APPLICATION OF PROBABILISTIC METHODS FOR THE SAFETY ASSESSMENT AND THE RELIABLE OPERATION OF RESEARCH REACTORS

ANNEXES

CONTENTS

Annex I

APPLICATION OF A LEVEL 1 PSA OF LIMITED SCOPE FOR THE IEA-R1 BRAZILIAN 5 MW RESEARCH REACTOR[1]

I–1. INTRODUCTION

This case study is based on an academic work originally developed at IPEN, São Paulo, Brazil, in 2009, as detailed in Refs [I–1, I–2].

I–1.1. Background and general features of the facility

The IEA-R1 is a pool type, lightwater cooled and moderated, graphite and beryllium reflected research reactor. The facility is located in the premises of IPEN, a Brazilian institute for nuclear and energy research, in the city of São Paulo, Brazil. The reactor was designed and built by Babcock and Wilcox in accordance with the Brazilian Nuclear Energy Commission (CNEN) and financed by the United States of America's Atoms for Peace programme.

The IEA-R1 reactor's thermal power is 5 MW and the date of its first criticality is 16 September 1957; it has been operational for almost 56 years. During this time, it has been used intensively for basic and applied research, training and the production of radioisotopes.

Although designed to operate up to 5 MW, the IEA-R1 reactor operated at 2 MW up to the mid-1990s. In 1995, as a result of the growth in radioisotope demand, IPEN developed a modification project to modernize and upgrade the power of the reactor from 2 MW to 5 MW and to increase its operational cycle from 8 hours a day, 5 days per week, to a continuous 120 hour period per week. The upgrading process of the reactor was concluded in 1997, when the reactor turned 40 years old. Since November 1995, the reactor has been operating a continuous 64 hour period per week. The project of increasing IEA-R1 reactor power required a general revision of the various existing systems, which resulted in changes in some systems, replacement of some structures, and the introduction of new systems in order to ensure adequate safety of the reactor.

The application of the probabilistic safety assessment (PSA) methodology to the IEA-R1 research reactor is summarized in the following sections.

I–1.2. Selection of initiating events

Two categories of accident initiating events were used as the basis for the application of a Level 1 PSA of limited scope: loss of flow and loss of coolant. In the complete study developed in Ref. [I–2], all of the initiating events that had been grouped in these two categories and included in the safety analysis report for the IEA-R1 reactor [I–3], were evaluated qualitatively (see Table I–1).

[1] The content presented in this annex has been contributed by a third party. It is based on an academic work and presentation entitled "Estimative of core damage frequency in IPEN's IEA-R1 research reactor due to the initiating events of loss of flow caused by channel blockage and loss of coolant caused by large rupture in the pipe of the primary circuit — PSA level 1" [I–1, I–2].

Among all the initiating events with potential to cause meltdown of the core fuel elements, the event characterized as blockage of a single fuel cooling channel has the highest probability of occurrence [I–4]. On the other hand, among the initiating events grouped in the loss of coolant category, a major loss of coolant accident (LOCA) has the potential to cause the worst consequences because this event can lead to uncovering of the core in a short period of time (approximately 6 min) [I–3].

Based on the screening criteria for selecting the initiating events with the highest probability of occurrence and/or initiating events that can lead to severe consequences to the reactor core, the following initiating events were selected:

(a) Loss of flow caused by a fuel cooling channel blockage;
(b) Loss of coolant caused by a large rupture of the primary circuit piping.

TABLE I–1. LIST OF INITIATING EVENTS GROUPED IN LOSS OF COOLANT AND LOSS OF FLOW CATEGORIES ACCORDING TO THE SAFETY ANALYSIS REPORT FOR THE IEA-R1 REACTOR

Category	Initiating event
Loss of coolant accident (LOCA)	• Rupture of the primary circuit boundary • Damaged pool • Loss of pool water — Loss of water through the water retreatment system — Loss of water through the drains • Failure of the primary circuit drain • Failure of irradiation pipes • Failure of pneumatic pipes for irradiated material • Failure in thermal column
Loss of flow accident (LOFA)	• Primary pump failure (power supply failure and failure of the pump shaft — locked) • Inadvertent closure of reactor pool isolation valves • Fuel channel blockage • Flow reduction due to core flow bypass • Loss of heat sink • Primary coolant flow reduction • Improper power distribution due to, for example, unbalanced rod position, in-core experiments or fuel loading • Malfunctioning of reactor power control

I–2. ACCIDENT SEQUENCE ANALYSIS AND QUANTIFICATION

The following assumptions were taken into consideration in the evaluation of the two selected accident initiating events:

(a) Before the occurrence of the initiating event, the reactor is in normal operation at full power;
(b) Before the occurrence of the initiating event, all the safety systems, electrical power supply and support systems are available;
(c) After the initiating event 'rupture of primary circuit piping', the reactor protection system is successfully actuated to shut the reactor down;
(d) The occurrence of initiating events and other random failures are statistically independent;

(e) Time to failure is a random variable exponentially distributed (i.e. component failure rates are constant in time);
(f) Components are non-repairable during the observation period of reactor operation;
(g) The initiating event occurs during the observation period of reactor operation;
(h) Each reactor operation lasts approximately 63 hours, which is the mission time adopted in the analysis.

I–2.1. Fuel cooling channel blockage

This initiating event may have different characteristics depending on the flow direction of the reactor coolant. The IEA-R1 reactor core is cooled by demineralized water in a forced downwards flow. Downward cooling flow can lead to the blockage of one or more channels caused by objects dropping into the pool. The reduction of coolant flow can cause local overheating in the fuel element plate followed by failure of the cladding.

This type of problem may be detected:

(a) By the operator, by visual inspection during reactor operation.
(b) Through the indication of a significant increase in pressure loss (decrease in differential pressure) in the core, measured by a pressure transducer located at the top of the reactor pool (corresponding to a value above 10% of nominal flow).
(c) Through the indication of a significant increase in coolant outlet temperature (above 48^{o}C).
(d) Through the indication of a high radiation level in the pool hall, measured by detectors installed below the movable platform supporting the core. In this case, some kind of damage may have occurred already.

The immediate or automatic detection of this initiating event, especially when few channels are blocked, is not implemented in the IEA-R1 reactor protection system. In this situation, the differential pressure and temperature sensors will not detect small variations in the outlet primary coolant flow. If the operator does not detect this problem during visual inspection, the reactor will not be shut down and this may cause local damage to fuel element plates.

Furthermore, in the case of a reduction of the fuel element plate cooling, caused by channel blockage, a plate melt may occur. In this case, a release of fission products to the pool water and to the atmosphere of the pool hall may take place. This event might be detected by radiation monitors and the reactor protection system will actuate to shut down the reactor automatically. The regular ventilation system of the hot area will be turned off, the emergency ventilation system will be activated and the hot area will be isolated. Therefore, the emergency ventilation system forwards the air to the filters, decreasing the release of radioactive material to the environment.

After the detection of the event by the operator, the following safety functions are necessary to mitigate the consequences of a channel blockage so that there is no damage to the core and the release of radioactivity to the environment is not above the permissible limits:

(a) Shutdown of the reactor by the operator or through the reactor protection system actuation;

(b) The regular ventilation system turned off and the emergency ventilation and containment isolation systems activated.

In this case, the expected sequence of events was:

(a) Blockage of a few fuel cooling channels caused by the drop of an object into the pool, without the possibility of automatic detection;
(b) Visual detection of the problem by the operator followed by manual reactor shutdown;
(c) Shutdown of the normal exhaust and blowing systems of the hot area and startup of the emergency exhaust;
(d) Isolation of the hot area.

The evolution of the accident sequences is shown in the event tree presented in Fig. I–1. Only one sequence leads to a state without damage to the core (SEQ 1). In SEQ 1, the reactor shutdown is initiated by an operator action after detection, through visual inspection, of a channel blockage. The other sequences (SEQ 2, SEQ 3 and SEQ 4) lead to local damage to the core. In these sequences, the actuation of the emergency exhaust system as well as the hot area isolation do not avoid damage to the core, but they might minimize the accident consequences.

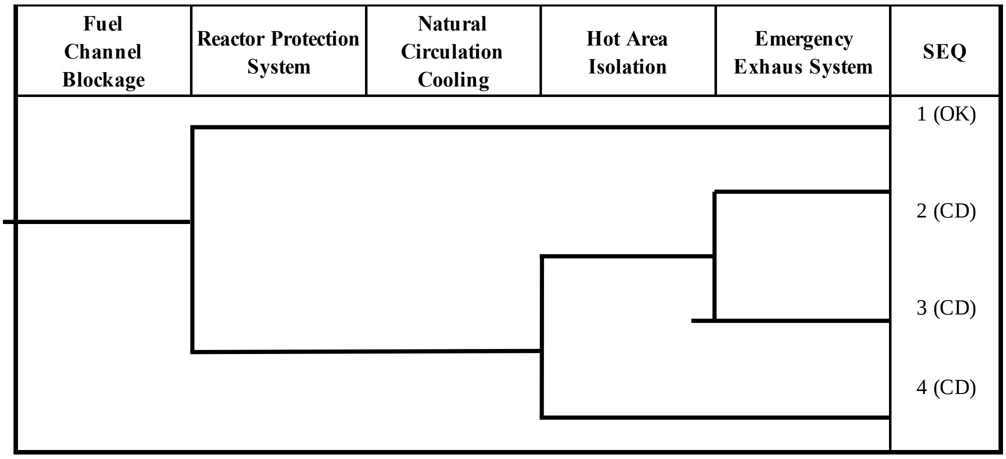


FIG. I–1. Event tree for the progression of a fuel channel blockage (adapted from original). CD — core damage.

The initiating event frequency was obtained from studies performed for similar reactors. The highest value chosen between the frequencies indicated in the PSA carried out for the Greek reactor [I–4] and in the preliminary PSA developed for the Australian reactor [I–5] was adopted. For the Greek reactor, the initiating event frequency is 10^{-2}/a, and for the Australian reactor, the frequency initially assigned to this initiating event is 1.3×10^{-5}/a. Both Greek and Australian reactors are open pool type research reactors with plate type fuel assemblies, similar to the IEA-R1 reactor. However, the Australian reactor has a nominal power of 20 MW(th).

The probability of failure of the reactor shutdown in case of a cooling channel blockage was calculated using the software SAPHIRE [I–6] and failure data were extracted from Refs [I–4, I–5, I–7, I–8]. The result obtained was 2.97×10^{-2}. This value was shown to be strongly influenced by the probability of an operator error. In fact, over 99% of the estimated value may be owing to the probability of occurrence of the following human errors:

(a) The operator fails to detect a channel blockage during visual inspection;
(b) The operator fails to proceed with the visual inspection;
(c) The operator fails to initiate reactor shutdown after detecting a cooling channel blockage.

For the IEA-R1 reactor, the probability of failure of reactor shutdown is 2.97×10^{-2} and the frequency of the initiating event 'fuel channel blockage' is 10^{-2}/a. Thus, the estimated value for the core damage frequency (CDF) owing to a fuel cooling channel blockage, is 2.97×10^{-4}/a. Although the estimated value is high, it can be considered to be acceptable because this type of accident would only cause minor damage to the core and would not cause large releases of radionuclides to the environment. The facility end state will be characterized by local damage to a few fuel plates in the core and the containment and the other safety systems will mitigate any potential release of radioactivity above the limits permissible for the population.

According to Ref. [I–3], the other initiating events grouped in the category 'loss of flow' may not lead to core damage in the IEA-R1 reactor. This conclusion was based on the assumption that the natural circulation of coolant through the core would be effective in removing residual heat and preventing the propagation of other accident initiating events in this category. However, this assumption was based on the success of the decoupling of the convection valve. If natural circulation of coolant fails, some damage to the reactor core may occur as a result of the occurrence of other initiating events grouped in this category. In this case, the most critical initiating event would be the failure of the pump shaft (locking), because the flywheel would not actuate, the forced circulation would be interrupted, and the amount of residual heat to be removed would increase significantly.

I–2.2. Large rupture in primary circuit piping

The postulated initiating event was a complete guillotine type rupture of the primary coolant return pipe, next to the reactor pool. In this case, it was supposed that the pool may empty out in approximately 6 mins [I–3]. Once the primary circuit is operating at low pressure and temperature, a guillotine type rupture of the pipe may only occur in the case of a missile crash. However, the primary circuit is well protected against external events and high magnitude earthquakes or aircraft crash accidents are very unlikely to occur according to Ref. [I–3].

In this case, the expected sequence of events is the following [I–3]:

(a) Rupture of the 250 mm primary circuit piping (return pipe to the pool).
(b) Alarm signal of low pool water level — 200 mm below normal level.
(c) Automatic reactor shutdown when the pool water level reaches 350 mm below the normal level.
(d) Automatic shutdown of the primary pump and closing of the primary circuit isolation valves when the pool water level reaches 400 mm below the normal level.
(e) The closure time of isolation valves is expected to be around 30–60 s, ensuring a minimum final pool water level of 6.0–7.5 m above the bottom.
(f) After the pool isolation and reactor core covering, the convection valve may be decoupled and the natural circulation cooling initiated; this procedure may be effective in removing the decay heat and maintaining the core at low temperatures.

(g) In the case of no decoupling of the convection valve, the natural circulation cooling will not be established, leading to local damage in the fuel plates [I–4].

(h) In the case of failure to close the isolation valves after the occurrence of a primary circuit piping rupture, the pool is expected to empty out in approximately 6 mins. When the pool water level reaches 4500 mm below the normal level, the emergency core cooling system (ECCS), for which actuation is passive, is required to provide the core cooling.

The evolution of the accident sequences is shown in the event tree presented in Fig. I–2. The four resulting accident sequences are:

(a) SEQ 1: rupture of the pipe followed by successful pool isolation, success in the decoupling of the convection valve and the establishment of natural circulation cooling. This sequence leads to an end state with no damage to the core.

(b) SEQ 2: rupture of the pipe followed by successful pool isolation, failure of the convection valve decoupling and failure of the natural circulation cooling. This sequence may lead to an end state with local damage to the fuel [I–4].

(c) SEQ 3: rupture of the pipe followed by failure of the pool isolation system and successful actuation of the ECCS. This sequence may lead to an end state with no damage to the core, because the ECCS is designed to cool the core and remove the decay heat adequately in this situation. It needs to be emphasized that this sequence may lead to loss of the radiation shielding provided by the pool water, resulting in direct exposure of the reactor core and, consequently, high radiation doses in the pool hall and inside the reactor building.

(d) SEQ 4: rupture of the pipe followed by failure of the pool isolation system and failure of the ECCS. This sequence may lead to an end state with core damage, because the core will be uncovered. This scenario is the most severe situation in relation to the melting of the core fuel and likelihood of a release of radioactivity. It needs to be emphasized that the reactor building ventilation system must be actuated to control potential releases of radioactivity.

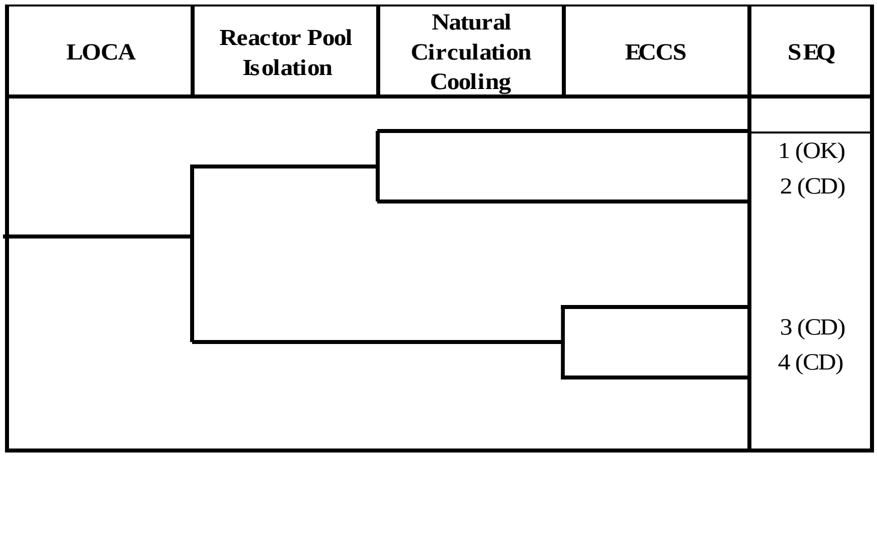


FIG. I–2. Event tree for the initiating event LOCA (adapted from original). CD — core damage.

The frequencies of occurrence of the four accident sequences described above are dependent on the following values:

(a) Frequency of rupture of the primary circuit piping;
(b) Probability of failure of the pool isolation system;
(c) Probability of failure of the natural circulation cooling;
(d) Probability of failure of the ECCS.

In order to obtain the probabilities of failure of both the pool isolation system and the ECCS, it was necessary to estimate the probability of failure of the power supply system for the following electrical panels:

(a) Motor control centre of 440 V — vital bus;
(b) Motor control centre of 440 V — essential bus;
(c) Electric distribution panel of 220 V — vital.

The probabilities of failure were calculated using fault tree analysis (with the software SAPHIRE [I–5]) and failure data were extracted from generic databases [I–7, I–9], studies of similar facilities [I–3, I–4] and the IEA-R1 specific database [I–9].

The following results were obtained:

(a) Probability of failure of the reactor pool isolation system = 1.53×10^{-3};
(b) Probability of failure of the ECCS = 1.97×10^{-4};
(c) Probability of failure of natural circulation cooling = 1.008×10^{-2} [I–4];
(d) Frequency of rupture of the primary circuit piping = 1.2×10^{-4}/a [I–4].

Thus, the frequencies of occurrence of the sequences that lead to core damage (SEQ 2 and SEQ 4) are equal to 1.21×10^{-6}/a and 1.35×10^{-10}/a, respectively.

I–3. CONCLUSIONS AND FINAL REMARKS

In the case of the initiating event ‘fuel cooling channel blockage’, it was shown that reactor shutdown is required and this is strongly dependent on operator action; therefore, the probability of failure of the reactor shutdown is strongly influenced by the probability of human error. For the IEA-R1 reactor, after the occurrence of a fuel cooling channel blockage, the CDF was estimated to be 2.9×10^{-4}/a. This frequency can be considered to be high, but this accident may result in minor local damage to the core, and consequently the occurrence of large releases of radionuclides into the environment is not expected. When compared with the CDF of similar facilities [I–4, I–5], the value obtained for the IEA-R1 reactor [I–1] was considered to be satisfactory.

In the analysis of the initiating event ‘loss of coolant due to a large rupture of the primary circuit piping’, two accident sequences were identified that might lead to core damage: SEQ 2 and SEQ 4.

The resulting frequencies of occurrence for these accident sequences were as follows:

(a) Frequency of occurrence of SEQ 2 = 1.21×10^{-6}/a;
(b) Frequency of occurrence of SEQ 4 = 1.177×10^{-12}/a.

For the conditions analysed, the reliabilities of the pool isolation system and ECCS were high. This was because of the redundancies implemented in the most critical points of these systems.

For the electrical power system, the probabilities of failure estimated for the CCM-E/V-11 buses were relatively high. This was because single failures of various components may lead to loss of power in these buses. To minimize this problem, the redundant valves of the same circuit of the primary system are supplied with electrical power in a crossover mode. Therefore, a failure of the pool isolation only occurs when both buses of the CCM-E/V-11 remain simultaneously without power (i.e. at least two components of the electrical system have failed).

The frequency of occurrence of SEQ 4 was very low and it was considered to be negligible. The frequency of occurrence of SEQ 2 was comparable to the values obtained in the PSAs of similar facilities reported in Refs [I–4, I–5]. SEQ 3 was not characterized as a totally safe scenario, because it may result in uncovering of the core, and the frequency of occurrence was estimated to be 1.0×10^{-7}/a.

Finally, from the results obtained in Ref. [I–1], it was concluded that the performance of the safety systems and operational procedures of the IEA-R1 reactor were deemed satisfactory when compared with other similar facilities. However, some recommendations were made in order to improve reactor safety:

(a) Implementation of a means for the automatic or immediate detection of a fuel channel blockage;
(b) Upgrade of the IEA-R1 electrical power supply system in order to improve its reliability and availability;
(c) Estimation of the probability of failure of the convection valve decoupling to calculate realistically the reliability of the natural circulation cooling function.

REFERENCES

[I–1] HIRATA, D.M., SABUNDJIAN, G., “Estimative of core damage frequency in IPEN’s IEA-R1 research reactor due to the initiating events of loss of flow caused by channel blockage and loss of coolant caused by large rupture in the pipe of the primary circuit — PSA level 1”, Proc. Int. Nucl. Atlantic Conf. (INAC 2011), Belo Horizonte, 2011, ABEN, Rio de Janeiro (2011).

[I–2] HIRATA, D.M., Estimativa da Frequência de Danos ao Núcleo Devido a Perda de Refrigerante Primário e Bloqueio de Canal de Refrigeração do Reator de Pesquisas IEA-R1 do IPEN-CNEN/SP-APS Nível 1, Master’s Thesis, Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo (2009), http://www.teses.usp.br/teses/disponiveis/85/85133/tde-02032010-081459

[I–3] INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES, “Relatório Final de Análise de Segurança — Reator IEA-R1” (1998).

[I–4] ANEZIRIS, O.N., HOUSIADAS, C., STAKAKIS, M., PAPAZOGLOU, I.A., Probabilistic safety analysis of a Greek Research Reactor, Ann. Nucl. Energy **31** 5 (2004).

[I–5] Summary of the Preliminary Analysis Report (PSAR) for the ANSTO Replacement Research Reactor Facility — Appendix — Probabilistic Safety Assessment. May 2001.

[I–6] IDAHO NATIONAL ENGINEERING LABORATORY, Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE), Version 6.41, INEL, Lockheed Martin Idaho Technologies Company, Inc. (1995).

[I–7] INTERNATIONAL ATOMIC ENERGY AGENCY, Generic Component Reliability Data for Research Reactor PSA, IAEA-TECDOC-930, IAEA, Vienna (1997).

[I–8] DE OLIVEIRA, P.S.P., et al., Análise Probabilística de Segurança e Integração de Sistemas – Sumário Executivo e Relatório Final do Projeto de Pesquisa Coordenado pela IAEA, Base de Dados de Confiabilidade para os Reatores IEA-R1 e IPEN/MB01 (Relatório Técnico — P&D.CENS.CENS.004.01) (2005).

[I–9] EIDE, S.A., CHMIELEWSKI, S.V., SWANTZ, T.D., Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs, EGG-SSRE-8875, Idaho Natl. Lab., ID (1990).

Annex II

APPLICATION OF A RELIABILITY ANALYSIS FOR THE BRAZILIAN IPEN/MB-01 RESEARCH REACTOR DURING ITS DESIGN PHASE[2]

II–1. INTRODUCTION

This case study is a summary of a project performed in 1985 which consisted of the application of the probabilistic safety assessment (PSA) methodology for the design review of a critical facility [II–1]. This assessment aimed to improve the prospective performance of systems and minimize the consequences of potential accidents.

II–1.1. Background

In the 1980s, one of the main nuclear engineering research and development projects in Brazil was the design and construction of a critical facility to be used in experimental neutron studies. Despite the low power levels of operation that characterize such facilities, reliability and safety were of particular concern, even in the facility's conceptual design phase when no precise results were available with respect to possible end states of the facility due to the propagation of accident initiators. Consequently, there was a strong motivation to evaluate at an early stage of the project the reliability characteristics of safety systems and the frequency of occurrence of potentially hazardous accident scenarios by means of PSA methods. The major objective was to try to integrate the reliability and safety assessment activities with those of design development in order to demonstrate potential hazards being statistically insignificant.

With this objective in mind, the preliminary design of the shutdown systems of the critical facility were submitted to a reliability analysis to evaluate the probability of a failure to scram. A goal of 1.0×10^{-5} for this probability was set at this phase, based on the performance characteristics of similar conventional shutdown systems of commercial nuclear power plants in operation. This reliability assessment, which is described in more detail in the following sections, led to improvements to the design of the shutdown systems.

Furthermore, with these improvements fed into the project, the frequency of occurrence of potentially hazardous accident scenarios was evaluated to compare them with the generally accepted 1.0×10^{-7}/a safety goal. Fault and event tree analyses were the basic tools used in this study. The following basic assumptions were made:

(a) Maintenance activities are always performed with the facility in shutdown condition;
(b) The facility will be operating 8 hours per day, 5 days per week, with a total mission time of 1920 hours for 1 year of operation.

The WASH-1400 [II–2] database was taken as the reference in the quantification of the basic events in the fault tree models, except for the 'rod fails to insert' event, for which data were obtained from Ref. [II–3].

[2] The content presented in this annex has been contributed by a third party. It is based on Ref. [II–1].

II–1.2. General description of the shutdown systems of the critical facility

The following shutdown systems are of interest throughout this case study:

(a) Rod insertion mechanism (RIM) — this system, when actuated, de-energizes the control/safety rod magnets, shutting the facility down if at least two out of four rods are inserted in the core;

(b) Moderator discharge system (MDS) — this system, when actuated, produces the opening of two valves, to let the water (coolant/moderator) flow out from the tank, shutting the reactor down if at least one of the valves operates successfully.

Both of these systems are actuated automatically by the protection system, which, in its original design, consisted of six nuclear instrumentation/protection channels (two period channels and four power channels). The RIM is actuated at the first abnormal period and power levels, and the MDS is actuated at the second abnormal period and power levels. A manual actuation (push button) is also provided for these systems. Furthermore, since the valves in the MDS are air operated and actuated by a solenoid valve, support system failures such as loss of electrical power supply or loss of air pressure are safe in the sense that they actuate the RIM or the MDS.

In Fig. II–1, a functional block diagram of the integrated shutdown systems is shown, where I1 and I2 represent the RIM and MDS interlock circuit, respectively, and the C*i* (*i* = 1, 2, 3,…, 6) represents each of the six protection channels.

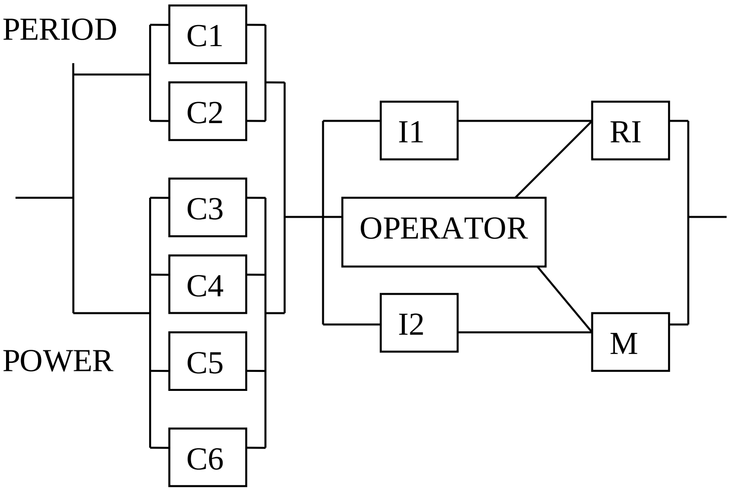


FIG. II–1. Functional block diagram of reactor shutdown.

II–2. RELIABILITY ANALYSIS OF THE REACTOR SHUTDOWN SYSTEMS

The reliability analysis of the reactor shutdown systems concentrated on evaluating the probability of the failure of a scram event, given a continuous reactivity insertion at a rate of 5 ¢/s. At that stage in design development, no precise information on the maximum reactivity insertion rate was available; the 5 ¢/s rate was suggested by the specialists as a reference.

In Fig. II–2, the power curves corresponding to the cases in which this insertion rate starts when the operating power equals 0.001 W, 1 W, 50 W and 100 W are shown. A closer examination of these curves, taking into account the fact that reactor shutdown occurs 1 s after RIM actuation and 8 s after MDS actuation, leads to the following conclusion: if reactivity insertion starts when the operating power lies between 0 W and 1 W, only the period channels will be able to produce reactor shutdown before power reaches excessively high levels. Similarly, if reactivity insertion starts when the operating power lies between 50 W and 100 W, only the power channels will be able to produce reactor shutdown before power reaches excessively high levels. For this reason, three accident conditions were taken into consideration corresponding to the reactivity insertion power ranges from 0 W to 1 W (condition AC1); 1 W to 50 W (condition AC2); and 50 W to 100 W (condition AC3). Under each of these conditions, credit was only given to those protection channels that could produce reactor shutdown before an excessive power increase. It is also worth noting that the reactor power operating range is 0–100 W.

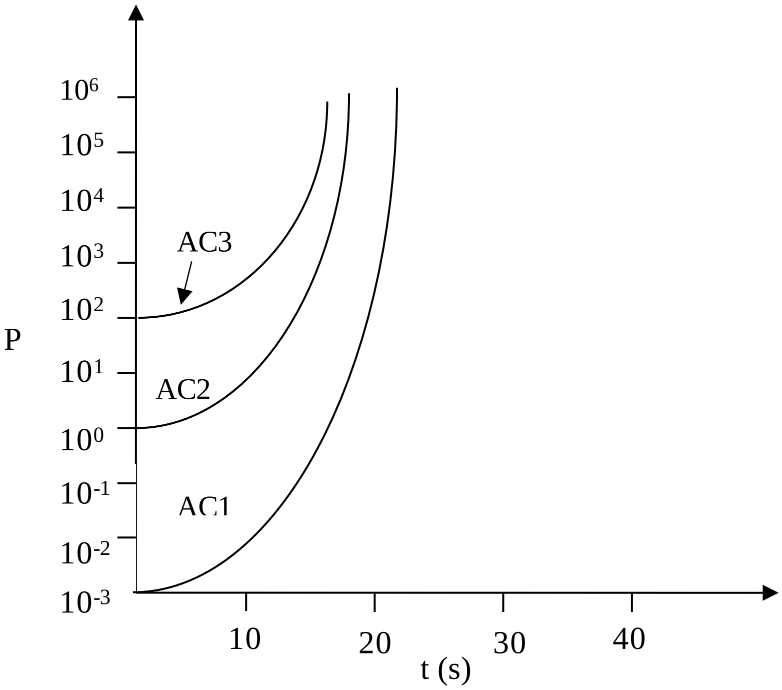


FIG. II–2. Power curves.

II–2.1. Failure to scram fault tree

The fault tree from which the results of this study were obtained was constructed from preliminary design documentation. The model covers not only RIM and MDS hardware, but also the nuclear instrumentation channels (protection logic) and interlock circuit hardware. Constructive details of this fault tree are presented in Ref. [II–4].

A first quantification of the fault tree was run in the most unfavourable case, which is that of unrepairable basic events. The results obtained showed that only under accident condition AC1 was the reliability goal of 1.0×10^{-5} for the probability of failure to scram not attained. In this case, failures of the protection channels contributed 95% of the total top event probability. It is worth noting that no credit was given to the MDS in this case, since it was anticipated that power could possibly reach excessively high levels within the time necessary for the MDS to shut the reactor down.

From this point on, the analysis concentrated on accident condition AC1 and examined the joint effect of alternative protection channel network configurations and periodic testing strategies on top event probability. More precisely, successive runs for fault tree quantification were made corresponding to combinations of two and three period channel alternatives for the protection system with one of the four periodic testing strategies of Table II–1. The main results obtained are shown in Table II–2. The results presented in Table II–2 indicate that better performance was possible provided that the protection channel network contained three period channels instead of two and maintenance procedures satisfied the requirements of periodic testing strategies A, B, C or D. It can also be observed from Table II–2 that further improvement to the failure to scram probability will depend predominantly on circuitry enhancements.

TABLE II–1. PERIODIC TESTING STRATEGIES

Basic event	Periodic testing strategy (hours)			
	A	B	C	D
Failure of channel to operate	8	8	8	8
Shift in channel calibration	480	320	160	80
Loss of power (RIM interlock)	1920	1920	1920	1920
Loss of power (other)	8	8	8	8

TABLE II–2. UNAVAILABILITY CONTRIBUTIONS

Strategy	No. of period channels	Shift in channels calibration	Loss of power in 3 out of 4 magnets	Loss of power in interlocks	Failure to insert 3 out of 4 rods	Total
Unrepairable	2	5.7×10^{-03}	$< 1.0 \times 10^{-10}$	3.1×10^{-04}	$< 1.0 \times 10^{-10}$	6.0×10^{-03}
	3	3.9×10^{-04}	$< 1.0 \times 10^{-10}$	3.1×10^{-04}	$< 1.0 \times 10^{-10}$	7.0×10^{-04}
A	2	3.8×10^{-04}	$< 1.0 \times 10^{-10}$	1.3×10^{-06}	$< 1.0 \times 10^{-10}$	3.8×10^{-04}
	3	7.5×10^{-06}	$< 1.0 \times 10^{-10}$	1.3×10^{-06}	$< 1.0 \times 10^{-10}$	8.8×10^{-06}
B	2	1.7×10^{-04}	$< 1.0 \times 10^{-10}$	1.3×10^{-06}	$< 1.0 \times 10^{-10}$	1.7×10^{-04}
	3	2.2×10^{-06}	$< 1.0 \times 10^{-10}$	1.3×10^{-06}	$< 1.0 \times 10^{-10}$	3.5×10^{-06}
C	2	4.3×10^{-05}	$< 1.0 \times 10^{-10}$	1.3×10^{-06}	$< 1.0 \times 10^{-10}$	4.4×10^{-05}
	3	2.8×10^{-07}	$< 1.0 \times 10^{-10}$	1.3×10^{-06}	$< 1.0 \times 10^{-10}$	1.6×10^{-06}
D	2	1.1×10^{-05}	$< 1.0 \times 10^{-10}$	1.3×10^{-06}	$< 1.0 \times 10^{-10}$	1.4×10^{-05}
	3	3.6×10^{-08}	$< 1.0 \times 10^{-10}$	1.3×10^{-06}	$< 1.0 \times 10^{-10}$	1.3×10^{-06}

II–3. ACCIDENT SCENARIO EVALUATION

The improved configuration of the protection system, with three period and three power instrumentation channels, was considered under maintenance strategy B and the following two categories of initiating events were examined: reactivity insertion and power distribution anomalies; and radioactive release from a system or component [II–4]. Of foremost importance in each of these categories were two initiating events:

(a) Initiating event 1 (IE1) — uncontrolled rod withdrawal at the speed of 1 mm/s (corresponding to the real continuous reactivity insertion rate of 1.8 ¢/s adopted in the facility design);

(b) Initiating event 2 (IE2) — experimental apparatus drop (corresponding to an instantaneous reactivity insertion of 66 ¢/s).

II–3.1. Event trees

The event tree headings are usually organized in a way to reflect the dependencies of a basic event heading on previous headings. Furthermore, in order to better represent the accident propagation chronology, an option was made to repeat system functions in the event tree headings.

Figures II–3 and II–4 are the event tree models for initiating events IE1 and IE2, respectively. PoC and PeC denote the power and period protection system network, respectively, and V*i* (*i* = 1, 2) denotes the valves of the MDS. Each of these models contains three accident scenarios that depict an undesirable final condition with the power level crossing the 1000 W threshold. No further quantification or qualification of the final conditions corresponding to the accident scenarios was possible at the time of development of this study.

II–3.2. Annual frequency of accident scenarios

The last columns of Figs II–3 and II–4 contain the annual frequencies of each accident scenario resulting from the propagation of initiating events IE1 and IE2 divided by their annual frequencies, F1 and F2, respectively. Whenever an undesirable or hazardous final condition is possible, an annual frequency below the generally acceptable 1.0×10^{-07} safety bound is obtained, provided that F1 and F2 do not exceed 1.0×10^{-05}/a.

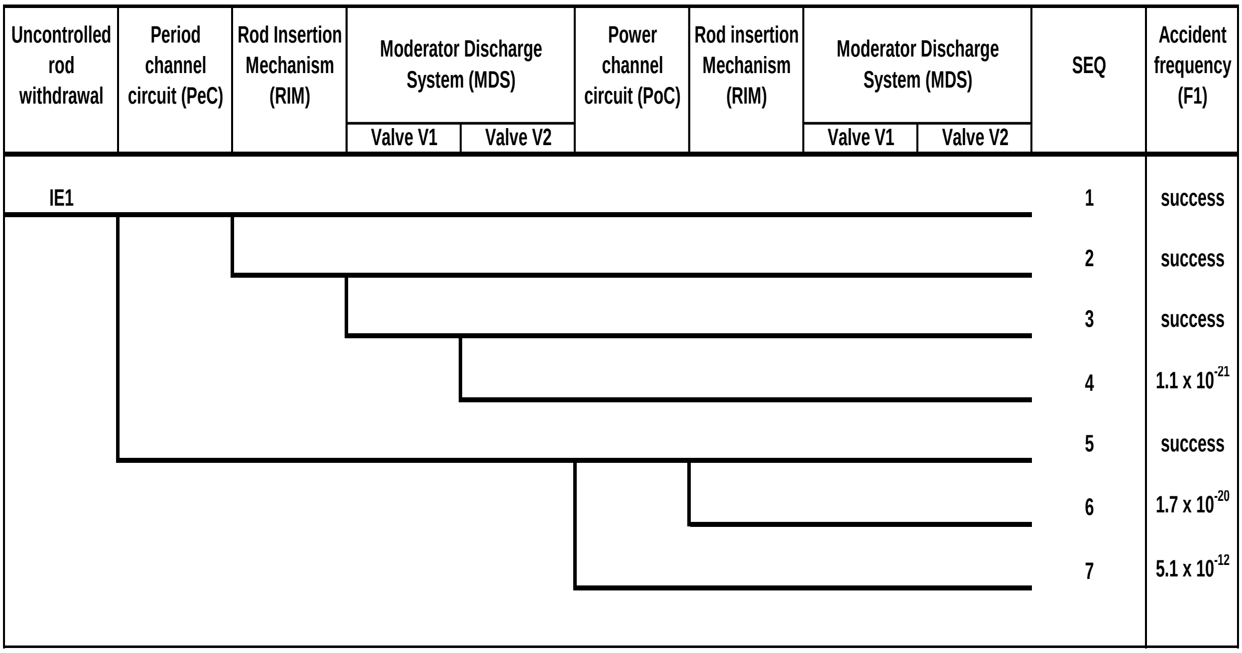

Uncontrolled rod withdrawal
Period channel circuit (PeC)
Rod Insertion Mechanism (RIM)
Moderator Discharge System (MDS)
Valve V1
Valve V2
Power channel circuit (PoC)
Rod insertion Mechanism (RIM)
Moderator Discharge System (MDS)
Valve V1
Valve V2
SEQ
Accident frequency (F1)
IE1
1
success
2
success
3
success
4
1.1 x 10-21
5
success
6
1.7 x 10-20
7
5.1 x 10-12

Fig. II–3. Event tree for initiating event IE1.

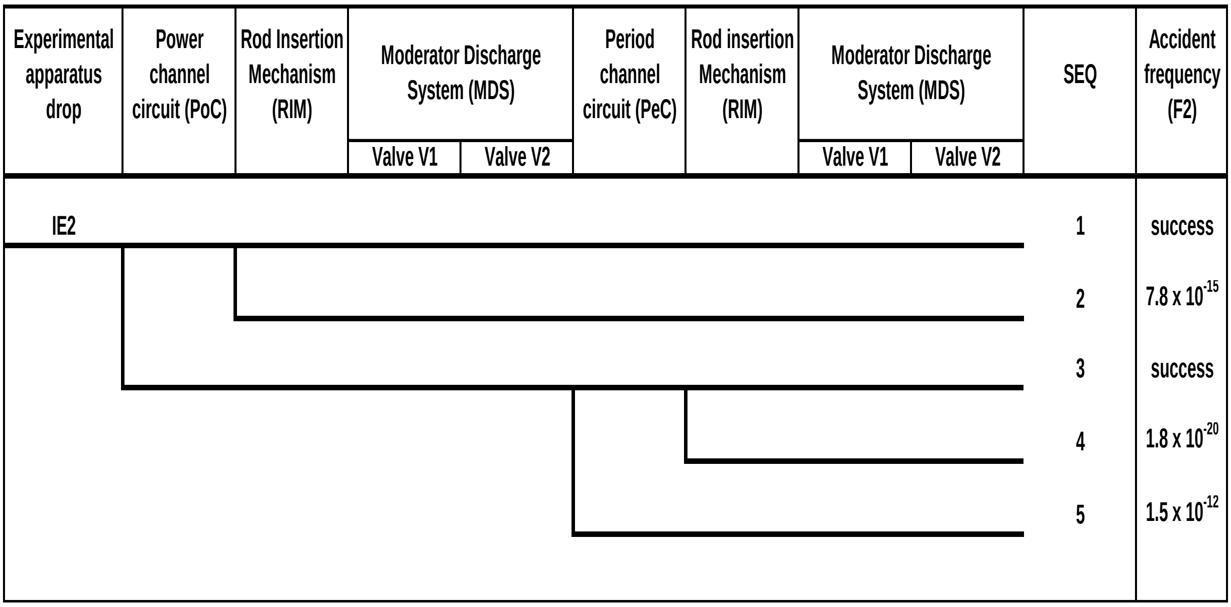

Experimental apparatus drop
Power channel circuit (PoC)
Rod Insertion Mechanism (RIM)
Moderator Discharge System (MDS)
Valve V1
Valve V2
Period channel circuit (PeC)
Rod insertion Mechanism (RIM)
Moderator Discharge System (MDS)
Valve V1
Valve V2
SEQ
Accident frequency (F2)
IE2
1
success
2
7.8 x 10-15
3
success
4
1.8 x 10-20
5
1.5 x 10-12

Fig. II–4. Event tree for initiating event IE2.

II–4. FINAL REMARKS

Since the analysis was conducted during the early stages of project development, concerns regarding common cause contributors were qualitative in nature. The application of other techniques, such as the beta factor method and Markov chain analysis, was left to the second stage of development, when more detailed documentation became available.

REFERENCES

[II–1] VIEIRA NETO, A.S., BORGES, W.S., "Reliability design of a critical facility: an application of PRA methods", Probabilistic Safety Assessment and Risk Management/PSA'87, (Proc. PSA'87 Zurich, 1987) Vol. 1, Verlag TUV Rheinland (1987), 716–721.

[II–2] US NUCLEAR REGULATORY COMMISSION, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, NUREG-75/014, USNRC, Washington, DC (1975).

[II–3] US NUCLEAR REGULATORY COMMISSION, Anticipated Transients without Scram for Light Water Reactors, NUREG-0460, USNRC, Washington, DC (1978).

[II–4] COMISSÃO NACIONAL DE ENERGIA NUCLEAR, Final Safety Analysis Report: Critical Facility, IPEN, CNEN/SP, São Paulo (1987).

Annex III

PROBABILISTIC SAFETY ASSESSMENT FOR THE OPAL RESEARCH REACTOR[3]

III–1.INTRODUCTION

This case study is a summary of the probabilistic safety assessment (PSA) developed for licensing the Open Pool Australian Lightwater (OPAL) research reactor. The analyses performed to conduct the PSA are described in Ref. [III–1], from which the material presented here was obtained.

III–1.1. General features of the facility

OPAL is an open pool type reactor. The reactor core sits in a deep pool of water that provides cooling of the core and protection against the effects of radiation. The pool's metallic liner is inserted in a high integrity reinforced concrete block. The reactor provides facilities for irradiation experiments and for the production of radiopharmaceuticals and silicon, as well as neutron beams for specialized research.

III–1.2. Objectives

The basic objective of the PSA was the quantitative evaluation of the risks associated with the operation of the reactor.

As part of this overall objective, the following specific objectives were pursued:

(a) Identification of internal and external events that may lead to accident conditions;
(b) Identification and analysis of the plant system responses to the initiating events identified as posing a relevant risk to the public and operators;
(c) Identification of systems, components and human actions that are important for the overall risk;
(d) Estimation of the impact of dependent failures on the overall risk;
(e) Estimation of the containment response and associated source terms for a few representative accident sequences;
(f) Comparison of representative accident sequences risks with the regulatory objectives;
(g) Pursuit of the following two additional operative objectives:
    (i) The development of a living PSA that will allow for any minor design change to be incorporated after the detailed engineering is finished, and preparation of an updated PSA for the final safety analysis report;
    (ii) The preparation of a comprehensive PSA document that will allow for auditing of the hypothesis, methods and assumptions included in it.

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

[3] The content presented in this annex has been contributed by a third party. It is based on "Highlights of the PSA Analyses Performed for the RRR", from the 9th Meeting of the International Group on Research Reactors (IGORR) [III–1].

III–1.3. Scope

The scope of the PSA was a Level 1 PSA with certain Level 3 considerations. The PSA included consideration of all envisaged operation modes of the reactor, 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 of performing the PSA, several conservative hypotheses were made.

III–1.4. Level 3 considerations

These considerations included the selection of a few accidents that were considered to be representative of the risk for 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 (i.e. with an upper bound frequency equal to or greater than 10^6 per year).

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 for the public expected for these source terms was also calculated, taking into account conservative weather and sheltering conditions.

III–2.ANALYSIS METHODS

III–2.1. Method for identification and selection of initiating events

The identification and selection of initiating events always raises the issue of the completeness of the PSA. For this PSA, source and event analysis was used. The source and event analysis method is a multistep, bottom up approach that consists of the following steps:

(a) Identification of the relevant radiation sources in the plant (e.g. core, fuel in the spent fuel pool, fuel in the shipping cask);
(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 source and event analysis method can generate a long 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 that 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 owing to its small inventory, it can be excluded for the purposes of the PSA in step (a) above. If a certain failure mechanism is known to occur very slowly (e.g. corrosion) and its status is readily identified, it may also be excluded in step (c) above.

A list of initiating events identified for this PSA is provided in Table III–1.

TABLE III–1. THE LIST OF INITIATING EVENTS IN PROBABILISTIC SAFETY ASSESSMENT FOR THE OPAL RESEARCH REACTOR

Category	ID	Description
A		**Reactivity transients**
	A1	Erroneous withdrawal of a control rod during startup
	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	Mechanical damage to the fuel assembly in the irradiated fuel assembly pool
	E2	Mechanical damage to the fuel assembly in the spent fuel storage racks in the reactor pool
	E3	Mechanical damage to the fuel assembly from an accident during transit
F		**Heavy water leak**
	F	Heavy water spill outside reactor pool
S		**Seismic events**
	S	Seismic event

III–2.2. PSA models and data

Once the initiating events had been established, the following steps were taken:

(1) An interference matrix was developed where each initiating event 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 helps in the definition of the success criteria for the event tree headers.

(2) 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 and I) drawings and the operational limits and conditions, where known, of each safety system, a fault tree was developed. These fault trees 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 (e.g. where all active components are in redundant sets).
The following systems were analysed in the fault trees:
(a) First and second reactor protection systems (FRPS and SRPS);
(b) First shutdown system (FSS);
(c) Second shutdown system (SSS);
(d) Flap valves and siphon effect breakers — which includes five conceptual headings:
(i) Siphon effect breakers (SEBs);
(ii) Suction and impulsion siphon effect breakers (S and I-SEBs);

(iii) Flap valves at level 6000 (FVL6000);
(iv) Flap valves at level 7000 (FVL7000);
(v) Flap valves at levels 6000 and 7000 (FV6 and 7);

(e) Emergency make-up water system;

(f) Emergency electrical power supply (EEPS).

(3) Qualitative event trees were developed. These trees were developed for each initiating event, with the corresponding headers obtained from the interference matrices. After the development of each event tree, a screening process was taken in order to eliminate those sequences that have no physical meaning or that are considered to be irrelevant.

(4) Once all the event trees and their corresponding headings had been delineated qualitatively, they were programmed in the SAPHIRE code [III–2]. These codified trees were then quantified at a component level. For the quantification process, the IAEA database on component failure was used [III–3, III–4]. 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.

(5) The Level 1 PSA results were analysed in order to obtain key end state frequencies, such as the core damage frequency (CDF) for the reactor. At this step, several importance measures were estimated, according to the Fussell–Vesely importance estimation, and sensitivity studies were 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.

(6) 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 1 PSA model. The objective was 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.

(7) In order to estimate plant behaviour beyond the scope of the Level 1 PSA, a few representative accidents were analysed to determine inventory, containment response and consequences of 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.

(8) 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 that a member of the public might receive, making conservative assumptions about parameters such as weather conditions and sheltering. The results were then compared against acceptance criteria and compliance was discussed.

III–2.3. Dependent failure analyses

Among the three types of dependent failure, namely functional dependencies, common cause failures and dynamic human interactions, the first and second types were incorporated in the PSA model, as follows:

(a) Functional dependencies between systems. These are where the success of one system is dependent on the success of another, for example owing 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 are modelled as a numeric fraction of the basic event failure probability that occurs independently (e.g. 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 effect were modelled as human errors:

- Design errors;
- Maintenance errors;
- Test, calibration and inspection errors.

These errors were developed as human error fault trees. The design errors were intended to represent the possibility that an underlying design fault causes the item to fail dependently with other items of its type (e.g. solenoid valves, which have an internal return spring that is susceptible to fatigue; control rods that might seize owing to an unforeseen interaction of lubricant and high humidity environment; or circuit breakers that might fail shortly after a high current event owing 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, 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 min. However, where credible operator actions that could jeopardize safety system functions were identified, they were included as basic events in the fault tree models. Furthermore, conservative assumptions were made regarding plant operations (e.g. that the operator prematurely shuts down the primary cooling system pumps following a trip).

III–3.RESULTS OF THE PROBABILISTIC SAFETY ASSESSMENT

Reference [III–1] indicates that the results presented are preliminary in the light of the stage at which the analysis was conducted. That is, the PSA models are based on the plant design at the end of the preliminary engineering phase. Operating and maintenance procedures, operational limits and conditions, 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.

III–3.1. Core damage frequency

The CDF obtained by the summation over all the frequencies of initiating event sequences that may lead to core damage is shown below:

- — Mean CDF: 5.5×10^{-8}/a;
- — 5% percentile CDF: 5.2×10^{-9}/a;
- — 95% percentile CDF: 2.1×10^{-7}/a.

These values, when compared with the safety limits and objectives, indicate with 95% confidence that the CDF fulfils the most stringent frequency of the safety objective (10^{-6}/a). Therefore, it can be stated that those accidents with the potential to cause significant damage to the core pose a negligible risk to the public in the vicinity of the reactor.

The relative contribution of each initiating event to the mean CDF is indicated in Fig. III–1.

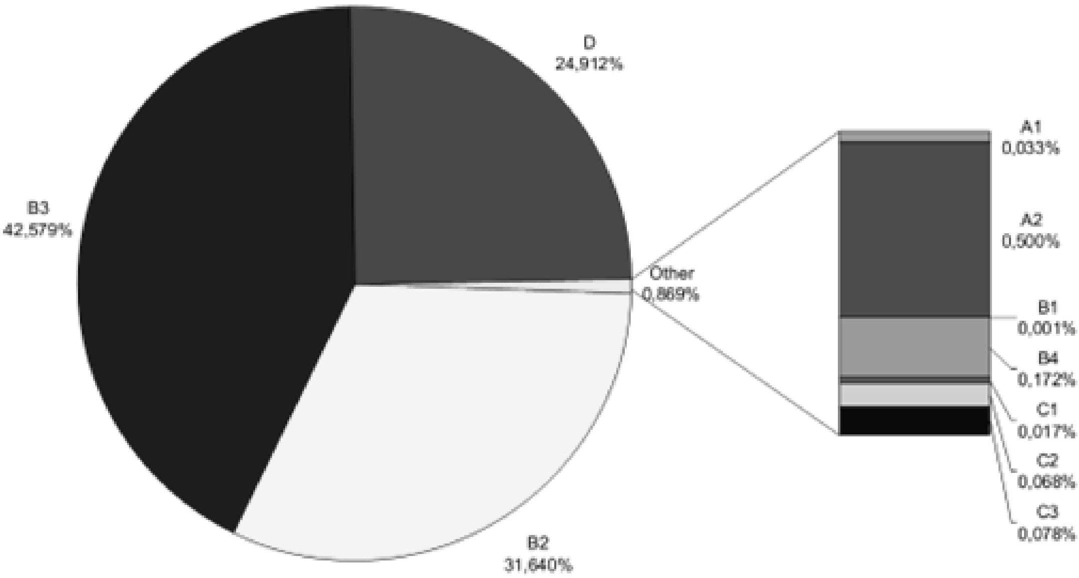


FIG. III–1. Relative contribution of each initiating event to the CDF.

The results highlighted by the authors of Ref. [III–1] include the following:

(a) It can be seen that the loss of flow and heat sink initiated transients makes a >99% contribution to the overall CDF.

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

(c) From the consequences point of view, it is important to note 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 approximately 100 × less likely to occur than those where the core remains covered.

The seismic contribution to CDF was analysed in Ref. [III–1], but this falls outside the scope of the current annex, which focuses on reactor operation.

III–3.2. Level 3 PSA results

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

These very low values fulfil the most stringent ARPANSA regulatory requirements for PSA frequencies. One of the reasons for this is that the PSA and the basic engineering were developed at the same time, and any design weak points identified during the system analyses for the PSA were referred to the designers, who in turn made the necessary improvements.

As a result, the representative risk scenarios do not involve significant core damage. These accident scenarios were analysed and quantified in terms of both frequency and potential radiation dose released to the public.

The release categories for the representative release events, even when modelled under extremely conservative assumptions, show that the expected risk contribution of the selected accidents is well below acceptable levels. It is also important to note that the maximum doses do not require any off-site emergency measures (e.g. sheltering).

REFERENCES

[III–1] BARÓN, J., NÚÑEZ MCLEOD, J., RIVERA, S., BASTIN, S., “Highlights of the PSA Analyses Performed for the RRR”, Proc. 9th Mtg of the International Group on Research Reactors (IGORR), Sydney, 2003.

[III–2] IDAHO NATIONAL ENGINEERING LABORATORY, Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE), Version 6.54, INEL, Lockheed Martin Idaho Technologies Company, Inc.

[III–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Generic Component Reliability Data for Research Reactor PSA, IAEA-TECDOC-930, IAEA, Vienna (1997).

[III–4] INTERNATIONAL ATOMIC ENERGY AGENCY, Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-478, IAEA, Vienna (1988).

Annex IV

APPLICATION OF PROBABILITY ASSESSMENT FOR THE SAFETY EVALUATION OF THE SAFARI-1 RESEARCH REACTOR[4]

IV–1.BACKGROUND

IV–1.1. Deterministic versus probabilistic analysis

Both deterministic and probabilistic safety analyses are necessary to comply with the licensing requirements of the South African National Nuclear Regulator (NNR). Neither analysis type alone is sufficient to provide complete disclosure of the hazards and risk of operation or to estimate the consequences and frequency of events for comparison with NNR safety and risk criteria. The need is therefore recognized for a robust and conservative deterministic analysis to demonstrate the fault tolerance of the engineering design and the effectiveness of the safety systems, complemented by best estimate probabilistic assessments to provide quantification of risks and assistance in design optimization.

Generally, a PSA provides a logical and systematic method to evaluate the overall safety characteristics of a complex engineering system. A PSA is a realistic, plant wide evaluation that considers the interdependence of frontline safety systems and supporting systems in quantifying the consequences to human health of accident scenarios. A PSA can identify events that are more or less likely to occur than the deterministically chosen set of bounding events. It considers the possible success or failure of each system or human action that might help to mitigate a sequence of events initiated by an internal or external event. A PSA examines multiple systems, components and human failures, and can provide a better understanding of which systems or human actions contribute significantly to the evaluated risk metric. A PSA can also be used for applications supporting the quest for optimal safety design of the plant. The capability of the PSA to be employed for this purpose depends largely on the scope and detail of the PSA, which in turn could be dictated by the maturity of the design.

In order to set up a reasonable PSA model of the plant, chapters of the safety analysis report have been extensively used to gain insight into the following aspects:

(a) The fuel, systems design and operation;
(b) Safety features;
(c) Sources of radiation and reactivity;
(d) Quality and safety management;
(e) Studying engineering diagrams, including the piping and instrumentation diagrams;
(f) Communicating with system and safety engineers regarding systems and plant behaviour;
(g) Interpreting system interactions (determination of system dependency matrix);
(h) Studying all relevant system and plant documentation;
(i) Actual operational experience and failures that have occurred in the past.

[4] The content presented in this annex has been contributed by a third party. It is based on Refs [IV–1] and [IV–2].

IV–1.2. SAFARI-1 reactor details

SAFARI-1 is a 20 MW tank in pool material testing reactor with lightwater moderated and cooled and beryllium reflected. It has been operational since March 1965 (>140 000 MW days). Primary activities include isotope production, silicon doping and beam port research. The reactor was fully converted to low enriched uranium fuel (U_3Si_2) and ^{99}Mo targets (UAl_2) in 2008–2009.

IV–2.LARGE LOSS OF COOLANT ACCIDENT

This case study presents the analyses performed for a large loss of coolant accident (LOCA) at SAFARI-1:

(a) The deterministic analysis, which provides the extent of core damage taking into account a number of additional concurrent failures;
(b) The probabilistic analysis, which considers the probability for those failures analysed deterministically to provide insights into the frequency of various extents of core damage.

IV–3.DETERMINISTIC ANALYSIS OF LOSS OF COOLANT ACCIDENT

Numerous LOCA scenarios involving a break in a section of the reactor’s primary system piping exposed to the atmosphere (as opposed to cover in concrete or pool water) have been analysed for SAFARI-1 and have considered a number of credible aggravating conditions. The safety analysis report identifies that a break in the primary inlet line to the reactor, at the elevation of the pipe tunnel floor (about 6.5 m below the core centreline) and downstream of the flow measuring orifice, envelopes all other conceivable break locations.

IV–3.1. Break formulation

The break considered in the analyses is a double-ended guillotine type break, which assumes that the 500 mm nominal diameter inlet pipe experiences a circumferential rupture and that the two broken ends separate sufficiently to eliminate any interaction between them during the ensuing transient.

The result is the exposure of two primary system openings into the pipe tunnel environment, each equal to the full bore of the primary inlet pipe. A further assumption is that the pipe tunnel environment is large enough to continuously present nominally ambient conditions in the vicinity of the break. Break scenarios include the following:

(a) Successful scram;
(b) Failed scram;
(c) Available electrical power (primary pumps operate);
(d) Simultaneous loss of both off-site and emergency electrical power (all pumps fail);
(e) Damage to the pool structure to the level of the instrument gallery floor, with accompanying loss of pool water inventory to that level.

All transients were run for 1000 s, at which time a clear quasi-equilibrium condition was attained for each transient. This means that the immediate evolution of each transient, driven by the initial decay heat of the core, core uncovering and reflooding, as well as the thermal hydraulic deterioration caused by the LOCA, has by then yielded its highest fuel temperatures.

IV–3.2. Discussion of deterministic results

The results of the set of LOCA analyses performed are presented in Table IV–1. In Table IV–1, the temperatures shown are the maximum temperatures experienced throughout the transient at the indicated location. Parenthesized peak temperatures indicate that the maximum temperature is, in fact, the nominal operational temperature at the start of the transient — in other words, the scenario only leads to a temperature reduction at the given location and no post-PIE temperature peaking is evident.

Normally the reactor vessel will reflood, after initial core uncovering (see Fig. IV–1), by means of the vessel vent connections which, under normal operation, transfer non-condensable gases from the reactor vessel to the pressure reference system, which is vented to off-gas.

During a LOCA with core uncovering, the pressure head of the pool will cause pool water to enter the reactor vessel through these connections. Such reflooding is also assisted by part (~50%) of the pool water entering at the tops of the Hartford loops that drop towards the vessel.

Reflooding by these pathways can be fairly slow. The availability of an additional reflooding path by means of a dedicated 50 mm inside diameter nozzle with a rupture disc, located in the vessel top, is also examined in these analyses and may be proposed as an upgrade.

The only scenario that yields fuel temperatures that are likely to result in fuel damage is that of transient LOCA-2a, in which a failure of scram and of off-site power is postulated. Core power is decreased by temperature feedback, but the absence of forced flow leads to a limited amount of fuel damage. The addition of the dedicated reflood nozzle eliminates this problem, as can be seen in the results of transient LOCA-2b.

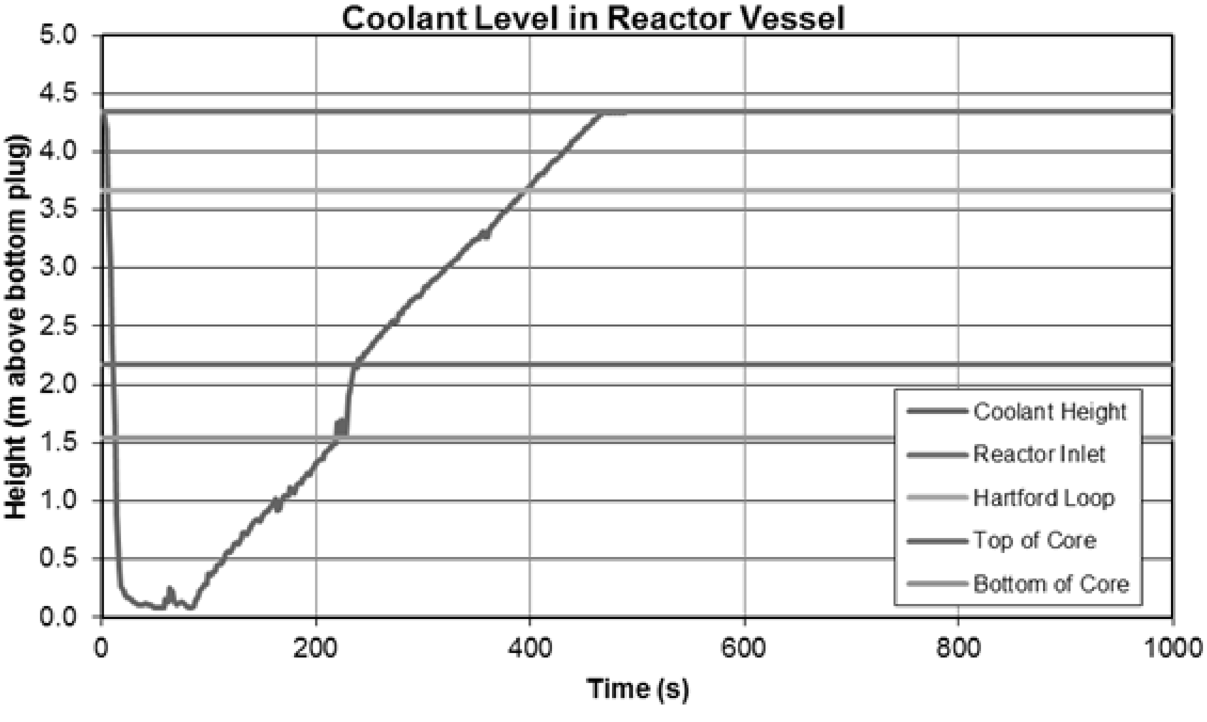


FIG. IV–1. Typical core uncovering and reflooding during a LOCA.

TABLE IV–1. TRANSIENT RESULTS FROM THE LOSS OF COOLANT ACCIDENT ANALYSES

Transient ID	Scram success	Primary pumps available	Reflood nozzle installed	Pool structure damage to instrument gallery floor level	Peak fuel temperatures (°C)[a]				Time of uncover; reflood (s)	Fuel damage	Time to core damage (s)
					Hot spot	Hot plate	Hot element	Balance of core			
LOCA-1a	Y	N	N	N	135.3	109.4	103.0	140.6	20; 169	None	n.a.[b]
LOCA-1b	Y	N	Y	N	(127.7)	(91.0)	(80.2)	(63.2)	21; 122	None	n.a.
LOCA-1c	Y	Y	N	N	(127.7)	97.6	98.4	120.1	11; 195	None	n.a.
LOCA-1d	Y	Y	Y	N	(127.7)	(91.0)	(80.2)	(63.2)	11; 141	None	n.a.
LOCA-1e	Y	Y	Y	Y	(127.7)	(91.0)	(80.2)	(63.2)	11; 261	None	n.a.
LOCA-2a	N	N	N	N	1062.9	832.55	834.22	250.8	20; 170	~1–2 FE[c]	55–70
LOCA-2b	N	N	Y	N	145.5	110.9	96.4	72.9	21; 122	None	n.a.
LOCA-2c	N	Y	N	N	136.1	111.3	294.6	138.2	11; 237	None	n.a.
LOCA-2d	N	Y	Y	N	(127.7)	(91.0)	(80.2)	68.9	11; 159	None	n.a.
LOCA-2e	N	Y	Y	Y	(127.7)	91.6	84.6	74.9	11; 235	None	n.a.

[a] Parentheses indicate that the maximum temperature is the nominal operational temperature at the start of the transient.

[b] n.a.: not applicable.

[c] FE — fuel element.

IV–3.3. LOCA management

A number of PIEs could result in transient LOCA-2a. One such PIE is an earthquake, which could simultaneously cause the rupture of the reactor inlet line, prevention of control rods insertion due to their lateral deformation, and loss of off-site power, causing the main primary pumps to stop. The earthquake could also damage the emergency power system to an extent that would render the emergency pumps unavailable, as well as damage the pool structure above the floor of the instrument gallery. There is a large difference in the pool wall thicknesses above and below the instrument gallery level.

Without the additional dedicated reflood nozzle, a limited amount of fuel damage (the equivalent of one or two fuel elements) could result. The addition of this reflood nozzle eliminates even this limited fuel damage (LOCA-2b). It is also clear that a failure to reflood the core will result in total core damage.

An additional shutdown capability independent of the control rods (a 'second shutdown system') would also eliminate fuel damage, as can be seen from the result of transient LOCA-1a.

Loss of a significant amount of pool water inventory owing to damage to the pool upper structure caused by the earthquake does not affect recovery from any of these transients.

IV–4.PROBABILISTIC ANALYSIS OF LOSS OF COOLANT ACCIDENT

The probabilistic analysis builds on the deterministic analysis by examining the probability for the various failures assumed and outcomes determined above. Table IV–2 presents the success criteria for various automatic and manual actions that are assumed to occur (or not to occur, as the case may be) following a loss of coolant caused by the break in the primary system line considered in the deterministic analysis. These criteria are then translated as follows to the top events in the event tree shown in Fig. IV–6:

- REACTOR SCRAM-6: automatic scram by the ΔP sensor trips;
- MANUAL SCRAM-4: manual scram by the operator;
- CORE COOLING N3: natural convection cooling of the core.

In the discussion below, a number of codes and abbreviations are used that have the following meanings:

- 2FEFS — two fuel elements damaged, release filtered via stack;
- CFEFS — total core damaged, release filtered via stack;
- CON — area contamination inside the building (at the location of the break and adjacent affected areas);
- IE — initiating event;
- RAD — high area radiation dose inside the building (at the location of the break).

TABLE IV–2. SUCCESS CRITERIA FOR LARGE LOSS OF COOLANT ACCIDENT

Event tree functional event	Event tree success criteria	Operator action	Comments
Automatic reactor scram will be initiated by the ΔP protection (REACTOR SCRAM-6)	Initiation of a reactor scram	None	The initiating event causes high radiation and contamination levels in the area where the break occurred and a reactor scram cannot prevent this. If the reactor does not scram automatically, the operator will be alerted by the core parameter alarms to scram the reactor manually. If the reactor is scrammed, the primary coolant is discharged from the system and the reactor vessel is reflooded with pool water, natural convection cooling of the core ensues that is sufficient to cool the core
Manual reactor scram (MANUAL SCRAM-4)	The operator, alerted by the core parameter alarms, scrams the reactor	Manual scram of the reactor	If the operator is not able to scram the reactor, the primary coolant is discharged from the system and the reactor vessel is reflooded with pool water, natural convection cooling is not sufficient to cool the core within 1 min
Core reflooded by pool water following a large LOCA (CORE-COOLING-N3)	Natural convection cooling maintains the fuel temperature below the onset of nucleate boiling temperature limit if the core has been scrammed and reflooded	None	If the reactor does not scram automatically or manually and primary pumps are not available, core cooling by natural convection fails and fuel damage 2FEFS develops. Failure to reflood the core will lead to CFEFS

IV–4.1. Failure analysis of the relevant protection and shutdown system functions

The criteria in Table IV–2 are then examined further by means of a fault tree analysis (Fig. IV–2) to determine the success or failure frequency of each action (e.g. of the instrumentation to detect the break, the reactor protection system to generate a scram demand, the scram system to shut the reactor down, the operators to scram the reactor manually).

The main indication of a large break in the reactor coolant lines in the reactor protection system is the core ΔP monitoring and trip system. This is measured simply as the pressure differential between the reactor inlet and outlet lines in the main pipe tunnel approximately 6.5 m below the core centreline. It therefore includes pressure drops in addition to that of the core only, but is used as an alternative verification by the reactor protection system that there is adequate flow through the core. The flow measurement itself takes place at the same location, but it must be considered that the break is after the flowmeter orifice and the indicated flow will therefore not deteriorate when the break occurs.

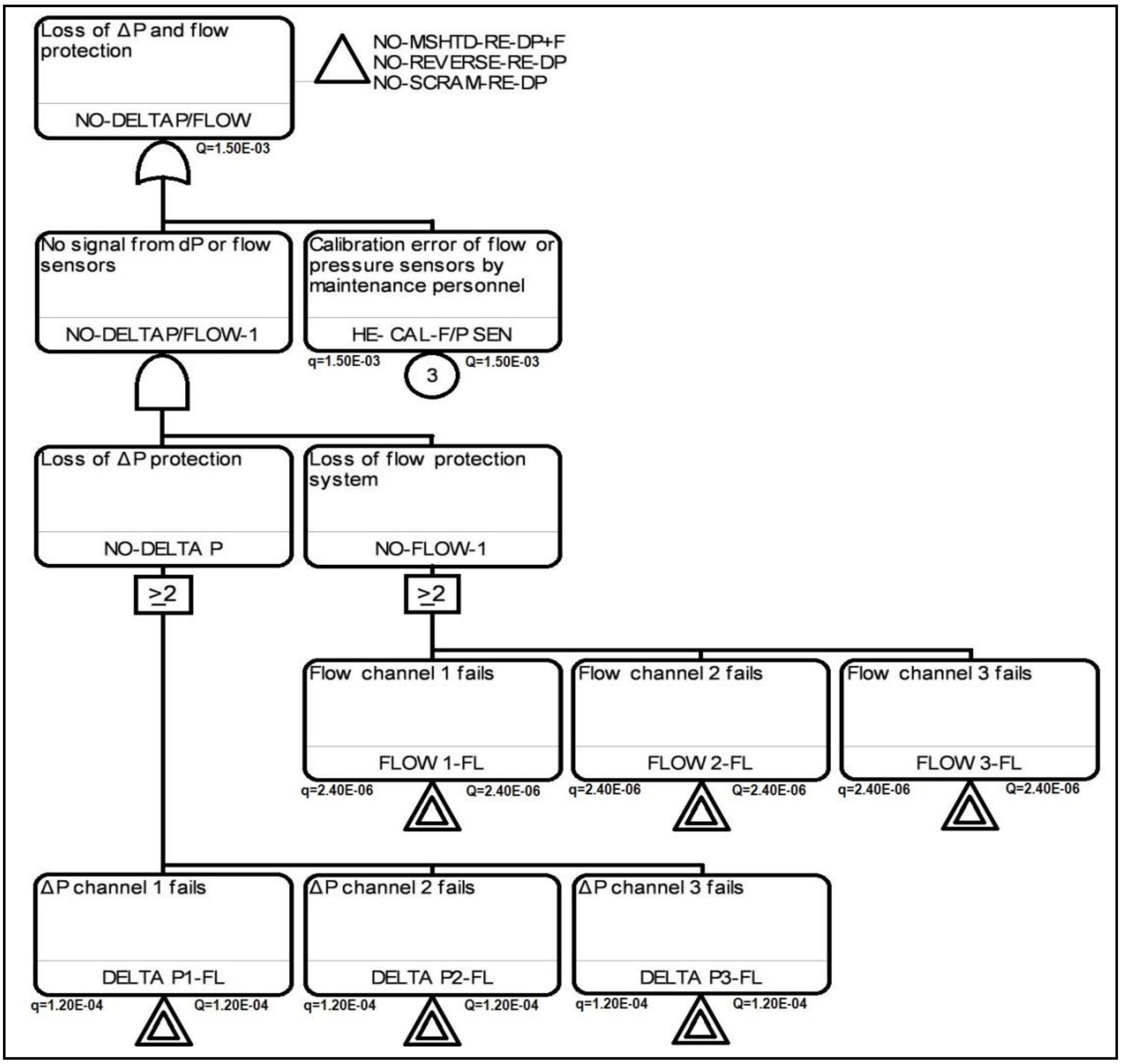
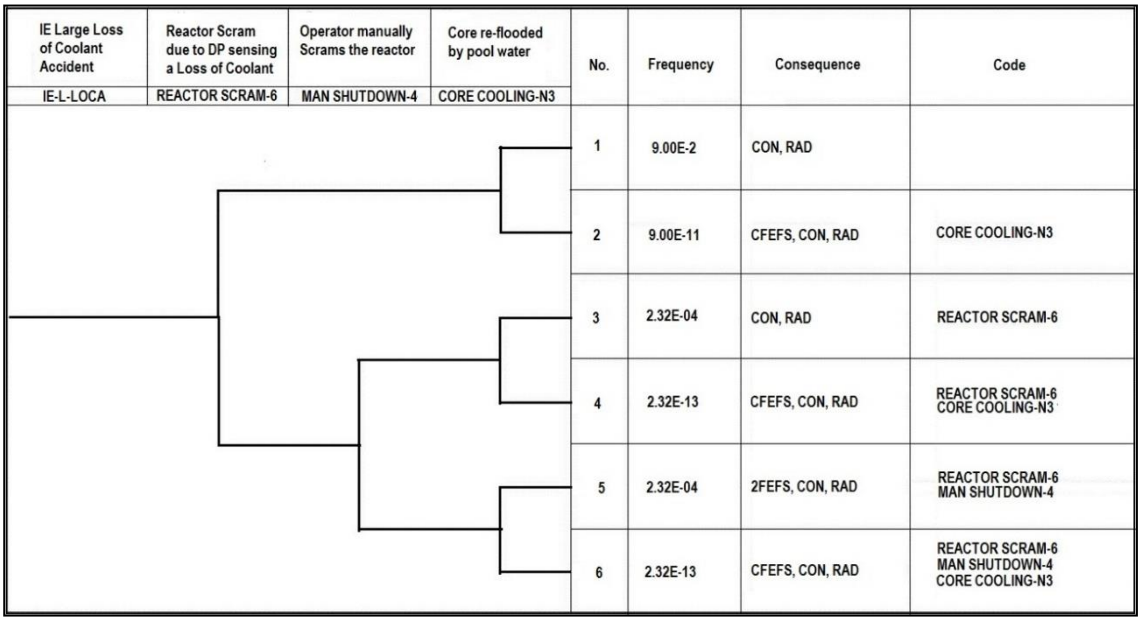


FIG. IV–2. Fault tree for the loss of ΔP and flow protection.

IV–4.2. LOCA event tree

With these inputs, the event tree shown in Fig. IV–3 can be developed and the frequency associated with each of the possible outcomes can be determined.



IE Large Loss of Coolant Accident	Reactor Scram due to DP sensing a Loss of Coolant	Operator manually Scrams the reactor	Core re-flooded by pool water	No.	Frequency	Consequence	Code
IE-L-LOCA	REACTOR SCRAM-6	MAN SHUTDOWN-4	CORE COOLING-N3				
				1	9.00E-2	CON, RAD	
				2	9.00E-11	CFEFS, CON, RAD	CORE COOLING-N3
				3	2.32E-04	CON, RAD	REACTOR SCRAM-6
				4	2.32E-13	CFEFS, CON, RAD	REACTOR SCRAM-6 CORE COOLING-N3
				5	2.32E-04	2FEFS, CON, RAD	REACTOR SCRAM-6 MAN SHUTDOWN-4
				6	2.32E-13	CFEFS, CON, RAD	REACTOR SCRAM-6 MAN SHUTDOWN-4 CORE COOLING-N3

FIG. IV–3. Event tree for the large loss of coolant. DP — differential pressure (sensor).

IV–4.3. Design basis for LOCA

A design basis threshold frequency, selected according to best international practice, determines the design basis upon which to build the defence against core damage caused by a large break in the reactor coolant inlet line.

IV–4.4. Release analysis for LOCA

In those scenarios analysed that lead to core damage, the fission products are released from the primary system into the reactor confinement system. The deterministic safety assessment provides information on release quantities and the PSA provides the focus for further transport analyses to determine the extent of the migration of these releases to points of emission to the environment, such as the following:

(a) Ventilation filters controlling releases to the ventilation stack, also considering failure of the filters;

(b) Breaches in the reactor building (failure of confinement, including collapse of the ventilation stack in an earthquake) leading to ground releases;

(c) Designated on-site and off-site zones, with consequent doses to employees, the public and the environment.

REFERENCES

[IV–1] SAFARI-1 Safety Analysis Report RR-SAR-0016 Rev 05, Ch. 16, “Safety Analyses”.

[IV–2] SAFARI-1 Safety Analysis Report RR-SAR-0021 Rev 02, Ch. 21 “Probabilistic Safety Analysis”.

Annex V

DEVELOPMENT OF A RISK MONITOR FOR AN INDIAN RESEARCH REACTOR[5]

V–1. INTRODUCTION

The traditional approach to operations and maintenance management in a nuclear plant is based on engineering judgement. Here, defence in depth and conservative criteria form the basis of decisions. Ideally, it is expected that the decisions are based on both the performance of the systems, structures and components (SSCs) and the quantified estimates.

The probabilistic safety assessment (PSA) methodology has matured sufficiently to be used in support of real time decision making in a nuclear facility. The failure rate estimates for SSCs are used as input for the PSA model to predict the performance in general and underline the degradation of SSCs. The system's unavailability and core damage frequency (CDF) are used as integrated indicators of the safety at system and plant levels, respectively. A risk monitor is an application of the facility's PSA model; combining the traditional deterministic approach with the probabilistic approach provides the existing performance status of SSCs, which is reflected as quantified changes in plant safety indicators and supports decision making.

A risk monitor for a research reactor has been developed as part of a research and development programme concerning the application of risk informed research for research reactors at BARC [V–1]. The results of a Level 1 PSA study in terms of equations for minimal cutsets, along with plant engineering information, form the major input. The uncertainty analysis module is one of the major features of the risk monitor that captures statistical variation in the data and the model. The risk monitor is envisaged to be operational in the plant control room to support decision making.

The state of the art in PSA enables a representation of the performance parameters for the components, safety and human actions in the form of reliability and safety. This approach provides a probabilistic, systematic and logical framework for the optimization of parameters in decision making. The outcome of this approach can be used for several decision making applications.

V–2. DEVELOPMENT OBJECTIVES AND APPROACH

The objectives for the development of the risk monitor, in addition to risk based plant configuration management, include the following:

(a) Assessment, evaluation and optimization of surveillance test interval and allowed outage time (AOT) as given in the technical specification of the plant and comparing the same with the existing deterministic rules;
(b) Identification and prioritization of technical issues;
(c) Decisions based on comparisons between operational risk and shutdown risk;
(d) Uncertainty characterization and sensitivity analysis;
(e) Shutdown scheduling;

[5] The content presented in this annex has been contributed by a third party. It is based on Refs [V–1] and [V–2].

(f) Implementation of a mechanism for incorporating international experience in support of decision making.

The approach has the following major features:

(a) Development of Level 1 PSA for full power as well as shutdown states of the research reactor;
(b) Preparation of core software specifications that take into account requirements for graphic user interfaces and plant operations;
(c) Development of software with sample cutset equations;
(d) Update and modification of the output of PSA studies, taking into account on-line risk monitor applications;
(e) Finalization and incorporation of the unavailability equation at system level and the accident sequence list at plant level in the core module of the software;
(f) Incorporation of plant reliability data for quantification of parameters;
(g) Performance of a test run as part of the validation and verification of the system.

V–3. CASE STUDIES

V–3.1. Uncertainty analysis

An uncertainty analysis for the research reactor PSA was carried out at two levels — the system and plant levels. An error factor of 3.0 was taken for all systems as both plant specific and generic data were used in the analysis. Generally, an error factor of 2.0 at component level is used if the data are plant specific, and an error factor of 3.0 is adequate to account for variability in generic data. Monte Carlo simulation was carried out using the risk monitor to propagate uncertainty in the fault tree from the component level to the system level and subsequently from the system level to the plant level. The median value of CDF comes out as 4.50^5 [V–2].

V–3.2. Configuration control

During the operation of a nuclear plant, the availability of equipment varies as a result of equipment failure or maintenance. The operating modes of available equipment can also change because of operational considerations. Plant configuration at a certain point in time can be characterized by the status of the equipment (e.g. out of service, open, closed, running, on standby). The status of significant safety equipment can directly influence risk. Even the status of non-safety related equipment can have an important impact on risk. For example, an activity to test equipment could increase the probability of the occurrence of an initiating event. Therefore, different combinations of equipment status, which include equipment under testing and maintenance, will result in different configurations of plant and different levels of risk. Risk based configuration control has two tasks, risk planning and risk follow-up. The former supports the preparation, planning and scheduling of plant activities and configurations.

An established risk based configuration control programme enables plant personnel to maintain and manage changes in risk owing to changes in plant configuration within acceptable levels under all states of plant operation. Examples of changes in facility configuration control are presented in Table V–1 [V–2].

TABLE V–1. FACILITY CONFIGURATION CONTROL

No.	Configuration	Time for configuration (h)	Core damage probability	Following 1 % acceptance criteria
1.	DG #1 is removed from class III system	240 (10 days)	1.46×10^{-06}	Yes
2.	MV-3101, class II, BRM V-3101	2	1.56×10^{-06}	No
3.	V-3139 and rupture disc #2	0.5	7.80×10^{-07}	No
4.	Pump #3	120	9.73×10^{-07}	Yes

V–3.3. Allowed outage time

The AOT for a particular system or component specifies the time period during power operation of the plant within which repair or maintenance have to be completed. If the system or component outage during operation is more than the AOT, the plant operating configuration or mode must change, or the plant has to be shut down.

AOTs were originally defined for corrective maintenance. Plant owners and regulatory authorities increasingly agree that planned preventive maintenance during power operation introduces potential benefits, such as improved equipment reliability, improved operational flexibility and outage work planning, as well as reduced risk during plant outages. Therefore, AOTs are now also used to control the times for preventive maintenance. For a risk based evaluation, the primary quantitative assessment focuses on the risk impact due to the AOT period. This requires assessment of three types of risk:

(a) Instantaneous risk while the component is in maintenance;
(b) Cumulative risk over the AOT period;
(c) Average risk over a long period (e.g. yearly), taking into account the frequency of maintenance performed on the component.

A number of redundant system components were chosen from the system component list to find the maximum permissible outage time during reactor operation. The observed results are presented in Table V–2 [V–2].

TABLE V–2. ALLOWED OUTAGE TIME FOR FACILITY COMPONENTS

No.	Equipment description	Equipment	Maximum AOT (days)
1.	Pump	Injection pump	6.57
2.	Valve	MV-3104	22
3.	Valve	MV-3101	16.5
4.	Valve	MV-3739	235
5.	Diesel generator	DG-1	23

V–4. CONCLUSION

The risk informed asset management methodology that uses the risk monitor mainly involves resource allocation and shutdown scheduling planning. The risk monitor that has been developed features all of the elements necessary for risk based management:

- CDF calculation;
- Generation of risk profile graphs for past configurations;
- Estimation of system unavailability and the contribution of the initiating event to CDF;
- Performance of importance analysis and uncertainty analysis;
- Storage of login sessions;
- Comparison of risk based surveillance test intervals with traditional surveillance test intervals and scope for technical specifications;
- Facilitation of shutdown maintenance planning and scheduling.

In view of these features, the risk monitor enables plant operators and managers to evaluate the risks and problems associated with plant configuration and maintenance activities. The risk monitor will therefore benefit plant managers and operating staff in the decision making process.

REFERENCES

[V–1] AGARWAL, M., VARDE, P.V., “Development of risk-informed approach for asset management — a case study on nuclear plant (VII-3A)”, 21st Int. Conf. Struct. Mech. Nucl. Reactors (SMiRT-21), New Delhi, 2011.

[V–2] VARDE, P.V., et al., Dhruva Level 1+ PSA, Internal Report, BARC, Mumbai (2002).