

**ARPANSA Public Forum
Safety of Proposed Replacement Research Reactor (RRR)
December 14 & 17, 2001
Sydney**

**Report prepared by:
Garry Schwarz
Canadian Nuclear Safety Commission**

Overview

I would like to take this opportunity to commend Dr. John Loy, CEO of ARPANSA for taking the initiative to hold this public Forum. It was clear from the remarks made by many of the participants that this opportunity to express their views in an open public setting was highly appreciated. Also worthy of note, is the professionalism displayed by all participants at the Forum and their willingness to engage in open and frank discussions on the issues. Without this type of cooperation by the participants, it would be very difficult to attain the objectives of a public forum.

Major Issues Arising From the Forum

I consider the following to be major issues arising from submissions and discussions at the Forum:

- A. Spent Fuel and Radioactive Waste Management Strategies
- B. Security Threats
- C. Emergency Response Plan
- D. Safety Analysis
- E. PSA
- F. Design

Following is a summary of my views on each of the preceding.

A. Spent Fuel and Radioactive Waste Management Strategies

Spent Fuel Management

This is clearly a significant issue for a number of the participants. As I understand the situation, the strategy is to have spent fuel reprocessed outside Australia and the products of reprocessing returned to Australia for storage. Several participants expressed strong scepticism that the reprocessing or conditioning of Replacement Research Reactor (RRR) spent fuel in France or Argentina as planned would be achievable given emerging situations and existing legalities in these countries. ANSTO outlined why it believes that the path it is pursuing with COGEMA (France) will be successful, and why it believes that the backup arrangements it has with INVAP in Argentina are viable. ANSTO also indicated that it is sufficiently confident in its plans that it has not considered a contingency plan that could involve reprocessing or conditioning of spent fuel in Australia.

In an effort to alleviate public doubts on this matter, I suggest that ANSTO update the information available to the public regarding the arrangements that have been made for the reprocessing of spent fuel from the RRR. ANSTO should indicate clearly the basis for its confidence that the arrangements will be successful. The public can

review this additional information and convey any further comments it may have to ARPANSA.

As indicated at the Forum, the public should be aware that as technology continues to evolve and governments reconsider current policies, a change in the approach for the management of RRR spent fuel over the lifetime of the RRR is a possibility. It is my opinion that any change will tend towards decreasing the risk associated with spent fuel management to the public and the environment.

Radioactive Waste Management Strategy

Several participants expressed dissatisfaction with the process leading to the determination of the low level and intermediate level radioactive waste management strategy. Of particular concern relative to the RRR is the case that facility operation may begin before the national low level and intermediate level radioactive waste repositories are built and ready to accept waste. The participants urged ARPANSA not to issue a construction licence until a viable plan for dealing with RRR radioactive waste is in place.

An application to construct a reactor should contain sufficient information about the management of radioactive wastes generated over the lifetime of the plant to give the regulator and the public reasonable assurance that this will be accomplished in a proper manner without undue risk to the workers, the public and the environment.

The Department of Industry, Tourism and Resources (DITR) indicated that it would be able to provide milestones for the repositories to ARPANSA in time for ARPANSA's deliberations on the construction licence application. These milestones, and the major prerequisite activities associated with each of them, should be submitted to ARPANSA in support of the construction licence application. However, it must be recognized that notwithstanding the best efforts to predict the milestone dates, milestones pertaining to such facilities often take longer to accomplish than originally predicted due to unforeseen circumstances. Sufficient contingency should be included in the RRR design to accommodate the temporary storage of radioactive wastes for a period of time which allows for reasonable delays. This information should also be submitted to ARPANSA in support of the construction licence application.

The discussion on this issue also identified several items that should be taken into account in the design considerations pertaining to the intermediate level waste repository. In particular:

- a) A design life of 50 years is generally regarded as too short.
- b) The design requirements must be such that all current (including wastes stored abroad) and future wastes arising from the reprocessing or conditioning of spent fuel can be accommodated by the repository.

B. Security Threats

Postulated Sabotage Events

Most participants expressed the need for a much closer examination of security threats to the proposed facility in light of the events of September 11, 2001. In their view sabotage is not adequately addressed in the PSAR. A proposal was put forward for a

postulated scenario that could be used to bound the radiological consequences to the public for any sabotage event on the RRR.

ANSTO indicated that a new analysis of a sabotage event has been completed but cannot be released to the public for security reasons. The new analysis involves the crash of a large aircraft into the RRR resulting in major core damage and the release of significant quantities of radioactive products. However, the consequences to the public have been shown to be so low that public countermeasures are not needed. The improved atmospheric dispersion of releases that would occur in the event of a large fire following the crash is likely the main reason for the predicted low consequences.

I commend ANSTO for considering a large aircraft crash and thereby responding to public questions on the potential consequences of such a sabotage event. A version of the analysis, which doesn't compromise security aspects, should be made available to the public to give the public some indication of the severity of the event considered, and why there are no predicted consequences of any significance to the public.

In my view, this analysis alone does not respond adequately to public concerns regarding potential sabotage events. ANSTO should also consider other sabotage possibilities that could result in major core disruption and significant radioactive releases. Since many scenarios can be postulated, it may be efficient to attempt to bound them using a severe accident analysis. The degree of protection afforded by such an analysis would depend upon the severity of the accident postulated. Such an analysis typically considers core disassembly with or without containment bypass, which results from a series of failures such as a loss of core cooling combined with failure of emergency cooling and failure of the reactor to shut down. Such an event could also be used as the basis for the off-site emergency plan.

Utilizing a severe accident analysis to bound the consequences of sabotage events should not remove the obligation from the designers to attempt to identify how saboteurs could produce such severe consequences. This is necessary to allow for the possible introduction of measures to minimize the likelihood of such an event occurring.

Security Measures

The Australian Safeguards and Non-Proliferation Office (ASNO) outlined the activities taking place in the preparation of the security plan for the facility. From the discussion, I have the impression that the activities are consistent with current good practices in this area. I suggest that consideration be given to include in the plan, routine security exercises involving simulated attacks on the facility to demonstrate that the security capability continually meets the expectations of the plan.

From a transparency perspective, it was my impression that the public generally accepts that security details should not be released. However, the public does want sufficient information to satisfy itself that security threats are being adequately addressed. ASNO should consider making available to the public the general principles that it is applying in preparing a plan to provide adequate security for the site.

C. Emergency Response Plan

Several participants indicated that there is no Emergency Response Plan in effect for the HIFAR facility. I understand that a plan does indeed exist involving various levels of local and state governments. To dispel any confusion on the issue it may be prudent for ARPANSA to provide an explanation of the plan to the public. The need for the distribution of potassium iodide pills could also be addressed in this explanation, as this was an issue with some participants.

Several participants took strong exception to the PSAR's contention that emergency off-site countermeasures, such as sheltering or evacuation, are not needed for the facility. In their opinion an event can arise which will result in significant off-site radioactive releases to the public. Terrorist attacks were given as an example of how such an event could occur.

I understand the public's desire to have in place an emergency response plan that can handle significant off-site releases even though the safety analysis contends that such a situation is extremely improbable. Such a plan provides reassurance to the public that even if the safety analysis predictions are off, they have another level of defence to protect them.

Two possibilities that ARPANSA may wish to consider for addressing this issue are as follows: One is to use the results of a severe accident analysis to bound terrorist attacks as the basis for the off-site emergency response plan. The second is to apply the approach used for HIFAR, which I understand is not related to any particular accident scenario, but which is based on conservative deterministic assumptions about core release, containment effectiveness and environmental conditions. Incidentally, the HIFAR approach, similar to the severe accident approach, affords a degree of protection against terrorist attacks by virtue of the large source term considered and the resulting release of radioactive products to the public. The approach used should be included in ARPANSA's reactor safety philosophy to make clear its role in the safety of the reactor and the protection of the public versus the design basis events considered in the safety analysis. It is important to ensure that the inclusion of such a severe consequence case does not remove incentive for designers to provide reliable and effective safety provisions to mitigate the consequences of the design basis events.

It was clear from the discussions that the public would like to have this issue resolved prior to issuance of a construction licence. In my opinion the accident basis (what some refer to as the 'Reference Accident') for the off-site emergency response plan and the responsible parties for developing the plan should be identified prior to the construction licence, but completion of the detailed plan can be left as a prerequisite for first criticality of the reactor.

D. Safety Analysis

Adequacy of the safety analysis

In summary, a number of participants were of the opinion that the PSAR does not adequately demonstrate the safety of the plant. There was a general feeling that the events analyzed were not severe enough. The opinion was given that some of the

beyond design basis events should be regarded as design basis, and that some probabilistic predictions seem overly optimistic.

Currently, the prediction of the probability of failure of equipment and systems is still sufficiently imprecise that results can be inaccurate and misleading. The uncertainty associated with probabilistic predictions is often larger than indicated, in particular when taking into account the limitations of the designers to understand and predict all possible failure modes of the design over the proposed lifetime of the plant including human error.

Regulators worldwide take a conservative approach when it comes to judging the safety of a nuclear reactor. For the reasons mentioned in the preceding paragraph, regulators usually find that when the selection of design basis events is influenced significantly by probabilistic arguments, the resultant safety analysis does not give sufficient confidence that a proposed nuclear facility will be adequately safe.

To compensate for the limitations of probabilistic predictions, most regulators rely extensively on engineering judgement and deterministic requirements when considering the design basis events that are to be included in the safety analysis. The results of a probabilistic assessment (PSA) are not ignored, but are used to confirm that no failure sequences defining design basis events have been overlooked, and that the classification of events in consequence categories and the associated reliability assumptions are conservative.

Application of the above approach normally leads to the identification of more demanding design basis events than would be arrived at through a probabilistic assessment. For example, excess reactivity insertion events would normally include a case involving the withdrawal of all reactivity devices (control plates) from the core at maximum speed with the core in its most reactive state, and loss of coolant events must consider pipe breaks up to guillotine failure of the largest pipe at the location leading to the highest consequences.

These analyses demonstrate the capability of the safety systems to limit the consequences of accidents up to the highest consequence case of each accident type that can be reasonably postulated. If safety systems cannot be shown to limit the consequences within defined regulatory limits, design improvements must be made, or adequate justification must be provided to the regulator, to demonstrate that the design is acceptable.

From the discussions at the Forum and my own look at the PSAR, I am of the opinion that the RRR safety analysis needs to include events that are more demanding of the safety features to better demonstrate their adequacy and the defence in depth of the RRR. This would give the regulator and the public more confidence that the plant is safe, and has a good measure of defence in depth against radiological consequences to the public.

Clearly, it is up to ARPANSA to decide on the path forward on this issue. I trust that the above information may be of assistance to ARPANSA in reaching its decisions.

Flow Blockage Event

Some participants questioned the basis for considering only 3 fuel plates melting.

The designers indicated that they do not believe that a fuel assembly can be damaged to such an extent during refuelling activities that the resultant coolant flow would be so low as to cause all fuel plates to melt during subsequent reactor operation. Blockage can also arise from debris, material or tools being accidentally left in the coolant system following maintenance activities.

The designers believe that the core flow system will detect complete blockage of one fuel assembly and indicated that a check for blockage could be performed following each refuelling. They also indicated that this feature could be demonstrated during commissioning tests.

Demonstration of the ability to detect flow blockage and the implementation of flow blockage checks prior to reactor restart following maintenance or refuelling will give added assurance of the low probability of this event. Nevertheless, it may be prudent to analyze the consequences of a total flow blockage of a fuel assembly to give assurance that even if such an event were to occur, the reactor is adequately protected and the consequences to the public are acceptable. The analysis may also provide further insight into such an event, which could lead to additional design or administrative measures to further minimize the likelihood of its occurrence.

E. PSA

Several participants raised concerns that the PSA results may be unduly optimistic, and that some influences, such as external events and fires, have not been adequately addressed. This input was based largely on the results of reviews of the PSA by two consultants. It was also noted that the prediction of core damage frequency was lower than results for other reactors by up to two orders of magnitude (10^2).

A PSA can be a very valuable tool for assessing the adequacy of the design. I commend ANSTO for producing this assessment as a part of the PSAR in support of the construction licence application. However, it appears that some improvements may be necessary to bring the PSA to current industry standards. ANSTO acknowledged that the core damage frequency prediction seems low and will review the assessment from that perspective. Also, a fire analysis will be undertaken and included. These are good initiatives by ANSTO but I am of the opinion that to settle the issue for both the regulator and the public will require an in-depth peer review by an individual recognized as a specialist in the field of PSA for reactors.

The outcome of the above activities could identify failure sequences that should be included as design basis events that might have been excluded previously on the basis of low probability. It could also identify the need for additional mitigating safety features to be included in the plant design. In view of this, it is my opinion that the activities mentioned in the previous paragraph should be completed before a decision on issuance of a construction licence is made.

F. Design

Design Status to Support Construction Licence Application

There was some discussion on the extent to which the design of the RRR should be completed prior to the issuance of a construction licence. Some participants felt that the design of the plant should be further advanced while others felt that the PSAR contained sufficient design information. It's an interesting issue about which there has certainly been a fair amount of discussion in my own country.

It's our experience that the design should be advanced to the extent that the regulator can have reasonable assurance that no significant design changes will be required following the issuance of the construction licence. In particular, the resolution of any remaining issues pertaining to the safety of the plant is not expected to result in the need for important design changes. Although this does not give an exact measure of how complete the design needs to be, experience has shown that the design of the major process and safety systems should be well advanced. Design requirements should be established and initial detailed design descriptions should be available.

Ultimately, it is up to the individual regulator (in this case ARPANSA) to decide on the degree of design completion that will give it reasonable assurance that significant design changes will not be necessary after construction begins.

Shutdown Systems

This subject received some discussion at the Forum. Most focused on the capability of the Second Shutdown System (SSS).

Effective and reliable shutdown systems are fundamental to the safety of any reactor. It is important that all safety significant issues relating to shutdown systems be satisfactorily resolved before issuance of a construction licence.

ARPANSA's regulatory guidelines state that nuclear reactors are to have two diverse and independent shutdown systems. This implies that each is fully effective for all design basis events and that each will be actuated in response to an accident to ensure the safety of the reactor. To achieve this, each shutdown system must have a full set of trip parameters, and adequate shut down speed and depth to be able to cope with each design basis event on its own. Failure of a shutdown system to meet any of the regulatory guidelines should be justified to ARPANSA on a case-by-case basis. Typically, a justification should demonstrate that the design change needed to meet the regulatory guideline is impracticable (crushing economic burden), and, in the absence of the change, the risk to the public is acceptably low.

First Shutdown System (FSS)

The control plates are used by both the reactor control system and the FSS. Reactors in other countries use the same approach successfully. However, it should be kept in mind that good safety practice everywhere minimizes common elements between process and protective systems to the extent that any identified cross-links can be clearly demonstrated to have no impact on the protective system. I understand that the designers have performed a review to check the RRR design for any mechanism associated with the reactor control system that might prevent the FSS from dropping the control plates to shut down the reactor when called upon. ARPANSA should

satisfy itself that the review was comprehensive and thorough, and that adequate compensating design measures have been taken to eliminate or minimize any such mechanisms that have been identified.

Second Shutdown System

There were some questions at the Forum related to the speed of dumping of the heavy water. A participant found that the PSAR did not contain sufficient information to allow an independent assessment of the adequacy of the design.

The issue of dump speed is a valid one as it is a fundamental requirement of any shutdown system to have adequate speed and depth to handle any accident situation. The PSAR should clearly state the design basis events that establish the design requirements for shut down speed and depth, and demonstrate that the design meets these requirements.

ANSTO claims that the design is adequate to handle all current design basis events. However, as indicated previously in this report, more demanding design basis events should be considered. This could prove to be a difficulty for the SSS as a more demanding event involving excess reactivity insertion may require a faster dump speed. Should the SSS, even with design changes, not be adequate to handle more demanding events, the acceptability of the design will need to be justified to ARPANSA.

Another issue of importance is the trip parameter coverage provided by the SSS. As stated previously, each shutdown system must have adequate trip coverage to handle all design basis events on its own. Primary and backup trip parameter coverage should be provided for all design basis events unless otherwise justified to ARPANSA.

Reliability of Shutdown Systems

Sufficient reliability analysis should be completed prior to the issuance of a construction licence to demonstrate that the shutdown systems will meet their reliability requirements during operation of the plant. It is common practice to set a design target significantly higher than the regulatory requirement to give added assurance that the reliability achieved during plant operation will meet the requirement.

At the Forum ANSTO claimed that the frequency of testing the control blades and dump valves, by testing only during reactor shut downs, would be adequate to demonstrate that the reliability requirements of the shutdown systems were being met. Assumptions such as this related to the testing of the system should be included in the reliability analysis. This analysis should be submitted to ARPANSA for review and acceptance prior to issuance of the construction licence.

Issues Not Covered At the Forum or in Public Submissions

Staffing and Training Program

Proposed staffing of the facility, including a staffing and training plan, should be submitted in support of the construction licence application. The staffing plan should include an organization chart with proposed staff numbers, the expected sources for

staff, and the qualification requirements. The training plan should include the development of a training program for RRR staff based on a Systematic Approach to Training (SAT) consistent with the recommendations of the IAEA. Schedules for staffing, training program development, and training should also be provided to give reasonable assurance that the applicant will be able to complete the required staffing and training within the timeframe established for the start up and operation of the facility.

It is our experience that staffing and training needs should be addressed at the construction licence stage to give added assurance that staffing and training will not be an impediment to reactor start up. It is also important that the regulator and the applicant come to a clear agreement on the staffing and training prerequisites pertaining to the start of reactor operation.

Configuration Management

Configuration management refers to the management of changes to a facility such that:

- a) The design, operation and safety documentation pertaining to the facility is always up to date,
- b) Changes receive a level of review appropriate to their safety significance. This may include regulatory acceptance of some changes such as those of importance to safety systems.

Configuration management is of benefit to the licensee and the regulator as it assures that information important to the safe operation of the facility, and the licensing basis, are kept current. To be effective, a configuration management system should be established early in the life of a project. For the RRR, I suggest that it be in place before issuance of a construction licence. I understand that the design of the RRR is essentially all computer based which should be of significant benefit in developing a practical and efficient system.