THE EXPERIENCE OF IPEN-CNEN/SP IN THE PROBABILISTIC SAFETY ASSESSMENT REGULATORY REVIEW FOR ANGRA 1 BRAZILIAN NUCLEAR POWER PLANT

P.S.P. OLIVEIRA, A.S. VIEIRA NETO, M.E.L.J. SAUER
Institute for Nuclear and Energetic Research (IPEN-CNEN/SP)
São Paulo, Brazil

Abstract

The objective of this paper is to present the methodology proposed by the Probabilistic Safety Assessment (PSA) group at IPEN-CNEN/SP, that has been involved in the regulatory review of some technical issues of the PSA for ANGRA 1 Nuclear Power Plant. The Brazilian nuclear regulatory authority, named CNEN, has been co-ordinating this task, and the working group at IPEN-CNEN/SP was requested to join the PSA review team. A structured and systematic approach has been especially developed at IPEN-CNEN/SP for reviewing three PSA technical issues, namely Event Sequence Analysis, Analysis of the Emergency Core Cooling System and Analysis of Data Required for the PSA. Review findings have been documented in reports addressed to the regulatory organization. These results would be useful in recommending modifications regarding the improvement of the PSA or changes to be made concerning the way the PSA is applied, or even changes related to the operation of the plant.

1. INTRODUCTION

ANGRA 1 is a 626 MWe nuclear power plant, located in the state of Rio de Janeiro, Brazil, with a two-loop PWR type reactor, Westinghouse design, and which has been in commercial operation since 1984. The organization responsible for managing and performing the PSA for ANGRA 1 has been the utility itself, named ELETRONUCLEAR. The analysis was performed by a multidisciplinary teamwork and the Nuclear Safety Advisory Group personnel were nominated task leader. During the development of the work, the PSA team at ELETRONUCLEAR used the Probabilistic Safety Assessment for Point Beach Nuclear Power Plant as a reference study, considering the similarities between these plants (Point Beach and ANGRA 1).

The PSA report [1] was presented to the Brazilian nuclear regulatory authority named CNEN (National Nuclear Energy Commission), in December 1998. An updated version is still in progress and has been undertaken to include some changes in PSA model and data. The recommendation for modifications in the PSA originated in the review conducted by an independent group of PSA experts, contracted by the utility. Meanwhile, the regulatory review has been based on Revision 0 of the PSA study.

The scope of ANGRA 1 PSA was set down by the regulatory authority as being a Level 1+ PSA, with the purpose of providing the plant with an input to some specific applications such as modifications / optimisation of Technical Specifications, improvement of Allowed Outage Times (AOTs) and Surveillance Test Intervals (STIs), review of the emergency operational procedures, identification of the most important precursors of significant accident sequences associated with incident reporting analysis, etc. [2] . In this way, the main objective of the regulatory review is to gain confidence that the PSA for ANGRA 1 has been performed according to an acceptable criteria. Thus it can be used as the basis for taking risk informed

decisions within the regulatory decision making process, in view of the issuance of the Authorization to Permanent Operation required by the utility.

The PSA review team, co-ordinated by the regulatory authority CNEN, is mainly composed of seven individuals and three of them have been working at IPEN-CNEN/SP. The experts at IPEN-CNEN/SP are experienced in state-of-the-art PSA methods and techniques since 1985 and also have been trained in quality assurance programmes.

The review team at IPEN-CNEN/SP has been in charge of the following technical issues:

Section 3.0 – Notebook of Event Tree Analysis
Section 4.2 – Notebook of Data Analysis
Section 4.5 – Notebook of the Emergency Core Cooling System

To review the technical issues mentioned above, the expert group at IPEN-CNEN/SP had proposed a schedule of work that included the definition of the methodology to be applied, the performance of the review of the PSA report itself and the documentation of the review findings. In this case, the timing of the review process was estimated in 1440 man-hour.

2. METHODOLOGY DEVELOPED AT IPEN-CNEN/SP FOR THE PSA REGULATORY REVIEW FOR ANGRA 1

The PSA review which has been carried out follows a structured and systematic approach that combines the guidance given by the IAEA-TECDOC-1135 on "Regulatory Review Guidance for Probabilistic Safety Assessment (PSA)" [3], the guidance given by the Swiss Federal Nuclear Safety Inspectorate on "A Probabilistic Safety Assessment Review Guidance for Swiss Nuclear Power Plants" [4], as well as the procedures and methods presented in the "PRA Review Manual" [5], prepared for the U.S. NRC.

The proposed methodology included the following steps:

Step 1 - Examination of the scope and applications of the PSA.

Step 2 - Definition of the attributes which would govern the review – organization, adequacy, correctness, completeness, clarity, coherence, consistency, accuracy, traceability, reproducibility and comparability. Besides that, the possible levels of compliance to each attribute must be classified.

Step 3 - Development of the checklists, for each of the technical issues, consisting of a number of questions addressed to the PSA. The questions were formulated in order to evaluate the compliance of the PSA work in relation to the attributes defined in the previous step.

Step 4 – Conduct of the review of each PSA technical issue.

During the development of Step 4, some other activities should be accomplished –

- Definition of activities that would support the application of the checklist previously prepared in Step 3 (preparation of tables, lists, etc.).
- Compilation and consultation of important references for the study (FSAR, internal / external reports, drawings, plant records, etc.).
- Comparison with some specific aspects of the PSAs of similar plants.

- Programme of visits to the plant with the purpose of consulting internal documents and/or asking for clarifications that should be provided by the PSA team at the utility

Step 5 - Preparation of a report, at the end of the review of each technical issue, to document the conclusions, main findings and possible non-conforming items. The reports should be sent to the regulatory authority responsible for co-ordinating the whole review process.

3. DETAILED REVIEW OF THREE TECHNICAL ISSUES OF THE LEVEL 1 PSA FOR ANGRA 1

The safety analysis developed for ANGRA 1 was a Level 1 PSA for initiating events occurring at full power, which identified the sequences of events leading to core damage. Thus, core damage frequency was estimated and the analysis also provided insights into the strengths and weaknesses of the safety systems and procedures available to prevent core damage.

As it was pointed before, the technical issues that are discussed in this paper are:

- Section 3.0 – Notebook of Event Tree Analysis
  This chapter contains the modelling of the response of the plant to each group of accident initiating events defined in Section 2.0 of the PSA report. The event tree model provides sequences of events that, following an initiating event, lead either to a reactor safe state or to a core damage state. In some cases, a sequence can also be transferred to other event tree. This chapter does not contain the modelling of the response of containment systems after a core damage event.

- Section 4.2 – Notebook of Data Analysis
  This chapter documents the acquisition and generation of all information necessary for the quantification of event tree and fault tree models. Includes: identification of the various models that describe the stochastic nature of certain phenomena related to the events of interest and the corresponding parameters that need to be estimated; determination of the nature and source of relevant data; and compilation and evaluation of the data to produce the necessary parameter estimation and associated uncertainties.

- Section 4.5 – Notebook of the Emergency Core Cooling System
  This chapter contains the modelling of the system in order to evaluate events related to the failure and success of the ECCS in the various event sequences determined for the plant. The event sequences are presented in Section 3.0 of the PSA report and were generated by modelling the response of the plant to each group of accident initiating events.

Tables 3-1, 3-2 and 3-3 show the checklists prepared for the detailed review of each of these technical issues, respectively. They are in accordance with Step 3 of the methodology described in Section 2 of this paper.

Table 3-1 Checklist for the Detailed Review of Section 3.0 – Notebook of Event Tree Analysis

	Checking Item	Corresponding Review Criteria
✓ 1	**General considerations of the methodology used in Section 3.0**	
1.1	Check if the methodology applied was described directly or by explicit reference, or implicitly;	Clarity Completeness
1.2	Check if the methods used are conventional or new. In the latter case, check if a justification was given for their use;	Adequacy; Comparability
1.3	Check if the study used the "small event tree / large fault tree" method, or the "large event tree / small fault tree", or other method for accident sequence definition;	Adequacy; Coherence
1.4	In case the event tree methodology had been used, check the type of headings adopted (e.g. functions, frontline systems, frontline systems and support systems, etc.);	
1.5	Identify the definition of "core damage state";	Clarity; Completeness
1.6	Check the end-state chosen for the accident sequences;	Clarity; Adequacy; Comparability
1.7	Verify if all accident initiating event categories defined for the plant were modelled;	Completeness; Consistency
✓ 2	**Definitions of safety functions, safety systems and success criteria**	
2.1	Check the list of safety functions that need to be performed to prevent core damage;	Completeness; Adequacy; Coherence; Consistency
2.2	Check the list of frontline systems required to perform these safety functions;	
2.3	Check the definition of success criteria for the safety functions / safety systems;	Completeness; Clarity; Adequacy; Coherence; Consistency
2.4	Verify if plant specific accident and transient analyses were performed as part of the PSA in order to determine the success criteria;	Adequacy; Traceability

Table 3-1 (continuation)

	Checking Item	Corresponding Review Criteria
2.5	Verify if frontline systems which would fail as a result of the initiating event were identified, and if this was taken into consideration when defining the success criteria;	Coherence; Consistency; Clarity; Traceability
2.6	Verify if the success criteria were depending on the prior success / failure of other safety function / frontline systems;	
2.7	Verify if the definition of success criteria included the requirements of support systems;	
2.8	Verify if the mission times for the safety systems were specified in the success criteria;	Completeness; Adequacy; Accuracy
2.9	Check the justification for the safety systems mission times (experts' opinion, transient analysis, etc.);	Coherence; Consistency
2.10	Verify if the operator actions required to bring the plant to a safe shutdown state were referred to in the success criteria;	Clarity; Completeness; Adequacy
2.11	Check the definition of available times for manually actuate the systems in case of failure of the automatic action;	Completeness Coherence; Consistency; Accuracy
2.12	Check and make up a list of system recovery times;	Completeness Coherence; Consistency; Accuracy
2.13	Prepare a table relating: frontline system, accident initiating event, frontline system success criteria, frontline system mission time;	
3	**Event Tree Model**	
3.1	Check if the PSA report contains a detailed description of the event trees;	Clarity; Completeness
3.2	Verify if the event tree analysis, for each initiating event category, involved all safety functions and required safety systems, according to the defined success criteria;	Completeness; Coherence; Consistency
3.3	Verify if the event trees were organized in a way which represented the progression of the initiating event (following a chronological or causal order);	Clarity; Coherence
3.4	Verify the description of the dependence between initiating events and those systems / functions that are required at a later time during accident progression;	Completeness; Clarity; Consistency; Coherence

Table 3-1 (continuation)

	Checking Item	Corresponding Review Criteria
3.5	Check the systems which are either disabled or degraded by the initiating event, and review the way they were treated in the event trees;	Coherence; Consistency
3.6	If some special conditions of success / failure of a system were modelled by means of "house events" in the system fault trees, verify the description of these events and respective interfaces with the event trees;	Clarity; Coherence; Consistency; Completeness
3.7	Verify if any event tree was used to model several initiating event categories. Check if this grouping was justified in the analysis;	Adequacy; Consistency; Coherence
3.8	If simplifications or assumptions were made in the development of the event trees, verify if their effects were identified and justified. Prepare a list of these simplifications / assumptions for a possible sensitivity analysis;	Clarity; Adequacy; Consistency; Coherence
3.9	Verify if transfers between event trees were considered and justified;	Adequacy; Coherence
3.10	Verify if there are sequences assumed out-of-scope of the PSA (e.g. pressurized thermal shock scenarios, induced steam generator tube rupture, etc.);	Adequacy; Coherence; Completeness
✓ 4	**Operator actions**	
4.1	Prepare a table relating: operator actions, time to start the action, time to complete the action and respective plant emergency procedures;	Completeness; Clarity; Consistency; Coherence; Accuracy
4.2	Check if the estimates of time for the operator actions were based on experts' opinion. Verify the justifications;	Coherence; Consistency
✓ 5	**Definition of "plant damage states"**	
5.1	Verify if "Plant Damage States" (PDSs) were defined and if the characteristics which could influence the containment response or the release of radioactivity to the environment were described. These definitions would be the interface with Level 2 PSA;	Clarity; Completeness; Adequacy
✓ 6	**Model Reproduction**	
6.1	Select one or more event trees and go through its preparation process; Suggestion: "Loss of off-site power", "Large / Medium LOCA" and "Loss of Service Water System".	Reproducibility
6.2	If there are any differences identified between the model presented in the PSA and the one developed according to item # 6.1, prepare explanations for the modifications required, and develop the revised event trees;	Comparability

Table 3-2 Checklist for the Detailed Review of Section 4.2 - Notebook of Data Analysis

	Checking Item	Corresponding Review Criteria
✓ 1	**Types of data included in Section 4.2**	
1.1	Check if Section 4.2 contains all necessary data for quantifying the event tree and fault tree models developed for estimating the Total Core Damage Frequency (CDF) for ANGRA 1: initiating event frequencies, component failure probabilities, component unavailability during periods of test or maintenance, common cause failure probabilities and human error probabilities;	Organization and Format; Completeness
✓ 2	**Sources of data used in the PSA of ANGRA 1**	
2.1	Check if all data sources were identified and adequately used in ANGRA 1 PSA;	Completeness; Adequacy
2.2	Evaluate the general criteria adopted while selecting the data to be used in the PSA. Verify if, where possible, plant specific data were used in the analysis;	Coherence; Adequacy
2.3	When specific data were not available, check if data from operation of similar plants were preferably used;	Coherence; Adequacy
2.4	Include a table showing the percentages of specific data, specific data with Bayesian updating, generic data and data from similar plants, used in ANGRA 1 PSA;	Adequacy
✓ 3	**Assessment of plant operational experience**	
3.1	Audit how the analysts used plant records (incident reports and operation and maintenance records) to generate specific estimates. Check the following items (3.2 to 3.6):	
3.2	Verify if incident reports and operation and maintenance records used as plant specific sources of information are organized and easily accessible;	Traceability
3.3	Compare the definitions of component boundaries and failure modes used in the PSA report with those used in plant specific records;	Coherence; Consistency
3.4	Check incident reports from which failure events were derived to ensure that they were properly interpreted;	Coherence; Traceability
3.5	Check the estimation of number of failures, number of demands, operating hours / standby hours, number of hours in test or maintenance, etc. in the analysis of component specific plant records;	Accuracy; Reproducibility
3.6	Technical visit to the plant to consult internal documents (failure data reports) generated from plant records;	Traceability

Table 3-2 (continuation)

	Checking Item	Corresponding Review Criteria
✓ 4	**Review of the calculations**	
4.1	Verify the statistical method used to treat and analyse the data;	Adequacy; Correctness; Accuracy
4.2	Verify the formulae applied for the estimation of the various basic event probabilities (component single failure probabilities, unavailability during periods of test or maintenance and common cause failure probabilities);	Adequacy; Correctness; Accuracy
4.3	Verify the use of Poisson distribution approach for time related failures and the Binomial distribution for demand related events;	Adequacy; Accuracy
4.4	Check the justification of the "mission times" used in the calculation of component failure rates;	Coherence; Consistency; Accuracy
4.5	Check if the impact of unscheduled maintenance was considered when evaluating component unavailability due to test or maintenance;	Coherence; Accuracy
✓ 5	**Bayesian approach for combining generic data and plant specific data**	
5.1	Check if Bayesian approach was used while updating (specialising) data for ANGRA 1. Identify and comment on the reasonableness of the prior distributions;	Adequacy; Accuracy; Completeness
✓ 6	**Dependent failures**	
6.1	Verify if a systematic analysis was carried out to identify all potential dependence between component failure events (common cause failures);	Adequacy
6.2	Ensure that any important common cause failure group was not omitted in the PSA;	Completeness
6.3	Assess the approach given in the quantification of common cause failure probabilities and check if they were estimated by using plant specific data;	Adequacy; Coherence; Consistency; Accuracy
✓ 7	**Uncertainty analysis**	
7.1	Check if uncertainty analysis was performed in the PSA for ANGRA 1;	Adequacy; Accuracy
✓ 8	**General aspects involving the Data Analysis for ANGRA 1 PSA**	
8.1	Check if Section 4.2 (Notebook of Data Analysis) contains a table showing mean / median estimates and associated inferior and superior limits, related to all basic events probabilities that appear in the event tree and fault tree models;	Completeness; Organization and format; Clarity
8.2	Check if specific data are still being collected, if they are being extended to other systems of the plant and if there is a Reliability Database for ANGRA1. Verify if this database is computerized and has been updated regularly;	Consistency;

Table 3-3 Checklist for the Detailed Review of Section 4.5 – Notebook of the Emergency Core Cooling System

	Checking Item	Corresponding Review Criteria
✓ 1	**System Description**	
1.1	**System / Subsystem Operating and Actuating Modes**	
1.1.1	Verify if the conditions for system actuation were described;	Completeness; Clarity;
1.1.2	Verify if each system / subsystem operating mode was described;	Completeness; Clarity;
1.1.3	Identify specific operator procedures for each system / subsystem operating mode;	Completeness; Clarity; Adequacy
1.1.4	Check the definition of available times for the operator manually actuate the systems / subsystems;	Completeness; Coherence; Consistency
1.2	**System configuration**	
1.2.1	Verify if system / subsystem boundaries were defined;	Clarity; Completeness; Consistency; Adequacy
1.2.2	Check if the component types for each system / subsystem were specified;	Clarity; Completeness;
1.2.3	Check for the requirements related to support systems;	Coherence; Consistency; Clarity; Traceability
1.3	**Test and Maintenance Procedures**	
1.3.1	Verify if all data related to Test and Maintenance were specified (repair times, test intervals, etc.)	Completeness; Accuracy
✓ 2	**Relation of the System with the Accident Sequences**	
2.1	Verify the definition of system / subsystem success criteria for each accident sequence;	Completeness; Clarity; Adequacy; Coherence; Consistency
2.2	Verify if the accident sequence description allowed the identification of the conditions (success / failure) of other systems before the actuation of the ECCS;	Clarity; Consistency; Coherence;
2.3	Check the justification for possible differences between the accident sequences (related to the system) obtained in the current version of the analysis and the sequences determined in previous versions;	Comparability; Completeness; Adequacy;

Table 3-3 (continuation)

	Checking Item	Corresponding Review Criteria
3	**Qualitative Analysis**	
3.1	**Failure Mode and Effect Analysis**	
3.1.1	Verify if a Failure Mode and Effect Analysis (FMEA) was developed for the system and included in the PSA. In case that it was not included in the PSA report, check if it was presented in other reference document;	Completeness; Consistency
3.2	**Fault Tree Analysis**	
3.2.1	Verify if the list of fault trees includes all top events defined for the ECCS;	Completeness;
3.2.2	Verify if the support system failures were considered in the ECCS fault trees;	Adequacy; Completeness;
3.2.3	Verify if all components were included in the fault trees;	Completeness
3.2.4	Check for the justification of components not included in the fault trees;	Completeness; Consistency; Coherence
3.2.5	Check if all pertinent component failure modes identified in the FMEA were included in Fault Tree Analysis;	Completeness; Consistency; Coherence
3.2.6	Verify if all pertinent failure effects that were previously identified in the FMEA were considered in the fault tree events;	Completeness; Consistency; Coherence
3.2.7	Check if the minimal cut sets were determined;	Completeness; Correctness
4	**Quantitative Analysis**	
4.1	**Initial Assumptions**	
4.1.1	Check if "mission times" were specified;	Completeness; Adequacy; Accuracy
4.2	**Component Analysis**	
4.2.1	*Failure Data*	
4.2.1.1	Check if all component failure mode probabilities were quantified;	Completeness; Accuracy
4.2.1.2	Verify the justification for the Life Time Probability Distribution adopted for each component;	Adequacy
4.2.1.3	Check if component failure probabilities were estimated from plant operational experience;	Accuracy; Adequacy; Consistency
4.2.1.4	Evaluate the generic database used as prior distribution in the Bayesian analysis of component failure data;	Adequacy; Consistency; Accuracy
4.2.2	*Common Cause Failures*	
4.2.2.1	Verify if common cause failures were considered in system analysis; Ob.: This topic will be further investigated in the review of PSA Data Analysis.	Completeness; Adequacy; Coherence; Consistency

Table 3-3 (continuation)

	Checking Item	Corresponding Review Criteria
4.2.3	*Human Errors*	
4.2.3.1	Verify if human errors were considered in system analysis; Ob.: This topic will be further investigated in the review of PSA Human Reliability Analysis.	Completeness; Adequacy; Coherence; Consistency
4.2.4	*Component Reliability / Availability*	
4.2.4.1	Verify if the mean availability associated to each component failure mode was calculated;	Completeness; Accuracy
4.2.4.2	Verify if the reliability associated to each component failure mode was calculated;	Completeness; Accuracy
4.2.4.3	Verify if component mean availability was calculated;	Completeness; Accuracy
4.2.4.4	Verify if component reliability was calculated;	Completeness; Accuracy
4.2.5	*Importance Analysis*	
4.2.5.1	Verify if at least one method was used to assess component / failure mode importance in relation to system failure;	Completeness; Adequacy; Accuracy; Consistency; Coherence; Traceability
4.2.6	*Accident Importance Analysis*	
4.2.6.1	Verify if at least one method was used to assess component / failure mode importance in relation to the accident sequences;	Completeness; Adequacy; Accuracy; Consistency; Coherence; Traceability
4.3	**Minimal Cut Sets**	
4.3.1	Check if all relevant minimal cut sets were quantified;	Completeness; Accuracy
4.4	**System Analysis**	
4.4.1	Evaluate the computer code used in the analysis (qualification, application, etc.);	Adequacy; Correctness; Traceability Comparability; Consistency
4.5	**System Reliability / Availability**	
4.5.1	Verify if system reliability and / or availability was calculated;	Accuracy
4.5.3	Verify if uncertainty analysis was applied in the calculation of system reliability / availability.	Adequacy; Accuracy

4. CONCLUSIONS

Although there are several good references and guidance concerning PSA regulatory review, the PSA group at IPEN-CNEN/SP found it necessary to reorganize and restructure the methodology presented in these documents, by the time the regulatory review of ANGRA 1 PSA was performed. It was relevant to verify some PSA aspects in relation to the attributes to be accomplished to obtain quality in PSA [6]. These attributes were associated to questions addressed to the PSA, generating checklists, as an outline for the review of the technical issues.

In this way, the adoption of a systematic and structured method facilitates and contributes to the conduct of the PSA technical review, since:

- It clearly establishes the boundaries between each stage of PSA development and the extent of the PSA as a whole.
- It allows the logic ordering of the checking items, characterising a step by step approach to the review process.
- It provides clarity as far as PSA features and attributes being assessed are concerned.
- It facilitates the identification of PSA features and attributes not accomplished in the analysis.

Furthermore, some points related to the review of the ANGRA 1 PSA can be mentioned, as for instance, the results from the review of the Data Analysis. The review of this technical issue was mainly directed to the verification of plant specific data collection and treatment, including the consultation and evaluation of internal documents prepared during this process, used as reference in the analysis. As a result, it was identified the need of a Reliability Database for ANGRA 1 NPP. This database should be related to a computerized system to collect and statistically analyse data obtained from incident reports and plant operation and maintenance records. Firstly, this would allow the implementation of more accurate methods to estimate component reliability parameters. In addition, it would be used to update the PSA and to extend its use to other safety related applications.

5. REFERENCES

[1] ELETROBRÁS TERMONUCLEAR S.A. – ELETRONUCLEAR, Probabilistic Safety Assessment for ANGRA 1 Nuclear Power Plant, Rio de Janeiro (1998).

[2] GIBELLI, S. M. O., "The role of Probabilistic Safety Assessment in the Licensing of ANGRA 1 Nuclear Power Plant", (Paper presented at the IAEA Technical Committee Meeting on Advances in Reliability Analysis and Probabilistic Safety Assessment for Nuclear Power Reactors, Budapest, September, 1992).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Review Guidance for Probabilistic Safety Assessment, IAEA-TECDOC-1135, Vienna (1999).

[4] SWISS FEDERAL NUCLEAR SAFETY INSPECTORATE, A Probabilistic Safety Assessment Review Guidance for Swiss Nuclear Power Plants, ERI/HSK 92-1115, HSK-NA-2517, Villigen (1992).

[5] UNITED STATES NUCLEAR REGULATORY COMMISSION, PRA Review Manual, NUREG/CR-3485, BNL-NUREG-51710, Washington DC (1985).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Framework for a Quality Assurance Programme for Probabilistic Safety Assessment, IAEA-TECDOC-1101, Vienna (1999).