Highlights of the PSA Analyses Performed for the RRR

J. Barón[♣], J. Núñez Mc Leod[♣], S. Rivera[♣] and S. Bastin[♦]

ABSTRACT

In July 2000, ANSTO signed a contract with the Argentinian company INVAP S.E. for the design, construction and commissioning of a replacement research reactor (RRR). INVAP contracted CEDIAC to prepare the Probabilistic Safety Assessment (PSA) for the RRR in support of the ANSTO application for the construction licence.

The PSA is complementary to the Safety Analysis, in the sense that it asks questions such as "What if the Postulated Initiating Events were to occur and more than one piece of equipment were to fail? What if several things were to go wrong?" The PSA attempts to determine all the possible combinations of how the plant could respond to an initiating event, group all the possible outcomes, obtain conservative estimates of the frequency, and bounding estimates of the consequences (i.e., doses to the worst exposed individual of the public). The frequency and consequence constitute the risk, and when evaluated for all possible events can be compared against the safety objectives set out in the regulatory principles.

Besides the basic objective of the PSA, which is the quantitative evaluation of the risks associated with the RRR, and its comparison to the regulatory objectives, the PSA studies have been performed in parallel with the basic engineering phase of the project. Therefore, preliminary results from "the risk point of view" were used as input to the design process, thus permitting improvements to be made to the design, and resulting in an effective reduction of the residual risk.

To perform the PSA studies several methodological developments were made, in order to obtain a representative list of internal and external initiating events, to treat component and human-related failures, to consider common-cause failures, and to consider some specific aspects of the design (i.e., fail-safe components, passive systems, and lack of need for support systems).

The PSA studies were performed to obtain not only quantitative estimations of the risk, but also quantitative estimations of the uncertainty associated with them.

The overall results of the PSA indicate a very low residual risk for the RRR, and provide a valuable tool to analyse detailed engineering alternatives. The reactor design meets the regulatory safety objectives. Several design characteristics of the RRR contribute to the very low risk estimations (e.g., two completely independent shutdown systems, the lack of need for support systems for the safety functions, the absence of in-core experiments, the redundancy on the cooling modes, etc.)

The PSA proved to be a valuable tool to increase the safety level of the RRR, and this was possible because of the good communication and interaction between the PSA analysts and the designers.

Presenting author: J. Barón, jbaron@uncu.edu.ar

[♣] CEDIAC Institute (under contract by Invap), Facultad de Ingeniería, CC 405, Universidad Nacional de Cuyo, Parque Gral. San Martín, 5500, Mendoza, Argentina

[♦] ANSTO, Australian Nuclear Science and Technology Organisation, New Illawarra Road, Lucas Heights, NSW 2234, (PMB #1, Menai 2234) Australia.

INTRODUCTION

The proposed RRR is an open pool type reactor, that is, a reactor where the core sits in a deep pool of water that provides cooling of the core, and protection against the effects of radiation. The metallic pool liner is inserted in a high integrity reinforced concrete block. The RRR will provide facilities for irradiating targets for the production of radiopharmaceuticals, and silicon and for experiments, as well as providing high quality neutron beams for specialised research.

OBJECTIVES OF THE PSA

Probabilistic Safety Assessment (PSA) is a valuable tool for the quantification of risks arising from the operation of nuclear reactors and other complex installations. By means of this risk quantification, the whole plant is analysed from the safety point of view, and the features that govern the risk in the plant can be identified and ranked by importance. Furthermore, individual safety issues can be analysed and their impact on the risk estimated. This procedure involves not only the existing issues, but the PSA can also be used as a tool to estimate the expected risk reduction benefits from proposed changes to plant design, operating and maintenance practices. In an overall sense, the PSA performed on a specific plant constitutes a realistic measure of its safety by quantitative means, that can follow the safety improvements of the plant in what is known as a living PSA.

The basic objective of the present PSA for the RRR is the quantitative evaluation of the risks associated with the operation of this reactor, according to the present PSAR and located in the proposed siting at Lucas Heights, NSW.

As part of this basic objective, the following particular objectives were pursued:

a) The identification of internal and external events that may lead to accident conditions.

b) The identification and analysis of the plant systems responses to the initiating events identified to pose a relevant risk to the public and operators.

c) The identification of systems, components, and human actions important to the overall risk.

d) The estimation of the impact of dependent failures in the overall risk.

e) The estimation of the containment response and associated source terms for a few representative accident sequences.

f) The comparison of the representative accident sequences risks with the regulatory objectives.

Besides these objectives, the following two operative objectives were also pursued:

g) The development of a living PSA that will allow for the inclusion of any minor design change to be produced after the detailed engineering is finished, and preparation of an updated PSA for the FSAR.

h) The preparation of a comprehensive PSA document (eg this report) that will allow for the audit of the hypothesis, methods and assumptions included in it.

Moreover, since this PSA was developed in parallel with the basic engineering phase of the RRR, the preliminary results were used as input to the design process, thus permitting improvements to be made to the design.

The scope for the present PSA is a Level I PSA with certain Level III considerations. These considerations include the selection of a few accidents which are considered to be representative of the risk of the installation. Accidents were selected for consequence analysis if their estimated upper bound frequency was greater than the most stringent frequency set in the safety objective of the ARPANSA regulation (*ie* having an upper bound frequency equal to or greater than 10^{-6} per annum

For these accidents, release fractions were derived, based on conservative assumptions, and the containment response was analysed, in order to obtain representative source terms for the installation. The dose expected for these source terms on the public was also calculated, taking into account conservative weather and sheltering conditions.

The corresponding dependent failure analyses helped to verify the segregation and redundancy of safety functions. Several lessons learned in these analyses were fed back into the design process.

The PSA includes consideration of all envisaged operation modes of the RRR, and all expected radiation sources that may exist in the plant. However, as the detailed engineering and the specific operating and maintenance manuals were not available at the time the PSA was performed, several conservative hypotheses were made. In a later revision of the present PSA, more realistic assumptions may be made, and this is expected that there will be a corresponding reduction in the risk estimations from the present PSA. In this sense, the present results are considered to be a bounding estimation of the risk.

ANALYSES METHODS

Method for Identification and Selection of Initiating Events

The identification and selection of initiating events always poses a question as to the completeness of the PSA, and up to now there is no method that can guarantee this completeness. At some level, every method requires engineering judgement.

For this purpose, a specific systematic method was developed, known as Source and Event Analysis (SEA). This method is quite similar to the Master Logic Diagram (MLD) proposed in NUREG/CR-2300 [i] and has been derived from the approach indicated in IAEA-TECDOC-517 [ii]. It was used in [iii].

The SEA method is a multi-step, bottom-up approach that consists of:

a) Identification of the relevant radiation sources in the plant (eg core, fuel in the spent fuel pool, fuel in the shipping cask, etc.)

b) Identification of the barriers that separate the radiation sources from the public and/or plant personnel.

c) Identification of the primary failure mechanisms of these barriers.

d) Identification of the initiating events that may cause the identified failure mechanisms.

e) Systematic selection and grouping in a set of representative initiating events.

The SEA method can generate a large list of failure mechanisms and initiating events (which in fact is an advantage). To manage this list, a screening process is performed at each step, in order to eliminate those events which make a negligible contribution to the overall risk. For example, if a certain source of radioactive material (e.g., an ion-exchange resin) is assumed to pose a negligible risk due to its small inventory, it can be excluded in step a). If a certain failure mechanism is known to occur very slowly (e.g., corrosion), and its status readily identified, it may also be excluded in step c) for the purposes of the PSA.

Specific considerations are used for the definition of the external events to be analysed. For this purpose, a screening of possible events is performed according to the IAEA guidelines [iv]. After this screening process the local expected external events at the Lucas Heights site were analysed based on the experience of the HIFAR PSA [v].

A review of incidents in research reactors was prepared independently in chapter 16 of the PSAR and no additional initiating events were identified.

The list of initiating events identified for this PSA are indicated in the following table:

Categories	ID	Description
A		**Reactivity transients**
	A1	Erroneous withdrawal of a control rod during start-up
	A2	Erroneous withdrawal of a control rod during normal operation
B		**Loss of flow**
	B1	Core Bypass
	B2	Loss of electric power
	B3	Primary pump failure
	B4	Primary isolation valve undesired closure
	B5	Fuel channel local blockage
C		**Loss of coolant**
	C1	Primary LOCA caused by a rupture upstream of the primary pump
	C2	Primary LOCA caused by a rupture downstream of the primary pump
	C3	Pool cooling system LOCA
D		**Loss of heat sink**
	D	Loss of heat sink
E		**Mechanical damage to fuel assemblies**
	E1	Fuel assembly mechanical damage in the irradiated fuel assemblies pool
	E2	Fuel assembly mechanical damage in the spent fuel storage racks in the reactor pool
	E3	Fuel assembly fall while in transit
F		**Heavy water leak**
	F	Heavy water spill outside reactor pool
S		**Seismic events**
	S	Seismic Event

PSA Models and Data

Many sophisticated tools for the quantification of risks arising from the operation of nuclear reactors and other complex installations have been developed to perform this analysis. SAPHIRE (INEL) is one such package and was used for this study.

Once the Initiating Events (IE) were established, the following steps were taken:

a) An Interference Matrix, was developed where each IE was analysed and the possible accident sequences derived from it were mapped against the safety systems and functions that would be required along those sequences. This matrix shows which systems and functions are relevant to each initiating event, and therefore which systems must be modelled in Fault Trees and included in Event Trees. It also helped in the definition of the success criteria for the Event Tree headers.

b) Qualitative System Fault Trees were developed. For each of the Event Tree headings identified in the Interference Matrices, a success criterion was established. Using the success criterion, the Process and Instrumentation (P&I) drawings and the Operational Limits and Conditions, where known, of each safety system, a Fault Tree (FT) was developed. These FTs were simplified based on the criterion that the active components will have a larger contribution to the system failures than the passive components. Care was taken not to eliminate passive failures that might be significant in the overall system (for example where all active components are in redundant sets).

   The systems analysed in the Fault Trees were:

   - First and Second Reactor Protection Systems (FRPS and SRPS)
   - First Shutdown System (FSS)
   - Second Shutdown System (SSS)
   - Flap Valves and Siphon Effect Breakers – which includes five conceptual headings:
     - Siphon Effect Breakers (SEB)
     - Suction & Impulsion Siphon Effect Breakers (S&I-SEB)
     - Flap Valves at Level 6000 (FVL6000)
     - Flap Valves at Level 7000 (FVL7000)

- Flap Valves at Level 6000 and 7000 (FV6&7)
- Emergency Makeup Water System
- Emergency Electrical Power Supply (EEPS)

Note: The flap valves are systems which automatically open to permit natural convection cooling on loss of primary cooling pump outlet pressure. They also therefore break a siphon on the return side of the primary cooling system in the event of a LOCA in that section of the PCS.

c) Qualitative Event Trees (ET) were developed. These trees were developed for each IE, with the corresponding headers obtained from the Interference Matrices. After the development of each ET, a screening process was taken in order to eliminate those sequences that have no physical meaning or that are considered irrelevant.

d) Once all the ETs and their corresponding headings had been qualitatively delineated, they were programmed in the SAPHIRE [vi] code. These codified trees were then quantified at a component level. For the quantification process, the IAEA database on component failure [vii,viii] was used. The results were then integrated in order to obtain overall quantification. SAPHIRE also provides tools to perform importance, sensitivity and confidence analyses on the results.

e) The Level I PSA results were analysed in order to obtain key end state frequencies, such as the Core Damage Frequency for the reactor. At this step, several importance measures were estimated, according to the Fussel-Vessely importance estimation, and sensitivity studies were then performed on the parameters identified with highest importance. The various importance measures give an indication of how significant each basic event is to the overall top event probability, or to an end state frequency.

f) Each basic event in the PSA has some uncertainty associated with its probability. This uncertainty is represented by the associated confidence interval. Having obtained "best estimates" of all of the end state frequencies, it is usually of interest to understand the uncertainty associated with these estimates. This was achieved by "propagating" the uncertainties through the Level I PSA model. The objective is twofold: (1) to understand the limitations of the numerical results and (2) to obtain upper bound estimates of the end state frequencies at specific levels of confidence.

g) In order to estimate the plant behaviour beyond the scope of the Level I PSA, a few representative accidents were analysed to determine inventory, containment response, and consequences of such a release. The accident sequences were collated into similar plant damage states based on the potential for causing relevant doses to the public, and the expected frequency of this plant damage state (being the sum of the frequencies of the sequences collated into that state). In this sense, a few plant damage states encompass the risk characteristics of the plant.

Using conservative retention factors, and conservative assumptions about the containment response, source terms were derived for each of the selected plant damage states and these source terms were used to estimate the doses a member of the public might receive, making conservative assumptions about the weather conditions, and sheltering e*tc*. The results were then compared against acceptance criteria and its compliance is discussed.

Dependent Failure Analyses

Actual operating experience with complex plants demonstrate that, although the likelihood of a series of failures is quite small, it is numerically higher than would be estimated solely from a postulated chain of independent failures. This is because physical and human interactions result in dependent failures that increase the conditional probability of each successive failure in the chain.

The treatment of dependencies in the identification and quantification of accident sequences is called "dependent-failure analysis". Dependencies tend to increase the frequency of multiple, concurrent failures. Since essentially all important accident sequences that can be postulated for nuclear reactor systems involve the hypothesised failure of multiple

components, systems, and containment barriers, dependent-failure analysis is an extremely important aspect of PSA.

A detailed engineering analysis of dependent failures must consider the root causes of component failures and the degree of dependence among component failures with regard to each root cause. This is particularly important for a new reactor, where no operating, maintenance and testing experience exists.

There are three types of dependent failures:

a) Functional dependencies between systems. These are where the success of one system is dependent on the success of another, for example due to reliance on a support system or where there is a shared component or subsystem in two systems. In the present PSA, functional dependencies were treated explicitly in the event trees.

b) Dependencies or common causes between basic events. Traditionally in PSAs of existing plants, common cause dependencies (the second type of dependencies) are modeled as a numeric fraction of the basic event failure probability that occur independently (*eg* the beta factor, or multiple Greek letter methods). Parameters for these models make use of generic data, where available, which are then updated with plant-specific data. For the present PSA, in lieu of the more conventional method, common cause effects were modelled as follows. Components in redundancy sets were identified for inclusion in common cause groups. Three main types of common cause effects were modelled as human errors:
   - Design errors,
   - Maintenance errors, and
   - Test, calibration and inspection errors.

   These errors were developed as human error fault trees. The design errors were intended to represent the chance that there is some underlying design fault which allows the item to fail dependently with other items of its type, for example solenoid valves which have an internal return spring that is susceptible to fatigue; control rods that might seize due to some unforeseen interaction of lubricant and high humidity environment; or circuit breakers that might fail closed after a high current event due to welding of contacts. It is these errors that are normally modelled using beta factors or the Multiple Greek Letter Method.

   Maintenance and test errors represent any event in maintenance or testing that might disable a safety related item or system.

c) Dynamic human interactions. In the present PSA the actuation of the safety systems is automatic, and no credit was taken for manual actions or recovery actions. Therefore, the third class of dependent failures, which corresponds to dynamic human interactions (eg inability to act due to operator error in response to) is not relevant because it does not contribute to the failure of safety systems. It was difficult to anticipate how an operator might respond erroneously in a particular sequence, when in fact, no operator response is required in the first 30 minutes. However, where credible operator actions that could jeopardise safety system functions were identified, they were included as basic events in the fault tree models. Furthermore, conservative assumptions were made regarding plant operations (eg. that the operator prematurely shuts down the primary cooling system pumps, following a trip).

PRELIMINARY PSA RESULTS

It should be noted that these results, reported in the revision 0 of the PSA are preliminary in that they are based on the plant design at the end of the preliminary engineering phase. Operating and maintenance procedures, OL&Cs and precise plant room and equipment cabinet layouts were not available at that time. Therefore, for example, it was not possible to perform fire PSA, or to determine all potential for human error. However, because of the many inherent safety features in the plant design and the fact that operator intervention is not required in sequences, it is expected that these aspects will not make a significant change to the overall results.

Core damage frequency

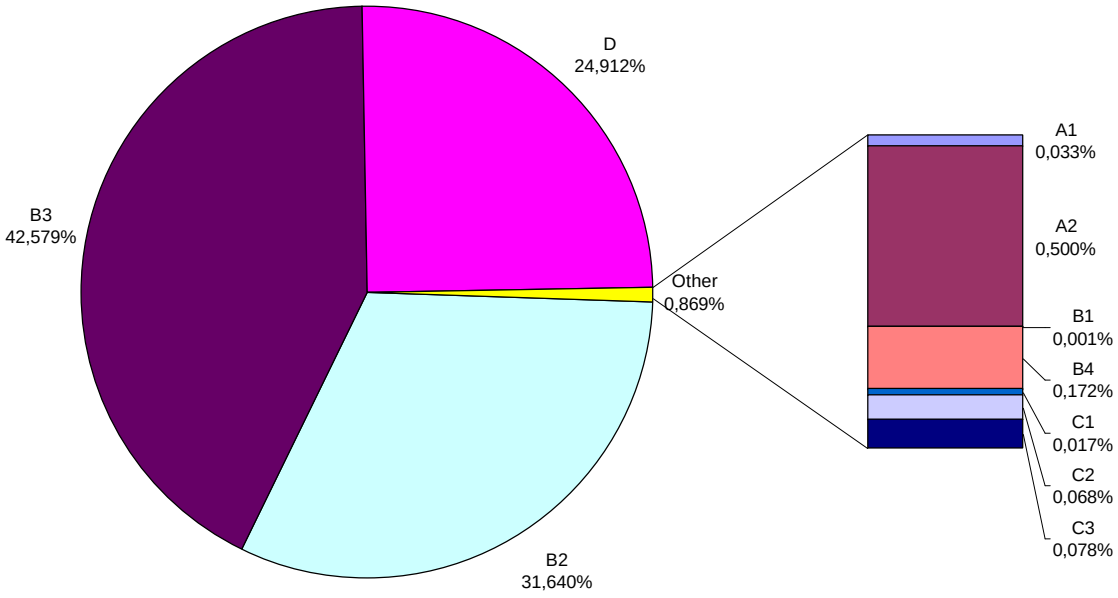
The core damage frequency (CDF) obtained by the summation over all the frequencies of internal event sequences that may lead to core damage is

Mean CDF:	**5.5×10^{-8}/year**
5% Percentile CDF:	**5.2×10^{-9}/year**
95% Percentile CDF:	**2.1×10^{-7}/year**

These values, when compared with the Safety Limits and Objectives, indicate, with a 95% confidence, that the CDF fulfills the most stringent frequency of the Safety Objective (10^{-6}/year). Therefore, it can be stated that those accidents with the potential to cause a significant damage to the core, pose a negligible risk to the public in the vicinity of LHSTC.

The relative contribution to the mean CDF due to each internal event is indicated in the following Figure 1.

Figure 1 Relative contribution of each initiating event to the CDF



It can be seen that the loss of flow and loss of heat sink initiated transients contribute to the overall CDF with more than 99%.

From the frequency point of view, it is important to note the very low likelihood of core damage.

From the consequence point of view, it is important to notice that although these transients have the potential to cause core damage, the overwhelming likelihood is that such events if they were to occur, would occur with the core remaining covered with water. This means that, despite the overall negligible frequency of core damage, those core damage accidents that lead to uncovering of the core are about one hundred times less likely than those where the core remains covered .

The seismic contribution to the Core Damage Frequency has been analysed in two different scenarios.

The first scenario considers the contribution to the CDF for those seismic events whose frequency is up to that stated for the SL2 earthquake, that is, with a frequency higher or equal to 10^{-4}/year. This scenario is considered appropriate from the standpoint that the critical systems in the RRR have been designed to withstand this seismic event, according to the IAEA recommendations. However, because of the design of all safety critical items to a high level of confidence, low probability of failure at the SL2, the estimated additional CDF from seismic events up to SL2 level is negligible.

The second scenario considers the contribution to the CDF for all the seismic events indicated by the Hazard Curve for the site. This scenario is not considered credible, but in any case it was analysed in order to have an estimation of the seismic events beyond SL2. The CDF obtained by the summation over all the frequencies of seismic event sequences (for the full hazard curve) that may lead to core damage is

Mean CDF:	**3.3×10^{-8}/year**
5% Percentile CDF:	**5.69×10^{-9}/year**
95% Percentile CDF:	**2.5×10^{-7}/year**

These values, when compared with the contribution of internally initiated events, contribute in 32% to the overall CDF. Therefore, it can be stated that those seismically initiated accidents with the potential to cause a significant damage to the core, for the whole hazard curve (*eg* beyond SL2 level), pose a risk comparable to that posed by internal initiators to the public in the vicinity of LHSTC.

The total CDF including internal events and seismic events (bearing in mind that it is not usual nor meaningful to analyse the seismic hazard beyond return periods of about 100,000 years) is therefore

Mean CDF:	**8.8×10^{-8}/year**
5% Percentile CDF:	**1.1×10^{-8}/year**
95% Percentile CDF:	**4.5×10^{-7}/year**

Given the very low CDF estimates, the authors of the preliminary PSA felt it was no longer valid to have screened out certain other external events such as aircraft crash. Conservative frequency estimates of these other external events were added to the total CDF in that version of the PSA. Note, however, that recent work has shown that the estimates of these other external events were overly conservative and it is anticipated that these other external events will be screened out in the next revision of the PSA.

Level III PSA results

It is usual that the accident scenarios that contribute the most to the risk of a nuclear reactor are those that involve substantial damage to the reactor core. However, the very robust design of the RRR, with a high degree of redundancy and independence of its safety functions, makes these sequence to be of such a low probability, that they are not considered as credible.

These very low values fulfil the most stringent ARPANSA regulatory requirements for PSA frequencies. One of the reasons for this is that the PSA was developed at the same time the basic engineering was developed, and any weak points identified during the system's analyses for the PSA, were retrofitted to the designers, who in turn improved those system designs.

As a result, for the RRR the risk representative scenarios do not involve significant core damage. These accident scenarios were analysed and quantified both in their frequencies and their associated potential doses on the public.

The release categories (RC) for the representative release events, even when modeled under extremely conservative assumptions, show that the expected risk contribution of the selected accidents is well below the acceptable levels.

It is important to notice also, that the maximum doses do not require any off-site emergency measure (eg sheltering).

REFERENCES

i NUREG/CR-2300, PRA PROCEDURES GUIDE, , NRC, USA, 1983, pp. 3-21.

ii IAEA-TECDOC-517, “Application of Probabilistic Safety Assessment to Research Reactors”, Vienna, 1989.

iii J. Barón, J. Núñez y S. Rivera, "A Level III PSA for the Inherently Safe CAREM-25 Nuclear Power Station", Probabilistic Safety Assessment and Management 96, Cacciabue & Papazoglou (Eds.), 1996 Springer-Verlag, London, ISBN 3-540-76051-2, pp. 553-558.

iv SAFETY SERIES N° 50-P-7, “Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants”, International Atomic Energy Agency, Vienna, 1995.

v “A Level I + Probabilistic Safety Assessment of the High Flux Australian Reactor”, Pickard, Lowe & Garrick, January 1998

vi “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 6.54”, Idaho National Engineering Laboratory, Lockheed Martin Idaho Technologies Company, Inc., USA.

vii IAEA-TECDOC-930, “Generic Component Reliability data for Research Reactor PSA”, Vienna, 1997.

viii IAEA-TECDOC-478, Component Reliability Data for use in Probabilistic Safety Assessment, IAEA, Vienna, 1988