



Contents

[I. Living PSA Level 1 5](#_Toc475107078)

[I-1. Main activities 6](#_Toc475107079)

[I-1.1. General understanding of LPSA in power mode 6](#_Toc475107080)

[I-1.2. Main task description 8](#_Toc475107081)

[I-1.3. Input data and deliverables 17](#_Toc475107082)

[I-1.4. Software 18](#_Toc475107083)

[I-2. Timetable of work 19](#_Toc475107084)

[I-2.1. Major milestones 19](#_Toc475107085)

[I-3. Work resources 21](#_Toc475107086)

[II. Living PSA Level 2 23](#_Toc475107087)

[II-1. Main activities 24](#_Toc475107088)

[II-1.1. Introduction 24](#_Toc475107089)

[II-1.2. Main task description 25](#_Toc475107090)

[II-1.3. Input data and deliverables 37](#_Toc475107091)

[II-1.4. Software 39](#_Toc475107092)

[II-2. Timetable of work 40](#_Toc475107093)

[II-2.1. Major milestones 40](#_Toc475107094)

[II-3. Work resources 42](#_Toc475107095)

[III. Development of risk monitoring of Bushehr Nuclear Power Plant 43](#_Toc475107096)

[III-1. Technical part 44](#_Toc475107097)

[III-1.1. Background 44](#_Toc475107098)

[III-1.2. Terminology used 44](#_Toc475107099)

[III-1.3. Advantages of Risk Monitoring 50](#_Toc475107100)

[III-1.4. Purpose and scope 51](#_Toc475107101)

[III-1.5. Engineering activities on development LPSA into Risk Monitor 51](#_Toc475107102)

[III-1.6. Input data and deliverables 58](#_Toc475107103)

[III-1.7. Risk monitoring software 58](#_Toc475107104)

[III-2. Timetable of the work 60](#_Toc475107105)

[III-2.1. Major milestones 60](#_Toc475107106)

[III-2.2. Scheduling of proposed activities 60](#_Toc475107107)

[III-3. Work resources 62](#_Toc475107108)

List of tables

[Table I‑1. LPSA Level 1 project major milestones 19](#_Toc475107109)

[Table I‑2. LPSA Level 1 project schedule 20](#_Toc475107110)

[Table I‑3. LPSA Level 1 work resources 21](#_Toc475107111)

[Table I‑4. LPSA Level 1 training resources 22](#_Toc475107112)

[Table II‑1. LPSA Level 2 project major milestones 40](#_Toc475107113)

[Table II‑2. LPSA Level 2 Project Schedule 41](#_Toc475107114)

[Table II‑3. LPSA Level 2 work resources 42](#_Toc475107115)

[Table II‑4. LPSA Level 2 training resources 42](#_Toc475107116)

[Table III‑1. Risk Monitor project major milestones 60](#_Toc475107117)

[Table III‑2. Risk Monitor project schedule 61](#_Toc475107118)

[Table III‑3. Risk Monitor work resources 62](#_Toc475107119)

[Table III‑4. Risk Monitor training resources 62](#_Toc475107120)

List of figures

[Figure I‑1. Framework of a Level 1 PSA for internal initiating events 8](#_Toc475107143)

[Figure II‑1. Main steps of the study 26](#_Toc475107144)

[Figure II‑2. CET structure - Event tree/Fault tree approach (RiskSpectrum) 32](#_Toc475107145)

[Figure III‑1. Risk measures used in PSA – average/ baseline/ point-in-time risk 46](#_Toc475107146)

[Figure III‑2. Risk measures used in the Risk Monitor 47](#_Toc475107147)

[Figure III‑3. Risk measures used in PSA – Cumulative risk 47](#_Toc475107148)

Executive summary

The present proposal is presented following an Invitation to tender for contract titled **“Establishment of the PSA based methods and development of risk monitoring tool for the Bushehr nuclear power plant unit 1”**.

It should be noted that LPSA (living PSA) is understand as update of existing PSA studies to reflect current status of the BNPP unit 1.

Therefore the framework of this proposal relates to carrying out the PSA, which can allow BNPP to maintaining it as a Living PSA and using it as part of a risk-informed decision making process.

Generally, the scope of the PSA to be undertaken should be correlated with the national safety goals or criteria, if the latter have been set. At a high level, quantitative results of PSA are often used to verify compliance with safety goals or criteria, which are usually formulated in terms of quantitative estimates of core damage frequency. Safety goals or criteria do not usually specify which hazards and plant operational modes have to be addressed. Therefore, in order to use the PSA results for the verification of compliance with existing safety goals or criteria, a full scope PSA involving a comprehensive list of initiating events and hazards and all plant operational modes should be performed unless the safety goals or criteria are formulated to specify a PSA of limited scope.

The PSA models of internal and external hazards are based on the internal events PSA model, modified to include the impact of the identified hazards scenarios in terms of causing initiating events, and failing equipment used to respond to initiating events. Therefore development PSA for internal events is the first and basic step in conduction of full scope PSA. At the next step/s all other hazards (internal and external) can be developed sequentially or together.

Based on these reasons this proposal is limited to internal events PSA.

Our experience shows that the development of PSA in power mode together with shutdown mode gives many advantages related to implementation of different PSA task and cost constraints. Therefore in our proposal development of power mode and shutdown mode models are compiled.

Technically, the proposal is divided in three general parts:

* Proposal for LPSA Level-1 (at power and shutdown mode)
* Proposal for LPSA Level-2 (at power and shutdown mode)
* Proposal for Risk Monitoring (in power and in shutdown mode)

Each part contains general information of main activities required for successful implementation of the relevant part, tentative time-table (working schedule) and preliminary estimation of work resources.

# Living PSA Level 1

## Main activities

### General understanding of LPSA in power mode

#### Background

Probabilistic Safety Assessment (PSA) provides a consistent and integrated model of nuclear power plant safety. It is a conceptual and mathematical tool for deriving numerical estimates of risk for nuclear power plants (and industrial installations in general).

Level 1 PSAs have now been carried out for most nuclear power plants worldwide.

The production and use of a PSA is a formal regulatory requirement in many countries. For many, this is done through the requirement that a Periodic Safety Review be conducted on operating plants as part of their regulatory system (in accordance with IAEA Safety Standards) and the companion requirement that a PSA be performed as part of these Periodic Safety Reviews. In other instances, the requirement for PSA is an integral portion of the regulatory structure; e.g., Canada, United Kingdom. In some countries, the use of PSA by licensees seeking regulatory change is voluntary. However, once that choice is made, substantial guidance is available on the nature of the analysis required and acceptable analytical results (e.g., France, USA).

However, in most cases the regulatory system encourages the production and use of PSAs to provide information to complement and support the defence-in-depth philosophy used by most regulatory bodies, and to aid operational configuration decisions. PSA has been shown to provide important safety insights in addition to those provided by deterministic analysis. PSA provides a methodological approach to identifying accident sequences that can follow from a broad range of initiating events and it includes a systematic and realistic determination of accident frequencies and consequences.

In general, the PSAs are being maintained as Living PSAs that are updated regularly to take account of any changes at the nuclear power plants (NPP). As a part of these updates efforts are being made to improve the quality and realism of the PSAs produced for NPPs so that they provide an accurate model of how the plant behaves in accident conditions.

#### Objectives of the study

PSA methodology integrates information about plant design, operating practices, operating histories, component reliabilities, human behaviour, thermal hydraulic plant response, accident phenomena, and taken to it conclusion potential environmental and health effects. In practice PSA aims to achieve completeness in defining possible mishaps, deficiencies and plant vulnerabilities, producing a balanced picture of safety significant issues across a broad spectrum.

As we understand the updated of BNPP PSA Level 1 in power and shutdown modes are required to fulfil the following principal objectives:

* Provide an estimate of the core damage frequency (CDF) and identify the major accident sequences;
* Demonstrate that a balanced design has been achieved and provide confidence that small changes of conditions that may lead to a catastrophic increase in the severity of consequences (cliff-edge effects) have been prevented. This can be demonstrated as achieved if no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risk, and the first two levels of defence-in-depth bear the burden of ensuring nuclear safety;
* Identify plant vulnerabilities and systems for which design improvements or modifications to operational procedures could reduce the probabilities of severe accidents, or mitigate their consequences. Identify those components or plant systems whose unavailability significantly contributes to the core damage frequency;
* Identify any functional, spatial and human induced dependencies within the plant configuration which contribute significantly to the core damage frequency;
* Support in service inspection (ISI) program;
* Support in service testing (IST) program;
* Evaluate and rating the plant operating experience;
* Evaluate the plant technical specification and limiting condition of operation;
* Assess the adequacy of emergency operating procedures;
* Support risk monitoring program, including configuration control and monitoring of safety indicators;
* Support decisions on backfitting and design modifications;
* Support of PSR and evaluation of other possible safety issues.

In general, PSA aims at extending and widening the understanding of the important issues that affect the safety of a nuclear power plant. By doing so, design and operational problems can be identified and areas for improvement or future study can be identified.

We will ensure engraving of the objectives in implementation of particular tasks by ad-hoc planning and timely execution of activities.

#### Scope of the study

Definition of the Scope of the PSA is of most importance in order that the defined scope meets the overall objective for undertaking the study. The scope of a PSA Level 1 is defined by the challenges included in the analysis and the level of analysis performed.

Specifically, the scope of this PSA study is defined in the following terms:

* **Power mode –** Level 1 PSA will address all operational conditions of the plant (i.e. full power, low power and shutdown).
* **Radioactive sources** – To address the total risk from the plant Level 1 PSA will include contributions arising from reactor core.
* **Risk characterization** for PSA Level 1 in power mode is typically expressed by core damage frequency (CDF). Core damage frequency is defined as the sum of the frequencies of those accidents that result in uncovery and heat up of the reactor core to the point at which prolonged oxidation and severe fuel damage are anticipated and involving enough of the core, if released, to result in offsite public health effects.

The following description of main activities is represented by different event categories taking into account their specificity and relationships.

### Main task description

Implementation of internal event analysis will follow the state of the art international practice. General analysis framework of a Level 1 PSA for internal initiating events is shown on Figure I-1.

The following briefly discusses the objective of each technical task represented the main steps in performing the PSA Level 1 for internal events.

It should be noted that PSA model for internal events is the basis for modelling (in particular, sequence analysis and system analysis) the other hazards taken into the scope of PSA study.



Figure ‎I‑1. Framework of a Level 1 PSA for internal initiating events

#### Plant operational state (POS)

This task is performed only for purposes of shutdown mode analysis. The current practice for modelling this changing plant operational environment during low power and shutdown in the PSA is to define a number of POSs which are used to describe the operational stages during the outages.

The definition of POS is one of the main stages in the implementation of the activities for PSA Level 1 realization for low power and shutdown reactor.

The purpose of this SPSA task is to establish a list of operational states within which the main unit parameters and system configuration may be accepted as permanent. That allows to develop a probabilistic model for each separate state, thus ensuring the completeness of the investigation and all more essential changes in the system configuration and unit parameters are taken into account. Each POS defines boundary conditions for a “Mini PSA".

The definition of operational states will include the following subtasks:

* Interface of PSA Level 1 for unit power operation and PSA Level 1 for low power and shutdown reactor;
* Definition of outages types;
* Making a list of operational states;
* Estimation of POS frequency and duration.

The building of an integral PSA model requires introduction of an adequate boundary between FPSA model and SPSA model. Usually, power level, for which the FPSA model is already not applicable, is assumed as boundary between the FPSA and SPSA models..

The study will address the following outages types:

* refuelling outages,
* planned maintenance outages,
* unplanned outages.

Determination of POS will be based on pre-POS. A pre-POS is defined as a plant configuration where all parameters of interest could be considered stable for the duration of the POS. Such a condition is a prerequisite for the development of accident sequences. Within a POS, the PSA model may consider a stable plant situation where changes (unavailability due to maintenance, failures etc.) are modelled probabilistically.

A pre-POS is characterized by some or all of the following:

* Reactor power / core subcriticality;
* Core decay heat level;
* Reactor coolant system temperature / pressure;
* Reactor coolant system water level;
* Reactor coolant system integrity (open / closed);
* Available core cooling systems;
* Available safety systems;
* Operating / standby system alignments;
* Location of fuel;
* Containment integrity (open / closed).

The pre-POSs will be defined on the basis of actual operational experience.

#### Initiating Events Analysis

##### Selection of initiating events

Initiating Events (IE) Analysis is one of the most critical parts of the PSA. This is one of the tasks, which ensures completeness of the PSA within its defined scope, as the omission of one or more events of significance can have a profound effect on the overall results. IE analysis identifies and characterizes the events that challenge normal plant operation during power and require successful mitigation by plant equipment and personnel to prevent core damage from occurring.

The existing IE list and grouping will be reviewed. The review will check that a systematic procedure has been employed to identify the set of initiating events used in the existing PSA.

The purpose of this task is to identify set of initiating events identified is as complete as possible, within the scope decided. It is recognized that it is not possible to demonstrate absolute completeness. However, by using a combination of different methods, it is possible to gain confidence that the contribution to risk from initiating events, which have not been identified, would be small.

Therefore based on results of review additional methods to verify list of IE will be applied. This will involve a number of different approaches including:

* Analytical methods such as hazard and operability studies or failure mode and effects analysis or other relevant methods for all safety systems to determine whether their failures, either partial or complete, could lead to an initiating event; (not just safety systems, but any systems/component (such as support or even normal operation) which their failure have a negative impact on reactor core safety
* Deductive analyses such as master logic diagrams to determine the elementary failures or combinations of elementary failures that would challenge normal operation and lead to an initiating event;
* Comparison with the lists of initiating events developed for the Level 1 PSAs for similar plants and with existing safety standards and guidelines. Review of the deterministic design basis accident analysis and beyond design basis accident analysis and the safety analysis report;

Generally, Initiating events are identified on the basis of the analysis of operating experience from the BNPP-1 and from similar plants.

##### Initiating event grouping

A number of initiating event groups will be defined for the identified initiating events. An initiating event group will include initiating events which can be analysed using the same event tree and fault tree model, in other words the same accident sequences are applicable for all initiating events in the group. In general terms, the following criteria form the basis for grouping initiating events:

* all initiating events in the group have a similar effect on safety and support system
* all initiating events in the group have similar success criteria for safety and support systems
* all initiating events in the group place similar requirements on the operator
* the expected response of the operators is similar for all initiating events in the group

For shutdown mode will be constructed a table which summarizes the applicability of the initiating events to the POSs defined for the study. The applicability of the initiating events is based on the applicability of the events which comprise the group. (regarding to the duration of each of POSs, their related frequencies should be in cluded in the noted table,)

#### Accident sequence analysis

##### Event tree development

Accident sequence analysis models, chronologically the different possible progressions of events (i.e., accident sequences) that can occur from the start of the initiating event to either successful mitigation or core damage. The accident sequences account for the systems that are used (and available) and operator actions performed to mitigate the initiator based on the defined success criteria and plant operating procedures (e.g., plant emergency and abnormal operating procedures) and training. The availability of a system includes consideration of the functional, phenomenological, and operational dependencies and interfaces between the various systems and operator actions during the course of the accident progression.

As a result of this analysis, to which the system analysis modelling will ultimately provide an input, event sequences expressed in terms of the initiating event and the success or failure of mitigating systems are created, each for which a frequency can be quantified.

In terms of project objectives it is better to develop new Event trees then to use the existing one. The benefits of such approach can be determined with better traceability, study consistency and adequacy for future applications. (as BNPP-1 PSA moles have been developed, it should check existing model rather than construct from scratch. Some modification may be adequate in this approach)

To model accident sequences the “small event tree/large fault tree” approach will be applied. In the small event tree/large fault tree approach, event trees with safety functions as headings are first developed and then expanded to event trees with the status of front line systems as headings. The front line system fault tree models are developed down to suitable boundaries with support systems. The support system fault trees may be developed separately and integrated at a later stage into the front line system models.(in current BNPP-1 PSA event tree models, such above approach is not applied and headings, incorporate safety fuctions which are constructed of safety, supported and normal operation systems)

##### Success criteria determination

For purposes of Event Tree development, the success criteria will be determined. Success criteria analysis determines the minimum requirements for each function (and ultimately the systems used to perform the functions) to prevent core damage (or to mitigate a release) given an initiating event. The requirements defining the success criteria are based on acceptable engineering analyses that represent the design and operation of the plant. Realistic approach will be used performing thermal-hydraulic analyses. This approach consists of:

* The selected values of the initial parameters are realistic with regard to acceptance criteria for the corresponding class of transient and emergency conditions;
* Boundary conditions are defined in accordance to the PSA model. Operation of all safety systems and normal operation systems affecting accident sequences is taken into account with exception of those failed in the PSA;
* Design parameters such as maximum temperature of the fuel cladding are usually very conservative. For the purpose of PSA revised values or new parameters are used. In the realistic analysis operator actions are also realistically considered. Late or wrong actions are also taken into account. (the criteria is reaching to 1200°C of clad temperature)

Our computer codes used to perform the success criteria analyses are validated and verified for both technical integrity and suitability to assess plant conditions for the reactor pressure, temperature, and flow range of interest, and they accurately analyze the phenomena of interest.

#### System analysis

System analysis provides the detailed modelling of the constituent events of the accident sequences defined by the accident sequence modelling. The most usual events that are modelled are the success or failure of a safety system. Fault tree analysis is the most widely used method for developing system models.

The review of existing fault trees will check that they have been developed for each of the safety system failure states identified in the event tree analysis. The review will check level of details, boundary conditions, assumption and simplification to be sure that system analysis is performed in an acceptable level of quality. A special attention will be paid to systems alignments. Based on review results all necessary changes will be identified. (existing fault trees are based current safety functions defined as headings in existing event trees. As above notation which is encountered an important comment, this proposal considers new event trees development which is under question essentially by itself. So, it’s an obvious discrepancy)

Similarly to event tree analysis the fault trees will be developed as a new one (keeping the correct and unchanging logic). The benefits of such approach can be determined with application of suitable basic events coding system, reflecting of necessary improvements, providing opportunities for use in other categories of IE and for shutdown mode model as well as better traceability.

Usually there are number of systems which are required for accident mitigation in both power and shutdown modes. For such systems, the fault trees developed for power modes will be used for shutdown mode (taking into account the necessary adjustments reflecting POS). This approach will ensure consistency in systems modelling and will provide the conditions for establishing an integrated model which will allow easier use in future PSA applications.

#### Analysis of dependent failures

The objective of the dependent failure analysis is to support other PSA tasks with dependent failure information and assure that all possible dependencies are correctly considered. Correctly modelling dependencies is essential to the development of the PSA model. The dependent failure analysis tasks provides the vehicle for confirming that all dependencies, including subtle dependencies, are included in the PSA, either by explicit modelling or by common cause failure modelling.

There are four different types of dependencies that can occur:

* Functional dependencies arise when the function of one system or group of components depends on the function of another system or component. Usually occurs due to shared components, common actuation systems, common isolation requirements or common support systems (power, cooling, instrumentation and control, ventilation, etc.).
* Physical dependencies (also referred to as spatial interaction dependencies) due to an initiating event that can cause failure of safety 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 plant staff that either contribute to, or cause, an initiating event, or lead to the unavailability or failure of one or more items of safety system equipment so that they do not operate when required following an initiating event.
* Component failure dependencies due to errors in design, manufacture or installation or errors made by plant personnel during plant operation. These are addressed by a common cause failure analysis.

A systematic review will be carried out of the design and operation of the BNPP-1 to identify all the potential dependencies that could arise, leading to the unavailability of safety system components or a reduction in their reliability in providing protection against initiating events. (again, not only safety systems but also any systems that its failure has a negative impact on safety such as some normal operation systems which their functions are necessary during the accident/initiating event mitigation)

As mention above all functional and physical dependencies will be modelled explicitly in the event tree or fault tree model. Human interaction dependencies and component failure dependencies will also be modelled in farm of corresponded task activities.

#### Common cause analysis

Typically all dependent failures which are not considered explicitly in the PSA model are modelled with Common Cause Failure models. Usually this included the sets of redundant equipment.

There are a number of methods available for modelling common cause failure in a Level 1 PSA and the method chosen should be supported by the collection of data. (the needed data and related methodology should be described)

Typically screening Common Cause Failure (CCF) analysis will be used at the preliminary stage and more detailed model such as Multiple Greek Letter (MGL) model will be used for the dominating CCF groups in PSA.

The common cause analysis will consider both intarsystem and intersystem common cause failure events as a good practice.

#### Human reliability analysis

Human reliability analysis identifies and provides probabilities for the human failure events that can negatively impact normal or emergency plant operations. Taking into account of human errors is a very important part of the PSA process. It has been proved that most of accidents worldwide are result of wrong human actions. Typically Human actions are divided into 5 types according to:

* Type 1 (also known in some references as Type A): These are human actions which are developed prior to the initiating event and may affect system or function reliability. They are also called pre-accident actions.
* Type 2 (Type B): These are human actions, which may lead to an initiating event. They are also called human induced initiating events.
* Type 3 (Type C1): These are human actions, developed by operators, during an accident, following established procedures, for mitigating the consequences of an accident. They are also called post-accident human actions.
* Type 4 (Type C2): Plant personnel, attempting to follow procedures, can make mistake that aggravates the situation or fails to terminate the accident. These are also called mis-diagnosis actions.
* Type 5 (Type C3): By improvising, plant personnel can restore and operate initially unavailable equipment to terminate an accident. These are called recovery actions.

Type 2 actions are generally implicit in the selection of the initiating events. They are usually included in the outage-frequency data base, but are not always identified as specific causes.

A structured and systematic approach will be adopted for the identification of human errors, the incorporation of the effect of such errors in the plant logic model (event trees and fault trees) as human failure events and the quantification of the probabilities of such events, i.e. human error probabilities. This structured and systematic approach will provide confidence that a comprehensive analysis has been carried out to determine the contributions to the frequency of core damage from all types of human error.

There is no unanimity about the best methods to perform human action analysis as far as there are a lot of limitations applying these methods. We suggest an approach that has been proven during our practice in PSA development.

Performance of analysis for type A operator actions (pre-accident human errors) to the unavailability of safety and support systems will include:

* Adopted procedure for analysis in compliance with international approaches (IAEA, international good practice);
* Quantitative screening analysis for important systems; (Pre accident HRA is not just for Important systems. Moreover, prior to PSA comprehensive quantitative analysis (PSA whole model), important system, cannot be identified truly, because one of the most important of PSA results is importance analysis section)
* Detailed human action assessment.

Performance of analysis for type C (post-accident) operator action will include:

* Assessment of the important post-accident operator actions, applying the most appropriate methods, included in the EPRI calculator for full power operation; (as a similar comment mentioned above, post-accident human actions are not identified prior to PSA quantification )
* Incorporation of the new HEPs for type C actions into a PSA model for internal events and performance of dependency analysis (post-processing analysis);
* Documentation of the results.

A special procedure will be applied for dependence analysis. The dependent cut-sets will be assesses according to different types of dependence, described in NUREG/CR-1278.

#### Data analysis

Data analysis (parameter estimation) quantifies the frequencies of the initiating events, as well as the equipment failure probabilities and equipment unavailability of the modelled systems. The estimation process includes a mechanism for addressing uncertainties and has the ability to combine different sources of data in a coherent manner, including the actual operating history and experience of the plant when it is of sufficient quality, as well as applicable generic experience. (various techniques based on Bayesian estimation should be applied in parameter estimation. In some technique, non informative or constrained noninformative distribution may be applied which does not require sufficient data)

As a first step of implementation of this task the review of existing data will be performed. One of the main issues with data is their applicability to the plant, plant’s particular components and operating modes. It is not often that there is much data available which are entirely applicable, and the review need to recognize that the analysts will have to use their judgment in selecting the best sources for each case.

Clearly, plant specific data are always to be preferred to generic data but, even for a plant which has been operating for a number of years such as BNNP, the plant specific data are often rather sparse and have to be combined in some way with generic data. A balance has to be struck between the use of a small amount of more applicable (plant specific) data and the larger amount of less applicable data. The review will check that the maximum use has been made of plant specific data, compare this with the generic data, and satisfy themselves that there are reasonable explanations for any notable differences. This is important even when the two sources are combined — for example, using a Bayesian approach. In any case, the review will check that the data have been sufficiently well justified in the PSA documentation and shown to be relevant, item-by-item. (many components have specific reliability design data which should be considered intelligently in Bayesian approach as a prior distribution parameters. For example the mean values of some reliability parameters (such as MTTF) are usually given in design documents. In such cases, one way may be using of that mean value in prior distribution with other needed parameters (such as standard deviation) from generic data. Obviously, the acceptable algorithm is needed for this type of analysis)

In accordance to plant operational experience additional data analysis will be performed if necessary. Data from the operation of similar plants will be preferred as generic data, such as that from other VVERs-1000. (for data analysis Bayesian approach must be applied. Design, generic and specific data will be constitutions of the analysis definitely)

The approach for data estimation and definition of equipment reliability parameters would not depend from operation mode (full, low power or shutdown), since the failures will be counted for whole observed calendar period not taken into account the time when the given equipment is out for maintenance. The same approach will be used in determine actual working hours and number of demands. That is why it will be possible to use quantitative results for all plant operating modes. (for standby components, the actual time of standby should be identified and applied in a good manner to quantify the related standby failure rate or combined standby-operation failure rate. NUREG 6823 offer some practical solution for parameter estimation of standby components)

Generally tasks forming data analysis are defined by performance and documentation of the following activities:

* Definition of basic events;
* Identification of different models describing stochastic nature of curtain phenomena related to basic events and corresponding parameters subjected to estimation;
* Determination of suitable data sources to perform the estimation. Gathering and processing the data;
* Selection and application of appropriate estimation method.

(data analysis should be done for all of possible component failure modes. So as a preliminary action, FMEA may be useful for identification of failure modes and their possible consequences)

#### Quantification, uncertainty and sensitivity analysis

The main objective of the model integration and quantification process is to develop an integrated plant-specific PSA model that will be used to estimate the core damage frequency and to develop an understanding of the contributors to core damage model. The calculations are based on point values, but they need to incorporate the propagation of uncertainties throughout the analysis, yielding a probability distribution for the frequency.

Using the RiskSpectrum software we can apply the procedure which verifies the PSA quantification process is technically correct and thorough, and that key dependencies are correctly accounted for in the quantification process.

The main purposes of quantification process are to demonstrate that the accident sequences/cut sets identified do actually lead to core damage. Where cut-offs will be used in the quantification process (either on cut set order or frequency), the procedure will check that they have been set at a sufficiently low level such that they would not lead to a significant underestimate of the frequency of core damage. The procedure will determined that the quantification process is documented in a clear and balanced manner.

In addition, an important part of this task is to identify the key sources of uncertainty in the model and assess their impact on the results.

Sensitivity studies will be made for the important assumptions and the relative importance of the various contributors to the calculated results.

#### Analyses and interpretation of the results

The objective of the results analysis and interpretation activity is to derive an understanding of those aspects of plant design and operation that have an impact on the risk.

A special attention will be given on the significance to risk of individual contributors (initiating events, accident sequences, functional failures, system failures, component failures, human failures, etc.) are explored to derive an understanding of the risk profile of the plant, i.e., what is the impact of various aspects of plant design and operation on risk.

#### Training

At the end of the project, a one week training will be given for Client PSA involved personnel. The sessions foreseen theoretical and practical part. The stress will be put on the practical training for working with the PSA Level 1 model. The main topics of training course will be:

* Initiating event selection;
* Plant operating state definition and determination;
* Event tree development – accident sequence analysis and success criteria;
* System analysis;
* Human reliability analysis;
* Data analysis;
* Model quantification.

The training program is subject of additional negotiation, since it is highly dependent on the skills of the trainee personnel.

### Input data and deliverables

#### Input data

For the purpose of the study it is expected that the Contracting Authority will provide:

* The safety analysis report (SAR);
* Plant Technical specification;
* System descriptions, instructions;
* List of performed plant changes, if any;
* As built (as is) system drawings (piping and instrumentation diagrams);
* Electrical line drawings, including circuit diagrams and trip criteria for the electrical bus protection system;
* Control and actuation circuit drawings;
* Normal operating procedures, emergency procedures, test procedures and maintenance procedures;
* Analyses pertinent to the determinants of mission success criteria of systems;
* Plant operational experience records, reports and analysis of incidents;
* Plant specific databases for failures and defects of selected system components;
* Plant databases and/or the computerized management system for maintenance, if available;
* Plant layout drawings;
* Drawings of piping location and routing;
* Drawings of cable location and routing;
* Plant walkdown reports, if available;
* Regulatory requirements;
* Other relevant plant documents.

Based on information in the mention documentation we can ask for additional data related to various aspects of the PSA Level 1 development.

In order to systematize the input data used a common database for the project will be organized. The main attributes of this database will provide the ability to identify the document (registration and/or number in the archive database of BNPP) and the respective areas of the PSA where the information from it is used. This data base will assist in the maintenance of the model in the future.

#### Deliverables

The reports that will be prepared by the Consultant and issued officially to the EC in due course within the framework of the project activities and in accordance with the project schedule are:

* The administrative reports,
* The Technical Delivery documents,
* Other communication documents

Reports produced in this study will be written in English.

##### Administrative reports

In order to optimise work process development a monthly report will present a progress mark-up of the agreed baseline study time schedule with ‘by exception’ corrective actions for any deviations to plan and any unresolved issues.

##### Technical delivery documents

The final technical deliverables are:

* Updated BNPP-1 PSA Level 1 in power mode report. This report will document the assumptions of the analyses and the relevant results. It will be provided in paper and electronically. (power and shutdown modes)
* Electronic copies of all relevant PSA models, important work files and output files of the analyses.

The objective is to ensure adequate documentation of the updated BNPP PSA Level 1 in power mode to allow review of the PSA development and its results, as well as to provide a written basis for any future uses of the updated BNPP PSA.

Draft reports will be submitted by email, final reports by email and in hardcopy.

### Software

The software to be used is given in the following Table.

|  |  |  |
| --- | --- | --- |
| Name | Version | Application |
| RiskSpectrum PSA | 1.3.2 | Probabilistic part of the study – PSA L1&L2 interface and CET |
| RELAP/SCDAP\* | 3.4 | Accident sequence analysis and human reliability analysis |

## Timetable of work

### Major milestones

The following table contains major milestones. The milestones are defined as date of a deliverable.

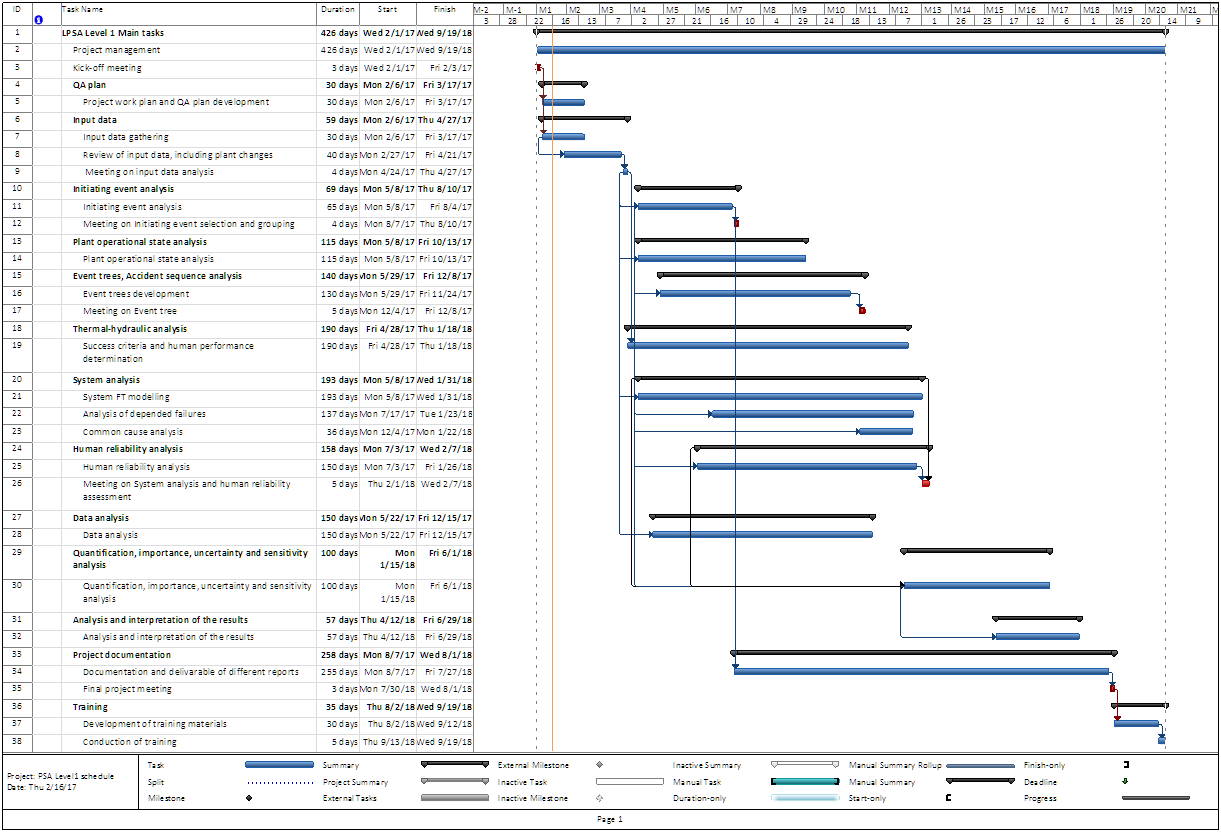
Table ‎I‑1. LPSA Level 1 project major milestones

|  |  |  |
| --- | --- | --- |
| Milestone | Cumulative time end | Comment |
| 1 | T0+ 20 days | Kick-off meeting |
| 2 | T0 + 1 month | Project work plan and QA plan |
| 3 | T0 + 2 months | Input data gathering |
| 4 | T0 + 6 months | Meeting on Initiating event selection and grouping |
| 5 | T0 + 10 months | Meeting on Event tree |
| 6 | T0 + 12 months | Meeting on System analysis and human reliability assessment |
| 7 | T0 + 18 months | Deliverable of Level 1 PSA report |
| \*T0 – date of commencement | | |

#### Scheduling of proposed activities

On the following page, project schedule is presented. Given dates are conditional, since they depend on the project start date. The actual schedule will be updated after contract signing. The months given in Major milestones table and in the schedule are different, since the training course is considered to be out of the study. Training course schedule will be negotiated during the project execution. (in this proposal training program is just considered as a short training course with one week duration, but the following time schedule table has essential difference from Major milestones table which is under question. For example kick-off meeting is so different in two tables that is not relate to training program. This comment is valuable for the later corresponding tables)

Table ‎I‑2. LPSA Level 1 project schedule



## Work resources

According to the presented brief information concerning the different activities the following resource could be formed expressed in man-days:

Table ‎I‑3. LPSA Level 1 work resources

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task | Human resources [Man-days] | Professional Category | | |
| Project Manager | Senior Expert (over 10 years) | Senior Expert (5 to 10 years) |
| Task management | 80 | 80 |  |  |
| QA plan development | 10 |  | 10 |  |
| Review of input data, including plant changes | 100 |  | 80 | 20 |
| Determining plant operational state | 200 |  | 200 |  |
| Initiating event analysis | 200 |  | 200 |  |
| Accident sequence analysis | 300 |  | 300 |  |
| Thermal-hydraulic analysis needed for success criteria and human performance | 500 |  | 350 | 150 |
| System analysis | 720 |  | 720 |  |
| Analysis of depended failures | 50 |  | 50 |  |
| Common cause analysis | 100 |  | 100 |  |
| Human reliability analysis | 500 |  | 500 |  |
| Data analysis | 150 |  | 150 |  |
| Quantification, importance, uncertainty and sensitivity analysis\* | 170 |  | 170 |  |
| Analysis and interpretation of the results | 30 |  | 30 |  |
| Internal events PSA documentation | 250 |  | 180 | 70 |
| **Total:** | | | | 3360 |
| **Total man-days in REL home office** | | | | **3240** |
| **Total man-days in Tehran/site IRI office** | | | | **120** |

\* In reality it can increase depends on the number of sensitivities analysis.

Proposal does not include any travel or accommodation expenses. Proposal for training is separated as an optional activity. The human resources needed are summarized in the following table.

Table ‎I‑4. LPSA Level 1 training resources

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task | Human resources [Man-days] | Category | | |
| Project Manager | Senior Expert (over 10 years) | Senior Expert (5 to 10 years) |
| Training materials development | **45** |  | **45** |  |
| Conduction of a one week training | **15** |  | **15** |  |
| **Total:** | | | | **60** |
| **Total man-days in REL home office** | | | | **45** |
| **Total man-days in Tehran/site IRI office** | | | | **15** |

# Living PSA Level 2

## Main activities

### Introduction

The Level 2 PSA models the plant's response to the Level 1 PSA accident sequences that resulted in reactor core damage. Such core damage sequences are typically referred to as severe accidents. Toward that end, a Level 2 PSA analyzes the progression of an accident by considering how the containment structures and systems respond to the accident, which varies based on the initial status of the structure or system and its ability to withstand the harsh accident environment.

Once the containment response is characterized, the amount and type of radioactivity released from the containment can be determined. Thus, the Level 2 PSA estimates the second measure of risk - radioactivity release - which is the input to the Level 3 PSA.

#### Objectives of the study

PSA methodology integrates information about plant design, operating practices, operating histories, component reliabilities, human behaviour, thermal hydraulic plant response, accident phenomena, and taken to it conclusion potential environmental and health effects. In practice PSA aims to achieve completeness in defining possible mishaps, deficiencies and plant vulnerabilities, producing a balanced picture of safety significant issues across a broad spectrum.

As we understand the updated of BNPP PSA level in power and shutdown modes are required to fulfil the following principal objectives:

* Verify compliance with probabilistic targets, if set;
* Provide an estimate of the Large Early Release Frequency (LERF) and/or Large Release Frequency (LRF) and identify the major accident sequences. Provide assessments of the probabilities of occurrence for different release categories, and assessments of the risks of major radioactive releases to the environment;
* Provide assessments of the probabilities of occurrence of severe core damage states and assessments of the risks of major off-site releases necessitating a short term off-site response, particularly for releases associated with early containment failure;
* Identify systems for which design improvements or modifications to operational procedures could reduce the probabilities of severe accidents or mitigate their consequences;
* Assess the adequacy of SAMG;
* Support in service inspection (ISI) program;
* Support in service testing (IST) program;
* Monitoring of safety indicators;
* Evaluate and rating the plant operating experience;
* Support risk monitoring program, including configuration control and monitoring of safety indicators;
* Support decisions on backfitting and design modifications;
* Support of PSR and evaluation of other possible safety issues.

In general, PSA aims at extending and widening the understanding of the important issues that affect the safety of a nuclear power plant. By doing so, design and operational problems can be identified and areas for improvement or future study can be identified.

We will ensure engraving of the objectives in implementation of particular tasks by ad-hoc planning and timely execution of activities.

#### Scope of the study

The scope of PSA Level 2 will follow PSA Level 1 scope. Specifically, the scope of this PSA study is defined in the following terms:

* **Power mode –** Level 2 PSA will address all operational conditions of the plant (i.e. full power, low power and shutdown)
* **Radioactive sources** – To address the total risk from the plant Level 1 PSA will include contributions arising from reactor core
* **Risk characterization** for PSA Level 2 in power mode is typically expressed by Large Early Release Frequency (LERF) and/or Large Release Frequency (LRF). The definition of LERF and LRF is specific for each country and expresses large releases early in time (LERF) and or sum of all large releases to the environment (LRF)

The following description of main activities is represented by different event categories taking into account their specificity and relationships.

### Main task description

Generally, main tasks of the study and their relations are shown on the figure bellow. Then, the major activities and their goals and specific are explained. Note that there are a lot of interrelations between the tasks.



Figure ‎II‑1. Main steps of the study

#### PSA Level 1 & Level 2 interface

An interface between a Level 1 and Level 2 PSA establish the connection between the Level 1 event tree model and the Level 2 event tree model. The Level 1 PSA identifies a large number of accident sequences that lead to core damage. It is neither practical nor necessary to treat each accident sequence individually when assessing accident progression, containment response and radionuclide release in the Level 2 PSA.

Generally, there are two approaches recognized in practice:

* Explicitly modelled interface between Level 1 and Level 2 via so called bridge trees – this is the most used approach;
* Not explicit interface between Level 1 and Level 2 – start with IE and ends with source term.

In the current study the first approach will be used. Since this first approach will be followed then accident sequences will be grouped together into plant damage states (PDS) in such a manner that all accidents within a given plant damage state can be treated in the same way for the purposes of the Level 2 PSA. This means that PDS will represent groups of accident sequences taken from Level 1 model that have similar accident timelines and which generate similar loads on the containment, thereby resulting in a similar event progression and similar radiological source terms.

##### PDS attributes

Attributes of accident progression that will influence the chronology of the accident, the containment response or the release of radioactive material to the environment will be identified. The attributes of the plant damage states provide boundary conditions for the performance of severe accident analysis.

Generally, plant damage states can be classified into two main classes: those in which radioactive material is released from the reactor coolant system to the containment and those in which the containment is either bypassed or is ineffective. Thus, the plant damage states will specify the containment status (e.g. intact and isolated, intact and not isolated, failed or bypassed) and, for plant damage states where the containment is bypassed, will be specified the type and size of the bypass (e.g. loss of coolant accident in interfacing systems, steam generator tube rupture). If the reactor building or secondary containment is likely to have a major influence on the source term, then its status is specified by means of the plant damage state as well. For plant damage states in which the containment is intact, a containment event tree analysis will be performed. For other plant damage states, only source term analysis may be necessary, although the containment event tree may be needed to address possible plant features that can reduce the source term (e.g. scrubbed releases versus unscrubbed releases).

Other attributes that need to be considered in characterizing the PDSs are plant failures that could influence either the containment challenge or the release of radioactive material:

* the type of initiating event can, for example, affect the rate of discharge of fluid to the containment, progression of the core melt and hydrogen generation, and the timing of the release of radioactive material. This attribute can be accounted implicitly;
* the failure mode of the core cooling function affecting the timing of core melt;
* the primary system pressure at the onset of core damage and the status of safety/relief valves and other components that could change RPV pressure before failure of the RPV lower head;
* Status of emergency cooling system and other cooling systems – all systems that may prevent further core degradation will be considered, since that might have great influence on the course of accident progression;
* Containment status – there will be a great difference in releases for cases with not isolated containment (or open containment during refueling stages) compare to isolated containment;
* Status of the containment’s engineered safety features. This may have an impact on containment cooling, the removal of radioactive material, the mixing of combustible gases present, etc.

##### Mission time

Mission times will be defined for the probabilistic system failure analysis. Mission times to consider in a Level 2 PSA are usually longer than in a Level 1 PSA. Mitigating systems may need to be in operation for a long time period to limit the source term. Mission times for each individual system may vary depending on each accidental sequence and each success criteria. It is important to use a correct mission time for each item of equipment, both for supporting Level 1 and 2 PSA quantifications and results presentations.

##### System Analysis

The system analysis approach is the same as for the PSA Level 1 (see ‎I-1.2.4).

##### Human reliability

The human reliability analysis approach for actions up to core damage will be similar as for the PSA Level 1 (see ‎I-1.2.7). For actions executed during severe accident progression, the approach will be changed to account for the conditions, number of crews and available time for the cognitive and manual part of the actions. Since there is no common approach adopted, estimation of these actions is frequently based on expert judgment assessment. (expert judgment is only accepted if there is not enough input data are available.

#### Accident progression analysis

Plant specific analysis of the progression of accidents is the preferred method for evaluating severe accident behaviour. As a minimum, calculations will be performed for each of the plant damage states that are significant contributors to the core damage frequency of the plant. In addition, calculations will also be performed for those plant damage states that may have a small frequency of occurrence, but which have the potential to result in large and/or early releases of radioactive material to the environment. Such plant damage states typically involve either direct containment bypass or early failure of the primary and/or secondary containments. If detailed calculations are performed for plant damage states with high frequency of occurrence and high consequences, a sufficiently wide range of information will usually be generated to estimate the response of the plant for other plant damage states that are not addressed in detail. In addition, generic studies of severe accident phenomena and containment response reported in the literature for similar plants and containments could also be used to complement the scope of plant specific calculations to include a broader set of conditions. Moreover, calculations will be needed for the source term analysis as well and for particular questions in containment event tree. (detailed calculation in needed. It’s not a conditional issue)

##### Phases and related Phenomena

The severe accident progression is generally separated into 3 phases:

* In-vessel core degradation phase,
* Vessel rupture phase,
* Ex-vessel phase.

The most important phenomena that are relevant to each of the listed phases are:

* In-vessel core degradation
* Core degradation and fission product release from the core,
* Induced-RCS rupture including Induced-SGTR,
* Hydrogen production,
* Vessel cooling from outside,
* Consequences of in-vessel water injection (coolability, hydrogen production, RCS pressurisation, recriticality, etc.),
* Containment atmosphere composition (recombiners/igniter effect) and containment pressurisation,
* Containment venting,
* Hydrogen distribution/combustion (deflagration, detonation) and consequences due to pressure and temperature load (containment leak, failure or system degradation),
* Corium criticality,
* In-vessel steam explosion and consequences (leak in the RCS, vessel rupture, containment rupture),
* Vessel breach phase
* Direct Containment Heating, including H2 combustion and vessel uplift,
* Ex-vessel steam explosion,
* Ex-vessel phase
* Molten Core Concrete Interaction (MCCI),
* Production of steam and non-condensable gases and fission product,
* H2/CO combustion,
* Evolution of containment atmosphere composition and long term pressurisation,
* Containment venting,
* Pool scrubbing,
* Corium criticality ex-vessel.

All these phenomena will be analysed for their relevance for Bushehr NPP unit 1 and will be addressed either by MELCOR code or by expert judgment assessment. (expert judgment is only accepted if there is not enough input data for MELCOR calculation. Moreover the expert judgement should be based on similar plants)

#### Containment performance

Fission product confinement and control is one of the main safety functions that the containment shall address and initial containment leaktightness and isolation are important issues in Level 2 PSA. The timing and the way in which the containment fails is a crucial factor influencing the magnitude of the offsite consequences. The primary objective of an assessment of containment performance is to develop a realistic characterization of the modes (mechanisms) of, and criteria for, containment leakage or failure under severe accident conditions.

Design criteria for the containment are generally not adequate measures of capacity of the containment because of the safety factor built into such values. Actual values of the ultimate pressure capacity of the containment have sometimes been found to exceed design values by a factor of two to four. Further, containment design limits may not take into account the harsh environmental conditions that can develop inside the containment during a severe accident. None of the design basis accident scenarios involve rapidly increasing containment loads. Assessment of beyond design accident sequences shows that, in some cases, significant containment loading can occur, reaching or exceeding the design loads. Therefore, transient loads like fluid jet impingement, direct containment heating, rapid deflagration or detonation of hydrogen pockets which may occur during severe core degradation accidents, may pose significant threats to containment integrity.

For the Level 2 PSA purposes, a plant specific estimate of the ultimate strength of the containment will be performed. This will be done by carrying out plant specific structural calculations.

Containment performance analyses will be based on validated structural models supported by data and reasonable failure criteria. In the analysis, consideration will be given to various types of load on the containment, e.g. static pressure loads, pressure ramp rates, localized heat loads and localized dynamic pressure loads. The supporting analyses will provide an engineering basis for containment failure mode, location, size and ultimate pressure and/or temperature capabilities.

In determining the structural performance of the containment, the uncertainties associated with estimation of the structural capacities necessary for withstanding extremes of pressure and/or temperature will also be assessed. Such uncertainties can be determined by techniques for uncertainty quantification and propagation, as part of the structural capacity assessment. Alternatively, expert judgement supported by simple analysis could be used to establish the failure pressure and/or temperature distribution for various credible failure modes (leaks and ruptures). (as said before, expert judgement is only accepted if there is not enough input data for calculation)

Consideration will also be given in the Level 2 PSA to the possible effects of temperature on the structural performance of containment. The temperature of the containment could affect the strength characteristics of the structural materials as well as cause degradation of penetration seal materials. (Obviously effects of pressure should be considered)

##### Dynamic loads versus quasi-static loads

Quasi-static pressure loads would results from the protracted generation of steam and non-condensable gases through MCCI, the interaction of molten core material with the concrete floor beneath the RPV. This pressurisation could last from several hours to several days, depending on accident specific factors, such as the availability of water in the containment and the operability of engineering safety features (ESFs).

Some of the phenomena associated with severe accidents, modelled in Level 2 PSA, are characterised by very short time scales, typically a few seconds, e.g. hydrogen combustion and direct containment heating. The loads from such energetic events are characterised by short term high pressure spikes. As dynamic loads are difficult to translate into experiments for a specific containment, the dynamic loads can be transferred to an equivalent quasi-static load on the containment. (the effect of applying quasi-static load instead of dynamic load should be clarified quantitatively)

The equivalence value between dynamic and quasi-static loads changes with the natural frequencies of vibration of the containment. Non-linear 3D containment analysis techniques will be used, where the load is decomposed using the Fourier series (harmonics) to obtain the first modes (axial symmetry, lateral displacement and ovalising) and the eigen-frequency of the containment structure.

##### Fragility curve

To obtain a fragility curve, different failure modes of the containment need to be evaluated. This includes but may not be limited to:

* Penetrations;
* Expansion joints;
* Air locks;
* Seals;
* Changes in stiffness;
* Containment expansion hindrances;
* Global failure due to inner or outer pressure.

Each failure mode is then classified as either a break or leak condition of the containment. A break in the containment may be treated with a sufficiently large break area that deposition of fission products in the containment can be neglected, but a leak condition has a sufficiently small area that significant deposition of fission products in the containment is possible. The value of the border between a break and a leak of the containment may vary depending on the size of the containment but, as a working value, 0.1 m² is suggested. (justification is needed for choosing of this suggestion)

#### Containment event tree development

The containment event tree, also called accident progression event tree, provides a structured approach for systematic evaluation of the containment capability to cope with severe accidents. The CET is used to characterize the progression of a severe accident and to identify containment failures modes that could lead to fission product release.

In Level 2 PSAs, event trees are used to delineate the sequence of events and severe accident phenomena after the onset of core damage that challenge the successive barriers to radioactive material release. They provide a structured approach for the systematic evaluation of the capability of a nuclear plant to cope with core damage accidents.

For each PDS, several accident scenarios are possible depending on the occurrence of the different events. Uncertainties can highly influence the relative probability of possible accident scenario paths. This possibility of multiple consequences analysis is the main interest of the Level 2 PSA modelling in comparison with deterministic analysis that mainly focuses on a single accident path.

A sound knowledge of severe accident issues in general and on the plant specific accident progressions in particular is needed for setting up a CET. While general knowledge can be obtained by studying appropriate publications, plant specific information has to be acquired by particular analyses. The centre of such analyses is the calculation of a set of reference sequences with state-of-the-art integral thermal hydraulics codes.

##### CET structure

RiskSpectrum code will be used for CET development. Therefore small CET method will be used, similar to those used in the level 1 PSA, which includes top event questions concerning the major severe accident phenomena, supported by fault trees or decomposition event trees.

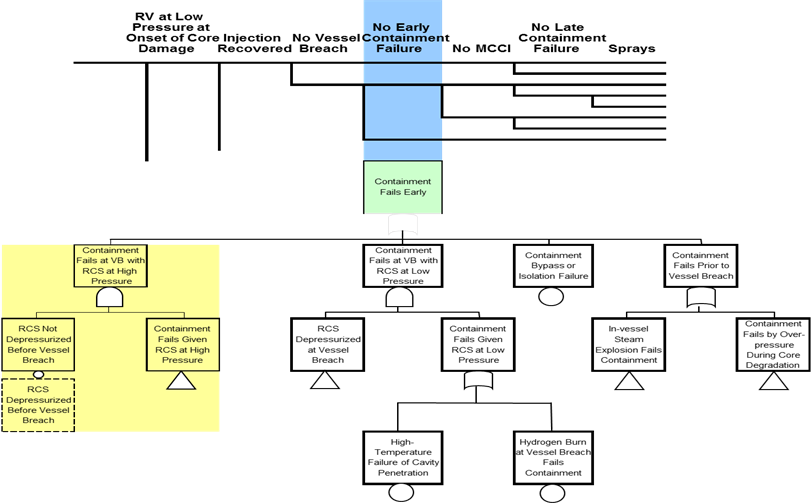


Figure ‎II‑2. CET structure - Event tree/Fault tree approach (RiskSpectrum)

##### CET quantification

The quantification of the branch probabilities will take into account calculations and analyses using mechanistic computer codes (e.g. MELCOR), parametric codes and engineering judgment (especially for phenomenological questions), as well as systems analysis for questions related with systems availability. The differences in the above methods do not diminish the quality of the results as long as the important features that influence the evolution of the accident are treated in detailed, and the dependencies between questions are properly handled.

As it is already said, system analysis approach is identical to the one performed for PSA Level 1. For operator action, quantification methods, currently used, are similar to the one in PSA Level 1. Containment response (failure probability) is represented by fragility curves for different modes of failure. Therefore, the biggest difference between Level 1 PSA and Level 2 PSA quantification methods are related to probability assignment of the phenomena (parameters).

There several approaches are usually used in phenomena quantification. The most spread are:

* Expert judgment - represents an analyst's quantitative measure of the likelihood of an event given the available supporting information;
* Risk-Oriented Accident Analysis Methodology (ROAAM);
* Response surface method.

##### Treatment of dependencies

Different types of dependencies that will be accounted in the model are:

* Dependencies between Level 1 PSA and Level 2 PSA

Certain functions or events in the Level 2 PSA of the model have dependencies to the Level 1 PSA of the model. A single event or combination of basic events representing or contributing to a failure in the Level 2 PSA may already have occurred in the Level 1 PSA. This has to be properly addressed in the Level 2 PSA.

Human actions may have been modelled for Level 1 purpose and the same or related type of actions is used in the Level 2 PSA. Again, this information has to be carried over to the Level 2 part, and be properly taken into account in the human reliability analysis of the L2PSA.

* Dependencies between events in CET

The probability of an event may depend on the values of physical variables. This probability will thus change if another event, occurring previously, changes the values of these physical variables. The CET development will be optimized to tackle dependencies between events.

##### Integrated vs. separated model

There are two approaches in developing the probabilistic model of a Level 2 PSA:

* Integrated model,
* Separated model.

One key difference between the two approaches is the way how the interface transfers information from Level 1 PSA to Level 2 PSA. The necessary degree and precision of information transfer is defined by the needs of Level 2 PSA analysis, and it has to be provided whatever the approach.

With regard to the interface between Level 1 and Level 2 and quantifications made for the plant damage state, the main difference between the two approaches is the mode of documentation and data transfer from Level 1 to Level 2.

For the purposes of the current study we propose to use integrated approach. This is possible using RiskSpectrum code.

#### Source term analysis

The next step in the Level 2 PSA is the calculation of the source terms associated with the end states of the containment event tree. Source terms determine the quantity of radioactive material released from the plant to the environment. Main steps of this analysis are:

* Specifying the release categories;
* Grouping the end states of the containment event tree into the release categories;
* Carrying out the source term analysis for the release categories;
* Grouping the release categories into source term categories for use in the Level 3 PSA.

The source term assessment provides information about the characteristics of the release categories in terms of composition of the release and the time of release.

##### Specifying the release categories

Containment event trees have a large number of end states, each of which represents a sequence of events that occurs following core damage. Many of these events have a significant influence on the release of radioactive material from the containment. Characteristics of such events include:

* The failure mode of the reactor coolant system;
* The mode and time of failure of the containment;
* The cooling mechanisms of the molten core material;
* The retention mechanisms for radioactive material.

However, many of the end states of the containment event tree are identical or similar in terms of the phenomena that have occurred and the resulting release of radioactive material to the environment. Similar end states will be grouped or binned together to reduce the number of distinct accident sequences that need deterministic source term analysis.

##### CET end states grouping

The end states of the containment event tree are grouped into the specified release categories. Since this involves the grouping of typically thousands of end states of the containment event tree into a small number (typically tens) of release categories, a systematic process need to be applied to this grouping process.

The grouping of the end states of the containment event tree is carried out with regard to the various factors that affect the release of radioactive material.

Each end state of the containment event tree within a particular bin is expected to have similar radiological release characteristics and off-site consequences, so that the source term analysis carried out for the group characterizes the entire set of end states within the group and reduces the amount of source term analysis that needs to be carried out.

The frequency of the release categories will be calculated by summing the frequencies of all the end states of the containment event tree that are assigned to the group. (Direct summing is not correct, instead, all of dependencies should be considered)

##### Source term analysis

Many plant design features and accident phenomena have been shown to influence the magnitude and characteristics of source terms for severe accidents. These include fixed plant design characteristics, such as configuration of the fuel and the control assembly and material composition, core power density and distribution, burn-up and concrete composition. These plant design characteristics will be the same for all the end states of the containment event tree. In addition, there are a number of factors that can vary from one accident sequence to another, including:

* The pressure of the reactor coolant system during core damage and at the time of breach of the reactor pressure vessel. More relevant for BWR;
* Availability of cooling water (in-vessel and ex-vessel);
* Depth and composition of ex-vessel core debris;
* Operation of containment safety equipment (suppression pool, sprays, ice condensers, etc.);
* Size of containment breach (i.e. leak rate);
* Location of containment failure and resulting transport pathway to the environment.

For this study plant specific source term analysis will be performed using integral code (MELCOR) to determine the magnitude and attributes of the source term for each of the release categories.

In the source term analysis, all the processes that affect the release and transport of radioactive material inside the containment and in adjacent buildings need to be modelled. This includes:

* Releases of radioactive material from the fuel during the in-vessel phase;
* Retention of radioactive material within the reactor coolant system;
* Releases of radioactive material during the ex-vessel phase;
* Retention of radioactive material inside the containment and adjacent buildings.

The analysis is carried out for a sufficient number of accident sequences in each release category, to provide confidence that the source term for the group has been accurately characterized. In practice, if the release category contains very similar accident sequences and the phenomena that drive the release have a relatively low uncertainty, it may be acceptable to carry out the source term analysis for a relatively small number of accident sequences.

Another option is to use the source term analysis from another plant where the design and features of the reference plant relating to the progression of severe accidents are sufficiently similar to the plant being analysed and the results of the deterministic analysis are available. In that case, all technical bases should be established to support the contention that the plant under study is sufficiently similar to the proposed reference plant. (as BNPP-1 is under operation for about three years, many specific data are available and should be included in LPSA instead of using similar plants data. Only, in some few cases which the BNPP-1 specific data are not available, general or similar plant data may be used for related calculation. In this cases, some expert judgement based on strong justification/hard profs may be applied)

##### Results of Source term analysis

The overall results of the source term analysis will be clearly presented and documented. The frequencies and characteristics of the source term categories will be clearly presented. The source terms and frequencies of the release categories are then used to determine the large release frequency or the large early release frequency for comparison with numerical safety criteria if they are set.

The insights gained from such a quantitative evaluation of radionuclide releases will be summarized and discussed. The results of the quantitative sensitivity analysis or uncertainty analysis will also be presented and discussed. This task is called analysis and interpretation of the results and covers all results from CET and source term analysis. (the results should include of tables of population radiation doses versus of distance and time of releases for initial (10 days) and long time (1 year) after the accident. These analysis at least should be performed for whole bode and thyroid gland)

#### Uncertainty and sensitivity analysis

##### Sources and types of uncertainties

Generally, the uncertainties arise in three areas of the PSA Level 2:

* Definition of plant damage states;
* Simulation of the problem, including event tree construction and models (computer codes) used to simulate the physical-chemical processes involved;
* Data used to feed models.

This is what classically has been considered scenario, model and data uncertainty. Nevertheless, attending to the real origin of uncertainty, these types of uncertainty may be re-classified as aleatory and epistemic or lack of knowledge uncertainty. Note that system and human reliability analysis is covered by aleatory uncertainty and severe accident events (phenomena) are usually characterized by epistemic uncertainty.

##### Sensitivity vs. uncertainty analysis

As part of this task we will identify the dominant sources of uncertainty in the analysis and will quantitatively characterize the effects of these uncertainties on the baseline (point estimate) results. This is typically accomplished using two methods:

* sensitivity analysis and
* uncertainty analysis.

Whereas sensitivity analysis is used to measure the extent to which results would change if alternative models, hypotheses or values of input parameters were selected (and thus provides an evaluation of uncertainty in respect of a particular issue or a particular group of related issues at a time), uncertainty analysis examines a range of alternative models or parameter values, assigns each model or value a probability and generates a distribution of the results, within which the baseline results represent one possible outcome. Each result within the full distribution is accompanied by a (subjective) probability representing the degree of belief in that result. Cumulative probability levels for the results can be calculated (e.g. the 5th, 50th and 95th percentiles represent 5%, 50% and 95% probabilities, respectively, and the ‘true’ result is below the respective level for which each of these probabilities is stated).

##### Uncertainty analysis process

In general, the process of quantification and propagation of uncertainties in the Level 2 PSA can be divided into four principal steps:

* Specification of the scope of the uncertainty analysis;

The sources of uncertainty in a Level 2 PSA are numerous and it is impractical to address all of them quantitatively. Experience in performing uncertainty studies for limited aspects of severe accident phenomena suggests that the effects of uncertainties from some sources are larger and more dominant than the effects of uncertainties from other sources. In an integral sense, then, the aggregate uncertainty in Level 2 PSA results can be estimated by selecting the dominant sources of uncertainty and treating them in detail.

* Characterization and/or evaluation of uncertainty issues

After the definition of the scope of the analysis, the second step is to identify the range of values of uncertain parameters. Each value within the range of values that the uncertain parameter can take on is associated with a probability, thereby creating a probability density function or probability distribution. In many cases, such density functions or probability distributions will have been determined in the assessment of probabilities for branch points in the containment event tree. Additional parameters that may also be characterized or evaluated by means of probability distributions may be, for example, source term calculation parameters not explicitly addressed in the containment event tree. Sensitivity analysis is a useful tool to guide the selection of dominant sources of uncertainty.

* Propagation of uncertainties

Examples of available propagation techniques include:

* Use of discrete probability distributions;
* Direct simulation methods based on either simple (Monte Carlo) random sampling;
* Stratified (Latin hypercube) sampling procedures.
* Display and interpretation of results

The results are usually displayed using histograms, probability density functions, cumulative distribution functions and tabular formats showing the various quantiles of the calculated uncertainties, together with the estimates of the mean and median of the probability distributions.

If a sensitivity analysis is used as a surrogate for a comprehensive uncertainty analysis, metrics should be developed to indicate the influence of alternative models or parameter values on the results of the Level 2 PSA.

#### Training

At the end of the project, one week training will be given for Client PSA involved personnel. The sessions foreseen theoretical and practical part. The stress will be put on the practical training for working with the PSA Level 2 model and MELCOR model. The main topics of training course will be:

* PSA Level 1 and Level 2 interface – explanation of the model, main assumption and practical training;
* Containment event trees model - explanation of the model, event probabilities assessment and practical training;
* MELCOR model - explanation of the model and practical training;
* Containment structural model - explanation of the model, main assumption and practical training.

The training program is subject of additional negotiation, since it is highly dependent on the skills of the trainee personnel.

### Input data and deliverables

#### Input data

For the purpose of the study it is expected that the Contracting Authority will provide:

* The safety analysis report (SAR);
* Plant Technical specification;
* System descriptions, instructions;
* List of performed plant changes, if any;
* As built (as is) system drawings (piping and instrumentation diagrams);
* Control and actuation circuit drawings for selected systems;
* Normal operating procedures, emergency procedures, test procedures and maintenance procedures;
* Severe Accident Management Guidelines;
* Emergency plan;
* Analyses pertinent to the determinants of mission success criteria of systems;
* Plant operational experience records, reports and analysis of incidents;
* Plant databases and/or the computerized management system for maintenance, if available;
* Plant specific databases for failures and defects of selected system components;
* Plant layout drawings;
* Drawings of piping location and routing;
* Drawings of cable location and routing;
* Plant walkdown reports, if available;
* Regulatory requirements;
* Requirements and regulations related to PSA specific for the country;
* Other relevant plant documents.

Based on information in the mention documentation we can ask for additional data related to various aspects of the PSA Level 1 development.

In order to systematize the input data used a common database for the project will be organized. The main attributes of this database will provide the ability to identify the document (registration and/or number in the archive database of BNPP) and the respective areas of the PSA where the information from it is used. This data base will assist in the maintenance of the model in the future.

#### Deliverables

The reports that will be prepared by the Consultant and issued officially to the EC in due course within the framework of the project activities and in accordance with the project schedule are:

* The administrative reports,
* The Technical Delivery documents,
* Other communication documents.

All reports will be written in English.

##### Administrative reports

In order to optimise work process development a monthly report will present a progress mark-up of the agreed baseline study time schedule with ‘by exception’ corrective actions for any deviations to plan and any unresolved issues. The format of the reports will follow Annex 2 of the Framework Agreement.

##### Technical delivery documents

The final technical deliverables are:

* Updated BNPP-1 PSA Level 2 in power mode report. This report or set of reports will document the assumptions of the analyses and the relevant results. It will be provided in paper and electronically; (LPSA level 2 should include shut down modes)
* Electronic copies of all relevant Risk Spectrum models, important work files and output files of the analyses;
* Short description of the accident progression and structural analysis models and all relevant output files of the results.

The objective is to ensure adequate documentation of the updated BNPP PSA Level 2 in power mode to allow review of the PSA development and its results, as well as to provide a written basis for any future uses of the updated BNPP PSA.

Draft reports will be submitted by email, final reports by email and in hardcopy.

### Software

The software to be used is given in the following Table.

| Name | Version | Application |
| --- | --- | --- |
| MELCOR | 2.2 | Deterministic part of accident progression analysis including source term analysis |
| RELAP/SCDAP\* | 3.4 | PSA L1&L2 interface. Additional definition of the CD characteristics |
| RiskSpectrum PSA | 1.3.2 | Probabilistic part of the study – PSA L1&L2 interface and CET |
| LS-DYNA | v8.1 | Non-linear static and dynamic analyses, crash simulations, explicit dynamics – containment structural analysis |
| SOLVIA\* | v3.0 | Non-linear static and dynamic analyses, implicit dynamics– containment structural analysis |
| SAP2000 | v14.2 | Linear static and dynamic analyses– containment structural analysis |
| Geo-Studio | 2012 | Linear and non-linear geotechnical analyses– containment structural analysis |

Comment: This software is optional

## Timetable of work

### Major milestones

The following table contains major milestones. The milestones are defined as date of a deliverable.

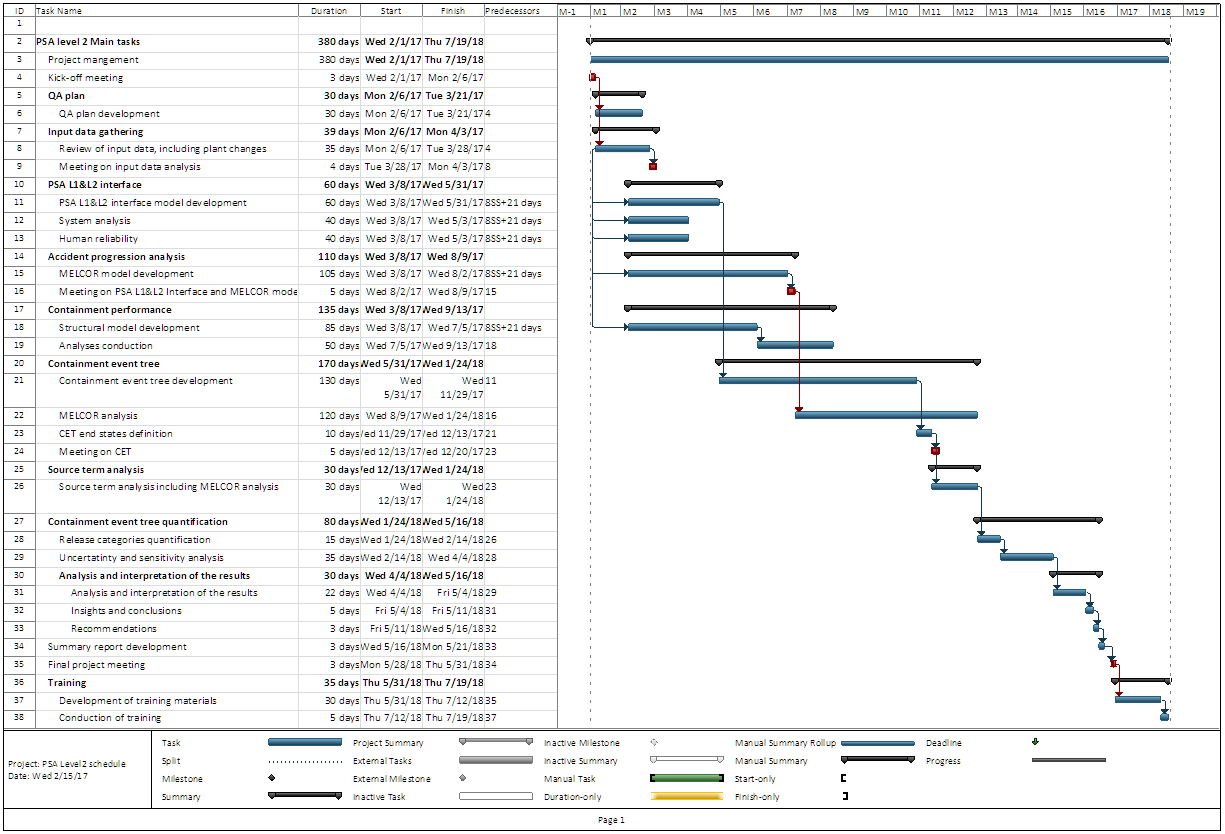
Table ‎II‑1. LPSA Level 2 project major milestones

|  |  |  |
| --- | --- | --- |
| Milestone | Cumulative time end | Comment |
| 1 | T0+20 days | Kick-off meeting |
| 2 | T0 + 1 month | Project work plan and QA plan |
| 3 | T0 + 2 months | Input data gathering and meeting |
| 4 | T0 + 7 months | Meeting on PDS and Severe accident progression model |
| 5 | T0 + 12 months | Meeting on Containment Event Tree |
| 6 | T0 + 16 months | Deliverable of Level 2 PSA report |
| \*T0 – date of commencement | | |

#### Scheduling of proposed activities

On the following page, project schedule is presented. Given dates are conditional, since they depend on the project start date. The actual schedule will be updated after contract signing. The months given in Major milestones table and in the schedule are different, since the training course is considered to be out of the study. Training course schedule will be negotiated during the project execution.

Table ‎II‑2. LPSA Level 2 Project Schedule



## Work resources

According to the presented brief information concerning the different activities the following resource could be formed expressed in man-days:

Table ‎II‑3. LPSA Level 2 work resources

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task | Human resources [Man-days] | Professional Category | | |
| Project Manager | Senior Expert (over 10 years) | Senior Expert (5 to 10 years) |
| Management | **80** | **80** |  |  |
| QA plan development | **10** |  | **10** |  |
| Review of input data, including plant changes | **80** |  | **50** | **30** |
| PSA L1&L2 Interface event tree model and quantification | **80** |  | **80** |  |
| System analysis | **100** |  | **100** |  |
| Human reliability analysis | **80** |  | **80** |  |
| MELCOR model development for reactor installation | **420** |  | **300** | **120** |
| Accident Progression analysis | **600** |  | **450** | **150** |
| Containment performance | **160** |  | **80** | **80** |
| Source term analysis | **80** |  | **50** | **30** |
| CET development | **380** |  | **380** |  |
| CET quantification | **30** |  | **30** |  |
| Uncertainty and sensitivity analysis | **140** |  | **140** |  |
| Analysis and interpretation of the results | **30** |  | **30** |  |
| PSA L2 documentation | **250** |  | **120** | **130** |
| **Total:** | | | | **2520** |
| **Total man-days in REL home office** | | | | **2420** |
| **Total man-days in Tehran/site IRI office** | | | | **100** |

Proposal does not include any travel or accommodation expenses. Proposal for training is separated as an optional activity. The human resources needed are summarized in the following table.

Table ‎II‑4. LPSA Level 2 training resources

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task | Human resources [Man-days] | Category | | |
| Project Manager | Senior Expert (over 10 years) | Senior Expert (5 to 10 years) |
| Training materials development | **45** |  | **45** |  |
| Conduction of a one week training | **15** |  | **15** |  |
| **Total:** | | | | **60** |
| **Total man-days in REL home office** | | | | **45** |
| **Total man-days in Tehran/site IRI office** | | | | **15** |

# Development of risk monitoring of Bushehr Nuclear Power Plant

## Technical part

### Background

The term Risk Monitor has been defined by IAEA as “a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the Risk Monitor reflects the current plant configuration in terms of the known status of the various systems and/ or components – for example, whether there are any components out of service for maintenance or tests. The Risk Monitor model is based on, and is consistent with, the Living PSA. It is updated with the same frequency as the Living PSA. The Risk Monitor is used by the plant staff in support of operational decisions.” The first risk monitor system was put into service in UK in 1988 and has been widely used around the world from then on. The risk monitor system is able to indicate which components withdrawn should be restored first or which components should be avoided being out of service. It can also be used to optimize maintenance schedule to eliminate the high peaks in the risk and make the on-line maintenance more frequent and flexible, thereby shorten the refueling period and save cost for plant operation. The plant configuration is generally input into the risk monitor system manually by the plant staff. However, along with the development of risk monitor system, currently a few systems have realized automatic input of the plant configuration. Risk monitor also concerns about the trade-off between calculation speed and precision. Most risk monitors are able to maintain the calculation time within 5 minutes on an acceptable precision.

In many of the countries, risk information can be used as one of the inputs to satisfying regulatory requirements in the operation of a nuclear power plant, a Living PSA is an acceptable risk model of the plant and a valid Risk Monitor model developed from the Living PSA can be used to provide the risk information as long as it can be demonstrated that the analysis is fit for purpose in each specific application.

Risk Engineering Ltd. developed risk monitoring system for units 3 and 4 of “Kozloduy” NPP. The system is based on many quantitative calculations of actual PSA Level 1 model for different unit configurations. (just for power mode?)

In 2005 Risk Engineering Ltd. developed and implemented risk monitoring system for units 5 and 6 of “Kozloduy” NPP.

### Terminology used

#### Living PSA and Risk Monitoring

**Living PSA** - “A PSA of the plant, which is updated as necessary to reflect the current design and operational features, and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysts' assumptions in the absence of such information. The Living PSA would be used by designers, utility and regulatory personnel for a variety of purposes according to their needs, such as design verification, assessment of potential changes to the plant design or operation, design of training programs and assessment of changes to the plant licensing basis."

**Risk Monitor** - "A plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the Risk Monitor reflects the current plant configuration in terms of the known status of the various systems and/ or components – for example, whether there are any components out of service for maintenance or tests. The Risk Monitor model is based on, and is consistent with, the Living PSA. It is updated with the same frequency as the Living PSA. The Risk Monitor is used by the plant staff in support of operational decisions". In the definition given above, updating the Risk Monitor refers to keeping it consistent with the Living PSA. This does not refer to providing inputs to the Risk Monitor to reflect changes in the plant configuration and environmental factors which would be done frequently. Good practice is to do this every time the plant configuration changes so that the Risk Monitor follows changes in the point-in-time risk from the plant.

#### General terms

**Plant configuration** – This relates to the state of plant systems and components which are under the control of the operators and is defined in terms of the current:

* **Component outages** – the set of equipment which has been removed from service for test or maintenance. This could include situations where equipment has a partial function (for example, during a test, automatic start may be inhibited but manual start would still be possible) or the function is recoverable.
* **Plant alignments** – the selection of running and standby trains in normally operating systems, alignment of the support systems (electric power, cooling water, etc.) and whether cross connections between trains are open or closed.
* **Activities being carried out on the plant that affect the risk** – that is, where equipment damage, failures or human errors would lead to an increase in initiating event frequencies or component failure probabilities.

**Plant operational mode** – refers to the modes of operation of a nuclear power plant that are defined in the plant documentation or Technical Specifications. For a PWR, these typically include:

* power operation,
* hot standby,
* hot shutdown,
* intermediate shutdown,
* cold shutdown, and
* various refueling modes.

**Defense-in-depth** – In the context of this report, the term defense-in-depth relates to the provision of redundant and diverse trains of the safety systems that carry out the above safety functions. This is a more restrictive use of the term than normal usage which relates to the approach to safety at nuclear power plants that is aimed at preventing initiating events from occurring and, if this fails, mitigating their potential consequence and preventing progression to a more severe condition.

**Safety functions** – the functions that need to be performed to prevent degradation of the reactor fuel in the reactor vessel. For light water reactors, the safety functions typically include:

* reactivity control,
* reactor coolant inventory control,
* reactor decay heat removal/ post trip cooling,
* emergency core cooling,
* containment control,
* electric power supply

**Integrated decision making** – the process that is used by plant operators and regulators in which information from a number of sources is combined in reaching a decision on a plant safety issue.

#### Risk Measures

**Baseline risk** – the numerical value of the risk (CDF, LERF, etc.) calculated by the PSA with all components available to carry out their safety function.

**Average risk** – normally calculated by the Living PSA for full power operation. This is the level of risk that is calculated when average maintenance unavailabilities are introduced into the model and hence it is always greater than the baseline risk.



Figure ‎III‑1. Risk measures used in PSA – average/ baseline/ point-in-time risk

**Point-in-time risk** – the level of risk that arises from a specific plant configuration and this is what is calculated by a Risk Monitor.

**Incremental CDF (LERF)** – The incremental CDF (ΔCDF) is the increase in the Core Damage Frequency from a specific plant configuration. This is equal to the CDF for the configuration minus the baseline CDF. The incremental LERF (ΔLERF) is defined in the same way.

**Incremental CDP or (LERP)** - The incremental CDP (ΔCDP) is the increase in the Core Damage Probability from a specific plant configuration. This is equal to the incremental CDF for the configuration multiplied by the time spent in the configuration. The incremental LERP (ΔLERP) is defined in the same way. Can be used in the calculation of the Allowed Configuration Time.



Figure ‎III‑2. Risk measures used in the Risk Monitor

**Cumulative risk** – The cumulative risk is the sum of the incremental risk values for all the actual plant configurations that have occurred during a period of time. The annual cumulative risk is the one that is normally quoted but the cumulative risk for other periods or for the duration of a particular outage may also be calculated. This is used by plant operators as a performance measure which indicates how effective they have been in managing the risk from the plant which arises during maintenance outages.



Figure ‎III‑3. Risk measures used in PSA – Cumulative risk

#### Allowed Outage Time and Allowed Configuration Time

The discussion of Allowed Outage Time (AOT) and Allowed Configuration Time (ACT) given below relates to the maximum time for which a component/ train unavailability or a plant configuration is allowed to persist before some action has to be taken to move the plant to a safer state – for example, by returning items of equipment to service or by shutting the plant down.

**Allowed Outage time –** The AOTs for components and system trains are the times given in the plant Technical Specifications for typical/bounding plant configurations and are mandatory requirements that need to be met by the plant operators. These requirements have traditionally been based on deterministic criteria but now are often based in part on risk information obtained from the Living PSA.

**Allowed Configuration time** – In addition to the requirements given in the Technical Specifications, the time for which an actual plant configuration is allowed by plant procedures to persist is calculated and displayed by many Risk Monitors. This is sometimes referred to as an AOT and sometimes as an ACT depending on the Risk Monitor software used. In this report, the term Allowed Configuration Time is preferred and the term Allowed Outage Time is reserved for the mandatory requirements given in the plant Technical Specifications.

ACTs are calculated by comparing the incremental Core Damage/Large Early Release Probability or the incremental risk for the current plant configuration to a target value. Where the Risk Monitor addresses both CDF and LERF, ACTs based on both would be calculated and the shorter of the two times would usually be displayed.

#### Terms related to Living PSA and the Risk Monitor PSA model

**Plant Operational State**

The usual practice when developing a PSA model for the entire cycle of plant operation is to break it up into a number of Plant Operational States (POSs). Plant Operational States are typically defined so that the PSA can account for changes in safety system success criteria, differences in the initiating events that can occur and system modeling issues such as maintenance, alignment, operating configuration and human error probabilities that occur during the plant operating cycle. These arise due to changes in the decay heat removal system being used, the reactor decay heat level, coolant circuit temperature and pressure, coolant circuit status, on-going maintenance activities, etc. A distinct PSA model is usually developed for each of the Plant Operational States.

**Top Logic Model**

One of the basic requirements for a Risk Monitor is that it should be able to produce a result in a very short time - typically within 1 or 2 minutes, which is generally very much shorter than that achieved by the Living PSA. In the past, it was not possible to do this using a PSA logic model that is based on event trees/ fault trees and this PSA model needed to be converted into a fault tree that is logically equivalent. This large fault tree, which is referred to as a Top Logic model, was then optimized to further reduce the solution time.

**Support State Model**

A support state model (sometimes referred to as a linked event tree model) uses an approach in which one or more event trees is used to construct and evaluate the plant model including the representation of hardware and human error dependencies between systems. The support state approach can be contrasted with the fault tree method of risk analysis in which the entire plant model is represented by a set of linked fault trees instead of event trees. A number of split fraction values are required for each top event which are used according to a pre-defined split fraction logic and event tree structure to calculate the frequency of each accident sequence in the model. Since split fractions are constructed so as to be mutually independent, sequence frequencies can be determined by a simple product of their associated split fractions.

**Dynamic Events**

In the Risk Monitor PSA model, there are a number of initiating event frequencies and basic event probabilities that would change depending on plant conditions. The reasons why this might happen include changes in the:

* **Operational activities** – activities such as switchyard maintenance, reactor protection system testing, etc. could lead to an increase in the frequency of particular initiating events;
* **Decay heat level** – as the decay heat level reduces, the time available for the plant operators to carry out recovery actions would increase so that the human error probabilities would generally be lower;
* **Configuration of the plant** – the removal of trains of a systems from service would lead to an increase in the common cause failure probability due to the reduction in the level of redundancy and the removal of instrumentation from service would lead to an increase in the human error probabilities due to failure to diagnose the fault (where these increases would depend on the modeling approach adopted and the reason for the unavailability)

**Plant environmental factors** – the frequency of initiating events such as loss of off-site power would be expected to be higher during adverse weather conditions.

#### Maintenance Rule

The US NRC Maintenance Rule requires plants to assess the risk prior to entering a planned maintenance configuration and immediately after entering a non-voluntary configuration. This requirement applies to all the Plant Operational Modes.

#### Comparison between Living PSA and Risk Monitor

For the Living PSA, the key issues are that it is:

* Updated as necessary so that it reflects the current design and operation of the plant, is based on the most up to date analysis (thermal-hydraulic analysis, severe accident analysis, etc.) of how the plant behaves in fault conditions, uses data derived from plant operating experience where this is available and takes account of improvements made in PSA modeling techniques.
* Fully documented so that the analysis can be traced back to plant design information and the assumptions made in carrying out the analysis. This suite of documentation needs to be in a form that can be easily updated as the Living PSA is updated.
* Can be used by designers, utility and regulatory personnel and can be used for a variety of purposes.

Some applications require the PSA to be used on-line and for it to provide a more rapid indication of how the risk is changing as the plant configuration and the environmental factors change. This requirement can be satisfied by using a special tool called a Risk Monitor (or sometimes a Safety Monitor). For a Risk Monitor, the key issues are that it:

* Is used on-line as compared to the Living PSA which is used off-line.
* Provides an estimate of the point-in-time risk from the plant as compared to the Living PSA which provides an estimate of the average risk over all Plant Operational States and configurations.
* Reflects the current plant configuration as compared to the Living PSA which averages over all plant configurations.
* Is based on and is consistent with the Living PSA in that the safety system success criteria and much of the data used are the same. Hence, the Risk Monitor needs to be updated with the same frequency and in a manner consistent with the updating of the Living PSA model.
* Can be used by all plant staff (and utility and regulatory staff where they have access to it) in support of operational decisions rather than by PSA specialists only.

Updating the Risk Monitor refers to keeping it consistent with the Living PSA. Good practice is to do this every time the plant configuration changes so that the Risk Monitor follows changes in the point-in-time risk from the plant. (in deed, it’s better the Risk Monitor be sensitive to changes rather than recalculation of the model based on fixed setting time. This recomendation needs additional issues which should be considered intelligently)

### Advantages of Risk Monitoring

Basic advantages of Risk Monitoring could be summarized as follows:

**Configuration Control**

As a rule, control of configuration is laid down by deterministic rules given in technical specification of the plant, the rules being formulated in order to guarantee that servicing out is being monitored in a way that assure certain level of redundancy, variety, etc. of safety systems.

The up-to-date tendency leads towards making a complete decision using information provided by Risk Monitoring in order to guarantee that events and durations of plant configuration are being controlled in such a manner that both instant and accumulated risks are below prescribed levels. An example of such approach is Configuration Risk Management Program incorporated in the US by the NRC as decisions are to be taken based on information about risk.

**Control of safety functions**

Level of protection in depth for each of those safety functions is used as a basis for measures for quantitative assessment of risks as shown in many of implementations if Risk Monitoring.

**Integral time for decision making**

It allows determination if respective deterministic requirements such as defense-in-depth, limits of safety, etc. are met and if plant risk is being understood, managed, and maintained in prescribed allowable limits. Up-to-date systems for safety monitoring provide for the following:

* Capabilities for analysis of all levels of operation;
* Capabilities of planning of repair activities;
* Automated exchange of data with plant computer system and planning activities for repairing and servicing out of equipment;
* Capabilities of accounting for results of Level 2 PSA;
* Capabilities of recovery and storage of data for plant status for past periods;
* Capabilities for application of basic recovery actions by the operator;
* Capabilities for storage of data for equipment unavailability.

Basic information obtained from the system for safety monitoring could be summarized as follows:

* Current core damage frequency and cumulative probability for core damage for one year;
* System status;
* Review of reactor core damage frequency for a past period;
* Recommended time for maintaining of a given configuration in order to preserve core damage frequency in prescribed limits of objective indicators;
* Significance of currently available equipment;
* Risk profile for a given schedule of repairing activities and integral assessment of probability of core damage under a schedule.

### Purpose and scope

The present technical proposal is submitted by Risk Engineering Ltd. for development of risk monitoring of Bushehr Nuclear Power Plant.

The scope of Risk Monitoring development concerns operation of unit at full power, lower power and shutdown reactor. The scope of incorporation of external events (fires, floods, seismicity) will be further determined. (LERF should be monitored. In addition, time to boiling in the reactor in shutdown modes, where the reactor is opened, should be monitored)

### Engineering activities on development LPSA into Risk Monitor

#### Review of the suitability

The aim of the quantitative risk measures in a Risk Monitor is to provide a calculation of the point-in-time risk (typically the CDF, LERF or the frequency of boiling in shutdown conditions) when required by any of the users. The Risk Monitor will also determine how this changes as a function of the plant configuration, environment and the activities being carried out. To do this accurately, the Risk Monitor needs more information on the state of the plant than is used in the Living PSA and requires a different treatment of maintenance and system alignment. Hence, the Living PSA model cannot generally be used directly for a Risk Monitor application and changes need to be made. These changes are in addition to the typical conversion of the event tree/ fault tree model into the Top Logic fault tree model required by some Risk Monitors.

The basis for the PSA model used in the Risk Monitor is the Living PSA which reflects the current design and operation of the plant and is of a quality that is suitable to support PSA applications. This is particularly important when the plant is being upgraded, perhaps as part of a Periodic Safety Review. The PSA model that is produced is then suitable for use in risk-informed decision making including:

* The identification of the dominant contributions to the risk,
* The identification of areas where improvements could be made in the design and operation of the plant;
* The estimation of the change in the risk from any improvements,
* The prioritisation of design and operational issues.

It is good practice for the Risk Monitor to be developed from a PSA that is being maintained as a Living PSA. The Living PSA can also be used as an input into the development of risk-informed Technical Specifications, accident precursor analysis, etc.

The Living PSA, from which the Risk Monitor model is developed, is used to provide an estimate of the annual average risk and insights into the contributors to the risk. This information can be used to identify areas where improvements could be made to the design and operation of the plant. However, the aim of the Risk Monitor PSA model is to provide estimates of the point-in-time risk for a wide variety of plant conditions which include the different modes of operation of the plant (full power, low power and shutdown modes) and the actual plant configuration which includes the combinations of components removed from service, the selection of running and standby trains on normally operating systems, whether cross connections between trains are open or closed, the activities being carried out which affect the risk, etc. These configurations may lead to short term point-in-time risks that are much higher than the annual average risks estimated by the Living PSA.

In view of this, some of the assumptions made in the Living PSA may not be valid for the Risk Monitor application.

In addition, the Living PSA may not have taken credit for some of the plant features such as the interconnections between trains of electrical and cooling water systems since they were not significant with respect to the annual average risk. However, they may be much more important for the Risk Monitor which aims to model the actual configuration of the plant. Interconnections can become much more important when they are either used, or if they back up a system which is placed in maintenance.

The plant systems and safety functions must be modeled in more detail in a Risk Monitor model. If assumptions have been made with respect to running and standby trains of multitrain systems, these have to be revised to ensure that all trains of all important systems are fully modeled. Important system alignments can easily be determined by comparing component importance measures, or comparing risk increases for each of the trains out of service. (in general, component importance measures don’t determine aligned important systems. For doing this, grouping of basic events relevant to its related system should be done and importance analysis should be completed for systems)

The overall requirement of the PSA that is used as the basis for a Risk Monitor application is that it should be of a suitable quality for this application. In addition, it is good practice that the PSA is maintained as a Living PSA so that it is updated to take account of changes in the design and operation of the plant, new transient analysis which changes the success criteria used in the PSA, now data obtained from plant operating experience, etc. However, there may still be features of the Living PSA that will limit its direct use in a Risk Monitor. Some of the features of a Living PSA that have been modeled to identify weaknesses in the design and operation of a nuclear power plant may not be suitable for a Risk Monitor application. These features are listed below:

* Limitations in the Living PSA model:
* limitations in the range of initiating events included in the Living PSA model,
* limitations in the Plant Operational Modes addressed in the Living PSA model,
* limitations in the Level of PSA carried out (for example, Level 1 PSA only),
* Approach used for the Living PSA;
* Limits of applicability of the Risk Monitor;
* Calculation of the point-in-time risk.

##### Limitations in the Plant Operational Modes (Living PSA model)

There are often limitations in the Plant Operational Modes included in the Living PSA model, which will need to be recognized when it is used as a basis for a Risk Monitor. Common limitations are discussed below.

*Limitations in the range of initiating events included in the Living PSA model*

The approach often adopted for the development of the Living PSA is to address internal initiating events (transients and LOCAs) initially. The scope of the PSA may subsequently be expanded to include internal hazards (fire and flood internal to the plant) and external hazards (earthquake and extreme environmental conditions). It is often the case that the Living PSA that is used for the Risk Monitor application does not include some of the initiating events that could make a contribution to the risk. If the scope of the Living PSA is limited, it needs to be recognized that the insights provided by the Risk Monitor relate to the limited set of initiating events included. It is also common to combine like initiating events, based on plant response. However, plant response and the resulting risk results can be significantly different when the plant configuration differs from that assumed in the Living PSA.

*Limitations in the modes of operation addressed by the Living PSA*

In producing a Living PSA, it is often the case that the initial analysis is carried out for full power operation only. This may subsequently be expanded to cover low power and shutdown conditions. The Risk Monitor will only provide information for the modes of operation included in the Living PSA.

*Level of PSA carried out*

The Living PSA that has been carried out may only be a Level 1 PSA to determine the average CDF. This will address the safety systems that are incorporated to prevent core damage following an initiating event. However, this PSA will not address the role of the containment systems in mitigating the effects of a severe accident and this will require the PSA to be extended to a Level 2 analysis. Alternatively, the containment systems could be addressed using qualitative risk measures. (the realted method should be described explicitly)

##### Approach used for the Living PSA

There is a wide variety of different approaches which have been used for carrying out a Living PSA and a large number of software packages which have been applied. The most usual approach nowadays is to use a combination of event trees and fault trees - small event trees/ large fault trees or large event trees/ small fault trees. However, there are also examples of where the analysis has been done using event trees only or fault trees only. In principle, it is possible to convert a PSA developed under any of these approaches for use as a Risk Monitor. Conversion requirements can depend on the Risk Monitor software requirements, and whether the risk results are to be solved in real time or pre-solved.

##### Limits of applicability of the Risk Monitor

Even with an accurate and complete Living PSA model conversion and expansion, limitations of Risk Monitor software need to be considered in the assessment of risk for each plant configuration. Limitations can also result from software features not fully utilized or developed.

All Risk Monitors require the development of an interpretation database. This database includes development of relationships between the naming system used for plant components and the naming system used for basic events in the Living PSA. A plant component taken out of service would result in the corresponding basic event in the PSA being set to TRUE. A plant alignment may result in a set of house events set to true or false. A plant test may result in an initiating event increasing by a set factor. Development of these interpretation databases is one of the most time consuming steps in the development of a Risk Monitor model. It also introduces some limitations in that the risk results are only as accurate as the model interface developed by the PSA analysts.

Development of these interface databases is the main limitation for any Risk Monitor. The various Risk Monitor software products support the interface database development in different ways that affects the overall implementation at a given plant.

##### Calculation of the point-in-time risk

In order for the annual cumulative risk to be calculated by summation of individual risk contributions, the initiating event frequencies need to be calculated on the basis that the existing configuration would continue for a whole year. It is common to include weighting factors in the Living PSA which adjust each initiating event for the fraction of a year the plant would remain at full power (or in other operational states). If such weighting factors are included in the Living PSA, adjustments are needed for use of the Living PSA model in the Risk Monitor.

The Living PSA models should be reviewed for any average or assumed conditions in the model to ensure an accurate point-in-time risk is calculated for all configurations during the year. One specific aspect of this is the inclusion of basic events to model maintenance outages and there is a need to remove them for the Risk Monitor PSA model.

#### Removal of simplifications from the Living PSA

Simplifications may have been made in the Living PSA to reduce the amount of detailed analysis required. In this context, such simplifications are acceptable for many Living PSA applications if it can be shown that they lead to a conservative estimate of the risk or that their contribution to the risk would be negligible. For example, the Living PSA may not take credit for some of the safety systems that provide protection for initiating events that already make a small contribution to the average risk and initiating events may be screened out of the Living PSA if it can be shown that they lead to a negligible contribution to the average risk.

These simplifications will usually need to be removed if there is potential that they could lead to the Risk Monitor giving incorrect results for some of the plant configurations that could arise. Typical simplifications that need to be removed from the Living PSA model.

In converting the Living PSA for a Risk Monitor application, the concern that needs to be addressed is whether the Living PSA model will provide accurate estimates of the risk for all the plant configurations that could arise. If this is not the case, changes need to be made to the Living PSA. The degree to which this will need to be done depends on the intended applications of the Risk Monitor. If it is to be used as a tool for basic configuration control, the need to make some of the changes identified below might be less important than if it is to be used for a wider range of applications such as providing an input into risk-informed Technical Specifications or Allowed Outage Times.

Typical simplifications made in the PSA are:

* Lumped initiating event;
* System alignments;
* Systems not included in the Living PSA (included as undeveloped events or as very simplified fault tree models);
* initiating events screened out of the Living PSA;
* Maintenance modelling (maintenance is often modelled by including basic events which represent component outages for maintenance with a probability equal to the fraction of time that it is removed from service.); (should be applied some models which has more detail rather than using of incorporate of house event for any components?)
* Modelling running/ standby trains;
* Modular and undeveloped events;
* Support state model specific issues. (description is needed)

All this simplifications should be revised and resolved in the risk monitor.

#### Carrying out enhancements to the Living PSA model

Simplified models may have been used for some aspects of the Living PSA where they are not considered to be significant in determining the average risk from the plant. These simplified models may not be suitable for a Risk Monitor application and they may need to be replaced by a more detailed model which reflects the variations in the plant configuration.

Typical areas where enhancements need to be made to the Living PSA model are:

* the common cause failure (CCF) modelling in the Living PSA may need to be improved so that it is able to take account of the reduction in redundancy when components are removed from service for maintenance and when failures have been identified;
* the human reliability model in the Living PSA may need to be improved to take account of the potential for human errors during the various plant configurations;
* dynamic events may need to be incorporated to model changes in initiating event frequencies and basic event probabilities which arise due to changes in the plant environment;
* the modelling of initiating events which involve failures in support systems may need to be improved to take account of the actual failures which lead to the initiating event;
* automated recovery may need to be included for the Risk Monitor PSA model.

#### Dealing with software incompatibilities

The software to be used for the Risk Monitor may have different capabilities from that used for the Living PSA. In particular, the two software packages may handle NOT logic differently and may have different ways of handling house events that change value during event sequences. In addition, the Risk Monitor may require the event tree/ fault tree model developed in the Living PSA to be replaced by a large fault tree model (referred to as a Top Logic model). The conversion process from the Living PSA to the Risk Monitor needs to address any incompatibilities which could arise.

#### Development of the Risk Monitor databases

Each Risk Monitor application includes a series of data tables or files which need to be developed in order to use the converted PSA model in the quantitative risk solution portion of the Risk Monitor. Some of the tables are optional, and represent features of the software that may or may not be used. However, most of the tables need to be completed for the Risk Monitor to function accurately.

PSA related database tables and files will be developed. This includes basic event probabilities, basic event descriptions, etc. Most Risk Monitor programs complete these tables automatically when the PSA model and data are imported. However, each program requires some manipulation in order to use the Risk Monitor.

The majority of plant personnel who use the Risk Monitor are not familiar with PSA terminology or the shorthand naming schemes used to identify the basic events in the PSA model which represent the component failures. Risk Monitors typically use plant notation for inputting the components that are out of service, choosing system alignments, etc. This plant notation needs to be developed and inserted into the various tables.

In addition, the other tables in the plant database need to be completed. This includes plant description information, system and train designation, alignments, environmental factors, testing, Functional Equipment Groups.

As the Risk Monitor is providing measures of risk for the current plant configuration it is necessary to provide tables which relate all the information input by the user to make the necessary modifications to the basic PSA model.

Some of these tables require supporting calculations, while others do not.

#### Validation of the Risk Monitor models

##### Validation of the PSA model in the Risk Monitor

The last step in the development or update to a Risk Monitor model is the validation process. This process is performed to ensure that the quantitative results given by the Risk Monitor are accurate and the same as (or equivalent to) those given by the Living PSA. This validation process needs to validate all of the previous quality checks, such as review of the Top Logic model development, review of the plant-to-PSA cross-reference database, rule-based recovery file development, new model logic added for system alignments, etc. Without the validation process, it is likely that errors in the model and databases will be present.

The validation process needs to start with both the Living PSA and the Risk Monitor set in a “no maintenance” condition. Then all subsequent cases would accurately verify the Risk Monitor as it will be used. The main steps of a thorough validation process would be along the lines of the following:

* Check that the PSA cut-sets are reproduced when the Risk Monitor is set to the configuration assumed in the Living PSA. This baseline cut-set comparison needs to be performed for the first 500 to 1000 cut-sets. This Risk Monitor solution should include maintenance events as modelled in the Living PSA.
* Check that the PSA results, obtained by solving the model with one or more components in maintenance (basic events set to true), are reproduced by the Risk Monitor. This should be performed for numerous cases, with the cut-set review being performed for at least the first 200-500 cut-sets.
* Check that the Risk Monitor results are valid for alignments not originally included in the PSA. If the PSA model was also modified to include the alignments, the Risk Monitor and PSA results can be directly compared.
* Check that the Risk Monitor results are valid for dynamic events not originally included in the PSA. The validation should include a review of all types of dynamic events.
* Check cut-off. A series of runs should be conducted for a range of cut-offs with all equipment available and the precision of the results compared with the base case for the Living PSA.

##### Validation of the qualitative risk models in the Risk Monitor

In order to build the logic for the qualitative measures all the information is documented in a calculation note. This should include tables showing which combinations inputs provide the various risk levels for each function modelled. The validation process is performed by setting each of the inputs and confirming that the appropriate risk level is displayed.

#### Documentation

Whole process of risk monitoring development will be described in details in manner that meets regulatory and contractor requirements.

#### Training

Training course will be performed to introduce risk monitor software and risk monitor model to the Client. The proposal is for a one week training course, where training will be divided into theoretical and practical part.

### Input data and deliverables

#### Input data

The input data required to develop Risk Monitor is as follows:

* Actual PSA model;
* Plant Technical specification;
* System descriptions, instructions;
* Normal operating procedures, emergency procedures, test procedures and maintenance procedures;
* Plant databases and/or the computerized management system for maintenance, if available;
* Regulatory requirements.

#### Deliverables

The reports that will be prepared by the Consultant in accordance with the project schedule are:

* The administrative reports;
* The Technical Delivery documents;
* Other communication documents.

Reports produced in this study will be written in English.

##### Administrative reports

In order to optimize work process development a monthly report will present a progress mark-up of the agreed baseline study time schedule with ‘by exception’ corrective actions for any deviations to plan and any unresolved issues.

##### Technical Delivery documents

The final technical deliverables are:

* Electronic copy final BNPP Risk Monitor model;
* Electronic and hard copy of reports describing Risk Monitor development process;
* Electronic copies of all relevant PSA models, important work files and output files of the analyses.

The objective is to ensure adequate documentation of the updated BNPP PSA Level 1 in power mode to allow review of the PSA development and its results, as well as to provide a written basis for any future uses of the updated BNPP PSA. (it’s just a copy paste from PSA level 1, more attention is needed)

Draft reports will be submitted by email, final reports by email and in hardcopy.

### Risk monitoring software

Risk Monitor software is significantly different from the software that is used for the Living PSA. The essential difference is that the Risk Monitor is designed to be used by all nuclear power plant personnel as compared to the Living PSA which is expected to be used by PSA specialists only. The software is designed for use by operations and maintenance staff so that it should not depend on the user having any specialist knowledge of fault and event tree modeling or any of the other techniques used in the development of the PSA model. At many nuclear power plants, the Risk Monitor is on the plant computer and available to all plant personnel.

The Risk Monitor software will provide quantitative risk information relating to the level of risk – that is, CDF, LERF and ACT, and qualitative risk information relating to any deterministic requirement – for example, the level of availability of equipment to carry out safety functions and provide protection for plant transients, meet the requirements set out in the plant Technical Specifications or address any other deterministic criteria.

Risk Monitor software can address the following time frames:

* the past – to maintain a log of how the plant configuration has changed with time, provide risk profiles and calculate the cumulative risk;
* the present – to indicate the current plant configuration, calculate the level of risk and the ACT, give restoration advice, and evaluate the qualitative measures of risk;
* the future – to provide answers to “what if?” questions on how the risk would change if changes are made to the plant configuration, and to carry out maintenance planning for a number of activities carried out over a period of time.

The Risk Monitor software can be used on-line for the present timeframe, and off-line for the past and future timeframes.

The latest version of RiskSpectrum, RiskWatcher version 1.37, released in August 2016 will be used to develop Risk Monitor for BNPP.

## Timetable of the work

In the discussion of timetable and costs given below, it has been assumed that the starting point is a PSA that has been carried out to a standard that is suitable for a Risk Monitor application and is being maintained as a Living PSA regardless of its use in a Risk Monitor. (there is no any cost)

### Major milestones

The table below contains major milestones of the risk monitor development. The milestones are defined as date of deliverable.

Table ‎III‑1. Risk Monitor project major milestones

|  |  |  |
| --- | --- | --- |
| Milestone | Cumulative time end | Comment |
| 1 | T0 + 15 days | Kick-off meeting |
| 2 | T0 + 20 days | QA and work plan developing |
| 3 | T0 + 1.5 months | Meeting on input data gathering |
| 4 | T0 + 13 months | Validation of Risk Monitor model |
| 5 | T0 + 14 months | Final meeting |
| 6 | T0 + 16 months | Training conduction |
| \*T0 – date of commencement | | |

### Scheduling of proposed activities

On the following page, we present a project schedule based on the assumption that the project would start after PSA actualization.

Table ‎III‑2. Risk Monitor project schedule



## Work resources

According to the presented brief information concerning the different activities the following resource could be formed expressed in man-days:

Table ‎III‑3. Risk Monitor work resources

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task | Human resources [Man-days] | Professional Category | | |
| Project Manager | Senior Expert (over 10 years) | Senior Expert (5 to 10 years) |
| Project management | 60 | 1 |  |  |
| QA and work plan development | 10 |  | 10 |  |
| Gathering and review of the input data | 30 |  | 30 |  |
| LPSA conversion | 225 |  | 225 |  |
| LPSA enhancements | 280 |  | 280 |  |
| QA and validation of Risk Monitor model | 70 |  | 70 |  |
| Documentation | 60 |  | 60 |  |
| **Total man-days:** | | | | **735** |
| **Total man-days in REL home office** | | | | **700** |
| **Total man-days in Tehran/site IRI office** | | | | **35** |

Proposal does not include any travel or accommodation expenses. Proposal for training is separated as an optional activity. The human resources needed are summarized in the following table.

Table ‎III‑4. Risk Monitor training resources

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task | Human resources [Man-days] | Category | | |
| Project Manager | Senior Expert (over 10 years) | Senior Expert (5 to 10 years) |
| Training materials development | **40** |  | **40** |  |
| Conduction of a one week training | **10** |  | **10** |  |
| **Total:** | | | | **50** |
| **Total man-days in REL home office** | | | | **40** |
| **Total man-days in Tehran/site IRI office** | | | | **10** |

General Comments:

1. As the BNPP-1 LPSA (include of level 1 , 2 in power and shutdown modes) is a big project which need of much time to complete and because of our limited time, it is recommended to divide the project in to two main phases. In the first phase, data updating in current models is the most concern (by using of bayesian method and incorporating of general, specific design and operation data). Some crucial modification in these models is inevitable. In the next phase, other deterministic calculation (mostly in thermo-hydraulic analysis or HRA) can be accomplished properly. This approach (division of the project in to two main phases) may be a recommendation and need to be negotiated.
2. As we have bought the RiskSpectrum version 1.3 recently and by attention to current experiences in TAVANA company, there’s enough resources to cooperate with your company in performing BNPP LPSA project, more especially in Level 1 (in power and shutdown modes). Indeed, many related tasks can be done in TAVANA office in Tehran and be checked by Risk Engineering group and as a consequence be corrected if necessary. This issue is needed to be negotiated thoroughly (areas of cooperation and the way of its implementation)
3. BNPP has its PSA models and documents (Level 1, 2 in power and shutdown modes) which can be submitted to you by contract condition. So, development of relative model from the scratch is not needed. Instead modification in current model can be applied during the project. Therefore the man-day can be modified in your proposal.
4. Bayesain approach should be applied in BNPP PSA data analysis. General, specific design and operation data should be included in the analysis.
5. Unfortunately in the proposal, shutdown modes are neglected in section PSA level 2. It should be revised and additional tasks be added to the proposal.
6. HRA should be performed for BNPP Iranian/current operators/personnel. As you know, LPSA refers to current situation of the plant and using of general/similar plant data is prohibited in this stage.
7. Expert judgment is only accepted if there is not enough input data for related calculation. As you know, BNPP is under operation for about three years and so has many specific data which are documented properly. Moreover the expert judgement should be based on similar plants experiences.
8. In the end of each main three section (PSA level 1, 2 and Risk Monitoring in power and shutdown modes) of the proposal, its related application should be mentioned and short description of how they are been met should be noted explicitly. For example, optimization of maintenance plan, using of PSA result as one of major input in risk based decision making process, should be described properly.
9. Although BNPP is under operation for about three years, but on the other hand many of your requested data as an input data are not available now. Some of them such as “plant specific database for failure and defects” are being gathered by TAVANA, but some of them such as “plant walkdown report” are not available at all. In this case the following data are not available now and should be prepared:

* Analyses pertinent to the determinants of mission success criteria of systems;
* Plant databases and/or the computerized management system for maintenance;
* Plant specific databases for failures and defects of selected system components;
* Plant walkdown reports;
* Requirements and regulations related to PSA specific for the country;

1. The proposal doesn’t include any cost approximation.
2. More attention should be paid in preparing of the official proposal. In some cases, just a copy and paste is done regardless of the issue which is being discussed. Moreover repeated issues in some cases have no role in proposal completion.
3. As you’ve mentioned in each of three section of the proposal, training program is subject of additional negotiation and may be divided in two basic and advanced step during and at the end of the project.