysis (FMEAs).
- We apply this method successfully not only for PSA, but also to assess the reliability of systems in other projects.
Data assessment and parameter estimation

• Assessment of the frequency of initiating events
  ▪ Number of occurrences of the events and the total periods over which these events have been observed

• Assessment of the component reliability
  ▪ Standby systems, operating systems

• Assessment of common cause failure (CCF) probabilities
Reliability data assessment

- Statistic estimation of plant specific data or combination of plant specific and generic data from different sources are used.
- Integration of the data from more than one source is performed using a Bayesian approach.
- Generic data

- COMPONENT RELIABILITY
- UNAVAILABILITY PARAMETERS
- INITIATING EVENT FREQUENCIES
Human reliability analysis

- Modelling and analysis of pre-initiating event human errors (latent errors)
- Modelling and analysis of post-initiating event human errors
  - Selection of the approach
  - Misdiagnosis
  - The impact of the available time. Evaluation of time windows
- Human dependencies
Human reliability analysis

- A structured and systematic approach is used for the identification of human errors, the incorporation of the effect of such errors in the plant logic model (event trees and fault trees)
- Main methods
  - ASEP
  - THERP
  - Decision tree
Quantification of the results

• Determination of accident sequence Boolean equations

• Initial quantification of the accident sequences
  ▪ Screening values are used for human errors, mean values for primary events and IEs frequencies
  ▪ To make the sequences quantification practical it is necessary to truncate the analysis

• Final quantification of the accident sequences
  ▪ Requantification of accident sequences

• Uncertainty analysis

• Importance and sensitivity analysis
GENERAL STEPS FOR ANALYSIS OF INDIVIDUAL HAZARDS

CHARACTERIZATION OF THE HAZARD

Understand the hazard, its frequency and impact

INITIATING EVENT ANALYSIS

Identify what internal initiating events can be caused by the hazard, e.g., transients, LOCAs, LOOP

PLANT RESPONSE ANALYSIS

Analyse the response of the plant to the initiating events and how this response is affected by the hazard
Internal hazards

- **Internal fires and internal floods** usually contribute significantly to the overall risk from internal hazards and therefore they are subject for detailed analysis
  
  - Have the potential to damage multiple safety equipment
  
  - They may cause initiating events
  
  - Create harsh conditions
    - which together with the loss of equipment may affect or impede human response for mitigating the hazard and for shutting down the plant
  
  - Internal hazards may contribute significantly (in some studies up to 30% or more) to the plant risk
    - The contribution is highly dependent on physical separation of redundant equipment
General steps of the analysis

- Understanding the phenomenology of the hazard
  - Hazard identification and calculation of its frequency

- Familiarization with the plant:
  - Design, civil engineering, equipment layout
  - Fire protection, etc.

- Division of the plants in buildings and units of analysis

- Acquisition of information, plant walkdowns

- Screening analysis
  - Definition of qualitative and quantitative criteria

- Detailed analysis
  - Definition of Initiating Events
  - Modifications to the event trees and fault trees
  - Specific CCF analysis
  - Specific data analysis
  - Specific HRA
  - Quantification and analysis of results
    - Sensitivity, uncertainty and importance analyses

- Documentation
  - with special attention to assumptions and references used
Fire PSA Tasks

- Plant Information Collection
- Plant Walkdowns
- Cable Routing Information and Cable Location Database
- Initiating Events Caused by a Fire and Compilation of PSA Components List
- Fire Zone Definition
- Multi-Compartment Fire Analysis
- SCREENING
- Human Error Probability Analysis
- Risk Contributor Identification, Uncertainty and Sensitivity Analyses and Report Preparation
- Fire Frequency Evaluation
- Control Room and Cable Spreading Room Analysis + Circuit Analysis
- Detailed Analysis and Verification Walkdown
Flood PSA tasks

Data collection
- Plant information collection
- Plant walkdowns
- Flooding data

Identification of flooding scenarios
(equipment damage, flooding propagation paths, potential for human errors)

Screening by impact (qualitative)

Internal flooding assessment
- Identification of flooding sources and flood area characterization
- Flooding frequency evaluation

Screening by frequency (quantitative)
- Integration of internal flooding in PSA
- Quantification of core damage frequency

Detailed flooding assessment
- Flooding scenarios analysis
- Verification walkdowns
- Multiple hazards analysis

Internal flooding risk quantification
- Core damage frequency calculation (identification of contributors)
- Uncertainty and sensitivity analyses
External hazards analysis

1) Establishing the *quantitative screening criteria* for bounding assessment (for exclusion from detailed analysis)

2) Bounding risk assessment - for each hazard from the list of hazards subjected to the bounding assessment, the following needs to be done:

   a. The plant buildings, locations and systems are examined to determine conservatively the possible *impact* on structures, systems and components and operator actions from the hazard

   b. A set of *accident scenarios* is defined in terms of initiating events and equipment damage. For each scenario:

      - The associated *conditional core damage probability* is assessed
      - The initiating event frequency is defined using the *hazard frequency* associated with the scenario
      - The *risk* associated with the scenario is calculated

   c. Risks associated with *all scenarios* for the hazard are summed

3) Quantitative bounding screening
EXTERNAL HAZARD ANALYSIS PROCESS

1. Initial information collection

2. Identification of hazards and compilation of the list of potential internal and external hazards
   - Analysis of generic lists of internal and external hazards
   - Inspection of the plant buildings, plant site and the surroundings
   - Identification of plant specific and site specific internal and external hazards

3. Hazards screening analysis (all hazards)
   - Establishing the screening criteria (qualitative and quantitative)
   - Qualitative screening
   - Quantitative screening
     - Parameterization of hazards
     - Assessment of frequency of hazards

4. Hazard specific bounding assessment
   - Establishing the quantitative screening criteria for bounding assessment
   - Bounding risk assessment - for each hazard from the list of hazards subjected to the bounding assessment, the following needs to be done:
     a. The plant buildings, locations and systems are examined to determine conservatively the possible impact on structures, systems and components and operator actions from the hazard.
     b. A set of accident scenarios is defined in terms of initiating events and equipment damage. For each scenario:
        - The associated conditional core damage probability is assessed.
        - The initiating event frequency is defined using the hazard frequency associated with the scenario.
        - The risk associated with the scenario is calculated.
     c. Risks associated with all scenarios for the hazard are summed.

5. Hazard specific detailed analyses
   - Detailed analysis of accident scenarios aimed at realistic estimation of the damage potential from the initiating events induced by the hazards and calculation of the associated risk.
HAZARD SPECIFIC DETAILED ANALYSES

- The detailed analysis should be based on realistic models and data, including a comprehensive Level 1 PSA model that provides the possibility of modelling all phenomena associated with the external hazard under consideration.
  - Any credit for protection devices and recovery actions should be justified.
- The combined impact of external hazards should be considered when they have a common origin (e.g. earthquake and tsunami, high winds and lightening) or other dependencies (e.g. high level water due to precipitation and dam failure).

**Detailed Analysis Using PSA Model**

1. Hazard frequency analysis
2. Fragility analysis
3. Accident scenario modeling
4. Human reliability analysis
5. Systems analysis
6. Quantification of accident sequences and CDF calculation
HAZARD FREQUENCY ANALYSIS

- The purpose of the frequency assessment for external hazards is to acquire detailed site relevant information on the relationship between strength (as represented by some parameter for the hazard) and frequency of occurrence for each potentially relevant external hazard (the ‘hazard curve’).

- The hazards analysis (the estimation of the frequency of exceedance of a particular intensity) should be based on a probabilistic evaluation specific for the site that reflects recent available data, site specific information, and as-built and as-operated plant conditions if the corresponding data are available.

- Basis:
  - Historical data
  - Phenomenological models
  - Expert elicitation or another expert based process
1. SAFETY ASSESSMENT

To assess the overall safety of the plant and to develop an understanding of the main contributors to risk (this is the original motivation for the development of PSAs)

2. DESIGN EVALUATION

To provide support for design evaluation

3. NPP OPERATION

To provide support for day-to-day operation of the plant (not including permanent changes to design or operational practices)

4. PERMANENT CHANGES TO THE OPERATING PLANT

To assess the safety significance of proposed permanent changes to the plant design, hardware, or administrative controls (e.g., operating procedures, the licensing basis) as an aid to decision-making

5. OVERSIGHT ACTIVITIES

To support the regulatory functions of inspection, assessment of plant performance, and enforcement of regulations

6. EVALUATION OF SAFETY ISSUES

To evaluate safety issues
PSA APPLICATION GROUPS

- **CATEGORIES**
  - 1. SAFETY ASSESSMENT
  - 2. DESIGN EVALUATION
  - 3. NPP OPERATION
  - 4. PERMANENT CHANGES TO THE OPERATING PLANT
  - 5. OVERSIGHT ACTIVITIES
  - 6. EVALUATION OF SAFETY ISSUES

- **GROUPS**
  - NPP maintenance
  - Accident mitigation and emergency planning
  - Personnel training
  - Risk-based configuration control/ Risk Monitors
  - Plant changes
  - Technical specification changes
  - Establishment of graded QA program for SSC
  - Performance monitoring
  - Performance assessment
  - Risk evaluation
  - Regulatory decisions
Main results of PSA level 1 for Kozloduy NPP, units 5 and 6
Goals

- **Main**
  - Modernization Program measures
  - Operating experience gained
  - Experience and knowledge gained in the field of PSA

- **Specific**
  - Risk assessment
  - Main contributors
  - Recommendations on safety improvement
  - Comparison of results before and current
Scope

- Reactor - Full Power and Low power and shutdown
  - Internal IE
  - Internal fires
  - Internal floods
  - Seismic

- SFP - Low power and shutdown
  - Internal IE
  - Internal fires
  - Internal floods
  - Seismic
**Total Risk**

- Risk Distribution
  - Reactor core damage risk – 93 %
  - Full Power – 69 % (longer duration in time)
  - Low Power and Shutdown – 24 %
  - SFP risk – 7 %
- Result meets completely the requirements

<table>
<thead>
<tr>
<th>Internal IEs</th>
<th>Internal Fires</th>
<th>Internal floods</th>
<th>Seismic hazards</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reactor Core Damage Frequency, Full power</td>
<td>9.32E-06</td>
<td>3.11E-06</td>
<td>1.98E-07</td>
<td>3.34E-06</td>
</tr>
<tr>
<td>Reactor Core Damage Frequency, low power and shutdown</td>
<td>5.22E-06</td>
<td>1.98E-07</td>
<td>2.94E-08</td>
<td>3.66E-09</td>
</tr>
<tr>
<td>Fuel Damage Frequency in the SFP</td>
<td>1.50E-06</td>
<td>1.21E-07</td>
<td>1.67E-09</td>
<td>1.66E-08</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1.60E-05</strong></td>
<td><strong>3.43E-06</strong></td>
<td><strong>2.29E-07</strong></td>
<td><strong>3.36E-06</strong></td>
</tr>
</tbody>
</table>
Total Risk

By modes of operation

By IE categories

- Reactor Core Damage Frequency, Full power: 69%
- Reactor Core Damage Frequency, low power and shutdown: 24%
- Fuel Damage Frequency in the SFP: 7%

- Internal IE: 69%
- Seismic hazard: 15%
- Internal fire: 15%
- Internal floods: 1%

By IE categories
Main aspects:

- Total risk = $9.32 \times 10^{-6}$ [1/yr]
- 200 cut sets - more than 90% of the total frequency
- NO major contributor - evenly distributed risk
- NO cut sets with frequency more than $1.0 \times 10^{-6}$ [1/yr]
- Group contribution – less than 20 %
Internal Initiating Events - Full Power

LOCA – 66%
TRANSIENTS – 34%

Adequate operator actions and dependent failure

Adequate operator actions and equipment’s CCF

17 groups IEs
Main aspects:

- Total risk = 5.22E-6 [1/yr]
- 200 cut sets - more than 72% of the total frequency
- NO major contributor - evenly distributed risk
- NO cut sets with more 5% of contribution
Internal Initiating Events- Low Power & Shutdown

19 groups IEs
Internal Initiating Events – Low Power & Shutdown

Contributors:

- V1 group “LOCA outside the containment” - 31%:
  - Human error causing V LOCA
  - Operator’s actions on timely leak isolation
Contributors:
  - L3 “Small break LOCA” - 19%
  - L1 group “Large break LOCA” - 8%
    - Operator actions on ensuring the coolant mass balance
Internal Fires

Essential only at full power operation

Contributors:
1. Turbine Hall
2. SWG (switchgear’s)
3. I&C (UKTS)
4. Cable shafts

Full power operation – 20%

Low power operation
Shutdown – 4%

SFP – 7%
Seismic Hazards

Essential only at full power operation

Insights:
1. Good seismic capacity – 1.0E-04 [1/yr] = RL2
2. Equipment replacement by new one qualified for seismic hazards at the site
Internal Floods

NO flooding zones causing a failure of more than one safety system train

Full power operation – 1%

Low power operation
Shutdown – 0%

SFP – 0%

Insights:
Improving the reliability of the pipelines in the Turbine Hall
Comparison with previous results – full power
Comparison with previous results - shutdown
Recomendations

Human reliability:
- Procedure improvements (EWT filling, FSG isolation, ISLOCA isolation and etc.) – detail procedures
- Implement SBEOP for shutdown modes
- Studies of the possibilities to reduce the operator actions and to increase the automatic actions and operator information at MCR

Technological requirements:
- Analyze the possibility of ensuring availability and using system TQn3 (HPIS) under cold conditions and unsealed reactor
Scheduled Preventive Maintenance and repair schedules:
- Optimization of the outage duration
- Risk-informed system for the maintenance activities

Systems’ design modification:
- Automatic isolation of interface leakages - ISLOCA
- Power supply distribution optimization of the components related to secondary side heat removal
- Automatic filling of TX tanks or to provide an additional possibilities for RHR in hot or semi-hot conditions
- System for analysis of the equipment failures
Conclusions

The results from PSA Level 1 confirm that following KNPP Units 5&6 “Modernization Programme”, performed between 2001 and 2007, all basic engineering principals of the up-to-date defence-in-depth approach have been implemented, thus providing for high reliability in the fulfilment of all safety functions.