PNRA-RG-911.01 August, 2010

PROBABILISTIC SAFETY ASSESSMENT OF NUCLEAR POWER PLANT-LEVEL 1

REGULATORY GUIDE

PAKISTAN NUCLEAR REGULATORY AUTHORITY

For Further Details

Directorate of Policies & Procedures
PAKISTAN NUCLEAR REGULATORY AUTHORITY
P.O. Box 1912, Islamabad
www.pnra.org

TABLE OF CONTENTS

TABLE OF CONTENTS

PROBABILISTIC SAFETY ASSESSMENT OF NUCLEAR POWER PLANT-LEVEL 1

ABSTRACT

Probabilistic safety Assessment is an analytical tool for calculating numerical estimates of risk for nuclear power plants and industrial installation having considerable risk .PSA provides insights into plant design operation, performance and environmental impacts, including identification of dominant risk contributors and the viable actions for reducing risks. It offers a systematic approach to determine whether the plant design is balanced, mitigating Systems are adequate, the defense in depth requirements has been realized and the risk is within acceptable limits. PNRA regulation PAK/911 "Regulation on the safety of Nuclear Power Plant Design" clauses 3.4, 5.2, 5.8, 5.16, 5.30, 5.70, 5.74 requires PSA be performed by licensee. This regulatory guide would assist the licensees in developing PSA level-1 submissions in accordance with the requirements of PNRA regulations.

ABBREVIATIONS

AOPs	Abnormal Operating Procedures
CCF	Common Cause Failure
CDF	Core Damage Frequency
EOPs	Emergency Operating Procedures
FMEA	Failure Modes and Effects Analysis
HAZOPs	Hazard and operability studies
HEP	Human Error Probability
HRA	Human Reliability Analysis
LER	Licensee Event Reports
LPSD	Low Power and Shut Down
MCB	Main Control Board
PIE	Postulated Initiating Events
POS	Plant Operational States
PSA	Probabilistic Safety Assessment
RCS	Reactor Coolant System
SSD	Safe Shut Down
SCDF	Severe Core Damage Frequency

1 INTRODUCTION

The probabilistic safety assessment (PSA) is an important analytical tool in ensuring the safety of a nuclear power plant design in relation to potential initiating events that can be caused by random component failures and human errors, as well as internal and external hazards and to derive numerical estimate of risks to the workers and public.

PAK/911 states that, "A safety analysis of the plant design shall be conducted in which methods of both deterministic and probabilistic analysis shall be applied". On the basis of this analysis, the design basis for items important to safety shall be established and confirmed……" (para.5.70). [1]

Further to para.5.74 of Pak/911, a probabilistic safety analysis of the plant shall be carried out in order:

a) To provide a systematic analysis to give confidence that the design will comply with the general safety objectives;
b) To demonstrate that a balanced design has been achieved such that no particular function or PIE makes a disproportionately large or significantly uncertain contribution to the overall risk, and that the first two levels of defense in depth bear the primary burden of ensuring nuclear safety;
c) To provide confidence that small deviations in plant parameters that could give rise to severely abnormal plant behavior ('cliff edge effects') will be prevented;
d) To provide assessments of the frequency of occurrence of severe core damage states and assessments of the risks of major off-site releases necessitating a short term offsite response, particularly for releases associated with early containment failure;
e) To provide assessments of the frequency of occurrence and the consequences of external hazards, in particular those unique to the plant site;
f) To identify systems for which design improvements or modifications to operational procedures could reduce the frequency of severe accidents or mitigate their consequences;
g) To assess the adequacy of plant emergency procedures and
h) To verify compliance with probabilistic targets.

2 OBJECTIVE

The objective of this regulatory guide is to provide guidance and recommendations to the NPPs/licensees and technical support organization(s) for meeting the regulatory requirements and managing a PSA project and use it to support the safe design and operation of nuclear power plants.

3 SCOPE

This regulatory guide includes all plant operational conditions (i.e. full power, low power, and shutdown) and all potential initiating events and hazards necessary to be included in PSA level-1 studies such as,

a) Internal initiating events caused by random component failures and human errors, including loss of offsite power,
b) Internal hazards (e.g. internal fires and floods, etc.), and

c) External hazards (e.g. earthquake, fire, floods).

4 GENERAL REQUIREMENTS

Following steps need to be managed and organized before performing a PSA level -1:

4.1 Definition of Objectives and Scope

The objectives and applications of the PSA determine the scope and resources required for the study. The PSA model should reflect the actual plant configuration in the respective mode of operation for which PSA is performed (e.g. full power, low power and shutdown, etc.). Decision about the objectives should include whether plant design satisfies probabilistic safety goals or criteria, for example CDF/SCDF. The level of detail considered within each area of the PSA should be determined at an early stage of the analysis.

Agreement on format and contents of the PSA report (e.g. full power, LPSD, fire, etc.) with the regulatory body is an important step in developing a PSA project and it should be decided at an early stage. General format of level 1 full power PSA report is provided in appendix II.

4.2 Probabilistic Safety Criteria

The core damage frequency (CDF) or severe core damage frequency (SCDF) of level 1 PSA should be less than or equal to 1.0E-5 per reactor year.

4.3 Project Management

It is very important for the PSA analysis team to interact with plant operating and maintenance personnel in order to reflect plant design, operational features and practices during PSA. This kind of interaction and communication with plant staff needs to be organized and reflected in project management.

4.4 Team Selection, Organization and Training

The team selected should have intimate knowledge of the plant and PSA techniques. Therefore, the team should be organized in a way that facilitates the required multidisciplinary investigations necessary for performing the PSA. Specialized training in PSA techniques and plant practices should be provided to the PSA team as required.

5 FULL POWER PSA

This section addresses necessary technical features of a Level 1 PSA for full power operation of nuclear power plants based on internationally recognized good practices. The PSA documentation should be developed in a clear, traceable, and transparent manner so that it supports the review of PSA, PSA applications and future PSA upgrades. [2]

5.1 Initiating Event Analysis

The starting point of the Level 1 PSA is the identification of the set of initiating events that have the potential to lead to core damage if additional failures of the mitigating systems required to perform one or more of the safety functions occur [2].

5.1.1 Identification of Initiating Events

A systematic procedure should be used to identify the set of initiating events to be addressed in the Level 1 PSA. This may involve a number of different approaches as follows:

a) Analytical methods such as hazard and operability studies (HAZOPs) or failure modes and effects analysis (FMEA);
b) Deductive analyses such as Master Logic Diagrams in order to determine the elementary failures or combinations of elementary failures which would contribute to the loss of each safety function concerned;
c) Comparison with the lists of initiating events developed for the PSAs for similar plants and with existing safety standards and guidelines;
d) Initiating events identified from the analysis of operating experience of the plant under investigation and of similar plants.

A combination of different approaches should be used to get initiating events. The set of internal initiating events used as the basis should be as comprehensive as possible. In identifying initiating events, particular attention should be paid to any design features that are novel or peculiar to the plant in question as potential sources of new initiating events. The set of initiating events identified should include events of all frequencies. This will ensure that the initiating events of very low frequency with potentially large consequences are also included. For a site with more than one nuclear power plant, the set of initiating events that can affect both units at the same time should be identified and events that can arise in one of the plants and lead to an initiating event in another one should be identified.

The set of initiating events identified for the plant should be compared with that for similar plants to ensure that all the relevant initiating events have been included. Where differences are identified, additional initiating events should be defined or justification should be provided for not considering the initiating event. A review of the operating experience of the nuclear power plant and of similar nuclear power plants should be carried out to ensure that all the initiating events that have occurred are included.

5.1.2 Grouping of Initiating Events

In order to limit the analysis required for the Level 1 PSA to a manageable size, a grouping process should be carried out before proceeding to the accident sequence analysis. Only initiating events where the accident progressions and the success criteria for the mitigating systems are similar should be grouped together. The success criteria used for that specific group should be the most stringent criteria of all the individual events within the group. Where initiating events with slightly different accident progressions and/or success criteria for the mitigating systems have been grouped together, the accident sequence analysis should bound all the potential sequences and consequences of these initiating events.

The grouping of initiating events should be done in such a way that this does not introduce undue conservatism into the analysis. The initiating events which cause a containment bypass (e.g. steam generator tube rupture and interfacing systems LOCAs) should not be grouped with other LOCAs where the containment would be effective.

The PSA documentation should include a comprehensive list that includes all the initiating events that have been identified for the plant, gives a description of the initiating event and gives sufficient information to allow the initiating event to be traced back to the supporting analysis (that is, to the HAZOP, FMEA, Master Logic Diagram, review of operating experience) where it was identified.

After grouping, the final list of initiating events should be developed which will form the basis of Accident Sequences Analysis.

5.2 Accident Sequence Analysis

Next step in the analysis is to determine the response of the plant to each of the groups of initiating events identified above which require mitigating systems to operate in order to carry out the safety functions to prevent core damage. The event sequences that are identified should relate to the success or failure of the mitigating systems to perform the set of safety functions required for the initiating event groups. The end points of the event trees should correspond either to a safe state where all the minimum required functions have been performed successfully or to core damage (for CANDUs core damage may relate to single channel failure).

5.2.1 Core Damage

A criterion should be developed for what constitutes core damage. This is often done by adopting an indirect criterion where, for example, core damage may be assumed to occur following prolonged exposure of the top of the core or exceeding the maximum cladding temperature. If a significantly long time interval is required to cause core damage after exposure, then this should be taken into account in framing a realistic definition of core damage.

5.2.2 Safety Functions, Mitigating Systems and Success Criteria

The event sequence analysis should be carried out for each of the groups of initiating events identified above. The safety functions that need to be performed to prevent core damage should be identified for each of the initiating event groups. These also depend on the reactor type and typically include:

- Control reactivity;
- Remove core decay heat and stored heat;
- Maintain integrity of primary reactor coolant boundary (pressure control);
- Maintain primary reactor coolant inventory.

The mitigating systems available to perform each of the safety functions should be identified along with the success criteria for the mitigating systems in performing these safety functions. The specification of the mitigating systems should take account of any mitigating systems that would not be available as a result of the initiating event. The success criterion for each of the mitigating systems should be defined as the minimum level of performance required from the system. The success criteria should specify the mission times for the mitigating systems based on the thermal hydraulic analysis carried out. The success criteria should also define the requirements for the support systems based on the success criteria for front line systems. The success criteria should identify

the operator actions required to bring the plant to a safe, stable shutdown state as defined by the emergency procedures. The success criteria for the mitigating systems used in the Level 1 PSA should be justified by analysis. This would include the thermal hydraulic analysis for decay heat removal following transients and LOCAs, neutronics analysis for reactor shutdown and hold-down, etc.

The PSA documentation should include a table that lists the safety functions, mitigating systems and operator actions that are required for each of the initiating events to bring the reactor to a safe stable shutdown state.

5.3 Event Sequence Modeling

The accident sequences that could occur following each of the initiating event groups should be identified. This should involve success or failure of the mitigating systems and human actions in carrying out their safety functions. The event tree analysis for each of the initiating event groups should cover all the safety functions that need to be performed and the operation of the mitigating systems required as identified by the success criteria. The status of the mitigating systems, operator actions and recovery actions may form the headings on the event tree that directly affect the course of an accident. Any other event(s) with a direct and significant effect on the sequence may also be included as headings.

The event tree structure should account for all the dependencies in the event tree that can occur due to equipment failures and/or operator errors. Dependencies due to equipment failures may occur where the failure of a support system would lead to failures in two or more of the front line systems that are identified in the success criteria for an initiating event group. Dependencies due to operator errors may occur where an operator action is required before a mitigating System is able to operate. The dependencies can either be modelled in fault trees or event trees. The event sequence analysis should cover all the possible combinations of success or failure of the mitigating systems in response to the initiating event group and identify all the sequences leading either to a successful outcome or to core damage.

The PSA documentation should contain a detailed description of the event trees, the assumptions made, the conditions created by the initiating event and the mitigating System requirements for the different event tree branches. The event tree diagram itself provides no reasoning, only the results of reasoning, and hence cannot be understood completely without reference to an accompanying text. The documentation should explain and justify the selection of headings in the event tree (e.g. if the plant EOPs and system AOPs are used in selection of event trees headings, these should be explicitly mentioned), particularly for a complex event (such as a recovery procedure) or where more than one event is included under one heading. If simplifications or assumptions are made in the event trees, their effects have to be clearly identified and justified. [2]

5.4 Systems Analysis

The next step in the analysis is to model the systems' failures which are identified in the event tree analysis. This may be done by fault tree analysis where the top event of the fault tree is the system failure state(s) identified in the event tree analysis. The fault trees should extend the analysis down to the level of individual basic events which typically include component failures (that is, pumps, valves, diesel generators, etc.), unavailability

of components during periods of maintenance or test, common cause failures of redundant components, and operator errors. Operator errors both pre-accident (miscalibration of loops and restoration errors) and post accident may be modelled in the event trees or fault trees.

5.4.1 Fault Tree Analysis

The fault trees should be developed to provide a logical failure model for the mitigating system failure states identified in the event tree analysis. In some cases, more than one fault tree model may be needed for the same system to address the success criteria defined for different initiating event groups or in different branches of the event tree, depending upon the sequence of events prior to the demand for the system. This can be done by developing different fault tree models or by using house events to switch in the appropriate parts of the model depending on the success criterion. The basic events modelled in the fault trees should be consistent with the available component failure data. The component boundaries and component failure modes should be consistent with those defined in the component failure database. This should be equally valid for both active and passive components.

The fault tree models should be developed to the level of individual components (pumps, valves, diesel generators, etc.) and individual human actions and should include all the basic events which could lead either directly or in combination with other basic events to the top event. The set of basic events to be modelled in the fault trees should be identified and documented in a systematic manner.

The fault tree model should include all the safety system components that are required to be operational and all the support systems including electrical power systems, cooling systems and instrumentation and control systems etc. It should also include failures of passive components that could lead to failure of the system. This should be done in a way that ensures that all hardware dependencies have been taken into account. The fault tree models should take account of all the hardware and functional dependencies that could arise within systems. These should be identified and modelled explicitly in the fault trees. All these dependencies should be documented in a dependency matrix. The intersystem dependencies which could arise due to shared components should be identified and modelled explicitly in the fault tree analysis. The degree of resolution of the components in the fault tree should be sufficient to ensure that all the hardware dependencies can be modelled. The operator errors that can contribute to mitigating system failures should be identified and included in the fault tree models.

The common cause failures that can affect groups of redundant components should be identified and modelled in the fault trees. The analysis should identify all the relevant component groups and the important failure modes. The fault tree models should take account of individual components or trains of equipment in the mitigating Systems that can be taken out of service during the lifetime of the plant for testing, maintenance or repair. These should be identified and modelled in the fault trees. Maintenance un-availabilities modelled should be consistent with the plant Technical Specifications and the maintenance practices on the plant.

A well defined labelling scheme for all the basic events, system identification and other required information should be developed and applied consistently throughout the

PSA project.

5.4.2 Information Required for Systems

The system descriptions should be produced for each of the mitigating Systems modelled in the Level 1 PSA to ensure that there is a valid and auditable basis for the logical model being developed. The system descriptions should include the following:

- The function of the system;
- The mode of operation being modeled;
- The components that must operate/ change state and their normal configuration;
- Whether the component operations are manual or automatic, and
- The conditions that must exist for automatic signals to be received by the components.

Simplified schematic system diagram should be provided for each system which shows the system as modelled in the fault tree, including:

- All the system components modelled in the fault tree;
- The normal configurations of the components;
- The pipe segments or wiring segments connecting the components, and
- The support system interfaces (power, electric, cooling, etc.).

The system descriptions and schematics provided for any mitigating System should give a clear basis for the development of the fault trees. The PSA documentation should explain that how this information was used in the development of the fault trees.

5.5 Analysis of Dependent Failures

Treatment of dependencies should be modelled with care. There are four different types of dependencies that can occur as follows:

- Functional dependencies: due to shared components, common actuation systems, common isolation requirements or common support systems (power, cooling, instrumentation and control, ventilation, etc.);
- Physical dependencies: due to an initiating event that can cause failure of mitigating system equipment. This can occur due to pipe whip, missile impact, jet impingement or environmental effects;
- Human interaction dependencies: due to errors made by the operators during repair, maintenance, testing or calibration tasks that lead to the unavailability or failure of mitigating System equipment so that they will not operate when required following an initiating event, and
- Component failure dependencies: due to errors in the design, manufacture, installation and calibration or by operational deficiencies. These are modelled as common cause failure.

A systematic review should be carried out of the design and operation of the plant to identify all the potential dependencies that could arise leading to the unavailability of mitigating system components or a reduction in their reliability in providing protection against initiating events. All the functional and physical dependencies should be considered in modelling.

5.6 Common Cause Failure Analysis

The sets of equipment where component failure dependencies could arise should be identified and an allowance should be made in the PSA model for the common cause failure of these components. Justification should be provided for the common cause failure probabilities used in the PSA. This should take account of the level of redundancy in the system, the layout in terms of the levels of separation/ segregation/ equipment qualification/ etc., and the operational and maintenance practices for the system.

5.7 Human Reliability Analysis

A structured and systematic approach should be adopted for the identification of the human errors to be, the incorporation of these errors in the plant logic model (event and fault trees) and the quantification of the related events. The chosen HRA methods should be applied consistently and correctly.

5.7.1 Identification of Human Interactions

A structured and systematic procedure should be applied for the identification of the human interactions that need to be included in the Level 1 PSA. This should include all types of human interactions as follows:

- Type A interactions: human interactions occurring before the initiating event that have the potential to lead to the failure or unavailability of safety-related system equipment. These can occur during repair, maintenance, testing or calibration tasks;
- Type B interactions: human interactions that have the potential to cause an initiating event, and
- Type C interactions: human interactions that are performed by the plant operators following an initiating event. These actions have the potential to lead to failures of the mitigating Systems to perform one of the required safety functions and are usually the most important human interactions to be considered in the PSA.

A systematic review should be carried out of the plant procedures to identify the repair, maintenance; testing or calibration tasks carried out by the plant operators for the systems modelled in the PSA to identify Type A human interactions. The review should determine the potential for errors to occur and the effect of these errors on the unavailability or failure of mitigating System equipment. A systematic review should be carried out to determine the human errors that could occur leading to an initiating event (Type B interactions). As a minimum, a check should be carried out to ensure that the human errors causing initiating events are taken into account in the initiating event frequencies used in the analysis, e.g. by accounting the associated events in statistical incidence data. A systematic review should be carried out of the emergency operating procedures to identify the critical actions that need to be carried out by the plant operators after the occurrence of an initiating event to identify Type C human interactions with the plant. The review should determine the potential for errors to occur and the effect of these errors on the unavailability or failure of a component or system. Basic events should be incorporated in the logical models to represent human errors.

5.7.2 Derivation of the Human Error Probabilities

The human error probabilities used should reflect the factors that can influence the performance of the operator, including the level of stress, the time available to carry out the task, the availability of operating procedures, the level of training provided, the environmental conditions, etc. Qualitative descriptions should be given for each of the key human interactions that identify all the significant aspects associated with the actions of the plant personnel.

There are likely to be interdependencies between the individual human errors included in the logic model. These could arise due to incorrect procedures, an incorrect diagnosis or plan of action in carrying out post fault recovery actions, etc. These interdependencies should be identified and quantified in the analysis. The cut-sets involving multiple human errors should be identified and checked to verify proper dependency modelling.

5.8 Data Analysis

Plant specific data should be used whenever possible. However, this may not be available for new plants or for plants that have only been in operation for a short time. In this case, data from similar plants should be used and, if this not available, generic data from the operation of all types of nuclear power plants should be used. Justification should be provided for the data used in the PSA. It is highly recommended that available plant specific data should be used at the time of PSR (periodic safety review).

If a combination of plant specific and generic data from different sources is used, justification should be provided for the methods used for selection of the specific data or for integration of the data from more than one source. For equipment with a low failure probability, the data will be sparse or non-existent, even on a generic basis, and the values to be used in the PSA will then have to be assigned by informed judgement. The basis for these judgements should be explained. Bayesian updating may be used to combine generic and plant specific data.

5.8.1 Initiating Event Frequencies

A frequency should be assigned to each of the initiating events group modelled. This should take account of all the causes identified for the initiating event. One way of assessing frequencies of initiating events related to support systems is the use of fault tree modelling. The frequency of initiating events should be consistent with the operating experience from the plant under consideration or from similar plants. The frequency calculated for the initiating event groups should be the sum of all the individual initiating events assigned to that group.

Documentation should give a description of each of the initiating events identified for the plant along with a description of the initiating event, the mean value for the initiating event frequency, the justification for the numerical value assigned to it and an indication of the level of uncertainty.

5.8.2 Component Failure Data

Failure rate or demand failure probabilities assigned to each of the components/

component types should be consistent with the type of component, its operational regime, the boundaries defined for the component in the PSA model and its failure modes. Justification should be provided for the value used for the component failure rates & demand probabilities.

Documentation should give all the component failure data used in the quantification of the PSA. This should include a description of the component boundaries, failure modes, the mean failure rate or demand failure probability, the uncertainties associated with the data, the data sources used and the justification for the numerical value used.

5.8.3 Maintenance and Test Data

The quantification of the PSA should take account of the unavailability of components and systems for test, maintenance or repair. The numerical values used for the frequencies and durations for component outages should be a realistic reflection of the practices in use at, or planned for, the plant. Where possible, this should be based on plant specific data obtained from an analysis of the plant maintenance and component unavailability records. If this is not possible then generic data or manufacturer's data can be used as long as justification can be provided that this reflects plant operating practices.

5.8.4 Quantification of the Analysis

The quantification of the PSA should be carried out using a suitable computer code which has been fully validated and verified. The overall results of the quantification of the Level 1 PSA model should include:

a) Core damage frequency/severe core damage frequency;
b) The contributions to the core damage frequency arising from each of the initiating event groups;
c) Dominant minimal cut-set frequencies (MCS frequencies);
Plant Damage State frequencies;
d) The results of the sensitivity studies and uncertainty analysis;
Importance analysis;
e) List of at least Top 50 accident sequences with respect to core damage contribution;
f) List of Important Systems and components with respect to core damage contribution;
g) List of Important Human actions with respect to core damage contribution.

The analysts should check that the accident sequences/ cut sets identified do actually lead to core damage. The quantification of the Level 1 PSA will require that cut-offs are set to limit the time taken for the analysis. Justification should be provided that the cut-off has been set at a sufficiently low level so when the overall results from the PSA converge the cut-off does not lead to a significant underestimate of the frequency of core damage.

5.9 Sensitivity Studies, Importance and Uncertainty Analysis

Uncertainties in the models developed and the data used in the PSA should be addressed. This can be done by carrying out sensitivity studies or an uncertainty analysis

as appropriate.

5.9.1 Sensitivity Studies

Studies should be carried out to determine the sensitivity of the results of the PSA to the assumptions made and the data used. The sensitivity studies should be carried out for the assumptions and data that have a significant level of uncertainty and are likely to have a significant impact on the results of the PSA.

The results of the sensitivity studies should be used to indicate the level of confidence about the insights obtained from the PSA – that is, whether the core damage criterion/ target has been met, whether the design is balanced, whether there are potential weaknesses in the design and operation of the plant that have not been highlighted in the base case analysis.

5.9.2 Importance Analysis

Importance analysis should identify the important accident sequences, systems failures, component failures and human errors with regard to core damage frequency.

5.9.3 Uncertainty Analysis

An uncertainty analysis should be carried out to determine the uncertainty in the core damage frequency that arises from the parameters that have been used to quantify the PSA. Uncertainty distributions should be specified for the parameters used in the quantification of the PSA. This should be done as part of the data analysis. These uncertainty distributions should be propagated through the analysis to determine the uncertainty in the core damage frequency, initiating event group frequencies, etc. This should be used to give an indication of the level of confidence that risk criterion/ target has been met.

The results should be examined and documented. Modifications and recommendations based on these results should be documented.

6 LOW POWER AND SHUTDOWN PSA

6.1 Initiating Events

The initiating events should include LOCAs and transients as well as those initiators that are identified in the analyses of internal and external hazards. A generic list as a starting point should be compiled for analysis. Systematic identification techniques should be used. Methods that can be used are:

a) Systematic analytical methods, such as master logic diagrams, failure modes and effects analysis, and fault trees;
b) Systematic examination of plant procedures for changing RCS configurations, equipment testing and maintenance procedures.

For shutdown conditions some initiating events will be unique and different from the level 1 PSA for full power operation. In addition, many initiating events may be human-induced relating to maintenance activities or operational procedures. The major categories of initiating events which are of interest for a LPSD PSA should be events

which threaten critical safety functions like heat removal, primary circuit inventory or integrity, and reactivity control. This implies that end states will be core damage, fuel damage states, criticality events or damage to structures. A LPSD PSA should comprise of the following events:

a) Damage to fuel during handling;
b) Damage to fuel due to drop of heavy loads;
c) Criticality due to fuel configuration changes (either in the fuel pool or in-vessel);
d) Loss of cooling in the fuel pool.

To ensure adequate completeness of the PSA, the initiating event list and other sources of information should also be reviewed in addition to the list from full power such as

a) LPSD PSAs performed by other NPPs;
b) Plant operating history;
c) Experience at similar plants;
d) Generic data from low power and shutdown operation;
e) Generic studies (e.g. boron dilution events caused by inadvertent pumping of unborated water through the core);
f) Licensee event reports (LERs);
g) Event reports from international organizations and plant owner groups;
h) LPSD PSA related material (NUREG Reports, IAEA Safety Standard(s) etc.)

Initiating events should be grouped as appropriate. An initiating event group should include initiating events which can be analysed using the same event tree and fault tree model that is same accident sequence is applicable for all initiating events in the group. In some cases, initiating event groups may include events which do not completely satisfy the above conditions. In such cases, the group characteristics should be defined based on the most restrictive events within the group. The quantification of initiating event frequencies for shutdown and low power conditions should account for plant specific items such as equipment configuration, availability, technical specifications, and outage management, including refueling operations. Initiating event frequencies in a given POS should be quantified using following approaches:

a) Direct estimation from operational experience (the plant being analysed, other plants of similar design, or generic reactor types);
b) Estimation from full power level 1 PSA frequencies with supplementary analysis;
c) Use of a logical model including all the foreseen inputs leading to the initiating event.

If generic data is used, a justification should be provided. The overall results of assigning initiating events to POS should be presented in form of a table or a different type of overview.

6.2 Accident Sequence Modeling

The general approach to accident sequence analysis is given in section 7.2. The analysis should take into account the following aspects:

a) Due to disabling of automatic actuation of mitigating Systems, the availability of safety equipment may be reduced and the dependence on operator action increased;
b) The integrity of the primary cooling system and of the containment may be compromised;
c) The performance of a front line system depends in general on the initiating event, POS characteristics and decay heat level.

Functional performance criteria should be used to define the success criteria for the various systems, which may differ from the success criteria for a level 1 PSA for full power operating conditions.

Thermal-hydraulic calculations should be performed to determine realistic success criteria to assure that core cooling assumptions are correct. The level of detail of the thermal hydraulic analyses should correspond to the requirements of the systems analyses and the primary system configuration.

Event trees or equivalent presentations should be used to model the response of the plant and plant operators to initiating events.

6.3 System Modeling

The fault tree models constructed for the level 1 PSA for full power operating conditions should be revised as appropriate. Even if the logic and response of the system remain basically the same as at full power, possible changes of the conditional availabilities of components or systems should be taken into account, particularly if:

a) Existing system models are not suitable for describing the system behavior in different POS;
b) A particular system, which was in stand-by during full power operation, is operating during shutdown;
c) Actuation of a system is manual during shutdown in contrast to full power operation where it was automatic;
d) Required mission time may be significantly different;
e) Success criteria changes in different POS;
f) Number of trains initially available is different in each POS;
g) Time windows and conditions are significantly different, which could make success of recovery actions less probable;
h) System was not modeled as it was not needed for the full power condition.

6.4 Analysis of Dependent Failures

The dependencies may influence the logic and quantification of the accident sequence and system models. The main types of dependencies in this regard are functional dependencies on supply and support systems, hardware sharing between systems or process coupling, physical dependence including dependencies caused directly or indirectly by initiating events, human interaction dependencies, common cause failures (CCFs) and coincident repairs or maintenance of redundant components. These dependencies should be included in the analysis.

Revisions to the dependency models for full power operating conditions should be implemented as required, especially if the success criteria changes for low power and

shutdown operation or conditions for support and supply systems. Systems alignment and components outages should be considered as well.

6.5 Human Reliability Analysis

HRA should be performed in a structured and logical manner. HRA should aim to generate failure probabilities which are both consistent with one another and consistent with the analysis carried out in other portions of the level 1 PSA.

The extensive use of external maintenance staff from outside organizations, frequent overtime work and increased requirements for control room work should be reflected in the analysis.

For HRA analysis close interaction with plant operating and maintenance personnel in order to reflect plant design and operational features during low power and shutdown conditions should be practiced. If this is not possible, e.g. for a plant in the design or construction stage, the analyst should attempt to gain practical experience based knowledge from similar operating plants.

Type A Pre-Initiator Human Actions

Type A interactions consist of actions associated with testing, maintenance, repair and calibration which may degrade system availability. They may cause the failure of a component or component group or leave equipment in an inoperable condition, e.g. due to misaligned valves. If undetected, the component or component groups are unavailable when required after an initiating event. Particularly important are interactions that have a potential to result in concurrent unavailability of multiple trains or channels of mitigating systems. Typically these sources of unavailability are included in the system models at the component, train or system level. Due to the great variety of different maintenance measures, testing and changes of configuration it cannot be expected that all possible human errors have been observed in operating experience. Therefore, the potential of human failure before an initiating event occurs should be assessed. This assessment should distinguish human failures that lead to unavailability of components either immediately or as latent fault in case of a demand.

Type B Human Actions that may Cause an Initiating Event

As these interactions contribute to the frequency of initiating events, especially if associated with testing, HRA analysis should support the calculation of these frequencies in cases where the human error must be quantified explicitly, rather than being implicitly included in the frequency estimation which has been generated from operational experience. In addition to the evaluation of operating experience, a systematic review should be carried out to determine human errors that could lead to an initiating event.

Type C Post-Initiator Human Actions

Type C human interactions are particularly important during shutdown because of the reduced level of plant automation. Thorough consideration should be given to a realistic assessment of their failure probability. The methodology selected should account for the following aspects relevant to model and quantify Type C actions in the frame of LPSD PSA in a systematic manner:

a) Quality of procedural guidance;

b) Status of operator training;
c) Duration of time windows for response;
d) Quality of interface facilitating human actions at LPSD states.

If expert elicitations are used they should follow established procedures. Care should be exercised not to uncritically accept values generated by the use of time reliability correlations designed for power operation, since the time windows in shutdown operation may be well outside the applicable range of these correlations.

Errors in the diagnosis of initiating events should be addressed especially when event based procedures are used. Dependencies between human interactions should be taken into account.

6.6 Data Assessment

Acquisition of all data required for quantification of PSA should include:

a) Initiating event frequencies;
b) Data relating to human error probabilities;
c) Duration of POS;
d) Allowed outage times;
e) Component reliability data;
f) Maintenance un-availabilities;
g) Assessment of common cause failures;
h) Other data needs.

Justification for the data used should be provided. The unavailability of components during planned outages should be related to the average test duration and to the duration of the POS during which the component is tested. HEP to override test or maintenance if applicable and plant technical specifications relating to technical specifications for testing and maintenance should be assessed.

The possibility of repair should be considered because it can significantly increase mitigating system availability in POS and neglecting it may lead to an overestimation of risk. It should be restricted to cases in which plant experience shows that there are good possibilities for recovery or the success probability can be supported by engineering judgment and or established repair procedures valid under the conditions of the event sequence. Dependency of repair times on the POS should be taken into account.

The analysis team should be aware that components that are in standby during power operation might be running during an outage. If the shutdown operating policy is to cycle the use of redundant components or trains then an appropriate reliability model should be selected. The assumptions on mission times should be consistent with the sequence modeling. For the parameters used in the level 1 PSA, not only a point estimate but a full uncertainty distribution should be derived. Working with point values only should be justified.

6.7 Accident Sequence Quantification

Accident sequence quantification should be performed using the same techniques as for a level 1 PSA for full power conditions. However, in LPSD, long mission times or recovery times are often applicable; use of Markovian techniques instead of standard fault

tree/event tree evaluation methods may have the potential to yield more realistic results.

6.8 Uncertainty Analysis

An uncertainty analysis should be carried out to determine the uncertainty in the results of the LPSD. Uncertainty distributions should be specified for the parameters used in the quantification of the LPSD. This should be done as part of the data analysis. These uncertainty distributions should be propagated through the analysis to determine the uncertainty in the core damage frequency, initiating event group frequencies, etc. This should be used to give an indication of the level of confidence that risk criterion/ target has been met.

6.9 Importance and Sensitivity Analysis

Importance and sensitivity analyses should be performed using the same techniques as for a PSA for full power operation to account all these specific conditions that can actually occur during the POS.

7 FIRE PSA

Fire PSA takes into account the possibility of a fire at any location; fire detection, suppression and containment; the effects of fire on safety related components and cables; the possibility of damage to these equipment and in case of severe fires to the structural integrity of the walls, ceilings, columns, roof beams, etc. Fire PSA methods should introduce the likelihood of a fire at any plant location, the effects of the fire on pieces of equipment (components and control and power cables), and the impact of equipment failures and human actions coincident with the fire. The Fire PSA approach should be based on a systematic analysis of all plant locations. To facilitate this examination, the plant should be subdivided into distinct fire physical unit ("fire compartments"), which are then scrutinized individually. The intent should be to follow a select set of plant fire scenarios through the entire analysis process, i.e., a "top-to-bottom slice" of the complete fire PSA. Human Error Probability in the internal event PSA should be reviewed considering deviations from the Emergency Operating Procedures and specific procedures for fire mitigation. [3,4]

7.1 Data Collection and Assessment

Fire PSA project should collect the plant specific data required for fire risk modelling. The plant specific data for Fire PSA should include:

a) The physical characteristics of the fire compartments, and their inventory;
b) Fire occurrence frequencies;
c) Estimates of the reliability of fire detection and suppression systems;
d) Human actions and human error probabilities;
e) Fire induced equipment failure modes and damage criteria.

7.2 Fire Compartment Definition

Fire PSA project should divide all plant buildings and structures into distinct fire compartments, which are examined individually. Fire compartments should be characterized at least by their physical boundaries, fire protection features, included components and cables, adjacent fire compartment and fire load.

Examination of the internal events PSA logic models (e.g. fault trees and event trees) should be performed. Identification of all the cables and circuits associated to the Fire PSA components should be an integral part of this examination. A list of Fire PSA-related equipment should be elaborated for each fire compartment. [3,4]

7.3 Tasks and Procedures

Task 1: Plant Boundary Definition and Partitioning

The first step in a Fire PSA is to define the physical boundary of the analysis, and to divide the area within that boundary into analysis compartments.

Task 2: Fire PSA Component Selection

The selection of components that are to be credited for plant shutdown following a fire is a critical step in any Fire PSA. Components selected would generally include all components credited in post fire safe shutdown analysis. Additional components will likely be selected, potentially including some or all components credited in the plant's internal events PSA. Also, the proposed methodology would likely introduce components beyond either the post fire safe shutdown analysis or the internal events PSA model. Such components are often of interest due to considerations of combined spurious actuations that may threaten the credited functions and components.

Task 3: Fire PSA Cable Selection

This task provides instructions and technical considerations associated with identifying cables supporting those components selected in Task 2.

Task 4: Qualitative Screening

This task identifies fire analysis compartments that can be shown to have little or no risk significance without quantitative analysis. Fire compartments may be screened out if they contain no components or cables identified in Tasks 2 and 3, and if they cannot lead to a plant trip due to either plant procedures, an automatic trip signal, or technical specification requirements.

Task 5: Plant Fire-Induced Risk Model

This task involves steps for the development of a logic model that reflects plant response following a fire. Fire-specific procedures or plans should be used as these procedures may impact availability of functions and components, or include fire-specific operator actions (e.g., self-induced-station-blackout). Generally internal initiating events level 1 PSA model are adapted for the Fire PSA to incorporate fire specific aspects that are different from correspondent aspects of the model. Internal Events PSA models are based on EOPs. Fire may drive the operators to FEPs and unprotected trains of mitigation systems may be placed out of service. The Internal Events PRA model will need to be modified to take into account these changes.

Task 6: Fire Ignition Frequency

This task describes the approach to develop frequency estimates for fire compartments and scenarios. This task considers use of challenging events, considerations associated with data quality, and increased use of a fully component based ignition frequency model.

Task 7: Quantitative Screening

A Fire PSA allows the screening of fire compartments and scenarios based on their contribution to fire risk. This approach considers the cumulative risk associated with the screened compartments (i.e., the ones not retained for detailed analysis) to ensure that a true estimate of fire risk profile (as opposed to vulnerability) is obtained.

Task 8: Scoping Fire Modeling

This step provides simple rules to define and screen fire ignition sources (and therefore fire scenarios) in an unscreened fire compartment.

Task 9: Detailed Circuit Failure Analysis

This task provides an approach and technical considerations for identifying how the failure of specific cables will impact the components included in the Fire PSA SSD plant response model.

Task 10: Circuit Failure Mode Likelihood Analysis

This task considers the relative likelihood of various circuit failure modes. This added level of resolution may be a desired option for those fire scenarios that are significant contributors to the risk.

Task 11: Detailed Fire Modeling

This task describes the method to examine the consequences of a fire. This includes consideration of scenarios involving single compartments, multiple fire compartments, the main control room, cable room spreading and multiple hazard analysis. Factors considered include initial fire characteristics, fire growth in a fire compartment or across fire compartments, detection and suppression, electrical raceway fire barrier systems, and damage from flame, plume, flame radiation and ceiling jet. Special consideration is given to turbine generator (T/G) fires, hydrogen fires, high-energy arcing faults, cable fires, and main control board (MCB) fires.

Task 12: Post-Fire Human Reliability Analysis

This task considers operator actions for manipulation of plant components. The analysis task procedure provides structured instructions for identification and inclusion of these actions in the Fire PSA. The procedure also provides instructions for estimating screening human error probabilities (HEPs) before detailed fire modeling results (e.g., fire growth and damage behaviors) have been developed. Estimating HEP values with high confidence is critical to the effectiveness of screening in a Fire PSA. There are a number of HRA methods that can be adopted for fire with appropriate additional instructions that superimpose fire effects on any of the existing HRA methods. This would improve consistency across analyses i.e., fire and internal events PSA.

Task 13: Seismic Fire Interactions

This task is a qualitative approach to help identify the risk from any potential interactions between an earthquake and fire.

Task 14: Fire Risk Quantification

The final quantification of the fire CDF should be performed for the remaining fire

compartments considering the results of the detailed analysis. The quantification of the Fire PSA, uncertainty and sensitivity analysis should follow the recommendations for internal event PSA.

Task 15: Uncertainty and Sensitivity Analyses

This task describes the approach to follow for identifying and treating uncertainties throughout the PSA process. The treatment may vary from quantitative estimation and propagation of uncertainties where possible (e.g., in fire frequency and non-suppression probability) to identification of sources without quantitative estimation, where knowledge of a quantitative treatment of uncertainties is beyond the state-of-the-art. The treatment may also include one-at-a-time variation of individual parameter values to determine the effect on the overall fire risk (sensitivity analysis).

Task 16: Fire PSA Documentation

The PSA should be documented in a manner that facilitates its review, application and updating. Automated fire PSA information tracking tools should be used to keep updated information.

Documentation of plant boundary definition and partitioning should include:

a) A list of all examined locations within the plant that provides the basis for excluding plant locations–i.e., characterize the global plant analysis boundary;
b) A list of all fire compartments, map each fire compartment to plant fire areas/zones, and provide the basis, where necessary, for defining fire compartments;
c) A simple set of general plant layout drawings that identify the fire area and fire compartment boundaries;
d) Documentation of the confirmatory walk down(s), including findings, participating personnel, and basic characterization information for the defined compartments.

Documentation of the Post-Fire HRA should contain:

a) All human actions and associated human failure events considered in the fire analysis;
b) The description of the HFE and especially its context in the fire scenarios;
c) The quantification method (screening or best-estimate), including the method/tools that were used;
d) The basis for the derivation of the HEP with particular attention as to the evaluation of:
    i dependency considerations;
    ii the performance shaping factors and related fire effects, the assigned HEP uncertainty values and their bases;
e) An assessment of the assumption's sensitivity in the HRA modeling and quantification to the PSA risk measures.

Fire PSA documentation should include information on data sources used, plant partitioning and compartment definition and criteria employed, plant architectural

drawings that show the boundaries of every compartment, Fire PSA model of the internal events PSA or other safe shutdown models available. It should discuss the basis of the plant response model selected, changes made to the model and the process for selecting components. Circuit Analysis should discuss the circuit analysis done for different stages of the Fire PSA in terms of methodology employed, information sources, and results. The information collected should be entered into the Fire PRA Database. A comprehensive Fire PSA Cable List should be prepared. Equipment Failure Response Reports should be generated as supporting document. These reports should include a listing by compartment of equipment and associated cables that are affected by fire in the compartment, along with the specific equipment responses that are possible as a result of fire damage to the cables. Circuit failure mode probability reports should be generated. The reports should be a listing by plant area (compartment, Fire Area, fire zone, etc.) of the probability estimates for the circuit failure modes of concern for the components of interest. The results of the seismic-fire interaction assessment consistent with the level of detail afforded with other aspects of the analysis should be documented. Adequate documentation of the uncertainty and sensitivity analyses is as important as documentation of the baseline results. By including such documentation, users of the Fire PRA can consider the uncertainties as well as the "best-estimate" results, leading to improved decisions.

8 INTERNAL FLOOD PSA

An internal flood level 1 PSA should be the probabilistic analysis of events relating to release of liquids (usually water) occurring inside plant buildings and their potential impact on safety. The internal flood level 1 PSA report should include:

a) Description of the specific methods and data used to assess the internal flooding hazard;
b) Specific changes made to the level 1 PSA model aimed to account for internal flooding phenomenon effects;
c) Justification for the flooding scenarios screened out from the analysis;
d) Results of the detailed flooding scenario analysis;
e) The final results of the internal flooding level 1 PSA in terms of core damage frequency as well as selected intermediate results;
f) Report of the plant walk down for flooding analysis.

8.1 Data Collection and Internal Flooding Assessment

The internal flooding events should be identified and characterized. This task should consider:

a) The possible flooding sources: pipes, internal tanks, pools, valves, heat exchangers, connection to the river, etc;
b) The flooding mechanism: breaks, leaks, ruptures, spurious actuation of fire extinguishing systems or human errors during operational or maintenance related activities (wrong positioning or inadvertent opening of valves, etc.);
c) The characteristics of the flood: quantity, flow rate, pressure and temperature, possibility of steam;
d) Flooding related alarms and protective actions (such as equipment trip signals).

For operating nuclear power plants, plant walk downs should be performed to verify the accuracy of information obtained from drawings and other plant information sources and to obtain information on spatial interactions needed for the analysis of the damage effects from each potential internal flooding source. When identifying flooding events, specific attention should be paid to plant shutdown conditions and when many manual re-configurations of water pathways are performed.

The plant areas, which can be influenced by internal floods, should be determined and propagation paths of the water should be identified. Flooding areas should be defined by dividing the plant into physically separate areas where a flooding area is viewed as generally independent of other areas in terms of the potential for internal flooding effects and flooding propagation.

The frequency of internal flooding events should be evaluated following the recommendations given in full power PSA. Plant specific data should be provided as far as possible. The data should be selected for piping systems that represent significant internal flooding sources.

8.2 Identification of Flooding Scenarios

Each internal flooding event, structures, systems and components being affected by the flooding (submersion, temperature, pressure, spray, steam, pipe whip or jet impingement) should be identified. Consideration of components affected by internal flooding should take into account elevations, barriers, doors and drains. Potential drain blockages should be considered.

The possibility of flood water spreading from one area to another should be assessed. All possible routes for flood water spread should be taken into consideration, e.g. the possibility of normally closed doors or hatches left open, equipment drains, etc. The location of cabinets, terminal boxes for cables of safety related components and other sensitive equipment should be identified.

The type of plant operational disturbances potentially caused by the flooding should be assessed. Analysis of the potential impact of flooding on plant operation should include component or system actuation due to flooding effects, which could initiate special event sequences.

8.3 Screening by Impact

Screening by impact may be performed for selecting critical flooding scenarios according to the following qualitative criteria:

a) No equipment is present in the compartment which can cause an initiating event;
b) Neither systems needed for safe shutdown nor their support systems are located in the compartment;
c) There are no flood sources in the compartment.

8.4 Integration of Internal Flooding in the level 1 PSA for Internal Initiating Events

Internal flooding events may be further screened out for their potential contribution to the core damage frequency. Therefore, the internal initiating events level 1 PSA should

be modified to account for flooding phenomena (both system and operator actions). A complete review of the HRA analysis of the internal initiating events level 1 PSA should be performed. When applying HRA, performance shaping factors should be analyzed considering the specifics of the flood initiator.

Reassessment and readjustment of the human error probabilities should be performed taking into account specific procedures for flood mitigation. At least the following flood induced effects on the operators' performance shaping factors should be taken into account:

a) Accessibility of the compartments of interest after flooding;
b) Increased stress level;
c) Failures of indication or wrong indication;
d) Other flood impact on operators' behavior.

For the quantitative screening task, a conservative approach should be used assuming that all components in the compartment are being affected by the flooding failure. Quantitative criteria for screening by frequency should be defined for internal flood level 1 PSA.

8.5 Detailed Flooding Analysis

The quantitative detailed flooding analysis should address the following:

a) Timing calculations (flooding level versus time) for recovery;
b) Human reliability analysis assessment of the additional human actions to mitigate the flooding sequences;
c) Development of event tree/fault tree models for each scenario;
d) Quantification of corresponding event tree/fault tree with equipment failed due to the flood and interpretation of results including sensitivity and uncertainty analysis.

Flooding scenarios should describe the time-dependent course of an initiating flooding in a selected plant area and the subsequent component failures. A flooding scenario should be established by flooding event trees where all important features affecting flooding development (design of flooding barriers, flood detection and isolation of flooding sources) and probabilities of component failures are modeled. Generally, dedicated verification walk downs should be performed during the internal flood level 1 PSA to gather supporting information for the detailed flooding analysis.

Additional human actions that may be needed to mitigate the flooding sequences should be identified and assessed with respect to their probability of success/failure to detect and control the flooding. HRA approach should take into account the loss of I&C equipment and spurious indications that may be generated due to the flooding. Subsequent flooding and damage to systems, structures or components due to high energy pipe breaks should be treated in the internal flood level 1 PSA if it had not been included as part of the internal initiating events. Flooding due to activation of a fire extinguish system with a large amount of water should be addressed.

8.6 Internal Flood Risk Quantification

The specific models developed for the detailed analysis of the internal flood PSA

should be included into the whole level 1 PSA model. The final quantification of the core damage frequency induced by the internal flooding should be performed, including identification of the main contributors (e.g. flooding sources, flooding scenarios), uncertainty and sensitivity analyses.

8.7 Structure, System and Component Fragility Analysis

In the process of evaluation of flood fragilities of structures and components plant-specific data should be used. In the assessment of non-safety structures that could fall into/onto safety-related structures causing damage should be considered. The fragility analysis should include immersion, wave dynamic loads on SSC and foundation failures (soil erosion) leading to SSC damage.

8.8 Sequence and System Analysis

All combinations of failures of system, structure or component leading to postulated accidents should be identified and analysed. Assessment of external flood hazard should be performed either as an integral part of PSA or as an extension of PSA. Additional human actions that are required to mitigate the flooding sequences should be identified and assessed with respect to their probability of success/failure to detect and control the flooding.

8.9 Documentation for Level 1 PSA for internal flooding

Level 1 PSA for internal flooding should be documented in a manner that facilitates review, applications and updating of the Level 1 PSA. The following information should be included in the documentation:

a) Description of the specific methods and data used to assess the internal flooding hazard;

b) Specific changes made to the Level 1 PSA model for internal initiating events aimed at accounting for the effects of internal flooding;

c) Justification for the screening of particular flooding scenarios from the analysis;

d) Results of the detailed analysis for flooding scenarios, including description of the scenarios, and significant assumptions made in the analysis;

e) The final results of the Level 1 PSA for internal flooding in terms of core damage frequency, qualitative insights and recommendations;

f) Report of the plant walk down in support of flooding analysis.

9 EXTERNAL FLOOD HAZARDS

Level 1 Flood PSA should be considered hazards caused due to the following:

a) High river or lake water;

b) High tides;

c) Wind driven storms;

d) Extreme precipitation;

e) Tsunamis;

f) Seiches;

g) Flooding caused by landslides;

h) Human-induced floods (e.g. failures of dams, levees, dykes).

The combination of external floods with other hazard phenomena should be considered, with account taken of possible dependencies (e.g. high water level, consequential dam failures). The consequences of heavy rain and other flooding, such as water collecting on rooftops and in low lying plant areas, should be included in the scope of the analysis.

The external flooding sources around the plants should be identified and their damage potential to plant should be analyzed. The damage potential by external flooding can be characterized by the discharge, velocity, water level, duration, and contribution of wave action. Some or all of these parameters should be estimated for floods hazards characterization. Wind speed, direction and duration, which can occur simultaneously with the flood, should be taken into account as a potential combined hazard.

Qualitative screening of external floods should be performed by considering location, available warning time, type of water retaining structure and adjacent areas. For quantitative screening of external floods, a careful and detailed analysis should be performed on the basis of frequency of occurrence. For each external flooding event, structures, systems and components being affected (submersion, temperature, pressure, spray, steam, pipe whip or jet impingement) should be identified. [6,7]

Consideration of components affected by external flooding should take into account elevations, barriers, doors and drains. Potential drain blockages should be considered. The type of plant operational disturbances potentially caused by the flooding should be assessed. Analysis of the potential impact of flooding on plant operation should include component or system actuation due to flooding effects, which could initiate special event sequences.

The probability of accident due to external flooding, using the basic information (frequency of accidents or probability of occurrence) combined with plant response analysis, should be evaluated. Sensitivity analysis should explore the issues in the model used in the analysis, which are of importance.

9.1 Integration of External Flood Hazards in the Level 1 PSA Model

Level 1 PSA model for internal initiating events is used as a basis for the Level 1 PSA model for external hazards. The major impacts of the hazard that could lead to different initiating event (e.g. large loss of coolant accident, small loss of coolant accident, transient) or lead directly to core damage should be assessed in the selection of the appropriate event tree from the PSA model for internal initiating event. Appropriate hazard curves for, and fragilities of, important structures, systems and components should be incorporated in the Level 1 PSA model for external hazards. All important dependencies, correlations and uncertainties associated with the specific hazard should be accounted for in the Level 1 PSA model for external hazards. Probabilities relating to recoveries and post-trip human errors should be revised in order to assess the impact of the

external hazards on the credited recoveries and human actions modelled in the Level 1 PSA for internal initiating events. Level 1 PSA model for external hazards should reflect the as built and as operated plant conditions.

Consideration of accident sequences initiated by external floods should include the site specific hazard curves and the fragilities of all structures, systems and components for which damage may lead to the disabling of the equipment modelled in the Level 1 PSA. Probabilities of human errors should be adjusted to account for flood effects on performance shaping factors (in particular, the accessibility of the equipment). Also uncertainties, dependencies and correlations should be thoroughly accounted for in developing accident sequence models for initiating events induced by external floods.

9.2 Sequence and System Analysis

All combinations of failures of system, structure or component leading to postulated accidents should be identified and analyzed. Assessment of external flood hazard should be performed either as an integral part of PSA or as an extension of PSA. Additional human actions that may be needed to mitigate the flooding sequences should be identified and assessed with respect to their probability of success/failure to detect and control the flooding.

The analysis of dam failures should be performed for the conditions of the high flood level in the river with associated frequencies. In the process of evaluation of flood fragilities of structures and components plant-specific data should be used. In the assessment of non-safety structures that could fall into/onto safety-related structures causing damage should be considered. The fragility analysis should include immersion, wave dynamic loads on SSC and foundation failures (soil erosion) leading to SSC damage.

The core damage frequency induced by the flooding should be quantified. Sequence quantification of corresponding event tree/fault tree with flood affected equipment failed should be performed and analyzed with analysis of results including sensitivity and uncertainty analysis. All the analyses and quantification performed should be properly documented.

9.3 Documentation for External Flood

The Level 1 PSA for external floods should be documented in a manner that facilitates the review, applications and updating of the Level 1 PSA. The following information should be included in the documentation:

a) Description of the specific methods and data used for determining the hazard curves for external floods;

b) Specific changes made in the Level 1 PSA model to account for effects relating to external floods;

c) List of all structures, systems and components considered in the analysis along with justification for the structures, systems and components that are screened out from the analysis;

d) Methodology and data used to derive flood fragilities for all structures,

systems and components modelled in the Level 1 PSA;

e) Final results of the Level 1 PSA in terms of core damage as well as selected useful results.

10 SEISMIC PSA

10.1 Parameter Estimation

Seismic hazards are characterized by several parameters:

a) The intensity, which is a descriptive index to measure the effects and damage;
b) The ground motion, e.g. acceleration, velocity and displacement;
c) The frequency content, which is generally represented by a response spectrum;
d) The duration and, in some cases, the time histories, etc.

In a level 1 PSA the other parameters to be considered should include:

a) Peak ground motion acceleration;
b) The frequency content for the consideration of relay chattering and stress factors for operator errors;
c) The nature of local geology that should be taken into consideration in relation to secondary effects such as liquefaction, subsidence, slope instability, collapse, surface faulting or fracturing.

The spectral acceleration or the averaged spectral acceleration over a selected band of frequencies should be used when available data support the estimation.

Vibratory ground motion caused by earthquakes should not be eliminated from consideration (i.e. seismic waves can reach any point on the earth's surface). Earthquake ground motion should not be screened out. [5]

10.2 Frequency Assessment

The frequency of earthquakes at the site should be based on a site specific probabilistic seismic hazards analysis. A comprehensive up-to-date database should be established that reflect the current state of the knowledge, including:

a) Geological, seismological and geophysical data;
b) Local site topography;
c) Superficial geological and geophysical site properties.

As part of data collection, the catalogue of historically reported, geologically identified and/or instrumentally recorded earthquakes should be compiled. All credible sources of potentially damaging earthquakes should be considered. The seismic sources should be characterized by source location and geometry, maximum earthquake magnitude, and earthquake recurrence frequency. The aleatory and epistemic uncertainties should be included in source characteristics. The experts elicitation process used to characterize the seismic sources should be in compliance with the recommendations for HRA as given in section 5.7 of full power PSA.

The spectrum of the estimated seismic hazards parameters should be large and detailed enough to provide possibility for accurate estimates of the seismic risk and consistent with the physical data and interpretations. For the lower-bound parameter value for use in the hazard analysis, it should be proven that seismic events with lower parameter value will not cause any damage to structures and components. While assessing the seismic hazards frequency it should be assured that the size of the region considered and the scope of the investigations is adequate to characterize all credible seismic sources that may contribute to the estimated parameter frequency.

10.3 Structures and Components Fragility Analysis

The list of structures and components for the seismic fragility analysis should include all structures and components and their combinations that if failed could contribute to CDF.

All realistic failure modes of structures and components that interfere with the operability of the equipment during and after the earthquake should be identified through a review of the plant design documents and the walk-down. Fragilities should be evaluated for all relevant failure modes of structures (e.g. sliding, overturning, yielding, excessive drifts), equipment (e.g. anchorage failure, impact with adjacent equipment or structures, bracing failures and functional failures), and soil (i.e. liquefaction, slope instability, excessive differential settlement) that are found to be critical.

The fragility analyses should be supported by the walk-down. The walk-down should consider the anchorage and lateral seismic support and potential interactions with systems, structures and components (SSCs). The particular attention should be paid to the interactions between non-specifically qualified SSCs which can fall on seismically qualified item of the equipment. The potential for seismically induced fires and floods should also be covered in the walk-down.

The calculations of the seismic fragility parameters (e.g. median capacity and variability) should be based on plant specific data supplemented by earthquake experience data, fragility test data, and generic qualification test data. When structures and components of a high fragility are screened out based on the generic data, it should be proven that the generic data is used in a conservative manner and of a relevant plant and site specific features are not neglected. The seismic responses of the structures and components experienced at their failure level should be estimated based on the site specific earthquake response spectra anchored to a ground motion parameter (e.g. averaged spectral acceleration).

10.4 Integration in Level 1 PSA

The internal initiating events level 1 PSA model should be adapted for the seismic PSA to incorporate seismic specific aspects that are different from correspondent aspects of the model. A seismic PSA model should reflect the requirement for plant manual shutdown set in force for the seismic event over the certain magnitude (e.g. 50% design basis earthquake) even for cases where the power conversion system has high fragility and where automatic reactor scram can be avoided.

The seismic PSA model should include all important seismically-induced

initiating events that can lead to core damage. In particular, initiating events leading to scenarios of the following type should be modeled:

a) Failures of large components;
b) LOCAs of various sizes and locations;
c) Transients including losses of various support systems including loss of offsite power.

The specific accident sequence models should be added to those from internal initiating events when seismically induced initiating events lead to specific accident scenarios not considered in this model. The internal initiating events level 1 PSA model should be expanded for the seismic PSA purposes to incorporate failures of a wider scope of components or component failure modes, such as passive components failures (structures, buildings, distribution systems, cable trays, relay chattering, etc). The effects on reactor internals, in particular control rod sticking due to seismic impact onto reactor core should be considered.

All SSCs modeled in internal initiating events level 1 PSA and those SSCs whose seismically induced damage can impact accident sequences should be incorporated in the seismic PSA model. The seismic PSA model should include all non-seismic related failures, un-availabilities and human errors that can contribute measurably to the core damage frequency.

The model for seismically induced damage of SSCs should thoroughly account for all dependent failures of the equipment located in the building after damage of the building due to the considered seismic event. If dependencies of this type are eliminated from the model or if their significance is decreased, this should be justified. The seismic hazards, seismic fragilities, SSC dependencies, non-seismically induced failures, un-availabilities, and human errors should be appropriately integrated in the seismic PSA model.

A thorough check and associated adjustment should be performed in relation to the recovery actions and human errors probabilities. Recovery actions, which cannot be performed due to the impact of seismic events of certain magnitude, should be removed from the level 1 PSA model or probabilities to fail while performing the action should be increased.

All post-initiator human errors modeled in internal initiating events level 1 PSA should be revised and adjusted for the specific seismic conditions. At least the following seismically induced effects on the operators' performance shaping factors should be taken into account:

a) Availability of the pathways after seismic damage of specific SSCs;
b) Increased stress level;
c) Failures of indication or wrong indication;
d) Other impacts on operators' behavior.

Seismically induced fires and floods should be included in seismic level 1 PSA model, unless it is clearly justified that other seismic damages bound additional effects from seismically induced fire and floods. In quantifying the core damage frequency, the key information about each accident sequence and minimal cutset should be available as

the result of the model quantification in addition to the integrated results.

The seismic level 1 PSA model integration and quantification should be performed so that uncertainties from each of seismic level 1 PSA inputs (i.e. seismic hazards frequencies, seismic fragilities, dependencies and system analysis aspects), are properly propagated through the model for obtaining uncertainty characteristics of the core damage and release frequencies.

10.5 Documentation

The description of the specific methods used for characterization of the seismic sources and for selected parameters should be provided. In particular, the specific interpretations that are the basis for the modeling inputs and results should be thoroughly documented. The following information should be included in the documentation:

a) List of SSCs considered in the seismic PSA;
b) Fragility parameter values and the technical bases for them for each SSC;
c) Quantified damaged probabilities for the spectrum of seismic hazards modeled;
d) Dominant failure modes for SSC and the location of the SSC;
e) Specific adaptations made in the internal initiating events level 1 PSA model to account for seismic impact;
f) Comprehensive information on the dependencies (in particular spatial interactions) modeled in the seismic PSA as well as any assumptions applied to eliminate or decrease the impact of the dependencies.

The basis for screening out of any SSC should be fully described. The methodology and procedures used to quantify the fragilities should be documented. This should include the different aspects of seismic-fragility analysis:

a) Seismic response analysis;
b) Screening steps;
c) Walk down;
d) Review of design documents;
e) Identification of critical failure modes for each SSC;
f) Calculations of fragilities for each SSC.

The walk down procedure, team compositions, walk down observations and conclusions should be fully documented.

11 ASSESSMENT OF FULL SCOPE PSA

The completeness of the PSA includes a comprehensive set of internal initiating events, internal hazards, natural and human induced external hazards and all modes of operation of the plant including startup, operation at power, low power, shutdown and refueling. The risk significance insights from the PSA relating to accident sequences, structures, systems and components, human errors, common cause failures, etc., are derived from a comprehensive, integrated model of the plant. The assessment is required to include a full scope PSA for evaluating and assessing challenges to safety in various operational states, anticipated operational occurrences and accident conditions including a discussion of the results of integrated PSA.

12 REFERENCES

1) Regulation on the Safety of Nuclear Power Plant Design (PAK/911) (Rev.1), S.R.O No.43 (1)/2002;

2) Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), IAEA Safety series No. 50-P-4, Vienna, 1992;

3) Fire PRA Methodology for Nuclear Power facilities volume 1: summary & overview, EPRI/NRC-RES, NUREG/CR-6850, Washington, 2005;

4) Fire PRA Methodology for Nuclear Power facilities volume 2: Detailed Methodology, EPRI/NRC-RES, NUREG/CR-6850, Washington, 2005.

5) Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety series No. 50-P-7, Vienna, 1983;

6) Design Basis Flood for Nuclear Power Plants on River sites, Safety Guide, Safety series No. 50-SG-S10A, Vienna, 1983;

7) Design Basis Flood for Nuclear Power Plants on coastal sites, IAEA, Safety Guide, Safety series No. 50-SG-S10B, Vienna, 1983;

APPENDIX I: GLOSSARY

a) **"Authority"** means the Pakistan Nuclear Regulatory Authority established under section 3 of the Ordinance, 2001 (III of 2001);

b) **"Accident"** means any unintended event, including operating error, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of safety;

c) **"Core Decay Heat"** means sum of the originating from radioactive decay and shutdown fission and the heat stored in reactor related structures and in heat transport media;

d) **"Common Cause Failure"** means failure of two or more structures, systems or components due to a single specific event or cause;

e) **"Licensee"** means the holder of current licence;

f) **"Limit"** means the value of quantity used in certain specified activities or circumstances that must not be exceeded and is acceptable to or/ and notified by the Pakistan Nuclear Regulatory Authority;

g) **"Nuclear Safety (Safety)"** means the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of site personnel, the public and the environment from undue radiation hazards;

h) **"Postulated Initiating Events (PIE)"** means an event identified during design as capable of leading to anticipate operational occurrences or accident conditions;

i) **"Passive Components"** means a component the functioning of which does no depend on external input;

j) **"Redundancy"** means provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other;

k) **"Mitigating Systems"** means systems important to safety, provided to assure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents;

l) **"Safety Function"** means a specific purpose that must be accomplished for safety.

APPENDIX II: STRUCTURE OF LEVEL 1 PSA REPORT

General Structure of the level 1 full power PSA report should be as follows:

1. Summary Report
2. Overview of the Study
   a) Background and objectives of the study
   b) Scope of the study
   c) Project organization and management
   d) Project implementation
   e) Overview of the procedures and methods
   f) Report organization
3. Plant and Site Description
   a) General plant characteristics
   b) Plant systems
   c) Plant site
4. Identification of Radioactive Sources, Accident Initiators and Plant Response
   a) Sources and conditions of radioactive releases
   b) Selection of initiating events
   c) Plant functions and systems relations
   d) Plant system requirements
   e) Grouping of initiating events
5. Accident sequence modeling
   a) Event sequence modeling
   b) System modeling
   c) Qualitative dependence analysis
   d) Impact of physical processes in the progression of accident sequences
   e) Classification of accident sequences into plant damage states.
6. Data Assessment and Parameter Estimation
   a) Initiating event data and frequencies
   b) Component data and parameters
   c) Human Reliability analysis
7. Accident Sequence Quantification
   a) General concept of the quantification process
   b) Analysis of system models
   c) Accident sequence quantification
   d) Uncertainty analysis
   e) Importance and sensitivity analysis
   f) Description of computer codes used in the analysis.

8. Display and interpretation of results

   a) Dominant sequences contributing to core damage frequency
   b) Results of uncertainty analysis
   c) Results of importance and sensitivity analysis
   d) Interpretation of results, engineering insights
   e) Conclusions, recommendations and potential applications.

PAKISTAN NUCLEAR REGULATORY AUTHORITY
P.O. Box 1912, Islamabad