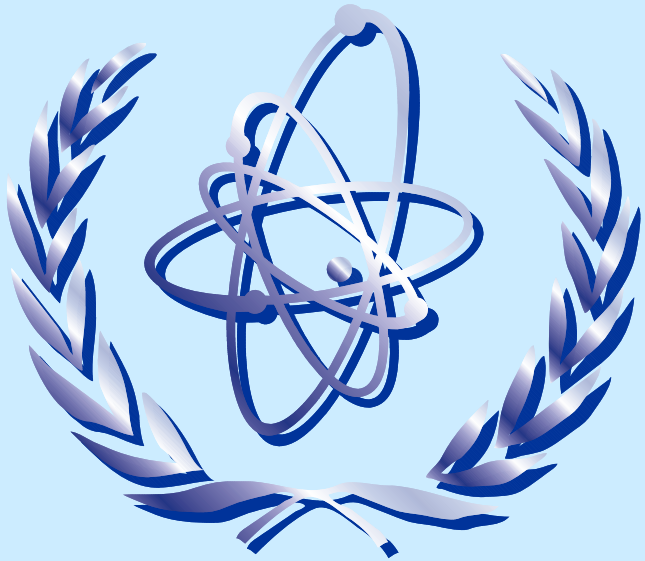
PSA Project



Regulatory review of Level 1 PSA

Content

- Overview
- Approach to the review
- Major PSA areas to be covered
  - Review of scope and objectives
  - Assessment of documentation
  - PSA tasks
  - Audit of the PSA QA
- References

Overview

Probabilistic Safety Assessment (PSA) has reached the point were it strongly affects design, construction, operation and regulatory decisions and therefore it exists an international consensus today that an intensive, thorough peer review by independent and experienced PSA practitioners should be an integral part of any PSA programme for Nuclear Power Plants.

Overview (cont.)

- It is important to recognise that, with the growing importance of PSAs in a risk-informed environment, involvement of the regulatory authority in the review and re-assessment is extremely important. The ability to have an independent review provides a degree of assurance of the scope, validity and limitations of the PSA, as well as providing better understanding of the plant itself.
- Additionally, the specific applications being looked at (e.g. optimisation of technical specifications, relaxation of specific requirements, etc.) will require the regulatory authority to have a high degree of confidence in the PSA.

Overview (cont.)

- **The increasing use of PSAs has led to the realisation that the production and use of a PSA requires substantial efforts by both the utility and the regulatory authority to carry out and review them.**

- **Inherent in the production and review of a PSA is the ability of those involved to determine what is acceptable. As industry further develops the use of PSA in justifying plant changes and modifications, the regulatory authority and other agencies need to understand how the PSA has been produced in order to be able to assess its applicability in the decision–making process. The review process becomes an extremely important phase in determining the acceptability since this provides a degree of assurance of the scope, validity and limitations of the PSA.**

Approach to the review

- **Timing of the Review - on/off line reviews**
- **Extent of the Review - extensive/limited reviews**
- **Documentation required for the review: plant description consistent with the PSA freeze date, PSA methods reference to supporting literature; supporting analyses; tables, figures and appendices**
- **Setting up the review team**

Approach to the review (cont.)

- Identification of/focus on important areas
- Comparison with other PSAs
- Reworking of the analysis by the regulatory authority
- Research
- Documentation of the review findings
- Interactions with the utility
- Audit of the PSA QA
- Development of regulatory principles for the review of the PSA

Major PSA areas to be covered

- Review of scope and objectives
- Assessment of documentation
- Identification and grouping of initiating events
- Accident sequence analysis
- System analysis
- Analysis of passive systems, components and structures
- Analysis of computer-based systems
- Analysis of dependent failures

Major PSA areas to be covered (cont.)

- Human reliability assessment
- Initiator and component data analysis
- Quantification of accident sequences
- External event analyses
- Sensitivity Analysis, Uncertainty Analysis and Importance Analysis
- Review of Interpretation of Results
- Audit of the PSA QA

Review of scope and objectives

- **The review should verify whether the scope and objectives of the PSA are indeed corresponding to what had been agreed initially.**

- **The review should check whether the PSA covers all plant operating modes in consideration and whether the degree of distinction between the different operating modes does correspond to the objectives of the study.**

- **A third aspect to be verified is the scope concerning some methodological aspects known to be important in PSA.**

Assessment of documentation

The reviewer should checked that:

- **the information used by the PSA performer as input for the plant modelling is clearly documented (system descriptions, T&M procedures, accident procedures);**
- **the methodology used for performing the different tasks of the PSA (event tree construction, fault tree structure, HRA, …) is adequately documented;**
- **all supporting analyses (e.g. thermal-hydraulic analyses for justifying system success criteria) are adequately referenced;**

Assessment of documentation (cont.)

- if these analyses are not included in the PSA documentation, they are available at the offices of the PSA performer for consultation by the reviewer;
- adequate reference to supporting literature is provided;
- all tables, figures and appendices are in place;
- others (see Appendix VIII of IAEA SS No. 50-P-4).

Identification and grouping of initiating events

- The reviewer should check that a systematic procedure was used for identification and inclusion of the major types of initiating events in the PSA study.

- The PSA should identify the different sizes and locations of LOCAs. The reviewer should pay particular attention to the locations of the initiating events, not only for interfacing LOCAs, but also for LOCAs in the reactor coolant system piping. For the latter ones, success criteria can differ (for the same size) depending on the location

Identification and grouping of initiating events (cont.)

- **For transient initiating events, the PSA should identify the basis for choosing an initial set of transients which is as complete as possible. The reviewer should check that the transient reference source is compatible with standard sources of transient definitions. The selected transients for the plant should be grouped according to the systems required to respond to the transient.**

Identification and grouping of initiating events (cont.)

The reviewer should pay specific attention to the plant specific features that need to be reflected in the assessment of initiating events. Typical examples of initiating events for PWRs, which depend on specific plant features, are given below:

- **Interfacing systems loss of coolant initiating events**
- **Steam generator tube ruptures**
- **Loss of secondary cooling through loss of feedwater, loss of condenser vacuum**
- **Presence of particular systems which are not present in plants of the same type (e.g. their spurious operation should be considered)**
- **Loss of the ultimate heat sink**

Identification and grouping of initiating events (cont.)

- The reviewer should verify that the basis for events grouping is correct. He/she should assure that the success criteria used for any group are the most stringent criteria of all the individual events in this group.
- Two final checks which can be performed by the reviewer to ensure completeness and accuracy are the following:
  - to verify that, in any case, all initiating events considered in the Safety Analysis Report are also considered in the PSA;
  - to compare the final list of initiating events and their grouping with the one found in PSAs of similar plants

Accident Sequence Analysis

Specific points to be reviewed in the detailed event trees are as follows:

- **Criteria for what constitutes core damage and to identify sequences as causing core damage;**
- **Detailed descriptions of the event trees and their associated assumptions;**
- **Success criteria for the systems required in each event tree; Realistic success criteria** (rather than conservative ones as in the SAR) **should be used. They should be justified by appropriate thermal-hydraulic analyses.**

Accident Sequence Analysis (cont.)

- If plant specific accident and transient analyses have been performed the following should be well referenced and documented: origin and version of the computer codes used; methods, models and users qualification; sources of primary plant data; input data; basic assumptions. Results from these analyses further used in the PSA study should be well identified.

- If conservative success criteria have been used in the PSA for some of the systems in any accident sequence, this should be clearly indicated and justified.

Accident Sequence Analysis (cont.)

- If simplifications or assumptions are made in the event trees, their effects should be clearly identified and justified.

- The procedures available to the operators to cope with the initiating event should be referenced in the event tree documentation. The reviewer should check whether these procedures have been analysed to identify all important operator actions. If expert judgement is used to estimate available time frames, the basis for the judgement should be checked.

Accident Sequence Analysis (cont.)

- The reviewer should check whether the impact of the initiating event on mitigating systems appearing in the event tree has been considered and whether dependencies between mitigating systems in the event tree are correctly accounted for.

- If one event tree is used to model several initiating event groups, the reviewer should verify whether this event tree indeed envelopes all sequences which can evolve from the different initiating event groups and whether this grouping does not introduce undue conservatism.

Accident Sequence Analysis (cont.)

- The reviewer should check that the personnel who prepared the event trees communicated with the personnel who participated in the systems analyses, human reliability analyses and sequence quantification in the development of the event trees.

- The reviewer should select an event tree and go through its preparation process in detail to assess the adequacy of the modelling, assumptions, simplifications and timing estimations.

System Analysis

- **To provide a valid and auditable basis for the fault trees, the reviewer should determine that functional descriptions are clearly documented for each system for which a fault tree is devised.**

- **The reviewer should also check that interfaces with plant personnel were established to check the accuracy of the schematic. If possible the reviewers should also check schematics of special interest at the plant.**

System Analysis (cont.)

- Hardware dependencies should be explicitly modelled in the fault trees.
- If separate systems perform the same function and have intersystem dependencies, these should be examined as well.
- The component boundaries and component failure modes should be consistent with those defined in the component failure database.
- The reviewer should also check that the degree of resolution of components is not so gross so as to hide hardware dependencies.

System Analysis (cont.)

- The reviewer should verify that the system logic model includes common cause failure events for component groups and that the component groups selected are complete and modelled correctly for each important failure mode.

- The reviewer should examine the treatment of maintenance in the fault tree analysis to ensure that proper allowance for maintenance unavailability is made.

System Analysis (cont.)

- The dependency of system success criteria on the initiator and event tree sequence conditions should be checked carefully.
- The reviewer should choose selected fault trees and review in detail their development.
- One selected important frontline system should be reviewed including its supports and supplies.

Analysis of passive systems, components and structures

- **Obviously, within a PSA for a NPP using passive systems the availability of these systems per demand has to be modelled.**

- **The reviewer should check first whether such systems and components were modelled within the PSA process and second, whether the methods and tools used are adequate to assess the reliability of these items.**

Analysis of computer-based systems

- **A significant issue in the PSA today is the assessment of computer-based control and safety systems reliability and in particular the identification of possible failure modes of the hardware/software system and the frequency of the possible failure modes.**

- **The review should focus on the completeness of the identified undesired failure modes and on the estimated frequencies for that failure modes.**

Analysis of Dependent Failures

- **The reviewer should check whether the following type of dependencies are treated adequately in the PSA: - initiators that cause safety related system failures ("common cause initiators"); functional dependencies; human interaction dependencies; component failure dependencies (common cause); external events (including fires and internal flooding).**

- **The reviewer should select some of these dependencies to review in detail**

Analysis of Dependent Failures (cont.)

- The reviewer should check that potential dependencies have all been covered in the PSA, have been modelled correctly in the fault tree, and have been quantified correctly and documented. It is particularly critical that the selection of common component groups was performed correctly to ensure that important common cause failure groups were not omitted. The reviewer should determine how the above potential dependencies were screened for and how their probabilities were assessed. Consistency of common cause failure probabilities with past experience should be checked.

Human Reliability Assessment

The review should examine the HRA process used by the PSA team to ensure that the HRA approach has been systematic and covers the following important steps:

- **Identification of HIs (human interactions)**
- **Establishment of the importance of the actions (qualitative and quantitative screening)**
- **Incorporation of the actions into the appropriate parts of the logic model**
- **Selection of suitable HRA models**
- **Quantification of the human interaction events.**

Human Reliability Assessment (cont.)

- **The reviewer should examine the screening guidance carefully to ensure that the screening process does not eliminate any human actions from detailed consideration which are significant for core damage.**

- **The reviewer should look for information in the PSA documentation, to ensure that the PSA team understands the situation influences on the plant personnel during the accident scenario.**

Human Reliability Assessment (cont.)

- **The reviewer should verify that important pre-initiator human actions that may affect systems availability have been identified and included in the assessment in a thorough and consistent manner, so that none are overlooked. This usually involves a review of the plant maintenance, testing, and calibration procedures to identify these actions for the systems modelled in the PSA.**

Human Reliability Assessment (cont.)

To assess post-accident operator actions modelling validly, the reviewer should check whether two sets of actions have been clearly identified and documented:

(a) post-accident operator actions required for systems to operate successfully;

(b) post-accident operator recovery actions associated with specific accident minimal cut sets.

Human Reliability Assessment (cont.)

- The reviewer should check specific evaluations of human error probabilities to assess the data and quantification process and to determine their consistency with the approach used.

- If screening values were used initially to help focus the analysis effort, it is very important to verify that the screening values represent an upper bound for the human error probability.

- The PSA should identify and justify the specific rules used for excluding and including recovery actions. This justification should be reviewed.

Initiator and Component Data Analysis

- **The reviewer should check the completeness and technical accuracy of the initiator frequency estimates.**

- **For initiating event frequencies, the reviewer should verify that an analysis of plant specific initiating events was performed if the plant has been in operation for more than a few years.**

Initiator and Component Data Analysis (cont.)

The following specific points should be assessed in reviewing the component data analysis of the PSA:

- **Selection of generic data for each type of component should be justified in the PSA documentation. Plant specific data is preferable, if available.**
- **If a combination of generic references is used, the methods used for selection of the specific references or for integration of the references should be given.**
- **The PSA should consider the use of plant specific experience and generic data in obtaining the final estimates and associated uncertainties for the PSA quantification.**

Initiator and Component Data Analysis (cont.)

- The reviewer should audit how the analyst used plant records to make plant specific estimates of the number of events or failures. The consistency between the definitions of failure modes and component boundaries used in the PSA and the definitions used in the data records should be checked.

- The estimation of the number of demands, operating hours or standby hours is important in the analysis of specific plant records. The reviewer should check this estimation for selected components.

Initiator and Component Data Analysis (cont.)

- **Mission times that are used for operating failure rates need to be justified. The mission time definitions should include considerations of minimal times to access or replace the components.**

- **If a plant specific analysis has been performed, the reviewer should do a spot check to determine if the calculations were performed correctly. If generic data is used, the reviewer should verify that the source is fairly recent and is recognised as an acceptable source.**

Quantification of accident sequences

- **The reviewer should verify that the PSA quantification process is technically correct and thorough, and that key dependencies are correctly accounted for in the quantification process. For cases where screening values are used, e.g. for HRA or common cause failure (CCF) assessment, the choice of cut-off probabilities for selection of events for which a more detailed assessment is required should be reviewed to ensure that key contributions are correctly quantified in the final iterations.**

Quantification of accident sequences (cont.)

- The PSA reviewer should check that sufficient PSA results are calculated in the accident sequence quantification to quantify the PSA comprehensively.
- The reviewer should check that the computer codes used are subject to a quality assurance (QA).
- The reviewer should check that there is a systematic, quality controlled process for determining the minimal cut sets to be used to quantify the system unavailabilities, accident sequence frequencies, plant damage state frequencies, and core damage frequency.

Quantification of accident sequences (cont.)

- The reviewer should check that the proper quantification formulae are used where applicable.
- If cut sets have been truncated in the analysis, either through the use of a cut-off probability or maximum cut set order, the reviewer should check that this truncation has not introduced errors into the results or the logic of the PSA.
- Where applicable, with regard to uncertainty analyses, the reviewer should assure that uncertainties are properly quantified and propagated.

External Event Analyses

- **The PSA should clearly identify the basis for selecting the external events that are analysed in the PSA. If external events are selected (screened) according to their potential contribution to core damage frequency, the screening criteria for selecting the external events should be clearly identified. Following the screening analyses, the reviewer should assess the validity of the more detailed external event analyses.**

Sensitivity, Uncertainty and Importance Analysis

- The reviewer should identify the assumptions or data that may significantly impact the PSA results, and verify that sensitivity analyses have been performed on these assumptions or data.

- When reviewing the importance analysis, the reviewer should check what type(s) of the importance measures is used, whether the importance analysis results are in general agreement with sensitivity analysis results qualitatively, and whether importance analysis results make logical sense.

Sensitivity, Uncertainty and Importance Analysis (cont.)

- The objective of uncertainty analysis is to provide quantitative measures and qualitative discussions of the uncertainties in the results of the PSA, namely, the frequency of core damage, the frequency of the dominant accident sequences and accident sequence categories. The reviewer should check if the following main uncertainties categories are considered in the study: (1) incompleteness, (2) model uncertainty, and (3) parameter uncertainty.

Review of Interpretation of Results

- **In addition to checking intermediate results, the reviewer should ensure that the global results of the PSA are plausible, that the interpretation and conclusions drawn from the results are logical and correct, and that the overall objectives of the PSA are met.**

- **The reviewer is suggested to check the basis of each conclusion carefully and determine whether the conclusions drawn from the PSA results have been derived in a logical way.**

Review of Interpretation of Results (cont.)

There is a number of effective ways that can be used to check the plausibility of global results. These means include:

- **Comparison with results of other relevant PSAs;**
- **Comparison with past real events;**
- **Comparison with applicable operating experience;**
- **Comparison with experimental results;**
- **Comparison with previous major expert opinions.**

Audit of the PSA QA

- **It may be a good practice to conduct PSA QA audits by the regulatory body during the process of the PSA development to ensure that the QA procedures are indeed followed, and the process for performing PSA is properly managed.**

References

- IAEA- TECDOC-1135 Regulatory Review of Probabilistic Safety Assessment (PSA) Level 1
- IAEA-TECDOC-832 IPERS guidelines for the international peer review services
- IAEA-TECDOC-1101 Framework for a quality Assurance programme for Probabilistic Safety Assessment