16.12 ANALYSIS OF LOSS OF HEAVY WATER EVENTS

Heavy water in the Reflector Vessel is used as the neutron reflector. The vessel is provided with a heavy water cooling and purification system. The rapid discharge of the heavy water from the Reflector Vessel also performs the function of the SSS.

Due to reactor design, loss of heavy water does not affect the core integrity. It is a source of radiological incidents only due to the tritium contained in the heavy water. For this reason the whole system has been designed to avoid and minimise leaks to the environment.

The heavy water circuit is a completely closed system contained within an airtight room. This room is not shared with any other system. Access to the room is restricted. The system is provided with helium as a cover gas.

The main components and features concerning safety aspects are:

a) The Reflector Vessel surrounding the core is connected to an expansion tank provided with heavy water level indication. There are redundant safety relief valves downstream of a venting valve located on the top of the Expansion Tank serving the system. These valves allow controlled cover gas venting upon detection of high pressure in the system. The venting valve can be opened manually from the MCR. Very high pressure in the Expansion Tank automatically opens the venting valve.

b) Two canned pumps are provided to move the heavy water around the system. They are canned to prevent leaks.

c) High quality piping and fittings.

d) Valves are of diaphragm type with safety seals. In this way leaks can be minimised.

e) Welded plate type heat exchanger in the primary reflector cooling circuit. Welded plates avoid and minimise leaks.

f) Intermediate heat removal loop. This is an additional barrier to avoid the release of tritiated water to the environment through the cooling towers.

g) The concentration of radiolysis gas is controlled..

h) Leak tightness to minimise isotopic degradation of heavy water. The degree of leak tightness is designed to allow for 10 years of operation before isotopic degradation becomes significant.

Besides these conservative design characteristics, a number of particular safety features are built into the design, e.g.:

a) On line control of deuterium and oxygen concentrations to avoid explosive mixtures as well as nitrogen control to prevent corrosion damage. Any failure of equipment would give rise to an alarm. The resultant likelihood of such a failure occurring as well as giving rise to an explosion is considered sufficiently low as to render such an incident beyond the design basis.

b) To avoid tritium release to the Reactor Pool, the Reflector Vessel operating pressure is lower than the Reactor Pool pressure at reactor core depth. Similarly, the intermediate loop pressure is higher than the reflector cooling loop pressure. Periodic radiochemical analysis provides information about isotopic quality, tritium levels and corrosion phenomena. Release of heavy water to the Reactor Pool or reflector cooling circuit is considered to lie within the design basis. The consequences of any leakage would be minor.

c) Monitors and leak detectors in the Heavy Water Room provide indication of leaks.

d) Dedicated instrumentation provides information on circuit variables. The reactor is shutdown in the event of low reflector cooling flow, high reflector temperature or very low level in the expansion tank.

e) An exclusive ventilation system is provided to permit the condensation and collection of any tritiated heavy water released to the Heavy Water Room. Any tritium release would be contained within the room and not transferred to other reactor areas or the environment.

f) The Heavy Water Room is at lower pressure than the neighbouring rooms.

g) There are no high energy lines (vapour, gas) inside the Heavy Water Room.

h) In the very unlikely event of beam tube failure (either cracks in the tube or failure of the seals), heavy water would leak towards the neutron beam tube where it would be contained. Humidity detectors in the neutron beam tubes would give rise to an alarm. As indicated in Section 16.11, failures of the beam tubes are considered sufficiently unlikely as to render them beyond the design basis.

i) In the very unlikely event of a failure of the vacuum vessel of the Cold Neutron Source, the introduction of heavy water would lead to loss of vacuum and give rise to an alarm. Such an event is considered sufficiently unlikely as to render it beyond the design basis.

j) The dropping of heavy objects on the Reflector Vessel does not represent a reactivity insertion hazard. Any failure of the vessel in this instance would lead solely to isotopic degradation of the heavy water. The Reflector Vessel is designed to withstand dropped loads and protection is in place to prevent damage to the Bulk Irradiation Facilities and the beam tubes. Dropping of heavy loads onto the Reflector Vessel is considered within the design basis. The consequences of any such drop would be minor.

Leaks of heavy water have no adverse impact on the core. Removal of heavy water from the Reflector Vessel results in an insertion of negative reactivity to the reactor core. If the heavy water leak persists, the RCMS would compensate the negative reactivity insertion by extracting control absorbers. However, the compensation is limited and a sustained leakage would lead to reactor shutdown.

The high quality of piping and fittings together with the small valves used in the system are such as to make the possibility of a catastrophic failure of the heavy water circuit so unlikely as to render it beyond the design basis.

Failure of any of the irradiation rig surrounds, including those of the pneumatic facility, results in leakage of pool water into the Reflector Vessel and subsequent isotopic degradation of the heavy water. Such failures lie within the design basis. They have minor consequences.

The radiological impact of the spillage of heavy water is confined to the Heavy Water Room. Therefore, the operators are the critical group for this event. Leaks of heavy water to the Heavy Water Room are considered within the design basis. The consequences of such a leak are minor. No release of tritium to the atmosphere is expected. For spillage of heavy water to the Reactor Beam Hall to occur, failure of a double barrier plus failure of the humidity detector in the beam tubes is necessary. The high quality of design ensures that this is a highly unlikely event and therefore beyond the design basis.

The floor in the Heavy Water Room has a slope directed towards a collection drain that directs the spilled water towards the heavy water storage tank. The slope is enough to drain all the spilled heavy water. After the heavy water has been drained, there would be a very fine layer of heavy water on the floor in addition to the water that has evaporated depending on the vapour pressure inside the room. A dedicated ventilation system would be actuated remotely by the operator. This operation continues until the heavy water has been completely removed from the room, as verified by the tritium monitor. In the unlikely event of an emergency that requires access to the room, the operator must wear a waterproof suit with external breathing air supply. Breathing air connections are supplied close to the entrance air lock. The air lock provides a barrier and control point.

On the basis of the above discussion, only minor leaks could eventually occur. The leaks and presence of tritiated heavy water would be confined to the Heavy Water Room , inside the containment. This room is not occupied during operation and is equipped with humidity and tritium detectors. Consequently, minor leaks are taken as the DBIE for the loss of heavy water.

16.12.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Heavy water circuit (cooling and purification circuit and second shutdown system) confined to Heavy Water Room, inside the containment
		Room is air tight and at lower pressure than the rest of the building.
		No occupancy of Heavy Water Room during operation; equipment controlled remotely.
		High quality materials
		Canned pumps.
		Nitrogen on line control to avoid corrosion
		On line control of deuterium and oxygen to avoid explosive mixtures
		Periodic visual inspection and appropriate maintenance programme
		All systems components made out of stainless steel
		Soft components (O-rings, diaphragms, gaskets, hoses and valve seats) made out of materials thoroughly resistant to radiation and severe operating conditions
		Low pressure system
		Special QA programme
		Overpressure protection device
		Valves with safety seals
		Welded plate heat exchanger
		Intermediate heat removal loop

Level	Main Characteristics	Safety Feature
		Control of leak detectors
		Design providing two barriers in the beam tubes
		Protections against missile over Reflector Vessel, irradiation rigs and beam tubes
		Reflector Vessel pressure lower than Reactor Pool pressure
		Intermediate cooling loop pressure higher than reflector cooling loop pressure
2	Operation control and response to abnormal operation	Alarms on: a) High water level in heavy water sumps b) Very low heavy water level in the expansion tank c) High system pressure (in some cases) d) Low flow of the reflector cooling system
		Humidity detection in the beam tubes
		Indication of abnormal neutron behaviour
		High tritium activity level.
3	Control of accidents within the design basis	Event causes shutdown through dilution of reflector
		FRPS reactor trip on; a) Very low level in the expansion tank b) low flow in the reflector cooling loop SRPS reactor trip on; Failure of the FSS,
		Slope in floor of Heavy Water Room to drain spillage to Heavy Water Storage Tank
		Camera in Heavy Water Room to monitor remediation operations.
		Dedicated ventilation system to retain tritiated heavy water.
		Breathing air connection in air lock

16.12.2 Design Basis Postulated Initiating Event

A summary of the previous discussions and identification of those DBIEs requiring further analysis are presented below:

PIE	Not applicable to the design	Sufficiently unlikely to occur (BDB)		Design Basis Initiating Events (DBIEs)		
				To be considered in other DBIE group	Bounded by other DBIE	Requires Analysis
Explosion due malfunction of the on-line control of deuterium and oxygen		X				
Leakage into Reactor Pool				Minor consequences		
Beam tube failure		X				
CNS vacuum vessel failure		X				
Heavy object drop onto Reflector Vessel				Minor consequences		
In leakage of light water into Reflector Vessel				Minor consequences		
Leaks into Heavy Water Plant Room						X

The identified DBIE requiring further analysis is a leak from the heavy water circuit, spilling 10 times the maximum expected annual leak volume (1kg), i.e., spilling 10kg.

16.12.2.1 Detection of the Initiating Event

The event is reported by alarms. The reactor is manually shutdown.

Alarms are triggered on the following variables:

a) High water level in Heavy Water Room sump

b) Very low level in the reflector expansion tank

c) detectors for tritium leaks in the Heavy Water Room

16.12.2.2 Design Basis Fault Sequence

a) Heavy water leaks.

b) Loss of heavy water triggers alarm due to tritium and water in sump in the Heavy Water Room.

c) The heavy water spilled into the room is drained.

d) Operator remotely starts ventilation system in the Heavy Water Room.

e) Unless already carried out, the operator manually shuts down the reactor.

f) Operator shuts down the Reflector Cooling and Purification System.

16.12.2.3 Numerical Analysis

No numerical analysis of this event has been performed since it does not affect adversely the core or irradiation facilities. If the leak cannot be made up, the loss of heavy water from the Reflector Vessel would insert negative reactivity into the core. The RCMS would compensate by withdrawing the control plates. The available reactivity would not be enough to compensate the loss of the reflector and the reactor would shutdown.

16.12.2.4 Radiological Impact Analysis

Due to the design of the Heavy Water Room and associated systems, no tritiated water would be released to the atmosphere. As stated above, failure of the Reflector Vessel would result in isotopic degradation of the heavy water due to inflow of light water rather than a leakage of heavy water to the Reactor Pool and thence to the Reactor Hall. Exposure of the operators to tritiated water or water vapour would be avoided by the action of the ventilation system of the Heavy Water Room and the passive drainage of the spillage to the heavy water storage sump.

16.12.2.5 Conclusions

Loss of heavy water results in safe reactor shutdown. This is an inherent design feature of a heavy water filled reflector. Although the RPS are capable of functioning automatically and shutting down the reactor, neither is required for this event. Loss of heavy water does not challenge nuclear safety. The tritiated heavy water would be contained and any releases of tritium to the facility atmosphere strictly controlled. Such releases would not represent a hazard to the operators or the public.

End of Section

16.13 ANALYSIS OF ERRONEOUS HANDLING OR FAILURE OF EQUIPMENT OR COMPONENTS EVENTS RELATING TO FUEL ASSEMBLIES

16.13.1 Introduction

This Section analyses the occurrence of a failure of equipment or components related to Fuel Assemblies. All of these events potentially have a direct impact on the operator. Failure of fuel plate cladding or mechanical damage to a Fuel Assembly could lead to release of fission products into the Reactor Pool, the containment and eventually the environment. However, extensive damage to the core due to cladding failure or mechanical damage is not credible. Consequently, the operators are the critical group for consideration of consequences.

16.13.2 Fuel Plate Cladding Failure

This section addresses localised fuel cladding failure during normal operation or Anticipated Operational Occurrences as a result of manufacturing errors. Mechanical damage due to mishandling or dropped loads is covered in the next section. The fuel matrix and the cladding of the fuel plates form the first barriers for the fission products generated in the fuel assembly. A frame and two covers of Aluminium alloy constitute the cladding. Section 5.3 presents a description of the fuel assembly design.

The design and manufacture of the Fuel Assembly minimises the defects that could lead to a localised failure of the cladding and liberation of fission products into the PCS.

The fuel assembly design and manufacture is carried out in accordance with the necessary QA practice applicable to the nuclear fuel industry for research reactors.

The design of the fuel assembly includes consideration of prevention or minimisation of the following effects:

a) Heat generation effects:

   (i) Reduction of cooling channel thickness due to thermal expansions of fuel plate.

   (ii) Thermal stresses on fuel plate as a consequence of non-uniform temperature distribution and external restraints to thermal expansions.

   (iii) Regardless of the high specific powers of most research reactors and taking into account the good thermal properties of aluminium and its alloys as well as the high surface to volume ratio in plate geometry, both maximum temperature values and thermal gradients are quite moderate. This minimises the deformation of the fuel plate due to thermal effects. The width of the cooling channels has been designed accounting for variations due to fuel plate dilation. Given the moderate temperature in the fuel plate, the potential variation in width is much less than the design value.

b) Hydraulic and mechanical loads:

   (i) Hydraulic instability due to excessive coolant velocities.

   (ii) Risk of plate elastic buckling due to lateral compressive loads.

   (iii) Mechanical stress on fuel assembly bottom nozzle due to interaction with reactor grid plate and fuel clamp.

   (iv) Mechanical stresses on fuel assembly structure during refuelling operations.

(v) Differential pressure between the inner and outer fuel plate.

(vi) Design limits on coolant maximum velocity prevent hydraulic instabilities.

(vii) The fuel plates withstand the eventual differential pressures between two cooling channels. No deformation is expected.

c) Radiation effects:

(i) Swelling and blistering of fuel plate due to build up of fission products.

(ii) Changes in physical and mechanical properties of fuel assembly materials (thermal conductivity, yield and ultimate strengths and ductility).

d) Chemical interaction with coolant:

(i) Uniform corrosion of exposed surfaces, especially on the hottest fuel plate.

(ii) Localised corrosion phenomena, such as pitting and galvanic corrosion.

On the basis of the arguments presented above and in Section 5.3, failure of fuel plates due to manufacturing faults and corrosion problems, although unlikely, will be considered to lie within the design basis.

16.13.2.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Low limit in maximum cladding temperature during normal operation.
		Variation in thermal and mechanical properties of Aluminium accounted for in design.
		QA programme for fuel assembly design and manufacturing
		High Surface to volume ratio in fuel plate favours heat removal and moderate temperature gradients.
		Design limit on maximum coolant velocity.
		Presence of gas inside fuel plate meat during manufacturing strictly avoided.
		Allowance in variation of cooling channel thickness due to swelling or deformation accounted for in the design.
		Changes in thermal and mechanical properties due to radiation effects considered in the design of fuel assembly and cooling system.
		Strict water chemistry control to avoid corrosion.
		Mild operating conditions (moderate temperature and controlled water quality).
		Adequate behaviour of the fuel matrix as a retention agent for fission products, particularly fission gases.
2	Operation control and response to abnormal operation	Alarm on presence of fission products in water

Level	Main Characteristics	Safety Feature
3	Control of accidents within the design basis	FRPS reactor trip on; a) high radiation at pool surface SRPS reactor trip on; a) Failure of the FSS

16.13.3 Mechanical Damage to Core or Fuel Assembly

This event refers to a failure that affects the physical integrity of the core or fuel assemblies. It can be caused by the impact of an object, impact of the fuel assembly on other objects during handling, flow induced vibration, seismic activity, radiation effects or corrosion.

The core and fuel assemblies are protected against the impact of heavy objects. During operation, a protective grid covers the top of the chimney, which can withstand the impact of a heavy Silicon ingot. This grid protects the core structures and the fuel assemblies from damage due to impact of falling objects during normal operation.

The fuel assemblies have been designed to avoid flow-induced vibrations. The core and fuel assemblies are designed to withstand the SL-2 earthquake. No damage to the cladding integrity would be expected in the event of seismic activity.

No deformation of the grid is expected due to radiation effects. The water chemistry is carefully controlled, and corrosion is unlikely to occur. The mechanical tolerances in the core grid, chimney and fuel storage racks prevent fuel from sticking and wear during handling.

Trained staff, following procedures and using adequate tools, carry out the loading and unloading of the fuel assembly in the core and its handling in the Reactor and Service Pools. This minimises the possibility of damage during handling and core reshuffling operations. The fuel assemblies are cold during reshuffling and refuelling operations, therefore there would be no significant release of fission products in the event of any mechanical damage. This consideration also applies to fuel assemblies in the storage rack inside the Reactor Pool and in the Service Pool. Should a fuel assembly be accidentally damaged during fuel shuffling manoeuvres, the operator would remove it to the storage rack inside the Reactor Pool.

Mechanical damage to a fuel assembly is considered to lie within the design basis. The magnitude of any fission product release as a result of mechanical damage would be minor. For this reason, the consequences of a release are considered bounded by those arising from fuel plate failure, discussed in the previous section.

16.13.3.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Chimney protective grid withstands impact by Silicon ingot.
		Support structure (comb) provides additional rigidity against flow induced vibration.
		Strict water chemistry control to avoid corrosion.
		Mild operating conditions (moderate temperature and controlled water quality).

		Handling of fuel assembly performed by trained staff with adequate tools and following procedures.
2	Operation control and response to abnormal operation	Damaged fuel assembly monitor in PCS
		Radiation alarm at Reactor Pool top.
3	Control of accidents within the design basis	FRPS reactor trip on; a) high radiation at pool surface SRPS reactor trip on; a) Failure of the FSS

16.13.4 Criticality in Fuel Storage

The fresh Fuel Assemblies are stored in a rack in a separate room. The rack's structure is a stainless steel lattice. Each lattice cell contains one fuel assembly inside a protective casing. Each fuel assembly is maintained centred inside the box. Criticality calculations (see Chapter 10) showed that when the fuel assemblies are properly placed in the rack even flooding would not cause a criticality incident. Thus the placement of fresh fuel assemblies in the storage rack is a safe arrangement from a criticality standpoint. Similarly, piling fuel assemblies on the floor without their boxes does not lead to criticality.

Spent Fuel Assemblies are placed inside containers in the Reactor and Service Pools. Each container can accommodate four fuel assemblies. The criticality calculations showed that, for FA storage in the Reactor Pool the array is subcritical. See Chapter 10 for a detailed description of the calculation.

The criticality analysis of the FA storage in the Service Pool shows that the array is subcritical. Scenarios with variations in water density, water level and manufacture tolerances have also been analysed. In all instances, the FA Storage array is subcritical. See Chapter 10 for detailed information.

The fuel assembly storage systems are designed to withstand the SL-2 earthquake and the racks are designed to withstand the impact of dropped loads.

Fuel assembly handling operators are well trained and fuel handling procedures prohibit storage of fuel assemblies outside the storage rack. The fuel assemblies follow a one way path inside the pool in routine operation, and all the fuel assemblies in the storage rack are removed to the Service Pool before core unloading is allowed to begin. The one exception to the 'one way path' for fuel assembly movements is associated with the full core unloading and reloading during extended shutdowns for in-service inspection.

Therefore, both fresh and spent fuel assemblies can be safely stored, with no criticality incidents occurring. A separate assessment of potential criticality is made when the fuel is prepared for loading into the transfer cask. On this basis, unplanned criticality of fuel elements, both fresh and spent, is considered to be eliminated by the inherent design provisions and is not analysed further.

16.13.4.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety	Fuel assembly array in storage lattice designed to remain subcritical at all times.

	features	Spent fuel storage containers designed to maintain optimum geometry for subcritical arrangement.
		Operational procedures to maintain safe geometry.
2	Operation control and response to abnormal operation	N/A

16.13.5 Loss of Coolant to Spent Fuel Stored in the Reactor and Service Pools

Loss of coolant to hot spent fuel during initial storage could only be due to failure of the Reactor or Service Pool boundary. Once removed from the core, the spent fuel is stored and left to decay in a rack inside the Reactor Pool before it is moved underwater through the Transfer Canal to the Service Pool. A spent fuel assembly requires cooling for a period before its decay heat falls sufficiently to preclude melting in air. No routine movement to the spent fuel rack would occur until well after that period. An exception to this routine could occur during extended shutdowns for in-service inspection. Appropriate procedures would be in place in such an event.

The inlet and outlet piping to the Reactor and Service Pools crosses the pool boundary above the level of the fuel assembly storage rack. Siphoning to below the level of the siphon breakers is not considered credible. In the event of a RSPCS loss of coolant accident with the isolation gate removed, the water in the Service Pool would fall to a level such that the spent fuel assemblies in the Reactor Pool would remain covered and cooled by the pool water. A loss of coolant from the PCS would be arrested at the level of the siphon breakers. Again, cooling of the spent fuel assemblies would not be jeopardised.

Lack of cooling to the spent fuel assemblies arising from loss of coolant through the Reactor and Service Pools' boundary is not considered credible. Failure of the pool boundary, although unlikely, is considered to lie within the design basis. Such a failure occurring in the Reactor Pool, however, would lead to a small leak that would easily be made up. The effect of a failure in the Service Pool boundary would be stopped at the level of the Transfer Canal isolating the Reactor Pool.

On the basis of the above arguments, particularly the ability of the flap valves and siphon breakers to arrest any LOCA, melting of spent fuel which is cooling in the Reactor Pool is considered so unlikely as to render it beyond the design basis. It will not be considered further.

16.13.5.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Water quality and mild operating conditions minimise the probability of damage to the pool leading to leakage
		Siphon breakers/flap valve levels higher than storage racks in Reactor and Service Pools.
		Siphon breaker/flap valve levels ensure enough shielding for fuel assembly handling
		Fuel transfer between pools done under water.

Level	Main Characteristics	Safety Feature
		Spent fuel will not melt if uncovered following the cooling period after removal from the core. No routine movement permitted until well after expiry of the cooling period.
2	Operation control and response to abnormal operation	N/A

16.13.6 Loss or Reduction of Proper Shielding

The loss or reduction of shielding implies a failure in any of the barriers that isolate active materials from the operators and the Reactor Building environment.

In the radial direction from the core, the heavy concrete of the reactor block provides the main shielding. Catastrophic failure of concrete in a seismic event is not credible. The concrete block is seismically designed and it can withstand the SL-2 earthquake. The pool water provides an additional barrier. Even in the event of a loss of coolant, the water barrier will not be lost at the level of the core. The pool drainage will be stopped at the upper or lower siphon breaker level depending upon the source of the loss. A loss of heavy water from the Reflector Vessel would not result in doses exceeding the limit for operators, since the reactor would be shutdown.

In the vertical direction, the pool water and the hot water layer provide shielding to an operator located at the Reactor Pool top. The dose rates to operators during normal operation are presented in Chapter 12. In the event of a loss of coolant, the pool water would drain and the shielding would decrease. A low pool water level signal would trigger the FSS and, in the unlikely event that this fails, the SSS would be triggered on very low pool level or failure of the FSS. The reactor would shut down. The drainage of the pool would stop when the water level reaches the siphon breakers. The water column would then still be well above the top of the core. This column provides sufficient shielding to protect the operator at the top of the Reactor Pool. The dose rate to an operator at the Reactor Pool top with the reactor at shut down state and water column above the Core to the siphon breakers is some 4 μSvh^{-1} shortly after reactor shutdown

During refuelling operations, an operator could lift a fuel assembly above the level of the Transfer Canal. The procedures for fuel handling during refuelling ensure that the operator cannot remove a Fuel Assembly that has remained in the storage rack less than the length of an operation cycle. Refuelling is done only during reactor shutdown, and fuel assembly transfer to the Service Pool is done only immediately prior to refuelling. The fuel assemblies follow a one way path during routine operations. During refuelling, all the fuel assemblies in the storage rack inside the Reactor Pool are moved to the Service Pool before any handling of the fuel assemblies inside the core. After the storage rack is empty, the spent fuel assemblies that are to be replaced are removed to the storage rack, reshuffling is carried out and only then is fresh fuel brought into the Reactor Pool. The spent fuel assemblies are not touched until the next refuelling, an operating cycle later. Lifting an irradiated fuel assembly to a height where shielding is insufficient would cause a local alarm at the pool top. This alarm is given by the dose rate area monitors connected to the FRPS that trip the reactor on high pool top dose rate. This alarm would indicate to the operator and the Main Control Room that the fuel assembly needs to be lowered to a safe location inside the Reactor Pool. Operating procedures and operator training programmes minimise the likelihood of operator mishandling of fuel. Fuel assemblies remain under water during all operations and would only be removed from the Service Pool in a transport cask. There is no routine process which requires removal of fuel elements from the water.

Loss of water in the Service Pool would lead to a loss of shielding from the spent fuel storage. The level of the pool water would fall to the siphon breaker level for the Service Pool piping, in the event of a loss of coolant via the RSPCS piping. In the event of a loss of coolant involving the PCS, the Service Pool level would drop to the level of the bottom of the Transfer Canal. The dose rates at the Service Pool top would be low enough to permit operators to engage in repair operations at the pool top.

Transfer of fuel assemblies from the Reactor to the Service Pool is performed during shutdown with the fuel assembly lifted by a tool from the storage rack and moved through the Transfer Canal. During shutdown, the PCS and RSPCS pumps are stopped (the RSPCS being operated in Long Term Pool Cooling mode). The most likely causes of a loss of coolant during shutdown are erroneous opening of a drainage valve, removal of an instrument or failure of the instrument connection pipe. All these pipes are of small diameter, causing a slow decrease in water level and stopped at either of the siphon breaker levels as explained above. The operators would have sufficient time to complete the transfer and would not be exposed to the FA with insufficient shielding.

The pool top dose rates will be surveyed regularly by Health Physics Staff. In addition, key points in the facility where shielding degradation could lead to operator exposure have dose rate monitors that alarm on high dose rate.

On the basis of the above discussion, the loss or reduction of water shielding is considered to lie within the design basis. Its consequences, however, are minor.

16.13.6.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Reactor block made of heavy concrete
		Siphon breakers in Reactor and Service Pools piping
		Spent fuel storage containers designed to maintain optimum geometry for subcritical arrangement.
		Neutron beam shutters
		Regular dose surveys by Health Physics staff
2	Operation control and response to abnormal operation	Alarms on low and very low pool water level
		Alarm on high dose rate at several key points in the facility (See Chapter 12)

16.13.7 Design Basis Postulated Initiating Events

A summary of the previous discussions is provided below together with the identification of DBIEs.

PIE	Not applicable to the design	Eliminated by inherent design provisions	Sufficiently unlikely to occur (BDB)		Design Basis Initiating Events (DBIEs)		
					To be considered in other DBIE group	Bounded by other DBIE	Further Analysis
Fuel plate cladding failure							X

PIE	Not applicable to the design	Eliminated by inherent design provisions	Sufficiently unlikely to occur (BDB)	Design Basis Initiating Events (DBIEs)		
				To be considered in other DBIE group	Bounded by other DBIE	Further Analysis
Mechanical damage to core or FA					X (Fuel plate cladding failure)	
Criticality in fuel storage and transfer between pools		X				
Loss of coolant to spent fuel in storage			X			
Loss or reduction of proper shielding				Minor consequences		

The following DBIE is identified for further analysis;

Failure of a fuel plate as a result of a manufacturing defect during normal operation.

The consequences of this event are expected to be minor, affecting only the operators. Release of fission products to the environment would not occur.

16.13.7.1 Detection of the Initiating Event

The detection of the Initiating Event will depend on the extent of the damage to the fuel plate. The Failed Fuel Element Monitor (FFEM) would detect the presence of fission products in the PCS water. Assuming extensive damage, with the release of the full inventory of fission products inside a fuel plate, the reactor would be shutdown due to high activity at the RPO top.

Alarms are triggered on the following variables:

a) Fission products in the PCS water (FFEM)

b) High activity in PCS water (ALMO)

c) High activity at the RPO top.

16.13.7.2 Design Basis Fault Sequence

16.13.7.2.1 Manufacturing failure

a) The visual inspection prior to FA loading fails to identify damage to fuel plate.

b) Reactor operation starts. Power is raised.

c) Fission products leak into the PCS water inside the chimney.

d) FFEM gives alarm of fission products in PCS water.

e) No credit is given to reactor shutdown by operator when he becomes aware of the FFEM alarm.

f) Activity in the pool becomes significant. No credit is given to the Hot Water Layer System (HWLS).

g) RPO top activity causes reactor trip.

h) In case the release reaches the venting stack, FRPS initiates Containment Isolation.

16.13.7.3 Numerical Analysis

No numerical analysis of this event has been performed since it does not affect the thermalhydraulic parameters of the core.

16.13.7.4 Radiological Impact Analysis

It is conservatively assumed that the full inventory of fission products present in a fuel plate is released due the mechanical damage.

Partition fractions, deposition and removal decay constants and leakage decay constants are the same used in Section 16.19.2. Atmospheric conditions during the analysed period are also identical to those in Section 16.19.2.

The release of the inventory of one fuel plate have been calculated as have the time periods over which the release occurs.

Calculations were performed with PC-COSYMA to determine the dose to an average person at 1.6km. It was assumed that the prompt release occurred at discharge stack but that all subsequent releases occurred at ground level. The results are shown below.

Distance	Prompt	Period 1	Period 2	Period 3	Period 4	Total
1600m	1.83μSv	0.62μSv	0.013μSv	0.03μSv	0.05μSv	2.54μSv

The collective effective dose for this scenario, calculated for the population within a radius of 22.5 km from the reactor is 0.04 Person-Sv, well below the 200 Person-Sv required by ARPANSA regulations.

Therefore full failure of a fuel plate, leading to release of the full inventory of fission products, would result in a dose to the public that is well below ARPANSA limits and require no emergency interventions or countermeasures.

16.13.8 Conclusions

The potential for erroneous handling or failure of equipment and components has been considered. The potential for inadvertent criticality of fuel is considered insignificant. Those events that result in a loss of shielding brought about by loss of pool inventory are stopped by the inherent design features of the plant and do not have significant consequences.

The complete failure of a fuel plate, with the release of all activity to the coolant, is considered most severe. Although numerous indications would exist, no manual or automatic actions are credited for the first 30 minutes. The effects of a failure of a fuel plate are well within ARPANSA acceptance limits.

End of Section

Table 16/13.1 Radioisotope Release from One Fuel Plate

Isotope	Prompt /Bq	Period 1 /Bq	Period 2 /Bq	Period 3 /Bq	Period 4 /Bq
Xe-131m	2.04E+10	8.80E+09	8.43E+09	5.40E+09	1.35E+11
Xe-133m	1.18E+11	4.77E+10	4.03E+10	2.27E+10	1.24E+11
Xe-133	3.90E+12	1.65E+12	1.52E+12	9.40E+11	1.19E+13
Xe-135m	6.63E+11	8.60E+09	0.00	0.00	0.00
Xe-135	3.04E+11	8.73E+10	3.47E+10	9.20E+09	6.10E+09
Xe-138	3.43E+12	4.07E+10	0.00	0.00	0.00
Kr-83m	3.01E+11	2.87E+10	3.04E+08	2.12E+06	2.25E+04
Kr-85m	7.00E+11	1.40E+11	2.16E+10	2.22E+09	4.07E+08
Kr-85	5.13E+09	2.24E+09	2.21E+09	1.46E+09	1.24E+11
Kr-87	1.40E+12	9.30E+10	1.35E+08	1.28E+05	1.83E+02
Kr-88	1.98E+12	2.80E+11	1.49E+10	5.23E+08	2.93E+07
I-130	5.73E+07	1.01E+07	1.35E+06	2.12E+05	1.65E+05
I-131	2.72E+09	6.00E+08	1.53E+08	4.63E+07	6.40E+08
I-132	3.93E+09	3.29E+08	2.12E+06	1.53E+04	2.99E+02
I-133	5.93E+09	1.15E+09	2.03E+08	4.23E+07	6.37E+07
I-134	6.60E+09	2.60E+08	4.73E+03	0.00	0.00
I-135	5.53E+09	8.13E+08	5.87E+07	4.97E+06	1.46E+06
Te-125m	4.73E+02	1.90E+02	1.58E+02	8.77E+01	4.37E+02
Te-127m	1.09E+04	4.37E+03	3.63E+03	2.02E+03	1.03E+04
Te-127	1.17E+05	3.16E+04	1.09E+04	2.49E+03	1.31E+03
Te-129m	6.77E+04	2.71E+04	2.24E+04	1.24E+04	6.03E+04
Te-129	4.50E+05	2.67E+04	1.75E+01	0.00	0.00
Te-131m	2.32E+05	8.20E+04	5.20E+04	2.20E+04	3.83E+04
Te-131	1.54E+06	3.28E+04	0.00	0.00	0.00
Te-132	2.61E+06	1.00E+06	7.53E+05	3.77E+05	1.15E+06
Te-133m	1.64E+06	7.80E+04	8.17E+00	0.00	0.00
Te-133	2.19E+06	2.28E+04	0.00	0.00	0.00
Te-134	3.77E+06	1.35E+05	0.00	0.00	0.00
Cs-134m	2.16E+06	2.98E+05	1.44E+04	4.60E+02	2.32E+01
Cs-134	1.49E+06	6.00E+05	5.03E+05	2.80E+05	1.45E+06
Cs-136	8.07E+05	3.21E+05	2.61E+05	1.42E+05	6.33E+05
Cs-137	1.29E+06	5.20E+05	4.37E+05	2.43E+05	1.26E+06
Cs-138	1.15E+08	3.16E+06	0.00	0.00	0.00
Rb-86	8.17E+04	3.26E+04	2.68E+04	1.46E+04	6.80E+04
Rb-88	5.80E+07	8.73E+05	0.00	0.00	0.00
Rb-89	7.50E+07	9.57E+05	0.00	0.00	0.00
Ru-103	6.10E+07	2.45E+07	2.03E+07	1.12E+07	5.50E+07
Ru-105	2.73E+07	5.10E+06	6.57E+05	5.63E+04	8.30E+03
Ru-106	3.47E+06	1.40E+06	1.17E+06	6.53E+05	3.37E+06

End of Tables

16.14 ANALYSIS OF SPECIAL INTERNAL EVENTS

This section refers to incidents originating in the facility that, while not arising from failures in the reactor, have the potential to affect its safety. They are summarised in the following list:

Internal fire or explosion

Internal flooding

Loss of supporting systems

Security incidents

Improper access to restricted areas

Each of these incidents is discussed in the following sections on the basis of their impact on reactor safety and the performance of the safety systems.

There are no high energy piping systems in the facility, therefore associated hazards (e.g, pipe whip, jet impingement) need not be considered. Compressed air tanks and lines have relief valves to prevent pressure build-up. The Cold Neutron Source deuterium lines are discussed in Section 16.15.6.

16.14.1 Internal Fire or Explosion

This Section assesses the impact of an internal fire or explosion on the safety of the Reactor Facility. It should be read in conjunction with Chapters 4 and 10. Chapter 10 presents a detailed description of the Fire Protection Systems. The different causes for a fire or explosion considered are:

a) Failure of the electrical system: The electrical system has been designed with fire-retardant materials in order to delay the onset and spreading of a fire following a short circuit. The rooms where potential sources of ignition are located (such as pump motors, switchboards, etc.) have epoxy finishes on the concrete wall.

b) Flammable gases inside the Reactor Building: the presence of flammable gases is strictly controlled inside the Reactor Building. Gas cylinders are located outside the building, in a special designated area. Gas supply to the interior of the building is by way of a piping network. Hot cells have a fire detection system that ensures early detection of fires, as well as fire suppression systems, with total flooding of the cell (carbon dioxide or equivalent).

c) Flammable liquids inside the Reactor Building: flammable liquids, in the form of paints or solvents, will be concentrated in workshops and store rooms. Since it is not possible to know beforehand the amount of solvent or paint that will be stored inside the building, the fire suppression system has been designed assuming that each store room contains paint and solvents together with cables and paper. There are four workshops/maintenance rooms in the Reactor Building:

   (i) pump maintenance
   (ii) instrument workshop
   (iii) active workshop
   (iv) rigs maintenance workshop

   Each of these rooms contains flammable liquids and solids. The walls and floors are all made of epoxy covered concrete, except for the Instrument Workshop, where the walls are painted and the floor is covered with vinyl. This is also the only room with permanent occupation during normal operation. The others will have eventual access but are not permanently occupied. Maintenance and repair of instrumentation are the tasks performed in this room, and a lower concentration of flammable materials is expected, compared to the other workshops.

Six storage areas can be identified in the Reactor Building:

(i) active equipment handling store
(ii) two general storage rooms
(iii) general storage area
(iv) store/delivery area Nuclear Technology
(v) APHCC store

All of these storage areas are expected to contain solvents and other flammable materials, as indicated above. Storage of hazardous chemicals follows Australian Standards.

d) The diesel generators are located externally in their own dedicated area remote from the main buildings. Appropriate separation is provided between the diesel generators to ensure a fire in one does not affect the others. In addition, each diesel generator is provided with appropriate means of fire protection

e) Accidents during maintenance or repair involving soldering or flammable materials: Metal cutting, machining and welding may cause ignition. These activities will be generally confined to workshops, where building and finishing materials are non-flammable. Workshops also store flammable materials. This combination of potential ignition sources and flammable substances has been taken into account in the design of the fire suppression system. In general, fire in any of these rooms would be self-contained and would be extinguished before it can spread. Fire retardant wiring insulation and non-flammable building and finishing materials limit the spread of the fire. Water hazards from fire sprinklers in this and other areas are controlled as detailed in Section 10.2.

f) Build-up of deuterium from the reflector: The Reflector Cooling and Purification System has a recombination system that controls deuterium build up. Failure of the deuterium recombiner gives rise to an alarm via the RCMS. The system has an alarm on high concentration at approximately 0.2% concentration, while the lower flammability limit for deuterium is 4%. The explosion hazard due to the presence of the Cold Neutron Source is discussed in detail in Section 16.15.

Fire has the potential to affect safety systems. To ensure the safety function of the safety systems, and according to the IEEE Category 1 classification, the triple redundant instrumentation train of the RPS are physically separated, with fire barriers separating the different areas. The same applies to cable trays and ducts.

The fire hazard in the Control Rod Drive Room is very small. The only potential source of ignition would be a spark from a Control Rod Drive motor. Fire in the Control Rod Drive motor would not impair the actuation of the FSS. Interruption of current due to the fire would result in actuation of the FSS and shutdown of the reactor. The Control Rod Drive components (rods, stems, plates) are metallic and not flammable. The fire would therefore not propagate to the Reactor Pool. The FSS is designed to fulfil its safety function with a misalignment in the Control Rod Drives, therefore, should the Control Rod Drives be affected by fire and deformed within this misalignment, they can still be inserted inside the core to shutdown the reactor.

The FRPS is based on dynamic signals. Thus the absence of a train of pulses caused by fire would lead to a safe reactor shutdown.

In the event of fire in the Main Control Room, the operators would evacuate to the Emergency Control Centre.

Internal fires and explosions are within the design basis of the facility and are considered as DBIEs. Their prevention and control is considered further in Chapter 4. Section 10.2 discusses the treatment of their consequences.

16.14.1.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Fire retardant material in wiring
		Safety venting valves in compressed air lines and tanks
		Deuterium recombination system in the Reflector Cooling and Purification System
		Nitrogen blanketing in Deuterium Cooling System of the Cold Neutron Source.
		Pressurised cylinders stored outside buildings.
2	Operation control and response to abnormal operation	Pressure monitor in the Cold Neutron Source deuterium line
		Alarm on deuterium build-up in the recombiner.
		Automatic fire fighting system
		Fire fighting procedure implemented at LHSTC.
3	Control of accidents within the design basis	N/A

16.14.2 Internal Flooding

As stated earlier, rupture of piping is considered very unlikely due to mild operating conditions (moderate temperatures and low pressures). The same applies to failure of seals or unions. A drainage valve left open can cause water spillage. The small diameter of these lines would lead to a low leakage flow rate. Piping is designed to withstand the SL-2 earthquake. The controlled water quality and mild operating conditions minimise corrosion.

QA procedures are in place for welding of unions in piping and components. High quality material is used for piping, and high quality components have been purchased from qualified vendors. All welds have been inspected. The start-up sequence for the reactor includes a walk through and confirmation of status on all drain valves to minimise leakage risks from incorrect valve settings.

A potential source of flooding is the valve in the refilling line of the Reactor Pool. The control loop could fail or the valve could fail open due to build-up of dust or small debris. The malfunction of this valve would result in a leak of the Reactor Pool water. This leakage would be detected once water reaches the LOCA pool.

From the flooding point of view, any water spillage would be drained through the LOCA sumps located at each building level to the LOCA pool. LOCA sumps are placed in every room that houses piping and in the Reactor Hall.

Flooding would be detected by presence of water in the LOCA sumps and in the LOCA pool. An alarm would sound in the Main Control Room.

Internal flooding is considered to lie within the design basis. Its consequences are bounded by a loss of coolant in the cooling systems of the reactor. The effect of a loss of coolant via the PCS or RSPCS on the behaviour of the reactor core is described in Section 16.11 and is not considered further here.

16.14.2.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Low temperatures and pressures in piping.
		Piping designed to withstand the SL-2 earthquake.
		QA procedure for welding
		High quality piping and components from qualified vendors.
		Pre-operational walk through.
2	Operation control and response to abnormal operation	LOCA sumps at each reactor building level.
		Alarms on water in LOCA sumps and LOCA pool.

16.14.3 Loss of Supporting Systems

This section discusses the loss of support systems important to the operation of safety systems and the reactor. The systems considered are:

a) electric power
b) compressed air
c) communications capabilities
d) lighting

16.14.3.1 Loss of Normal Power Supply

The facility has a Standby Power System. All the Engineered Safety Features are connected to the Standby Power System and Uninterruptible Power Supply, where required, back up for all design basis accidents. The loss of the Normal Power System is considered a DBIE. The effect of the loss of the Normal Power System on the reactor is analysed by numerical simulations in Section 16.7. It is not considered further here.

16.14.3.2 Loss of Compressed Air

Where a safety system requires compressed air for its operation, it is provided with a dedicated reservoir tank to allow for its actuation in the event of loss of compressed air supply. The loss of compressed air supply has no effect on the safe shutdown of the reactor, the continued cooling of the core and the isolation of the containment.

Failure of the compressed air supply is considered within the design basis. However, measures put in place to cope with such a loss ensure that there would be no undue consequences. No further analysis is therefore required.

16.14.3.2.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Each Engineered Safety Feature has its own compressed air tank to ensure supply.
		Shutdown systems are fail-safe.

2	Operation control and response to abnormal operation	Alarm on loss of compressed air
3	Control of accidents within the design basis	N/A

16.14.3.3 Loss of Communications Capabilities

The operation of the Reactor Facility is self contained in that there are no requirements for communication with the rest of the LHSTC site. In the absence of communication capabilities, safe reactor shutdown can be attained by the FRPS-FSS or SRPS-SSS, since none of these systems receive any input from the communication systems. Loss of communication capabilities therefore does not challenge the safety of the Reactor Facility. Section 10.3 describes the communications system and outlines its fault tolerant characteristics.

16.14.3.4 Loss of Lighting

This refers to loss of lighting not associated with loss of Normal Power. In accordance with Australian Standards, emergency lighting is provided in the Main Control Room, the Emergency Control Centre and containment areas for essential functions. Emergency lighting is also provided along escape routes. Thus, while loss of lighting is identified as a DBIE, it has no impact on the safety of the reactor and no consequence analysis is therefore required.

16.14.4 Security Incidents

The Reactor Facility is designed with defence in depth to suit the user requirement, IAEA document INFCIR/225/Rev4 and the requirements of the Director General, Australian Safeguards and Non-Proliferation Office. Security incidents are identified as a DBIE. Their design is based on a threat assessment performed by security specialists and approved by Australian Safeguards and Non-Proliferation Office in conjunction with ARPANSA. However, it is worth noting here that typical failures to plant arising from security incidents are bounded by many of the accident sequences described within the SAR.

16.14.5 Improper Access to Restricted Areas

Access to restricted areas is controlled by operational procedures.

Improper access to restricted areas is considered to lie within the design basis. The procedural controls in place ensure no undue consequences.

16.14.6 Design Basis Postulated Initiating Events

The information presented in the previous paragraphs in summarised in the following table:

PIE	Not applicable to the design	Sufficiently unlikely to occur		Design Basis Initiating Events (DBIEs)		
				To be considered in other DBIE group	Bounded by other DBIE	Further Analysis
Internal Fire or explosion						X (included in the design criteria of the building)
Internal flooding				X (LOCA)		
Electric power					X (Section 16.7)	
Compressed air				No consequence analysis necessary		
Communications capabilities	X					
Lighting				No consequence analysis necessary		
Security incidents				Not considered here		
Improper access to restricted areas				No consequence analysis necessary		

The identified DBIEs for this group are:

a) Internal fire or explosion: This event has been included in the design basis for the building and the dimensioning of the fire suppression system. There is no impact on the ability to shutdown and safely cool the reactor. The potential for explosions with the Cold Neutron Source are discussed in Section 16.15.

b) Internal Flooding. The effects of this DBIE are bounded by those considered in the LOCA group, Section 16.11.

c) Loss of Normal Power Supply. Analysed in Section 16.7.

d) Loss of compressed air. Considered in the design of the systems. No consequence analysis necessary.

e) Loss of lighting. Emergency lighting available to necessary areas. No consequence analysis necessary.

f) Improper access to restricted areas. Procedural controls and alarms in place. No consequence analysis necessary.

End of Section

16.15 REACTOR UTILISATION INITIATING EVENTS

16.15.1 Introduction

This Section assesses key initiating events arising from the utilisation of the reactor. Reactivity effects of the irradiation rigs are considered in Section 16.8. In addition to these analyses, a design evaluation included in Chapter 11 describes the built-in characteristics of these systems that prevent and cope with malfunctions.

The analysis applies to the effect that the irradiation facilities, neutron beams and CNS have on the behaviour of the reactor as well as to the radiological impact of the initiating events.

The utilisation of the reactor has safety implications, which are considered in the design. It can impact on the behaviour of the reactor systems and it can have a radiological impact on operators during utilisation activities.

The following systems / facilities will be considered within this event group:

a) Bulk Production Irradiation Facilities
b) Pneumatic Transfer System and Neutron Activation Analysis
c) Transfer, Loading and Pneumatic Cells
d) Large Volume Irradiation Facilities
e) Cold Neutron Source
f) Neutron Beam Facilities

16.15.2 Bulk Production Irradiation Facilities

A set of irradiation positions are provided for bulk targets which may generate considerable nuclear heat and which have irradiation times from days to weeks. These facilities are tailored to the production of molybdenum-99 from fission of uranium metal, iodine-131 from tellurium dioxide and iridium-192 from metallic iridium, among others.

Radioisotopes are irradiated inside rigs located inside irradiation tubes in the Reflector Vessel. The rigs are handled by operators standing at the operation bridge that runs above the Reactor Pool. The targets are cooled by forced circulation of reactor pool water.

Once irradiated, the rigs are transported into shielded hot cells, from where the radioisotopes are dispatched for processing in the Radiopharmaceutical buildings of the LHSTC, inside shielded transport casks.

Due to their effect on core reactivity, rigs with a reactivity greater than 200 pcm may only be loaded and unloaded from the Reflector Vessel during reactor shutdown, while the other bulk irradiation targets may be loaded and unloaded while the reactor is operating. All rigs have reactivity worth below 200pcm. Rigs with high reactivity are fixed during operation and have locked covers in place as an additional barrier to indicate to the operator that that irradiation rig cannot be removed. Reactivity incidents involving the manipulation of the irradiation targets and their effect on the core are considered in Section 16.8.

16.15.2.1 Excessive Power

Three molybdenum production targets are expected to be contained in a rig, depending upon the size of the target. Uranium enrichment, density and mass of targets will be limited and will be identified in a target specification.

Considering ANSTO’s conservative target design (qualified by tests) and operational procedures, as well as the conservative design of the RSPCS, the potential failure of a uranium metal target due to overpower is considered to have been eliminated by design provisions.

On removal from their irradiation position, the uranium metal targets are stored in the Service Pool and allowed to cool for a number of hours. While freshly irradiated uranium metal targets are being allowed to cool, others that have been cooled for the necessary length of time are transported up into the Hot Cells. The potential exists for an operator to mistakenly take the freshly irradiated uranium metal targets directly to the Hot Cell An interlock is in place to prevent freshly irradiated uranium metal targets being mistakenly transported to the Hot Cells. In addition, administrative controls are in place detailing the times at which the various targets have been removed from their irradiation positions and the time at which they can subsequently be moved. The likelihood of taking freshly irradiated uranium targets to the Hot Cells without sufficient cooling is considered sufficiently low as to render it beyond the design basis.

16.15.2.2 Failure of the Reactor and Service Pool Cooling System

The following malfunctions are identified:

a) Loss of flow within the RSPCS. During normal operation, the rig is cooled by forced circulation of water provided by the RSPCS. In the event of pool cooling flow being lost, a low flow signal from the RSPCS triggers the FSS and the reactor is shutdown. The flap valves in the RSPCS open and natural convection flow removes the power generated in the rigs. Loss of flow in the RSPCS due to loss of Normal Power Supply is analysed in Section 16.7. Failure of the pump could be due to seizure of the shaft or loss of power to the pump motor as a result of a local failure (e.g, malfunction of the pump switchboard). Failure of the pump motor is considered to be the more likely of the two and is considered to lie within the design basis. The seizure of the pump shaft, like that for the PCS pumps, is considered very unlikely given the monitoring instrumentation associated with pumps. Nevertheless, both types of failure are considered to lie within the design basis. However, while pump failure with FSS and SSS actuation is considered to lie within the design basis, the likelihood of a shaft seizure together with failure of the FSS, is considered so low as to render it beyond the design basis.

b) Loss of heat sink. A reduction in cooling arising from a loss of heat sink is addressed in Section 16.10.

c) Blockage: Downwards flow in the RSPCS implies that provisions need to be taken to minimise the likelihood of a blockage in the irradiation rigs. These provisions are divided into two groups:

   (i) Inherent design characteristics: The irradiation rigs are protected from falling objects by a protective box that rests over the reflector vessel. The lateral walls of the box are made of a fine mesh that allows cooling water to the rigs and prevents entrance of objects that may obstruct their cooling. The fixation of rigs to the protective box is achieved by means of a cap that prevents the entrance of foreign objects and inadvertent extraction of the rig. Rigs are designed in such a way that it is not possible to place, by mistake, a high heat generating rig into a lower cooling capacity facility. This is achieved by having different nozzle diameters in different rigs.

   (ii) Administrative procedures: In addition to the use of protective rig caps, administrative control procedures are in place that prohibit the entry of clear plastic to the reactor pool top area (this includes plastic bags and disposable plastic gloves). All clothing used by staff ensures that all lightweight objects, such as pens or pencils are securely contained. Irradiation positions remain open during rig exchange operations. To verify that no object has fallen and is blocking the flow of coolant, the operator verifies with a specially designed tool that the opening for coolant flow at the bottom of the irradiation channel is open. Tools used to handle objects in the RPO have been designed to prevent dislodging of parts that could lead to flow blockage.

With these design and administrative provisions in place, full blockage of an irradiation position is considered sufficiently unlikely as to render it beyond the design basis.

d) Spurious opening of an RSPCS flap valve. The pressure inside the piping while the RSPCS pumps are in operation prevents spurious opening of the flap valves. The flap valves are positioned inside the RPO in such a way as to avoid spurious opening by an operator during handling of irradiation targets and tools. A position switch would trip the reactor in the event the flap valve opens. This event is considered so unlikely as to render it beyond the design basis.

e) LOCA: In the event of a loss of coolant accident, Reactor Pool water level falls to the level of the passive siphon breaker. The water level covering the rigs would be sufficient to protect personnel from radiation and to facilitate natural convection. This event is considered in Section 16.11.

16.15.2.3 Rigs Exchange

Incorrect positioning/loading of a medium, high, or very high flux rig could occur due to human error. The potential introduction of a uranium metal target into an iridium irradiation position is of greatest interest. Iridium is a neutron absorber. The uranium metal targets are designed to produce molybdenum-99 by fission of uranium-235. These molybdenum targets introduce positive reactivity to the core while the iridium targets introduce negative reactivity. Iridium positions are placed at areas of the reflector with higher neutron flux than those of the uranium metal targets.

To avoid incorrect positioning of rigs, different rig geometry is used for different targets. Thus it is not possible to insert uranium metal targets into an iridium irradiation position. This event is considered to have been eliminated by the inherent design provisions and is not analysed further.

16.15.2.4 Staff Irradiation Due to Inappropriate Handling of Targets

All bulk irradiation targets are handled under water until they have decayed sufficiently to be removed and transported. The shelves for target manipulation are placed low enough inside the pool to provide appropriate shielding to the operator. Should the operator lift a target above the handling level, a radiation alarm would alert the operator and indicate that the target needs to be lowered to a safe position. The FRPS area monitors at the pool top provide this alarm. The design of the rig operation tools helps to prevent this event. Procedures are followed to ensure safe operation. There is no routine process that requires these rigs to be removed from the water. The likelihood of such an event, together with failure of the FRPS, is considered so low as to render it beyond the design basis. It will not be considered further.

16.15.2.5 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Control of target materials by administrative procedures and target and canning specification
		Two 100% pumps, one on standby
		A mesh at the top of the rigs protects them from falling objects and prevents coolant channel blockage
		Administrative procedures to minimise the likelihood of a lightweight small object falling into the pool.
		Administrative procedure to verify coolant flow before rigs loading.
		Different rig geometry for different targets to prevent misloading (geometrically safe design)
		Target cans are not opened inside the Reactor Building
		Irradiation authorisation procedures apply
		Procedures to assure safe handling.
2	Operation control and response to abnormal operation	Radiation alarm at pool top
		Failed targets monitor in RSPCS gives RCMS alarm on presence of fission products in water
3	Control of accidents within the design basis	FRPS reactor trip on a) low flow in the RSPCS b) open RSPCS flap valve c) high radiation at pool top SRPS reactor trip on a) Failure of the FSS

16.15.3 Pneumatic Transfer System and Neutron Activation Analysis

Targets are irradiated inside cans in rigs located in the Reflector Vessel. The cans are transported by means of a pneumatic transport system. The flow that provides the momentum for the transport also cools the cans. The rigs sit in wells within the Reflector Vessel, surrounded by light water.

16.15.3.1 Excessive Target Radioactivity

The potential exists for targets to develop levels of radioactivity above those levels normally expected due to:

a) target load being greater than required
b) neutron flux in the irradiation position being greater than anticipated, and
c) irradiation times being longer than foreseen

Compliance with the approved target and canning specification procedure minimises the potential for misloading of targets. Procedures are also in place to minimise the potential for sending the target to the wrong irradiation position. The installed Neutron Detectors provide an accurate indication of the flux in the facility and allow the operators to calculate the irradiation time to determine the required activity, in accordance with established procedures.

The production of targets with excess activity is considered to fall within the design basis. However, neither core damage nor exceedance of dose limits would occur in such an event. The consequences would be minor.

16.15.3.2 Excessive Target Heating Power

The heating power dissipated by an irradiation target in the pneumatic system may be larger than normal for the same reasons given above. The maximum design power in any rig is ~145 W per target, including the can. The can design temperature is well below the melting temperature of aluminium. The QA procedures for target preparation minimise the potential for erroneous loading of the cans. Target identification and handling procedures ensure that the target is sent to the correct irradiation position. Target handling is carried out in a hot cell that provides protection to the operator.

Should a can fail due to excessive heating, doses to personnel would be minimal, since the pathways of the Pneumatic Conveyor System are either shielded or inside the reactor block. The pipes penetrate the Reactor Pool below the water level, with enough water above them for shielding. The shielded pipes are not directly accessible, but the shielding may be removed if necessary to provide access. Design provisions are in place to decontaminate the pneumatic tubes and hot cells after failure of a can.

The failure of a target can through excess heating is considered to fall within the design basis. The radiological impact of this event is bounded by the failure of a can in the transfer hot cell.

16.15.3.3 Interruption of Cooling

A stream continuously cools the targets from the time they are sent to the irradiation position. Interruption or reduction of the cooling stream could arise following:

a) Blower Failure: There are three blowers, each 60% capacity, two are operated with one in standby. In the event of a blower failure, the standby blower is automatically started and the full flow rate restored. Failure of all blowers would only occur on loss of Normal Power Supply. Reactor shutdown would remove the main source of heating of the can.

b) Valve failure: If a valve is closed and the main stream of cooling is stopped, the cooling flow rate transducer in the inlet line, with 1 out of 2 redundancy, sends signals to the RCMS initiating a power reduction.

c) Failure of secondary cooling. If there is insufficient cooling by the SCS, cooling of the system is diminished, resulting in a power reduction via the RCMS.

d) Cooling failure in a single irradiation position. Each irradiation position is equipped with a thermocouple. A high temperature signal produces an alarm and the operator proceeds with the normal removal operation. If the very high temperature alarm is triggered, automatic target removal occurs.

e) The RCMS would initiate power reduction on Low Flow.

The above events are considered to fall within the design basis. Their radiological impact is bounded by the failure of a can inside a hot cell.

16.15.3.4 Stuck Sample

There are two position sensors to determine sample location. If, during the loading or removal operation, the can is trapped in transit:

a) Can cooling would continue.

b) The pneumatic control system would have knowledge of the situation by means of the two position sensors.

The cans would be removed by a burst of high pressure actuated manually by the operator.

The occurrence of a stuck sample is considered to lie within the design basis. Doses to personnel would be minimal, since the pathways of the Pneumatic Conveyor System are either shielded or inside the reactor block. The pipes penetrate the Reactor Pool below the water level, with sufficient water above them for shielding. The shielded pipes are not directly accessible, but the shielding may be removed if necessary for recovery actions.

16.15.3.5 Can Failure Inside Pneumatic System Piping

Hazardous or powdered target materials will be encapsulated in double aluminium can containers, providing two barriers against rupture. Mechanical failure of both cans is considered incredible.

Other solid targets may be contained in single cans. Failure of these cans is considered within the design basis. However, for these solid targets, no significant loss of radioactive material would occur in the event of rupture due to the solid state of the target.

The cooling system is provided with filters to collect any material that may escape into it. In addition, valves are provided to permit isolation of a section of piping in the event of it becoming contaminated. The pathway of the Pneumatic Conveyor System is shielded.

The mechanical failure of a can inside the Pneumatic Conveyor System has no effect on the behaviour of the core. The filtering system, the isolation valves and the shielding limit the radiological impact of this event. The consequences of the event are bounded by rupture of a can in a hot cell.

16.15.3.6 Can Rupture in Hot Cell

The hot cells are maintained at a negative pressure. Any air activity is controlled by the hot cell ventilation system and then retained in filters before the air is discharged to the atmosphere through the venting stack.

Of all the possible failures of a can in the hot cells, rupture of a can containing iodine is considered to represent the bounding event. The filters in the ventilation of the hot cells are designed to retain all the activity released by rupture of this can. The event would thus not result in a radiological hazard for the operator and there would be no release of activity to the environment.

The material of the floor and working table has an adequate surface finish to enable cleaning and decontamination.

Hot cell telemanipulators would be used to clean and decontaminate the working table/area.

Failure of a can in a hot cell is considered to lie within the design basis. The cell ventilation is in recirculation mode and the trapping of fission products other than the noble gases is very effective.

16.15.3.7 Failure of Electrical System

If the pneumatic transfer system switchboard fails, a low flow to the RCMS would initiate power reduction.

In the event of a failure of the Normal Power Supply (for example, in the main transformers), the reactor would shutdown automatically (see Section 16.7).

The event is within the design basis. No radiological consequences are expected and the event will not be analysed further.

16.15.3.8 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Three 60% capacity blowers, one on standby
		Two position sensors to determine sample location
		Double can containment for hazardous or powdered targets
		Software checks, interlocks and alarms to ensure target cans do not jam and safety incidents are avoided
2	Operation control and response to abnormal operation	Reactor power reduction for low coolant flow
		Reactor power reduction for low secondary coolant flow
		Alarm on high rig temperature
		Automatic removal of targets on very high temperature signal.
		Continuous cooling of stuck sample.
		High pressure blast available for removal of stuck sample
3	Control of accidents within the design basis	FRPS reactor trip on; a) Loss of Normal Power Supply SRPS reactor trip on; a) Failure of the FSS

16.15.4 Transfer, Loading and Pneumatic Cells

16.15.4.1 Erroneous Early Removal of Irradiated U-Mo Targets into a Hot Cell

U-Mo targets are moved during reactor operation. Irradiation time is shorter than the reactor cycle. The Mo is produced by fission of uranium 235. The heat generated by the uranium target is removed by the rigs cooling flow of the RSPCS during irradiation. The targets are left to decay inside the Service Pool for a time determined by the heat generation rate. An operator could erroneously move to the Hot Cell a U-Mo target that has been recently removed from the irradiation position without leaving it to decay for the required time. This would lead to failure of the aluminium cladding of the targets due to insufficient cooling when exposed to the air.

It is postulated that three U-Mo targets are erroneously removed from the decay rack in the Service Pool before having undergone adequate decay time and transported into the Hot Cell. It is further assumed that the interlock that inhibits the transport from the Service Pool into the hot cell due to high activity has failed. The occurrence of this event requires sequential failures in adherence to operating procedures and the presence of an unrevealed mechanical failure. This is a highly unlikely sequence of events.

Because of the number of failures required, the likelihood of this event is considered so low as to render it beyond the design basis. Nevertheless, its radiological consequences have been analysed for the reasons given in Section 16.1.

16.15.4.2 Failure of the Ventilation System

As indicated above, the cells operate at a negative pressure. No can opening or target processing occurs inside the hot cells if the ventilation system fails. None of these cans requires cooling. In the event of a ventilation system failure, the negative pressure would be lost. However, absolute filters are placed in the air exhaust stream of cells and minimal diffusion of activity through the cell walls would be expected.

The cells' ventilation system is connected to the Standby Power System. Loss of ventilation is thus very unlikely. Nevertheless, the event is considered within the design basis. However the radiological consequences would be minor and hence this event will not be analysed further.

16.15.4.3 Failure of ICE

Failure of the ICE is considered to lie within the design basis. No radiological consequences are expected from such an event and it is not analysed further.

16.15.4.4 In-Cell Fire

The hot cells will contain minimal amounts of flammable material thus having minimal fire loading. They are equipped with fire detectors. In-cell fires are considered within the design basis. The radiological consequences of a fire would be minor and, consequently, the event is not analysed further.

16.15.4.5 Failure of Power Supply

Emergency lights would automatically switch on in the event of loss of electric power supply. The same applies to the ICE.

The hot cells' ventilation system is connected to the Standby Power System.

Failure of the power supply is considered to lie within the design basis. The event does not challenge the integrity of the core or the targets in the rigs and would result in no radiological consequences.

16.15.4.6 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Cells are at a negative pressure with respect to the surrounding rooms
		Absolute filters are placed at the intake and exhaust of cells
		Cells equipped with fire detectors and a gas flooding system
		Area monitors inside hot cells

		Cells ventilation system connected to Standby Power Supply
2	Operation control and response to abnormal operation	Wagon can be manually moved in the event of failure of power supply.
		Radiation monitor would inhibit movement of a target too hot to be cooled in air.

16.15.5 Large Volume Irradiation Facilities

These facilities are supplied for the neutron transmutation doping of single-crystal silicon ingots and for bulk irradiation of ore samples for neutron activation analysis.

16.15.5.1 Fall During Manipulation

The beam tubes and reactor core are protected by means of grillwork against the fall of the heaviest silicon ingot (See Section 11.4). The strength of the Reflector Vessel is such that it too will withstand the impact of a silicon ingot.

Silicon ingots in their irradiation cans are removed from the rotating irradiation rigs using Operation Bridge and dedicated lifting tools and placed into a nominated location in the Reactor Pool Storage Rack. These Storage Racks are mounted to the side wall of the Reactor Pool. The cans are then transferred from the Reactor Pool Storage Rack to the storage facility located in the Service Pool by the operator using the Reactor Hall crane with dedicated NTD monorail and tools.

The dropping of a silicon ingot is within the design basis. Provisions in the design result in elimination of significant damage to the core and irradiation rigs as a result of the fall of a silicon ingot.

16.15.5.2 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Reflector Vessel, beam tubes and reactor core protected by means of grillwork.
		Interlocks for operation bridge movement
		Safe tools design.
		Submersed working table attached to operation bridge
		Operational procedures / staff training
2	Operation control and response to abnormal operation	N/A

16.15.6 Cold Neutron Source

The Cold Neutron Source is described in detail in Chapter 11, Reactor Utilisation. This Section is concerned with the potential events associated with the Cold Neutron Source that might challenge the core or the reactor safety systems.

16.15.6.1 Leak in Deuterium Pipe/Moderator Loop

The deuterium moderator loop, tubes, valve manifold and buffer tanks are blanketed by an inert gas. There are helium blankets for the in-pile part and piping, and nitrogen in the blanketing box of the Moderator System Manifold. This Gas Blanketing System contains pressure sensors so any leakage would immediately be signalled to the CNS CMS. This system avoids contact between deuterium and the environment (air or water), even in case of failure of the primary barrier, and prevents tritium releases to the Reactor Hall and Technical Floor, both inside the containment.

In the unlikely event of a leak occurring, once it is detected, the damaged zone would be isolated and the gas possibly vented.

The radiological consequences of a deuterium leak to the containment have been assessed as minor and are not considered further here.

16.15.6.2 Failure of the CNS Refrigeration Cryo-System

In the event of a failure of the CNS Refrigeration Cryo-system during Normal or Standby Operation modes (for example, if one compressor stops), a low helium flow signal to the CNS Protection System would result in a reactor trip request being sent to the FRPS.

The occurrence of a cooling failure during Standby Operation would additionally trigger the injection of helium in the CNS Vacuum Containment as a means of breaking the vacuum and therefore the thermal isolation of the CNS In-Pile Assembly.

Failures in the Cold Neutron Source Refrigeration Cryo-System would not have an adverse impact on the integrity of the core and would have no radiological impact.

16.15.6.3 Hypothetical Deuterium-Air Explosion

Hydrogen and its isotopes can, under certain circumstances, form mixtures with air or oxygen capable of explosion, with no relevant difference in behaviour from one isotope to another. Therefore, a deuterium explosion is analysed as a hydrogen explosion. The inventory of hydrogen in the CNS is small compared with volumes handled in the chemical industry, or even public transport[1]. The occurrence of a deuterium-air reaction is extremely unlikely to occur and the Vacuum Containment is the third level in a sequence of levels preventing the reactor from being affected by this event. The three levels of prevention are:

a) Level 1: Prevent the formation of any deuterium - oxygen mixture.

b) Level 2: Prevent the deuterium - oxygen from reacting in the In-Pile section.

c) Level 3: Prevent the reactor from being damaged by a hypothetical detonation of deuterium - oxygen mixture in the vacuum containment.

16.15.6.3.1 First Level - Avoidance of a Deuterium - Oxygen Mixture

This first level of protection consists of the avoidance of the formation of any deuterium - oxygen mixture by using pure deuterium, with no gas impurities and an inert gas barrier between deuterium and the atmosphere.

Pure deuterium moderator is used in the Cold Neutron Source Moderator System, with a content of oxygen below $1.\ 10^{-3}$ %vol. This amount of impurity cannot form a flammable mixture even if all the impurity content were concentrated in the Moderator Cell. A gas analyser is used to monitor impurities in the moderator before and after filling of the Moderator System.

[1] Ewald, R. "Liquid Hydrogen Fueled Automobiles: On-Board and Stationary Cryogenic Installations," Cryogenics, Vol. 30, September 1990, pp. 38-45

An inert gas blanket containing helium is used around the Moderator System to prevent any contact of air with deuterium in the event of any leakage. The blanketing pressure is monitored to ensure wall leak tightness.

The deuterium pressure in the system is always higher than atmospheric pressure in order to avoid the in-leakage of air into the Moderator System.

16.15.6.3.2 Second Level - Avoidance of Ignition

The second level of protection avoids the formation of ignition conditions in the CNS In-Pile section, in case the first level fails by means of:

a) Protection from static electricity, and

b) Inert blanket around the vacuum system to exclude air penetration into CNS In-Pile Thimble

This second level prevents ignition conditions for a detonation in a postulated event where a deuterium-air mixture is inside the Deuterium Loop. The energy required to ignite a deflagration is in the order of 20 μJ, an energy always available in a nuclear reactor environment. Ignition conditions for deflagration are thus present due to reactor radiation. This greatly minimises the possibility of having a detonation. The Deuterium Loop has protection from static electricity in order to avoid the possibility of a spark with enough energy to cause a detonation.

The CNS Vacuum System (CNS-VS) for the Vacuum Containment has an inert gas blanket (helium) that prevents air ingress into the In-pile Thimble volume. This blanket is needed because of two reasons:

a) In the unlikely event of CNS-VS boundary failure and air ingress during the Normal Operation mode, the cold surface of the CNS Thermosiphon is likely to collect incoming air from a leak. For small leaks, no vacuum failure would occur because the cold surface of the Thermosiphon would work like a vacuum cryogenic pump, and the air would freeze onto the surface of the Thermosiphon. In this event, nitrogen is able to form oxides, which in turn may react explosively with an energy release large enough to initiate a detonation. The CNS VS blanket excludes this possibility.

b) In the unlikely event of the simultaneous failure of the CNS Moderator System boundary and helium blanket within the In-pile (i.e. loss of first prevention level), the CNS-VS blanket excludes the possibility of having a deuterium-air mixture in the In-pile even in case of a further failure.

16.15.6.3.3 Third level - Preventing Reactor Damage

The third prevention level is provided by the Vacuum Containment that acts in the event that all the previous prevention levels fail. The Vacuum Containment is designed to withstand the explosion effects of a stoichiometric deuterium-air mixture, which is the mixture with the highest energy release.

Hence, the detonation of a deuterium-air stoichiometric mixture has been analysed as a hypothetical bounding accident for the design of the Vacuum Containment. The initial state the mixture is considered to be a temperature of 313 K with a pressure of 1 atm.

16.15.6.4 Reactivity Influence

The Moderator Cell of the CNS exerts an influence on the reactor reactivity during change in phase (from liquid to vapour and vice-versa). The value of this reactivity change has been conservatively calculated as 150 pcm. For operational and design basis transients, the speed of reactivity change is low (several minutes) and manageable by the RCMS. Due to evaporation, the lower density of the deuterium vapour would reduce the moderation of neutrons, essentially adding negative reactivity to the core. In the highly unlikely event of complete moderator chamber failure (i.e. simultaneous failure of moderator cell and helium jacket), the reactor would undergo the rapid insertion of 150pcm. Any other failure would cause a slower phase change of the Deuterium from liquid to vapour.

A positive reactivity insertion is given by the liquefaction of deuterium, and there is neither a failure nor a physical mechanism that could suddenly produce liquefaction.

These events are within the design basis. They are not considered further as they have no adverse effect on the reactor core and no radiological consequences.

16.15.6.5 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Adequate conservatism applied for the design of the Thermosiphon and the CNS Moderator System (CNS-MS) pressure boundary, in order to ensure its integrity
		QA program that controls design, analysis, procurement, manufacturing, installation, and operation of the part Cold Neutron Source
		The Moderator System has a closed and passive pressure boundary that minimises the possibilities of leakage. There are neither pumping devices nor operational valves
		The Moderator Cell is within a natural circulation loop, and therefore it has self-regulating trends: the increase in the heat load leads to an increase in circulation and therefore in heat removal.
		Deuterium moderator loop, tubes and buffer tank are surrounded by an inert blanket
		The conservative application of principles of simplicity, redundancy, fail-safe design, and passive safety features used throughout the design as much as feasible.
2	Operation control and response to abnormal operation	The CNS Control and Monitoring System (CNS-CMS), supervises the correct functioning of the CNS systems and takes the CNS from the Normal Operation (NO) Mode to the Standby Operation (SO) Mode when necessary. A separate functionally independent system, called the CNS Protection System (CNS-PS) takes protective actions in case of a CNS operational limit of the Moderator Chamber being threatened
3	Control of accidents within the design basis	The Vacuum Containment is designed to withstand the hypothetical detonation of the worst deuterium-air mixture

Level	Main Characteristics	Safety Feature
		FRPS trip on; a) low helium flow together with high deuterium pressure b) deuterium leakage into the helium blanket SRPS trip on; Failure of the FSS

16.15.7 Neutron Beam Facilities

16.15.7.1 Unauthorised Access to the Neutron Guide Bunker

Access to the bunker is not allowed during normal operation.

Local instrumentation is in place to monitor radiation levels. Interlocks and procedures will be used to ensure radiological protection of operating personnel during maintenance and repair tasks.

Unauthorised access to the Neutron Guide Bunker is considered within the design basis. It has no effect on the reactor core. Its radiological consequences would be minor and will not be considered further.

16.15.7.2 Inadvertent Opening of Primary Shutter

The shutter has spring actuated locks to prevent inadvertent opening. The movement control system has open/closed position signals and interlocks/alarms to ensure efficient and safe operation. Authorisation from the Main Control Room is needed to move the shutters. Local instrumentation and monitoring would alarm on inadvertent opening of the shutters.

Inadvertent opening of the primary shutters is considered to lie within the design basis. It has no effect on the reactor core. Its only consequences are radiological and limited to the Neutron Guide Bunker or to the Reactor Beam Hall which are controlled areas.

16.15.7.3 Failure of the Electrical System

In the event of a failure in the electrical system shutters remain in closed position if they were originally closed. Thus this event has no consequences relevant to safety. In the event of the shutters being open, they would fail open. Alarms would sound, signalling the need for manual closure and warning staff of the hazard.

This event is considered to lie within the design basis. It does not challenge the integrity of the core and its radiological consequences are limited to the Neutron Guide Bunker and Reactor Beam Hall.

16.15.7.4 Loss of Pool Coolant

The external connection is a stainless steel bellows. It has joints with flanges with a double metallic seal. If there is any leak of light water through the first seal, water is collected from the leakage pipe (located between both seals). This leakage pipe provides also a means to detect the leak. The plate on the reactor block face is the second barrier for a loss of coolant from the Reactor Pool through the beams. This loss of coolant has been discussed in Section 16.11. The simultaneous failure of both barriers is not considered credible. The event is therefore considered so unlikely as to render it beyond the design basis. It is not considered further.

16.15.7.5 Loss of Reflector Inventory

Beam tubes penetrate the Reflector Vessel by means of a welded flange. No seals are used. Heavy water leakage, although unlikely, would be stopped by the sealing plate at the reactor block face. The plate is designed to withstand the pressure of the pool water column. Any leak would be detected by the helium filling system. The event will not be considered further.

16.15.7.6 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Spring actuated locks in shutters
		Open/closed position signals and interlocks
		Double metallic H_2O seal with leak detection
		plate on reactor block face designed to withstand the height of the pool water column.
2	Operation control and response to abnormal operation	Heavy water detection in helium filling system
		Alarm for shutter position

16.15.8 Design Basis Postulated Initiating Events

On the basis of the above discussion, many of the events do not lead to accident conditions and cannot be considered as DBIEs. Other events can be included within a general envelope. A summary of the DBIEs is set out in the table below.

PIE	Eliminated by inherent design provisions	Sufficiently unlikely to occur (BDB)		Design Basis Initiating Events (DBIEs)		
				To be considered in other DBIE group	Bounded by other DBIE	Further Analysis
Excess power in the rigs		X				
Early removal of rigs from pool		X				
Loss of flow in the RSPCS						X
Loss of heat sink in the RSPCS				X(LOHS group)		
Blockage		X				
Spurious opening of a RSPCS flap valve		X				

PIE	Eliminated by inherent design provisions	Sufficiently unlikely to occur (BDB)		Design Basis Initiating Events (DBIEs)		
				To be considered in other DBIE group	Bounded by other DBIE	Further Analysis
Loss of Coolant in reactor pool				X (LOCA group)		
Rigs exchange	X					
Inappropriate handling of targets		X				
Excess target activity				Minor Consequences		
Excess target heating					X (Rupture of a can in hot cell)	
Blower failure					X (Rupture of a can in hot cell)	
Valve failure					X (Rupture of a can in hot cell)	
Failure of secondary cooling					X (Rupture of a can in hot cell)	
Cooling failure in a single rig					X (Rupture of a can in hot cell)	
Stuck can				Minor Consequences		
Mechanical failure of a can inside the Pneumatic Conveyor System					X (Rupture of a can in hot cell)	
Rupture of a can inside a hot cell						X
Electrical failure in pneumatic system				Minor Consequences		
Failure of the ventilation system				Minor Consequences		
Failure of ICE				Minor Consequences		
In-cell fire				Minor Consequences		

PIE	Eliminated by inherent design provisions	Sufficiently unlikely to occur (BDB)		Design Basis Initiating Events (DBIEs)		
				To be considered in other DBIE group	Bounded by other DBIE	Further Analysis
Failure of Transfer, Loading and Pneumatic electrical system				Minor Consequences		
Fall of a silicon ingot				Minor Consequences		
Leak in CNS piping				X (Cold Neutron Source Safety Analysis Report)		
Failure of helium cooling in CNS				X (Cold Neutron Source Safety Analysis Report)		
Detonation of mixture of deuterium and oxygen				X (Cold Neutron Source Safety Analysis Report)		
Reactivity insertion due to liquifaction of Cold Neutron Source moderator				Minor Consequences		
Unauthorised access to neutron guide bunker				Minor Consequences		
Inadvertent opening of primary shutter				Minor Consequences		
Failure of shutter electrical system				Minor Consequences		
Loss of pool inventory via Neutron Beam		X				
Loss of Reflector Inventory to Neutron Beam		X				

On the basis of the above, the following DBIE is identified for further analysis;

a) loss of flow in the RSPCS due to failure of pump or shaft seizure
b) rupture of a can in a hot cell

The low likelihood of shaft seizure, when coupled with failure of the FSS, renders the resultant sequence beyond the design basis.

The rupture of the can in a hot cell is not analysed here. Instead, the consequences are considered bounded by those from the beyond design basis accident of melting of a U-Mo rig in the hot cells. This is discussed in the section dealing with Beyond Design Basis Accidents, Section 16.19

16.15.8.1 Loss of Flow in the Reactor and Service Pools Cooling System

16.15.8.1.1 Detection of the Initiating Event

A flow meter detects low flow at the RSPCS discharge line. An alarm is raised in the Main Control Room. Reactor trip is initiated on the following signals:

a) First Shutdown System
   (i) Low flow in the RSCPS
b) Second Shutdown System
   (i) Failure of the FSS

16.15.8.1.2 Design Basis Fault Sequence

a) RSPCS pump stops.
b) Low flow alarm (by RCMS).
c) Reactor trip by FRPS on RSPCS low flow signal or SRPS on failure of FSS.
d) RSPCS flap valves open.
e) Rig decay heat removed by natural circulation.
f) After 30 minutes, the operator manually stops PCS pumps.
g) PCS flow coasts down and natural circulation is established.

16.15.8.1.3 Numerical Analysis

The modelling hypothesis and nodalisation are presented in Section 16.3.

The sequence is initiated following the failure of the RSPCS pump motor. The downward coolant flow through the rigs drops initially following the dynamics of the inertia flywheel. When the flow reaches 90% of its nominal value, the FRPS triggers the FSS, shutting down the reactor. Analysis of the initial temperature rise in the cladding as result of the cooling flow drop through the rigs has been undertaken and for the hot rig, the maximum cladding temperature has been found to be safe. After the reactor is shutdown, temperatures fall sharply.

Only one flap valve is postulated to open. When the valve opens, the pressure at the pipeline where the flap valve is located (pump suction line) increases and the flow through the rigs drops sharply. Coolant temperatures in the rigs increases and the buoyancy forces begin to govern fluid circulation. Upward flow is established with flow inversion through the hot rigs occurring. As a result of the flow inversion the highest coolant temperature is in the upper zone of the rig. The maximum coolant temperature is 84C.

Following the abrupt drop in temperature resulting from reactor shutdown, a gradual rise in temperature of the cladding of the inner face of the hot rig is noticed due to the reduction in coolant flow. When the flap valves open the sharp drop in the flow leads to an increase in the clad temperature reaching a maximum, just after flow inversion, without exceeding the water saturation temperature. Soon afterwards temperatures diminish in accordance with the new balance between buoyancy and friction forces of the natural convection circuit established. Towards the end of the analysed period temperatures continue falling more slowly, following the core decay power. As a consequence of the fluid flowing upwards, the highest cladding temperatures are in the central zone of the rigs.

The transient has also been analysed assuming failure of the FSS and actuation of the SSS. The SRPS triggers the SSS when no end-of-stroke signal is received from two or more CRs. Opening of one of the flap valves is assumed.

An analysis has been undertaken of the flows through the rigs and the total hot branch, including the flow through the siphon breaker. Their evolution is similar to results obtained for the event with actuation of the FSS. The point at which the SSS is triggered has been identified. The delay in shutting-down the reactor leads to a slightly higher rise in temperature in the rigs with respect to the event with FSS actuation. When the SSS is activated, the cladding temperature drops as a consequence of the sharp decrease in power. Since the insertion of negative reactivity by the SSS is slower than that produced by the FSS, the temperature drop is more gradual. The maximum cladding temperature is within safe limits.

There are no significant differences between both cases after reactor shutdown, when the flap valve opens, regardless of which shutdown system has actuated.

The response of the system after seizure of the RSPCS pump shaft has been analysed with actuation of the FSS. As a result of the seizure of the shaft, the flow falls abruptly. The FSS trip is produced only a fraction of a second after the shaft seizure. Due to the faster flow reduction in the hot branch, the only flap valve that is modelled, opens and an initial backwards flow is observed. The abrupt drop in the rigs flow rate causes temperatures to increase more rapidly than in the event with failure of pump motor. Because flow inversion occurs at higher rigs power, in respect to this sequence maximum temperatures are reached just after flap valve opening. Maximum coolant temperature in the hot rig is well below that which would result in clad damage and the maximum cladding temperature is within safe limits.

Radiological Impact Analysis

No damage to the rigs arises from the loss of flow in the RSCPS. There would thus be no off-site radiological impact.

16.15.9 Conclusions

The utilisation of the reactor does not lead to any accident with other than very minor radiological impact off-site. The only event considered to have potential to lead to a release would be a can failure in the hot cell. Design characteristics and administrative procedures minimise the likelihood of the occurrence of failures associated with reactor use and irradiation facilities.

The loss of coolant flow initiating event in the pool cooling system due to either the failure of the pump motor or to the shaft seizure is adequately covered by the safety systems. In other words, the trip parameters of the safety systems, their respective trip values and the safety systems work adequately in bringing the reactor to a safe shutdown state. In none of the cases analysed do flow temperatures reach the saturation value for water at the operating pressure. In a number of cases, the surface temperatures of the hot rigs exceed the onset of nucleate boiling temperature for a short period of time. This would not compromise the integrity of the rig's cladding.

End of Section

16.16 ANALYSIS OF EVENTS DUE TO SPURIOUS TRIGGER OF THE SAFETY SYSTEMS

This Section considers those events arising from the spurious initiation of the safety systems. The safety systems are actuated by the FRPS and SRPS. The trigger signals are sent to the FRPS and/or SRPS when the system reaches the set point value (see Chapter 8 for a description of the RPSs and their signals).

16.16.1 First Shutdown System

The FSS shuts down the reactor by fast insertion of the CRs. The spurious initiation of the FSS may be caused by a failure of the FSS, a spurious trip signal generated by the FRPS or by a fluctuation of a trigger variable. The FRPS is considered in detail in Chapter 8. Its failure would result in no trigger signal to the FSS.

A failure of the FSS could result in the insertion of one or more CRs without a triggering signal from the FRPS.

A fluctuation of the trigger signals is unlikely to cause spurious initiation of the FSS. The FRPS requires not only a trigger signal reaching the respective set point value but also its remaining there for at least 10 ms. A fluctuation is unlikely to last for the 10 ms required by the FRPS, and therefore would not cause the spurious indication of channel trip. In addition, two out of three channels of the variable would have to trip to produce a spurious trip of the FSS. The FRPS has self check diagnostics that are designed to trip a channel if it is not performing correctly, alerting the operator that a fault has occurred. Spurious initiation of the FSS is thus very unlikely.

In addition, spurious initiation of the FSS does not constitute a hazard to the plant. The spurious trigger would shut the reactor down, with no adverse impact on the reactor core or associated systems. Once it is verified that the trigger is indeed spurious, the reactor could be re-started within the time window of the xenon poisoning.

16.16.2 Second Shutdown System

The SSS shuts down the reactor by dumping of the heavy water from the Reflector Vessel. The spurious initiation of the SSS may be caused by a failure of the SSS, a spurious trip signal generated by the SRPS, by a fluctuation of the trigger variable, or by the spurious indication of failure of the FRPS. The SRPS is considered in detail in Chapter 8. Failure of both protection systems (FRPS and SRPS) is deemed very unlikely.

A failure of the SSS could result in the spurious opening of one or more dump valves without a triggering signal from the SRPS.

A fluctuation of the trigger signals is unlikely to cause spurious initiation of the SSS. The SRPS requires not only a trigger signal reaching the respective set point value but also its remaining there for at least 10 ms. A fluctuation is unlikely to last for the 10 ms required by the SRPS, and therefore would not cause the spurious indication of channel trip.

In addition, spurious initiation of the SSS does not constitute a hazard to the plant. The spurious initiation would shut the reactor down, with no adverse impact on the reactor core or associated systems. Given the refilling time of the Reflector Vessel (of the order of 1 hour), there is no possibility of restarting the reactor before xenon poisoning occurs.

The Reflector Vessel and its internals are designed to withstand the reduction in cooling due to the emptying of that portion of heavy water associated with the SSS. Since the loss of reflector leads to reactor shutdown, the heating is caused by decay gamma heating.

16.16.3 Spurious Containment Isolation

The Containment is isolated on high activity and high activity rate at the stack monitors (particulate, iodine and noble gases activity monitors). A spurious trigger of the containment isolation may be due to a failure in the Containment Isolation System valves' actuation system, a spurious signal from the stack monitors or a failure of the FRPS. The spurious signal from the stack monitors needs to be sustained for more than 10 ms to trigger containment isolation.

A failure in the Containment Isolation System valves' actuation system could lead to one or more Containment Isolation System valves closing without a triggering signal from the FRPS.

The spurious closure of the containment isolation valves does not constitute a safety hazard. In the event the normal operation HVAC is available, energy continues to be removed from the Reactor Building. In the event of a loss of Normal Power, the Containment Energy Removal System, connected to the Standby Supply, would remove the energy from the containment.

16.16.4 Spurious Diesel Generator Start-up

The diesel generators provide support the Standby Power Supply (SPS) (see Chapter 9).

When a signal of loss of Normal Power Supply is detected, a start-up signal is sent to the diesels. After a stabilisation time, transfer is established. These actions are hardwired.

There are two possible scenarios for the spurious start up of the diesel generators:

a) Automatic Transfer Switch in one of the switchboards that would initiate transfer from the NPS to the SPS. This event leads to the disconnection of the electric loads in that train until the diesel generator finally enters into service and the loads are reconnected. The operator would follow a procedure to cope with this situation. This event does not affect the fulfilment of the safety functions by the safety systems.

b) Spurious start up of a diesel generator. Each diesel generator starts up independently. Therefore it is unlikely that both generators could start up at the same time. The diesel would start up but it would not feed the corresponding switchboard. Spurious triggering of the diesel generators has no impact on the safety of the facility. Should it occur, it would be detected and corrected by the operator in the Main Control Room. In the event of a loss of Normal Supply occurring after a spurious trigger of a diesel and while it is still on, the transfer would be completed as designed, with no effect on the restoration of the Standby Supply.

16.16.5 Conclusions

The spurious initiation of safety systems does not challenge the safety of the plant or the capability of other safety systems to perform their safety function.

End of Section

16.17 EXTERNAL EVENTS

This section considers external initiating events. External initiating events are site dependent and contain aspects that are design dependent.

The site of the Reactor Facility is within the existing perimeter fence of the LHSTC site and covers an area of approximately four hectares. ANSTO maintains the existing buffer zone of 1.6km in radius, centred on the existing HIFAR facility, within which land use restrictions apply and residential development is excluded.

This section contains information originally presented in the HIFAR Probabilistic Safety Assessment and the Environmental Impact Statement (EIS) for the Reactor Facility. This information remains valid. The result of the reviews contained within these documents is an exhaustive list of natural and man-made external events. These events have been screened and evaluated to select those requiring detailed analysis. The screening criteria used for the external hazards identified were:

a) The event is of equal or lesser damage potential than those events for which the plant is designed.

b) The event has a significantly lower frequency of occurrence than other events with similar consequences.

c) The event cannot occur close enough to the facility to affect it.

d) The event is included in the definition of another event.

The screening of the external events is presented in Table 16.17/1.

The events that have been analysed resulting from the screening are presented in the following list:

Aircraft impact

Bushfire

Industrial activities

Military activities

Onsite activities (outside the facility)

Transportation accidents

Extreme wind

Seismic

Sabotage

Lightning

Local flooding

The impact of each of these events on the Reactor Facility will be considered in the following Sections.

16.17.1 Aircraft Impact

Two airports are located near the LHSTC: Kingsford Smith (Sydney) Airport, 19 km NE from the LHSTC and Bankstown Airport, 13 km N of the LHSTC. Kingsford Smith Airport is used by all types of aircraft, such as large commercial aircraft, general aviation and helicopters. The Bankstown Airport is used by light aircraft and helicopters. Aircraft travelling to and from Kingsford Smith are not expected to be in final approach or initial climb phases at such distances. Aircraft restrictions are in place preventing them from flying within one nautical mile of the LHSTC site below an altitude of 2000 feet above sea level. Lucas Heights lies under one of the main flight paths into and out of Kingsford Smith airport. Radar tracks indicate that about 2,500 jets per month fly through a 10 km x 10 km box centred on HIFAR. This corresponds to 30,000 flights per year in the vicinity of LHSTC having a potential trajectory that, in the event of an accident, could impact on the Reactor Building. This estimate, according to the EIS, is conservative. On the basis of the calculations performed for the HIFAR Probabilistic Safety Analysis, the probability of a large aircraft crashing on the Reactor Building is estimated as being less than one in five million per year.

According to the ARPANSA Safety Evaluation Report of the ANSTO Application for Licence to Prepare a Site for the Reactor, the estimated low probability of an aircraft crashing onto the Reactor facility would not require the design of the reactor to withstand aircraft crashes. Nevertheless, the impact of a lightweight aircraft has been placed within the design basis for the reactor core.

The design worst case external missile considered was a light aircraft.

The upper Reactor Hall envelope is considered the most vulnerable part of the structure since it comprises a single “skin” of structure (walls and roof) to resist aircraft impact.

A protective structural steel grille “shield” is provided over the upper Reactor Hall. This structure is built well clear of the main roof and walls to allow substantial deflection under aircraft impact without significant damage to the main building envelope. In the case of the Reactor Hall roof, the aircraft impact energy is shared between the grille of the protective shield and the Reactor Hall roof itself. The Reactor Hall roof structure comprises closely spaced steel beams acting together with a reinforced concrete slab constructed on steel permanent form work

Aircraft impact at the lower levels would be resisted by multiple walls and concrete floors, which have considerable energy absorbing capacity and which provide a buffer zone to keep the aircraft clear of the reactor block. Further details of the analysis of the protective shield are provided in Chapter 4.

In the event of aircraft impact, both the FRPS and SRPS would trip the reactor on signals from the accelerometers. The reactor would remain in safe shutdown state and no damage would occur to the reactor core.

The Containment, reactor block and pools would protect the core from any fires arising from the aircraft crash. Aircraft fires represent the bounding heat load on the Containment structure. The ability of the Containment to withstand the effects of aircraft fire is discussed in Section 4.4. The facility design includes fire-fighting capabilities (see Chapter 10). The core is protected from the impact of smaller debris by the Chimney Protection Grid.

The impact of a light aircraft on the cooling towers is bounded by the loss of heat sink. The impact on the facility substation could lead to loss of both Normal and Standby Power Supplies. The reactor would shutdown on loss of power, the decay heat being removed by evaporation of the pool water.

16.17.1.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Protective structure above reactor building roof to absorb most of the energy from the impact.
		Height restriction for flights over the LHSTC.
2	Operation control and response to abnormal operation	Operator can manually shutdown the reactor (not required)
3	Control of accidents within the design basis	FSS and SSS simultaneous reactor trip by signal from any one of the three seismic keys.
		Fire fighting capabilities
		Passive long term decay heat removal system by natural circulation and evaporation of pool water.

16.17.2 Bushfire

The location of the LHSTC is such that large bush fires can be expected every 8 to 12 years. These fires have the potential to burn to the site boundary. The fire intensity and duration is dependent on a number of meteorological factors including prevailing wind strength, direction, temperature, and humidity. The LHSTC site is on relatively flat ground with sparse vegetation, which would reduce the intensity of any fire coming over the ridge.

Previous work for HIFAR examined the effect on the containment building of the radiant heat from bush fires under steady state conditions. It has been shown by Beattie (1999)[1] that the radiant heat from a typical bush fire would be less than solar heating, and could only heat the containment building to a very modest level. Hence it is considered that the incidence of bush fires near the LHSTC site does not present any unique effects for consideration in the design and operation of the replacement reactor facility.

Nevertheless, bushfire management strategies are in place at LHSTC. Current bush fire management involves:

- Hazard reduction
- Bush fire preparedness
- Emergency planning exercises

A hazard reduction programme is carried out by ANSTO in conjunction with the Sutherland Rural Fire Service. The programme aims to provide a fire protection zone between building and areas of bushland within the site boundary fence and along the boundary fence, in order to eliminate or reduce available fuel for bush fires. The zone consists of a fuel-free zone, a maintained grassed area between buildings and the boundary fence; and a fuel-reduced zone, located between the site boundary and surrounding bushland, which is maintained as a high standard fire break of low shrubs and grasses. [1]

[1] *The Effect of Bushfires on Research Reactors at Lucas Heights,* David Beattie, ANSTO report NTD/TN 216, March 1999.

Existing precautionary and protective measures for bush fires in place at the LHSTC include:

a) A full time Fire Officer responsible for maintaining and updating bush fire precautionary measures, including hazard reduction programmes and fire control equipment.

b) A Building Warden and a Deputy within buildings having specific duties in the event of an emergency. Many other members of the staff have specific roles in the bush fires, which are documented in the existing ANSTO emergency plan.

c) Fire extinguishers and fire hoses located in buildings in accordance with fire regulations. The fire hydrants mains have been extended to the north of the site to provide defence in depth during bush fires. This line has a low pressure isolation device to protect the integrity of ANSTO’s mains system.

d) Fire fighting equipment, such as fire hydrants, hoses and a portable tanker unit. There are over 100 fire hydrants within the LHSTC. The hydrants are located both within and outside the existing site perimeter fence and so can be accessed by ANSTO staff and visiting fire fighting crews. Water pumps are present to ensure circulation from on-site storage facilities as well as a booster pump to increase water pressure if greater demand is placed on the system. Current portable fire fighting equipment includes hundreds of fire extinguishers, knapsack sprays and a small tanker unit that can be placed on four wheel drive vehicles to provide fire fighting support. ANSTO also maintains two specially equipped mobile emergency response vehicles.

e) Fire spotting. The existing water tower can be accessed during bush fires to allow the observation of fire fronts, and to locate and direct fire fighting crews.

f) Support facilities, including canteen amenities and a helipad, are made available to fire fighting crews during bush fire emergencies.

g) Support fire fighting. ANSTO have trained staff capable of responding to fires and assessing the need for assistance required to extinguished them.

h) An ongoing maintenance programme for buildings and gardens that follows the recommendations of Australian Standard HB36 “Building in Bush Fire Prone Areas – Information and Advice” (AS, 1993). This programme is conducted annually before the start of bush fire season.

i) ANSTO’s land management policy in the buffer zone addresses bushfires and their control.

Emergency planning at the LHSTC involves:

a) Standing Operation Procedures (that is, internal instructions) to support the ANSTO Response Plan and the Reactor Facility Emergency Plan for all staff with responsibilities in the event of a bush fire.

b) Training of staff in the use of fire fighting equipment and training of building wardens in bush fire procedures.

Preparation of emergency plans is undertaken in accordance with the “NSW State Emergency and Rescue Management Act”, 1989. Emergency planning and response is discussed in Chapter 20.

The main design considerations for avoiding or minimising hazards from bush fire include compliance with relevant Australian Standards for buildings; the use of appropriate construction materials; appropriate design to avoid the collection of combustible material on or near buildings (e.g. leaves settling in guttering, roof of eaves); and maintaining recommended fire hazard reduction distances from bushland as described in the Environmental Impact Statement (EIS). Specific measures in place for the Reactor Facility to reduce bush fire hazard and to assist in fighting bush fires are:

a) The minimum fuel-free zone (the distance between outer building alignments and the perimeter fence) is 22 m on the southern perimeter of the site and 20 m on the western and northern perimeters.

b) The minimum fuel-reduced zone width is 20 m.

c) Flammable materials are stored away from the perimeter of the site.

d) The buildings' design prevents entry of ember showers or smoke during major bush fires (isolation of Containment and ventilation system).

e) Smoke detectors and fire alarms are installed in all buildings of the facility.

f) Fire hydrants and fire-fighting equipment are available in all buildings.

g) Water is available in the cooling towers basin.

h) Regular maintenance is performed in all buildings.

i) Vegetation and fuel loads is maintained at a minimum within the fuel-reduced zone.

j) Grasses are regularly mowed and watered within the fuel-free zone.

k) Fire trails in the Buffer Zone are maintained to a high standard.

l) Erosion control on the fuel-free zone and access tracks is in place.

m) Trees and shrubs for ornamental planting are selected to include species not readily combustible, such as native rainforest species.

n) Before each bush fire season the site is assessed to determine the need for:

    (i) pruning landscape trees that overhang gutters and cover windows

    (ii) removing vegetation and litter accumulated around buildings and fences

    (iii) where appropriate, sealing crevices under roofs to prevent entry of wind borne embers and smoke into buildings

o) Ongoing training and awareness programmes for ANSTO staff.

16.17.2.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Non-flammable building and components materials
		Minimum fuel-free zone is 22 m on the S perimeter of the site and 20 m on the W and N perimeters
		Minimum fuel-reduced zone width is 20 m.
		Building design prevents entry of ember showers or smoke during major bush fires (isolation of containment and ventilation system).
		A full time Fire Officer, who is responsible for maintaining and updating bush fire precautionary measures, including hazard reduction programmes and fire control equipment

Level	Main Characteristics	Safety Feature
		Training of staff in the use of fire fighting equipment and training of building wardens in bush fire procedures
2	Operation control and response to abnormal operation	Smoke detectors and fire alarms in all buildings of the facility
		Fire hydrants and fire-fighting equipment in all proposed buildings
3	Control of accidents within the design basis	Fire Warden controls response in buildings
		Co-ordination with local fire fighting agencies
		ANSTO Response Plan in place.

16.17.3 Industrial Activities

Off-site accidents at nearby industrial facilities have the potential to affect the replacement research reactor facility through overpressure following explosions, fires, generation of missiles or release of toxic material. The potential impact of a nearby industrial accident on the facility is similar to that of transport accidents involving hazardous materials near the LHSTC site and onsite activities

The inventory of hazardous materials and the nature of activities in the buildings leased by companies at the ANSTO Business and Technology (BAT) Park show that the amounts of hazardous material are very small and the activities do not have any potential to impact the operation of the facility. This is confirmed by an independent review of the LHSTC Dangerous Goods Inventory List, which indicated that there are no potential threats to the habitability of the HIFAR control room from hazardous materials stored at the BAT. This conclusion also applies to the Reactor Facility.

Industrial accidents are bounded by transport accidents (See Section 16.17.6) and are therefore not analysed further.

16.17.4 Military Activities

The HIFAR Probabilistic Safety Analysis considered the likelihood of the HIFAR reactor being hit by a stray artillery shell from the Holsworthy Military Area. It concluded that the likelihood is incredible, less than 1 in 10 million years (10^{-7} per year). Even though the Reactor Facility is closer to the military area than HIFAR, this is a minor difference and does not affect the likelihood. The conclusion therefore also applies to the Reactor Facility. The impact of an artillery shell on the replacement reactor building is thus considered beyond the design basis and will not be analysed further.

16.17.5 Onsite Activities (Outside the Reactor Facility)

16.17.5.1 Activities in Other Site Buildings

Onsite activities have the potential to affect the Reactor Facility through overpressure following explosions, fires, generation of missiles and releases of toxic, cryogenic or radioactive material. The characterisation and management of LHSTC chemical hazards, including bulk chemical and other hazardous materials storage facilities, has been described previously in the EIS. The location of the chemical storage facilities in relation to the Reactor Facility site is such that, for all cases, the hazards presented by the type and quantity of chemicals and their distance from the reactor are bounded by the hazards presented by a road transport accident (see Section 16.17.6).

The potential for an accident leading to an uncontrolled release of radioactive material from any LHSTC building is small. The potential effect on the Reactor Facility of such an onsite accident is also small. The ventilation system of the Reactor Facility has isolation valves that can be closed to prevent ingress of the external toxic, cryogenic or radioactive material.

There are no large, high energy, rotating machines or large, high pressure machines on the LHSTC site. There is therefore no need to consider missiles arising from this source. The effect of the generation of missiles by other means is bounded by an aircraft crash.

Activities in other site buildings are considered within the design basis. Their consequences are bounded by aircraft crash.

16.17.5.2 Dual Operation

With the exception of the liquid effluents, the Reactor Facility is designed to be totally self contained. Nevertheless, several aspects need to be taken into account during the dual operation of the Reactor Facility and the HIFAR.

16.17.5.2.1 Services

Infrastructure requirements are adequate to support dual operation. Nevertheless, temporary arrangements have been made to ensure safe operation of all the essential support facilities during the approximately six-month period of dual operation.

16.17.5.2.2 Water Supply

The existing site distribution system has been extended to the site of the Reactor Facility. The system has been upgraded to satisfy the water supply demands during dual operation of HIFAR and the Reactor Facility.

16.17.5.2.3 Wastewater

The existing sewage treatment can accommodate the relatively small increase in demand during dual operation. The active B line wastewater and C line trade wastewater handling systems have the capacity to accommodate the increase in demand arising from dual operation. Storm water control during dual operation can be accommodated within the existing storm water system and its extensions. This extension of the storm water system has been designed and constructed to current best practice and in accordance with NSW Environment Protection Authority guidelines and monitoring requirements and ANSTO land management constraints.

16.17.5.2.4 Electricity

The electricity requirement during dual operation increases during dual operation. To meet this increase in demand, an upgrade of the power supply system has been undertaken. This has consisted of:

a) Modifications by Energy Australia to their main substation.

b) Installation of two new high voltage circuit breakers to Energy Australia's high voltage supply in the main zone substation.

c) Construction of a new high voltage/low voltage substation with switchgear located adjacent to or within the Reactor Building.

d) Installation of two new underground high voltage feeders from the main substation to the new substation.

16.17.5.2.5 Radioactive Emissions

Because of the period of full power operation required to build up substantial radioactivity, the inventory level in the core are not sufficient to represent a significant additional off-site hazard during dual operation.

For the same reason, no significant increase in individual worker exposure levels will arise. The collective dose for the group of reactor workers as a whole may be expected to increase because a greater number of workers will be involved in reactor operations during the handover period. However, the increase will be limited, as dose rates in the Reactor Facility will be low.

Concerning radioactive emissions generated by both reactors, for most of the commissioning phase of the Reactor Facility operations will be undertaken with the reactor at low power or in a shut down state. During dual operation, the majority of emissions may be expected to arise from radioisotope production which would not significantly alter in volume or in kind compared to that prior to dual operation.

16.17.5.2.6 Accidents in High Flux Australian Reactor

The potential for accidents in HIFAR is very small. An accident that might occur would most likely involve small amounts of radioactivity and would be contained within the HIFAR containment. The consequences would therefore be similar to those that might be expected from accidents in other site buildings.

In the very unlikely event of significant core damage in HIFAR, the local HIFAR area would be evacuated. Were the accident to progress further, it is possible that the Reactor Facility might require evacuation. The communication systems would allow early notification of such a necessity. In such an event, the reactor would be safely shutdown by the operators in the Main Control Room and all non-essential staff evacuated. This would ensure maximum resources were available to HIFAR.

The Reactor Facility would be protected from any activity released by HIFAR by the isolation of the Containment. In the event that the Main Control Room became uninhabitable for any reason, the operators would transfer to the Emergency Control Centre. The period of dual operation is short and for most of this time the Reactor Facility will be operating at low power.

The consequences on the Reactor Facility would be minor and are bounded by aircraft crash.

16.17.6 Transportation Accidents

The only hazardous substances regularly travelling the roads near to the LHSTC site are petrol and diesel. Sodium cyanide is carried by rail, but it is too far away from the site to pose a hazard in the event of an accident. Explosives carried by road are kept away from the LHSTC. DNV Consultancy Services performed an analysis of transport accidents on New Illawarra Road, 240 m from the site, and the nearest railway, 3000 m from the site. Five bounding scenarios were developed and assessed for road and rail transport accidents near the replacement reactor site. These were:

a) Boiling Liquid Expanding Vapour Explosion (BLEVE) of a full road tanker of Liquid Pressurised Gas (LPG).

b) LPG flash fire and vapour cloud explosion.

c) Fire with possible explosion of a full road tanker of petrol.

d) Explosion of a full semi-trailer load of ammonium nitrate.

e) Rupture of a full road tanker of chlorine.

The DNV analysis concluded that the bounding scenario for LPG BLEVE, petrol fire and ammonium nitrate explosion would have negligible consequences for any person in the open on the LHSTC site. This bounding scenario would have no significant impact on buildings, aside from the possibility of breakage of glass windows due to the explosion.

The rupture of a LPG road tanker and subsequent formation of a gas cloud and flash fire on the road 240 m from the site would have no impact on Reactor Facility operation or safety.

A rupture of a tanker containing chlorine could cause injury and fatalities to exposed people depending upon their location. Nevertheless, there is no transport of chlorine along roads near LHSTC and no such transport is planned by NSW authorities.

Transportation accidents are considered within the design basis. Their consequences on the Reactor Facility would be minor.

16.17.7 Extreme Wind

The HIFAR Probabilistic Safety Analysis presented a wind hazard analysis for the LHSTC site, including tornadoes. The analysis used an accepted statistical approach based on Kingsford Smith Airport data. The analysis determined that the fastest-mile wind speed for the LHSTC site is 170 kmh^{-1}. The highest tornado-type wind speed is 135 kmh^{-1}. The design basis of the building and structures includes not only the pressure effects associated with the wind but also the gusting effects and the pressure drop and missile effects in the event of tornado-type winds (Chapter 4). The effect of the impact of missiles on the building is bounded by the aircraft impact. All other effects are included in the design basis of the building.

Since the building is designed to withstand high winds, the most probable effect of this event on the facility is loss of electric power. Therefore, this event is bounded by the Loss of Normal Power Supply.

16.17.8 Earthquake

As described in Chapter 3, the LHSTC is located on a sandstone plateau in the Sydney Basin. The current earthquake map hazard map of south-eastern Australia produced by Standards Association of Australia in 1993, shows the Sydney Basin to be in a low intensity seismic zone. Local geological structures exhibiting recent seismic activity have not been identified and records suggest that, in the past 1000 years, no seismic activity has occurred at the Centre that would have caused damage to modern engineering structures.

In assessing the safety of a reactor, a Safe Shutdown Earthquake, or SL-2 earthquake, is defined as one which has a very low probability of being exceeded and represents the maximum level of ground motion to be used for design purposes. The International Atomic Energy Agency has observed that in some locations, the SL-2 event corresponds to a seismic activity that could occur once every 10,000 years. This is a much more stringent criterion than that used for any other building in Australia. The peak ground acceleration adopted for the SL-2 earthquake is 0.37g. Section 2.6 details the seismic design criteria adopted.

Both the FSS and SSS trip the reactor due to the signals from tri-axial seismic keys placed in different locations at the building. Earthquakes and aircraft impacts are the only initiating events that trigger both Shutdown Systems simultaneously. The seismic keys detect acceleration in all three directions. A seismic event is too fast to allow any action prior to the shutdown of the reactor.

All the Engineered Safety Features and the Reactor Facility buildings are designed to withstand the SL-2 earthquake. After the SL-2 earthquake, the reactor would remain in safe shutdown state. In addition, all the piping and components of the cooling circuits are designed to withstand the SL-2 earthquake. This event would not lead to a loss of coolant accident. The Reactor Pool is anchored to the heavy concrete reactor block, moving with it in the event of an earthquake. The same applies to the reactor internals attached to the Reactor Pool wall. In addition, the analysis in Chapter 4 indicates that the Reactor Building and structures can withstand higher accelerations than 0.37g by a factor of around 2. This gives high confidence in the seismic resistance of the Reactor Facility structures.

The water tanks are also designed for the SL-2 earthquake. Water supply is ensured in the event of loss of external supply, for fire fighting purposes and for compensation of evaporation of pool water. In addition, the Standby Supply is powered by Safety Category 1 diesel generators.

Seismic Category 1 systems include:

a) Items whose failure could directly or indirectly cause accident conditions.

b) Items required for reactor shutdown, monitoring of critical parameters, maintaining the reactor in shutdown condition and removing residual heat.

c) Items required to prevent radioactive releases.

Seismic Category 1 systems are designed to remain in elastic behaviour during the SL-2 earthquake. This means that they have capacity to accommodate seismic actions that could exceed the SL-2 earthquake.

The SL-2 earthquake is considered in the design basis of the facility. A safe shutdown state can be maintained after the SL-2 earthquake, with no possibility for core damage.

16.17.8.1 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Building, reactor components, piping and cooling circuit components designed to withstand the SL-2 earthquake.
		Reactor pool anchored to the reactor block.
		The water tanks are designed for the SL-2 earthquake.
		Building and components designed for elastic behaviour under the SL-2 earthquake.
2	Operation control and response to abnormal operation	N/A
3	Control of accidents within the design basis	FSS and SSS simultaneous reactor trip by signal from any one of the three seismic keys.
		Standby Power Supply
		Passive long term decay heat removal system by natural circulation and evaporation of pool water.

16.17.9 Sabotage

The Reactor Facility has design provisions to deter attacks or sabotage. To access the reactor Facility, a person must go through several physical barriers and ID checks and he/she needs to have the appropriate authorisation. Security measurements are incorporated in the design, based on a threat assessment undertaken by the security services and agreed with the Director General, Australian Safeguards and Non-proliferation Office, ASIO, and other Commonwealth agencies. Security measures also comply with all appropriate safeguards agreements as indicated in Chapter 4 and the Application, including the requirements of IAEA document INFCIRC 225/Rev 4.

Sabotage is not amenable to probabilistic treatment but is countered by information from the intelligence agencies on its likelihood (thus allowing heightened security measures) and by adequate provisions in the design. However, as part of the proving of the integrity of the design provisions, consultants in terrorist activity and explosives were involved in assessing the threat to the reactor from a range of explosive devices. These were analysed based on their impact on all the identified more vulnerable areas in the Reactor Facility. The result of this assessment was that none of these attacks would threaten the integrity of the reactor core or create radioactive releases greater than those analysed from other beyond design basis accidents.

Following the September 11 terrorist attacks, the design of the Reactor facility was reviewed again from the point of view of physical security. The review concluded that no significant changes to the design were needed.

Security threats are assessed elsewhere, but the design of the Reactor Facility is such that the response systems are scalable to meet foreseeable changes in the threat level.

16.17.10 Design Basis Postulated Initiating Events

According to the previous descriptions, some of the events are beyond the design basis of the facility. Other events can be included within a general envelope. Only those identified as requiring further analysis are discussed below.

A summary of previous considerations and identification of the DBIEs is given below.

PIE	Sufficiently unlikely to occur (BDB)		Design Basis Initiating Events (DBIEs)		
			To be considered in other DBIE group	Bounded by other DBIE	Further Analysis
Small aircraft impact					X
Large aircraft impact	X				
Bushfire					X
Industrial activities	X				
Military Activities	X				
Activities in other site buildings				X (Aircraft impact)	

Dual Operation				X (Aircraft impact)	
Transportation accidents			Minor Consequences		
Extreme wind				X (Loss of Normal Supply)	
Earthquake					X

On the basis of the above, three DBIEs are identified for further analysis:

Aircraft impact

Bushfire

Earthquake

16.17.10.1 Aircraft Impact

16.17.10.1.1 Detection of the Initiating Event

The seismic keys detect the movement of the building due to the impact.

16.17.10.1.2 Design Basis Fault Sequence

a) Aircraft crash on building

b) Reactor trip by FRPS and SRPS on seismic keys signal

c) FSS and SSS shutdown the reactor

16.17.10.1.3 Numerical Analysis

The design approach adopted for the impact of a light aircraft has been based on information provided by the aircraft industry. The approach can be summarised as follows:

a) Provide a ductile structural system for the Reactor building envelope.

b) Provide redundancy in the form of at least two layers of protective structure, as well as multiple load paths.

c) Utilise crushing, plastic and elastic deformation of structure to absorb impact energy.

The design philosophy is to provide a ductile structure that resists plane impact by energy absorption, i.e. by utilising the strain energy from structural deformations to absorb the kinetic energy of the aeroplane. A detailed description of the calculation method and results is presented in Chapter 4.

16.17.10.1.4 Radiological Impact

Since the design of the building and the protective structure protects the core from damage, no abnormal release is expected from this event.

16.17.10.2 Bushfire

16.17.10.2.1 Detection of the Initiating Event

The bush fire would be detected by observation outside the facility earlier than the detection by any facility system.

16.17.10.2.2 Design Basis Fault Sequence

a) Bush fire starts and reaches the vicinity of the facility.

b) The ventilation system is isolated from the exterior.

16.17.10.2.3 Numerical Analysis

Not applicable for this event.

16.17.10.2.4 Radiological Impact Analysis

No damage to the Reactor facility is expected due to a bush fire due to the specific design features and separation, therefore no abnormal release would arise from this event.

16.17.10.3 Earthquake

16.17.10.3.1 Detection of the Initiating Event

The seismic keys detect the movement of the building due to the earthquake.

16.17.10.3.2 Design Basis Fault Sequence

a) Earthquake causes vibration.

b) Reactor trip by FRPS and SRPS on seismic keys signal.

c) FSS and SSS shutdown the reactor.

16.17.10.3.3 Numerical Analysis

The response of the building to an earthquake is analysed in detail in Chapter 4. Each system is analysed with respect to its seismic response in the chapter where it is described.

16.17.10.3.4 Radiological Impact

Since the design of the building protects the core from damage, no abnormal release is expected from this event.

16.17.11 Conclusions

The design of the replacement reactor and associated facilities takes into account all relevant external events. The building is designed to withstand the SL-2 earthquake with a high confidence and the protective grille placed above the roof of the Reactor Building is designed to absorb the energy of a small aircraft impact. The reactor core is protected from damage by small aircraft impact from all directions. In addition, the reactor systems, cooling circuits piping and components, and tanks are designed to withstand the SL-2 earthquake. Therefore, no damage to the core and abnormal radioactivity release is expected after an earthquake or aircraft impact.

Bushfires are not expected to affect the building, given all the protective measures adopted at the site to maintain bushfires away from the site. Moreover, the thermal load on the building caused by radiated heat from a nearby fire is not significant in comparison with the effect of the sun.

External events with a credible likelihood of occurrence are not expected to result in any state other than safe shutdown.

End of Section

Table 16.17/1 Screening of the External Events

Event	Screening Criterion	Remarks
Natural Events		
Avalanche	4	Site location precludes event
Bushfire	1	Included in the design basis
Coastal or other erosion	4	Site location precludes event
Drought	5	Bounded by loss of cooling
Flooding – regional	4	Site location precludes any direct effect
Flooding – local or site	1	Considered in reactor building design
Extreme winds	1	Considered in reactor building design
Landslide	4	Site location precludes event
Lightning	1	Included in detailed design
Low water supply (from low lake, dam, or river level)	5	Considered in analysis of loss of heat sink
Low Winter temperature	1	Included in detailed design
High Summer temperature	1	Included in detailed design; bounded by bushfire
Intense precipitation	5	Included in site flooding analysis
River diversion	4	Site location precludes event
Sandstorm	4	Site location precludes event
Seiche	4	Site location precludes event
Sinkhole	4	Site characteristics precludes event
Seismic activity	1	Considered in building design
Snow Storm	4	Site location precludes event
Storm surge	4	Site location precludes event
Tsunami	4	Site location precludes event
Volcanic activity	4	Site location precludes event
Waves	4	Site location precludes event
Human Induced Events		
Aircraft crash	1	Included in the design basis for the building
Nearby industry – pipeline	5	Included in the design basis
Nearby industry – others	1	Effects considered in detailed design
Onsite activities	1	Effects considered in detailed design
Water supply quality	1	Effects considered in detailed design
Ventilation air quality	1	Effects considered in detailed design

Event	Screening criteria	Remarks
Military activities	3	Small likelihood of any effect at LHSTC site
Missiles from high energy equipment	5	Included in the analysis of onsite activities
Road and rail accidents	1	Effects bounded by aircraft crash
Screening Criteria: 1 The event has been included in the design basis 2 The event is of equal or lesser damage potential than the events for which the plant has been designed. 3 The event has a significantly lower frequency of occurrence than other events with similar consequences. 4 The event cannot occur close enough to the plant to affect it. 5 The event is included in the definition of another event.		

End of Tables

16.18 HUMAN FACTORS

16.18.1 Introduction

The interaction between the operators and the Reactor Facility has been taken into account in the design. The effect of operator actions on the Reactor Facility systems has been considered. Where appropriate, the need for the operator's intervention has been eliminated, such as in safety actions following the occurrence of an initiating event.

Analysis of the impact of the human factor on the facility will be kept under review as operating experience is gained.

16.18.1.1 Design Bases

The Reactor design and operational arrangements take into account the interactions between the reactor operations, maintenance, and utilisation staff with the facility and the impact of this interaction on the safety of the facility.

Throughout the plant the human-machine interface (HMI) is taken into account. The following specific design bases have been adopted:

a) The overall design of the plant is robust and error tolerant, with ample safety margins to accommodate deviation from normal operating conditions.

b) The staff are trained and provided with appropriate knowledge of the plant and its status.

c) Manuals, procedures and instructions ensure that all foreseeable situations the operator may face during the facility's lifetime are considered, and clear step by step instructions are provided to cope with them. Possible deviations in the execution of the instructions in a procedure are analysed and response actions are provided in all cases.

d) General procedures to deal with abnormal situations not covered by specific procedures are provided.

e) The operator's training program involves the operators facing abnormal situations and responding to them.

f) The facility simulator provides a training tool for implementing response actions to anticipated occurrences and evaluating their impact on the behaviour of the reactor in a real time sequence and using the same HMI.

g) Operating procedures give instructions for a facility walk through prior to each reactor start up to verify correct configuration of systems.

h) Emphasis has been placed on the HMI at the Main Control Room, Emergency Control Centre and relevant control switchboards.

i) The plant has been provided with automatic safety systems, which have been designed in such a way that the operator cannot interfere with their function.

j) Following an initiating event no actions by the operator are required during the first 30 minutes.

k) Maintenance and operation of the equipment follow procedures designed to minimise the Error Forcing Context (EFC).

l) Appropriate staffing, commensurate with the needs for operation of the facility will be present.

m) During abnormal conditions staff would be available on call from the LHSTC.

n) The HMI design promotes efficient and reliable operation through application of automated operation capabilities.

o) Safety systems monitoring displays and control capability are provided in compliance with pertinent regulations regarding electrical separation and independence.

p) The HMI design is reliable and provides functional redundancy such that sufficient displays and control are available in the main control room and remote locations to conduct a reactor shutdown even during design basis equipment failures.

The primary goal of the HMI design is to facilitate safe, efficient and reliable operator performance during all phases of normal plant operation abnormal events, and accident conditions. To achieve this goal, information, displays, controls, and other interface devices in the control room and other plant areas are designed and implemented in a manner consistent with good human factor engineering practices.

The ergonomic design of all HMIs minimises the possibility of erroneous reading or inadvertent adverse action by the operator. In particular, the display of information in the Main Control Room is designed to present the information in a clear and unambiguous manner. (Chapter 8 presents a detailed description of the design of the RCMS, RPS and HMI.)

16.18.1.2 Reactor Pool Top Operations

Due to the nature of a pool reactor and its utilisation the operator is responsible for the handling of equipment on a routine basis in the reactor pool, in proximity of the reactor core. This handling encompasses loading and unloading of targets for radioisotope production, silicon ingots for NTD production and fuel shuffling, as well as maintenance actions.

The Reactor Pool internal structures, tools and auxiliary equipment to be used for the handling have been designed taking into account ergonomic design practices. The layout of the different components within the Reactor Pool is such that the core and the two shutdown systems are protected from mishandling and mechanical damage.

The training of the operators together with the use of procedures minimise the likelihood of an initiating event caused by pool top operation. Events associated with specific pool top operations are discussed in the corresponding sections.

16.18.1.3 Maintenance Operations

Errors during maintenance operations have the potential to affect the full availability of systems.

The RRR has been designed with consideration of the maintenance activities of the systems and components that are critical for safety and plant performance.

The layout of plant systems and components has been designed to provide easy access for maintenance operations. Care has been exercised in areas with limited space (such as the lower part of storage tanks) to ensure accessibility by an operator of average size. Plant components are tagged to allow easy identification, preventing operation of the wrong component or wrong configuration.

As explained in Chapter 13 an appropriate organisation is established in the facility to carry all the activities related to maintenance in accordance to the facility QA Plan. This includes adequate maintenance planning, operator training and a structure of supervision, approval and review of maintenance and operation tasks that minimises the potential for errors.

The components undergoing maintenance are isolated, tagged and cleared by operations staff. In the same way, operations staff perform the restoration to service once the component is declared operable by the maintenance staff. If the component needs to be started to verify its performance prior to finishing the maintenance tasks, this action is undertaken in consultation with the operations staff.

The component configuration after the maintenance activity should be identical to the configuration at the beginning of the maintenance tasks.

16.18.1.4 Human actions and accident management

As indicated previously the RPS provide independent and highly reliable systems that monitor the safety parameters and initiate appropriate protective actions if any of the parameter values reaches the safety set point, bringing the reactor to a safe condition.

As discussed in Sections 16.8 to 16.17, the safety systems are successful in providing protective actions for the full range of design basis initiating events to terminate the event safely.

All protective actions are automatic. No operator action is required to guarantee the three main safety functions (shutdown, core heat removal and Containment integrity) during the first 30 minutes following the occurrence of an initiating event.

In the event of the safety systems being called upon to function, manual override of the RPS is not allowed.

The automatic protective actions can also be initiated manually. However once an automatic action is initiated, manual action cannot prevent or interrupt its execution.

Human actions as part of accident management include verification of safe shutdown status, adequate core cooling and containment integrity. Instructions for accident management are detailed in procedures.

A manual operator action is considered only if:

a) Adequate time is available

b) Information is suitably processed and presented

c) Diagnosis is simple and action is clearly defined

d) The demands imposed on the operator are not excessive

Recovery actions for safety and plant systems following an anticipated operational occurrence are carried out in close communication between the Main Control Room operators, personnel in the area and external support.

Since the reactor can remain in safe shutdown following an accident with the pool water acting as the ultimate heat sink, the main accident management measure is the addition of water to the pools in case the unlikely event the LTPC mode of the RSPCS is not available. Even in the case of a LOCA, there are more than 60 hours in which to implement these measures before the pool water level reaches below the lower flap valves. There are several different ways in which water can be added to the Reactor Pool following a LOCA. The routes for addition of water are:

a) Through the Hot Water Layer System (return line),

b) Through the Hot Water Layer System, using the suction line with a reverse flow. The valves being configured to pump the total flow only to the RPO.

c) Starting the pump dedicated for the skimming mode from the main control room

d) Through the Emergency Make-up Water System

e) Getting a hose in the drainage line valve and bypassing the trigger valves

f) Demineralised water supply is available through valves at the entrance of each pneumatic cell in the reactor hall, where a hose could be connected and discharged into the RPO.

g) External water reposition through the Demineralised Water Supply system.

h) Water from the LOCA pool can be pumped back into the RPO/EMWS through the Waste Management System.

i) Fire hoses are available at the reactor hall and in the basement, and thus water can be directly poured into the RPO, or indirectly into any of the plant systems system able to direct the water to the RPO.

16.18.1.5 Human Actions as Initiating Events

Even with all the preventive measures in place, human error can still initiate a failure.

The impact of the actions by the operator is assessed in the following sections as cause for an initiating event, contribution to the accident scenario and impact of mitigation actions on the safe shutdown status of the facility. Each of these aspects is assessed in the context of the DBIEs analysed in the preceding sections.

The accidents occurred in research reactors as reported in IAEA's IRSRR data base are discussed in Section 16.21. Where the initiating event was caused by an error of commission or omission of an operator, the features of the RRR design that prevent or minimise the likelihood of the error are discussed.

Further discussion of human error and its quantification is presented in the PSA.

16.18.2 Loss of Electric Power

The operator could cause a loss of electric power when performing maintenance of the electrical switchboards or substation. Maintenance tasks on the main switchboard will be performed during shutdown. Loss of Normal Power during refuelling would not change the safe shutdown status of the facility. The Standby Power Supply would feed the safety systems during the loss of Normal Power.

Erroneous operation of the main switch may cause loss of Normal Power. This event is identical to the loss of Normal Power due to external causes and the behaviour of the plant would be the same as analysed in Section 16.7.

Actions of the operator during recovery of the facility after loss of Normal Power are dictated by operating procedures. Start up of the diesel generators would be automatic, thus power supply would be available in both trains. Simultaneous failure of both diesels to start up is deemed very unlikely. Nevertheless, the analysis in Section 16.7 shows that the facility can cope with a failure to start up both diesels for up to 30 minutes.

The actions of the operator do not modify the scenario for this transient as presented in Section 16.7

16.18.3 Reactivity Insertion Transients

Human factors as a contributory cause of reactivity insertion transients is discussed in this section.

In all cases, once either of the RPS has requested reactor trip, the operator cannot interfere or prevent reactor shutdown. The transient would evolve as shown in the numerical analysis and the end result would be a safe shutdown situation. Actions to reset the reactor and restart operation would follow procedures.

16.18.3.1 Accidental Drop of a Fuel Assembly

This is an event where operator actions constitute the main cause. This event is considered within the design basis and analysed in Section 16.8.

From the point of view of reactivity insertion, this event does not lead to a transient. As mentioned before, the handling of FAs is done only during refuelling or with the chimney protective grid in place (during transfer of spent fuel from the Reactor Pool storage rack to the Service Pool). Refuelling is performed with the reactor in the Shutdown state with a large shutdown reactivity margin of safety.

The reactor operates with all its core grid positions filled with FAs. In the hypothetical event that a FA is handled with the reactor critical and with the protective grid removed from its place, the reactivity insertion caused by the fall of a FA on top of the core would be very small. This is bounded by other reactivity insertions analysed in Section 16.8.

Inadvertent ejection and reinsertion of a FA in the core grid during operation cannot be caused by any inadvertent action on the part of the operator. Leaving a fuel clamp inadvertently unlocked after refuelling operations is a violation of operation procedures. Visual inspection gives a clear indication whether a fuel clamp is unlocked because it interrupts uniformity of the fuel clamp lay out. Supervision ensures that more than one individual verifies that all the fuel clamps are locked before reactor start up. In case the operators ignore the indication of an unlocked fuel clamp, the FA would be dragged upwards by the forced flow when the pumps are started before power raise. No reactivity insertion would arise from this operator error.

The effect of FA mishandling on the integrity of the FA is discussed in Section 16.18.8.

16.18.3.2 Inadvertent Fast Insertion of Irradiation Fissile Material

Uranium – Molybdenum rigs are handled from the operation bridge. The insertion and extraction of these rigs is performed with a machine that lifts or lowers the rigs with constant velocity. Mishandling by the operator that could result in a U-Mo rig fast insertion in its irradiation position could be caused by not using the handling equipment and performing the operation by hand. As shown in Section 16.8.2.2, the RPS can cope with a fast insertion of a U-Mo rig.

16.18.3.3 Start up accident and Inadvertent Control Plate Withdrawal during Operation

As presented in Sections 16.8.3.1 and 16.8.3.2, these scenarios refer to the continuous withdrawal of a control plate at nominal speed during the start up sequence or during normal operation.

Several design features prevent the occurrence of this event due to an action by the operator. An RCMS interlock controls the withdrawal sequence and inhibits CP movement in case of high neutron flux rate. In addition, the RCMS supervises manual

CP movement and does not allow withdrawal beyond a pre-set limit. In case of failure of the RCMS, the operator could withdraw a CP at nominal speed and the transient will evolve as indicated by the numerical analysis.

16.18.3.4 Control Rod Drive or System Failure

As discussed previously, the robust design of the CRD, CP and associated structures implies that the failure of the system is highly unlikely. No action by the operator during normal operation can change this conclusion. The Failure Modes and Effects Analysis of the CRDs and the FSS have shown that no operation error during maintenance could prevent the FSS from fulfilling its safety function.

The CRD design minimises the need for maintenance. Control Rod Drive maintenance is performed by trained operators following appropriate procedures. The procedures include surveillance requirements to verify that the system has been assembled correctly. For example, the operator must verify that the disks have been fixed after the system has been aligned, verification of the correct position of the pin must be carried out, etc.

Removal of a CP is an operation that involves more than one operator. One operator has to disengage the CRD in the CRD room and detach the rod to allow the removal of the CP from the Reactor Pool top with a customised tool. Replacement of CP will be done with the reactor in the Shutdown state and the FAs removed from the core.

16.18.3.5 Inadvertent Control Rod Bank Extraction

As mentioned before, the RCMS has no bank extraction mode. No routine modifications will be made to the RCMS code after commissioning, therefore it is not credible that during routine maintenance a modification could be made to the RCMS to enable control rod bank extraction. In addition, the CRMPI would prevent bank extraction.

16.18.3.6 Inadvertent Extraction of a fixed absorbing Irradiation Material

Handling of fixed irradiation rigs is neither necessary nor authorised during reactor operation. All handling of fixed rigs is performed with the reactor shutdown. Operating procedures are designed to clearly identify the fixed irradiation targets to avoid their inadvertent movement during reactor operation. In addition, locks at the top of the irradiation positions in the Reflector Vessel further inhibit extraction of these rigs. Tools to unlock and remove fixed irradiation rigs are kept under lock and the key under the shift supervisor's control.

Nevertheless, the occurrence of this event has been analysed in section 16.8 with highly conservative values for reactivity worth. The analysis shows that the reactor can cope with this transient.

16.18.3.7 Irradiation Can with Excess Absorbing Material

As stated in Section 16.8, this scenario contemplates a QA violation in the preparation of the irradiation sample to be included in the can.

Operating procedures are designed in accordance with the QA plan in place for the preparation of irradiation targets for the pneumatic system, minimising the likelihood of operator errors. Operator error is the sole possible cause of this initiating event. As shown in Section 16.8, the reactor facility can cope with a target with many times more absorbing material than allowed for in the operation of the Pneumatic Conveyor System.

16.18.3.8 Spurious Actuation of the EMWS

The EMWS float valves and piping are encased in a protective structure to prevent spurious actuation due to the impact of a target or other object being handled inside the pool. The operator can actuate the float valve to test the system but cannot inadvertently actuate the system while moving objects inside the pool. Thus, the design minimises the likelihood of a spurious actuation by the operator. Moreover, the EMWS cannot inject water into the PCS when the pumps are running due to the higher pressure inside the PCS piping.

Nevertheless, should the operator actuate the system with the PCS in natural circulation mode, the reactivity inserted by the injection of cold water is bounded by the reactivity inserted by the withdrawal of a CP during start up.

16.18.3.9 Start up of the PCS Pumps in the Physics Test State

An interlock prevents the start up of the PCS pump when the reactor is in the Physics Test state. The operator cannot by pass the interlock.

Maintenance operations on a PCS pump are not performed during reactor operation. Verification of the normal functioning of the pumps after maintenance is performed with the reactor in the Power state before power is raised.

16.18.3.10 Variation of the Temperature of the Heat Sink

Operator actions on the SCS could lead to variations in the temperature of the SCS water. This variation would be compensated by the control loop that maintains the core inlet temperature constant. Changes in SCS temperature would be slow and compensated by the RCMS.

16.18.3.11 Inadvertent Refill of the Reflector Vessel

An RPS interlock prevents the start up of the Heavy Water Make Up pumps after actuation of the SSS. The operator cannot override this interlock. The interlock is redundant, therefore, in case of maintenance error that could result in the failure of one of the redundancies, the other redundancy will fulfil the safety function.

16.18.4 Loss of Flow Events

16.18.4.1 Pump Shaft Seizure and Pump Motor Failure

The PCS and RSPCS pumps are instrumented and give early alarm in case of malfunction. Maintenance tasks are performed by trained personnel following procedures with special attention to time frame and supervision and inspection after the maintenance operation has been completed.

The pumps are started up before the reactor is taken critical. Unusual functioning of the pump would be detected at this time.

Spurious stopping of one or both pumps is as analysed in Section 16.9.

16.18.4.2 PCS Blockage or Valve Failure

Blockages in the PCS or valves left in the wrong position (i.e. closed) after maintenance would be identified by a low PCS flow signal in the RCMS after pump start up and prior to power raise, as part of reactor start up procedures. Operating procedures require the operator to verify that the PCS flow rate is within normal values before power raise.

The PCS has no remotely operated valves that could be inadvertently closed. Manual valves require deliberate operation action to be closed. QA and careful inspection accounting for tools, cloths and packaging after commissioning and maintenance minimise the likelihood of an obstruction due to foreign objects inside the piping.

16.18.4.3 Core By Pass

Core by pass could be caused by a spurious opening of a flap valve by the operator. The design of the flap valves is such that opening one of them while handling objects inside the pool is virtually impossible. Nevertheless, to further protect the flap valves and reduce even more the likelihood of a core flow by pass, a protective mesh is in place around the flap valves.

16.18.4.4 Core Blockage

A protective grid at the top of the chimney and the upwards core flow are two measures preventing the access of foreign objects to the core during normal operation. Even during low power operation, the natural convection plume will push up lightweight objects. During refuelling, i.e., when the protective grid is removed, human error can contribute to core blockage through two mechanisms: a foreign object dropped into the pool and lodged inside, or at the entrance to, the core and damage to the fuel plates during FA handling and shuffling manoeuvres.

To minimise the likelihood of a foreign object being introduced inside the Reactor Pool during refuelling (i.e., when the protective grid is not in place and empty spaces in the core grid might provide a pathway for foreign objects to the lower plenum), administrative procedures will forbid clear plastic materials in the reactor hall. Clothing worn at the Reactor Pool top has zippered pockets to avoid the fall of objects such as ID cards, coins and dosimeters.

As indicated in Section 16.9, the design of the FA and handling tool minimises the likelihood of damage to the fuel plates during fuel handling operations. The FA side plates are more resistant than the internal fuel plates, providing additional protection against impact on a structure inside the Reactor Pool. Administrative procedures are in place to inspect FAs that have been hit and potentially damaged. Failure of an FA would be detected by the FFEM. The radiological impact of this scenario is analysed in Section 16.19.

16.18.4.5 Improper Power Distribution Due to Unbalanced Rod Positions, Radioisotope Targets or Erroneous Fuel loading

The most significant contribution of human actions to this scenario would be a mistake during fuel loading. Administrative control, a QA program in place for refuelling operations and operator training and supervision reduce the likelihood of an improper loading in the core. Nevertheless, this event has been discussed in Section 5.7 as an anticipated operational occurrence where it was shown that the RCMS can cope with the excess reactivity resulting from the maximum reactivity insertion due to human error with no effect on the safety of the Reactor Facility. .

Due to the RCMS limitation on CP manual movement, unbalanced rod position is considered unlikely. The operator is not allowed to move the CPs except within the constraints set by the RCMS.

16.18.5 Loss of Heat Sink

Maintenance errors in the SCS could contribute to loss of flow or loss of SCS water and contribute to the loss of heat sink initiating event. Foreign objects inside the SCS, incorrect operation of valves, mistakes in the maintenance of the SCS piping and equipment could lead to failure of the SCS.

Maintenance tasks are performed by trained personnel following procedures. Start up procedures prior to power raise would indicate any abnormal situation in the SCS, such as low flow.

Should an operator's error of omission or commission lead to SCS failure and loss of heat sink, the Reactor Facility would behave as shown in Section 16.10. Mitigation and recovery actions following a LOHS event would not affect the safe shutdown status of the reactor.

16.18.6 Loss Of Coolant Accidents

Maintenance errors in the PCS may contribute to the occurrence of a LOCA. Mistakes in the maintenance of the PCS piping and equipment or erroneous operation of a valve could lead to loss of coolant. Loss of coolant from a valve is bounded by the pipe failure analysed in Section 16.11.

Maintenance tasks are performed by trained personnel following procedures. The level of supervision is commensurate with the difficulties of the task at hand.

Start up procedures require the start up of the PCS pumps prior to power raise. Any open valve or loose flange that could originate a LOCA would be identified at this stage.

Beam tubes are protected by structures against the impact of heavy objects, such as silicon ingots.

Should an operator error generate a LOCA during operation, the Reactor Facility would behave as shown in Section 16.11.

16.18.7 Loss of Heavy Water

Operator actions could contribute to the loss of heavy water event by damage to the Reflector Vessel during pool top operations or by mistakes in the maintenance or operation of the Reflector Cooling and Purification System.

The Reflector Vessel can withstand the impact of objects normally handled inside the pool. Protective arrangements are also in place to preclude damage to beam tubes and irradiation facilities. In the unlikely event of damage to the Reflector Vessel, the higher pool water pressure would cause the pool light water to flow into the Reflector Vessel, minimising the release of tritium into the Reactor Hall.

Maintenance of the Reflector Cooling and Purification System is carried out by trained personnel following procedures. The heavy water system (piping, pumps, tanks, heat exchangers) is enclosed in the Heavy Water Room. The impact of any heavy water leak would be confined. The Heavy Water Room has tritium monitoring to alert operators of the presence of tritium in the room's atmosphere and breathing air connections for recovery actions following a heavy water spill.

16.18.8 Failure of a Fuel Assembly Caused by Erroneous Handling

This section deals with the mechanical damage that could arise from the mishandling of FAs.

During operation, the FA and core structures are protected by a grid placed at the top of the Reactor Chimney. This grid has been designed to withstand the impact of a silicon ingot. As mentioned in Section 16.13, FA handling staff are trained and use custom tools. Operating procedures for the handling of FAs require supervision commensurate with the level of difficulty of the task being undertaken.

Although the likelihood is small, the fall of an FA onto the core due to the mishandling of the FA handling tool has the potential to result in mechanical damage to one or more FAs in the core but no significant radiological release. After such an event, operating procedures would require that all the affected FAs be visually inspected (remotely, by use of a camera) to verify their mechanical integrity and to ensure that the cooling channels have not been deformed. It is exceedingly unlikely that the impact would cause an undetectable puncture that could result in fission product release after the reactor is started up. The FA is more likely to sustain extensive damage that can be easily observed and thus require replacement or no damage at all. Should any failure of the fuel cladding occur, the released fission products would be detected by the FFEM.

As indicated in Section 16.9, the design of the FA and handling tools minimise the likelihood of damage to the fuel plates during fuel handling operations. The FA side plates are more resistant than the internal fuel plates, providing additional protection against impact on a structure inside the Reactor Pool. Administrative procedures are in place to inspect FAs that have been hit or potentially damaged. The radiological impact of this scenario is analysed in Section 16.19.

Fresh FAs are stored in a dedicated room in racks designed to preclude criticality. Operator error associated with the storage of fresh fuel is limited to the mishandling and piling up of fresh fuel on the floor, disregarding the storage rack. Piling up FAs on the floor without their boxes would not lead to criticality.

Spent fuel is stored inside containers placed in storage racks in the Reactor and Service Pools. Fuel handling personnel are trained and fuel handling procedures prohibit storage of FAs outside the storage racks. The spent FA containers are designed to prevent criticality even in the case of crushing of the FA by a heavy object.

No operator action has been identified that could lead to inadvertent criticality in fuel storage.

During refuelling operations, an operator could erroneously lift a FA above the level of the Transfer Canal in violation of operational procedures or could remove from the storage rack an FA that has remained there for less than the time prescribed. In either case, if the shielding provided by the layer of water between the FA and the operator is not sufficient, the pool top activity detectors would give alarm and indicate to the operator and supervisor that the FA must be lowered.

There is no expected action that could lead the operator to inadvertently lift an FA from the water. Nevertheless, a FA can be cooled in air after period of decay. Therefore, should an operator inadvertently lift a FA that has been decaying in the Service Pool storage rack and bring it out of the water, the FA would not melt. The dose to the operator would be significant.

16.18.9 Internal Events

16.18.9.1 Internal Fire or Explosion

Internal fires and explosions are discussed in Section 16.14. As described in that section, the design of the Reactor Facility includes features that prevent the ignition of fires and, in the unlikely event they occur, slow down the progress and prevents propagation.

Storage of flammable liquids and gases are under strict administrative control. Metal cutting, machining and welding may cause ignition. These activities are confined to workshops, where building and finishing materials are non-flammable.

No action by personnel is required to actuate the automatic fire suppression system

ANSTO staff receives fire fighting training. A fire management program, consistent with LHSTC fire management procedures, is in place.

16.18.9.2 Internal Flooding

Faults in the operation of valves in the cooling system as well as latent faults in welds can lead to water spill and flooding. In all cases, the small diameter of pipes and the likely small size of the failure in a weld would lead to a small LOCA (see Section 16.11)

QA procedures are in place for welding of unions in piping and components.

The start up sequence for the reactor includes a walk through and confirmation of the status of all drain valves to minimise the potential for leakage from incorrectly set valves.

Spurious actuation of the fire suppression system can also cause flooding as well.

In all instances, flooding caused by any of these actions is bounded by the flooding caused by a PCS or RSPCS LOCA.

16.18.9.3 Loss of Compressed Air

Compressed air is supplied to the Reactor Facility from the LHSTC compressed air system. As with all containment penetrations, the compressed air lines have isolation valves (Group 1, See Chapter 7). These valves close automatically when containment isolation is requested, but can also be closed manually when the operator initiates Containment isolation. In these cases, the compressed air supply would be interrupted. However, continued supply to safety systems is ensured by dedicated compressed air storage tanks. In addition, a compressor located within the Containment would maintain the pressure in the compressed air lines.

No valves are located between a storage tank and the corresponding safety system, thus the operator cannot interrupt the air supply to a safety system.

Maintenance tasks on the Compressed Air System are performed by trained operators following appropriate procedures.

Low pressure in the compressed air line would raise an alarm and alert personnel that some abnormal event has occurred.

16.18.9.4 Improper Access to Restricted Areas

Access to restricted areas (due to potential for contamination or irradiation) is strictly controlled by administrative procedures. Zoning inside the building is clearly marked, with restricted areas clearly identified.

Operators must request authorisation from the Main Control Room to access a restricted area. The Heavy Water Room door raises an alarm in the Main Control Room when opened during operation.

16.18.9.4.1 Security Breach

Security arrangements have been reviewed and approved by ASNO, ASIO and other Commonwealth agencies. Access control and multiple levels of defence in depth are in place.

16.18.10 Events Associated to Reactor Utilisation

The Reactor Facility will be intensively used to produce radioisotopes and as a neutron source for different experiments. This section explores the operator actions related to reactor utilisation that could lead to the occurrence of an initiating event.

16.18.10.1 Bulk Production Irradiation Facilities

Due to their effect on core reactivity, targets with reactivity worth higher than 200pcm are not authorised to be loaded and unloaded from the Reflector Vessel when the reactor is in operation. Measures have been adopted to avoid mistaking large reactivity worth irradiation targets for targets with lower worth. Rigs that must remain in place until reactor shutdown are locked in place and a different tool used to unlock them. The tool is kept under lock and the shift supervisor keeps the key. Nevertheless, Section 16.8 shows that the safety systems can cope with the removal of a fixed irradiation rig during operation.

Uranium-Molybdenum rigs are moved while the reactor is in operation. The rigs are removed from the irradiation positions and they are placed in storage racks in the Service Pool to decay before they are transported to the Hot Cell for transport to the radioisotopes production facility. An interlock prevents extraction of a rig that has not decayed long enough to be cooled in air. The operators cannot override this interlock.

Loss of Flow in the RSPCS could be caused by a spurious stop of the RSPCS pump. In that case, the facility would behave as shown by the analysis in Section 16.15.

A foreign object dropped into the Reactor Pool could block a rig cooling channel. The protective mesh on top of the irradiation positions stops fallen objects while the rigs are in place. The annular shaped rigs have a central rod that protrudes over the top level of the Reflector Vessel and acts as an additional barrier for objects that could obstruct the inner circle in the annular geometry. Clear soft plastic objects (such as plastic bags and disposable gloves) are forbidden at the Reactor Pool top. All clothing worn by the staff has zippered pockets to keep ID cards, coins, dosimeters inside. Operating procedures require that the operators verify the irradiation position is not obstructed prior to loading a rig.

The flap valves are positioned inside the Reactor Pool in such a way to prevent spurious opening during handling of objects inside the pool. The opening of a flap valve would trip the reactor.

The impact of operators on the occurrence of a LOCA is similar to the impact on the PCS LOCA, as are design provisions to prevent or detect it. The consequences of a LOCA are analysed in Section 16.11.

Rigs exchange (i.e., placing a U-Mo rig in the position of an Iridium rigs) is prevented by different rig geometry. Thus, this event related to human error has been eliminated by inherent design provisions.

All bulk irradiation targets are handled under water until they have decayed enough to be removed and transported. The racks for target handling are placed low enough inside the pools to provide adequate shielding to the operators. Should the operator lift a target above the handling level, a radiation alarm would alert the operator at the pool top and the staff in the MCR that the target needs to be lowered to a safe level. The rigs operation tools are designed to minimise the likelihood of this event.

16.18.10.2 Pneumatic Transfer System

Errors in the pneumatic system target load, irradiation position and irradiation time can lead to higher level of activity for an irradiated target. Compliance with the approved target and canning specification procedures as well as appropriate training of operators minimises the potential for erroneous loading of targets. Procedures are also in place to minimise the potential for sending the target to the wrong irradiation position. The SPNDs provide an accurate indication of the flux at the irradiation position and allow the operator to calculate the irradiation time. Nevertheless, neither core damage nor an exceedance of dose limits would arise from this event.

Erroneous loading of a can could also lead to excessive can heating and potential can failure. Personnel would be protected in case of can failure because all can handling is done inside a hot cell.

Operator actions that could cause interruption of cooling to the cans would arise from errors in operation (spurious stopping of a blower, spurious closing of a valve in the main stream, faulty operation of the SCS, maintenance or operation errors leading to failure of the pneumatic system switchboard). Procedures and training will minimise the likelihood of an erroneous operation of this system. Maintenance actions are carried out by trained personnel following procedures. The level of supervision is commensurate with the difficulty of the task at hand. The pneumatic system has three blowers, 60% each, one on stand-by. The stand-by blower starts automatically when one of the two operating blowers stops. Any flow reduction would send a signal to the RCMS and initiate power reduction.

16.18.10.3 Hot Cells

Spurious stopping of the hot cells' ventilation system due to operator error or maintenance errors would lead to a loss of negative pressure. However, minimal diffusion of activity through the cell walls is expected.

Maintenance errors could cause the failure of the ICE. However, any failure due to human factor would not differ from the failure due to malfunction of the system, as described in Section 16.15.

16.18.10.4 Large Volume Irradiation Facilities

The most likely effect of an error during the operation of large volume irradiation facilities is the damage to structures, systems or components inside the Reactor Pool due to mishandling of silicon ingots. The systems most exposed to impact (such as the core and beam tubes) are protected by structures designed to withstand the fall of the heaviest silicon ingot. Design of the tools and procedures, as well as appropriate training of staff, minimises the likelihood of this event.

16.18.10.5 Cold Neutron Source

The Cold Neutron Source is operated automatically with no intervention of the operator in actions to protect the CNS or the reactor. Maintenance and operation of equipment of the CNS will follow the same requirements as the rest of the Reactor Facility. Training and procedures minimise the likelihood of errors that could lead to failures of the CNS and associated systems.

Should a failure arise from an action by an operator, the CNSPS would respond to the failure as in any other case and will trigger the protective actions needed to prevent damage to the CNS. Damage to the Reactor Facility is prevented, even in the case of detonation, by the vacuum chamber in the Reflector Vessel. See Chapter 11 and Section 16.15 for details.

16.18.10.6 Neutron Beam Facilities

Operator actions on the Neutron Beam Facilities are limited. The operator would expose him or herself by accessing the Neutron Guide Bunker without the required authorisation. Access to the bunker is not allowed during operation. Local instrumentation monitors radiation levels. Interlocks and procedures are in place to ensure the radiological protection of operating personnel during maintenance and repair tasks.

Inadvertent opening of a primary shutter is prevented by spring actuated locks. The pneumatic movement control system has open/closed position indication and interlocks and alarms to prevent erroneous operation. Local instrumentation gives alarm in case of inadvertent opening of a shutter.

If a human action (error of operation or maintenance) results in the interruption of electric power to the shutters, the anti-rotation locks will keep the shutters in their original position. If they remain open, an alarm would sound signalling the need for manual closure of the shutters.

16.18.11 Spurious Actuation of the Safety Systems

The safety systems can all be tripped manually by the operator in the MCR. However, human action cannot interfere with the actuation of the safety systems once it is initiated. Spurious actuation of the safety systems has no adverse impact on the safety of the plant.

16.18.12 Defence in Depth Barriers

Level	Main Characteristics	Safety Feature
1	Conservative design and inherent safety features	Robust design that can accommodate deviations from operational set points.
		RCMS interlocks prevent reactor start up
		No operator actions needed during the first 30 minutes of a transient to ensure three main safety functions.
		Supervision, approval and review of operation and maintenance activities.
		Ergonomic design of all human-machine interfaces.
		Plant layout facilitates access for maintenance tasks.
		Plant components tagging ensures operation of right component and minimises wrong configuration
		QA system for production of irradiation targets.
		Operating procedures for dealing with transients.
		Operator training and retraining
		Safety Culture in facility staff.

Level	Main Characteristics	Safety Feature
		Protective structures to avoid damage to components inside the Reactor Pool during handling of objects from the pool top.
2	Operation control and response to abnormal operation	Fully automatic RPSs.
		Operator cannot override safety systems’ actuation once is initiated.
3	Control of accidents within the design basis	FSS and SSS trigger following abnormal parameter indication originated by operator action.
		Alarm on dose rate above allowed limits at Reactor Pool top.
		Passive long term decay heat removal system by natural circulation and evaporation of pool water needs no configuration or intervention by the operator.

End of Section

16.19 BEYOND DESIGN BASIS ACCIDENTS

As shown in Sections 7 to 18, the design of the reactor is very robust and can cope with all the design basis accidents with no damage to the core. On the basis of the analyses performed, a number of beyond design basis accident sequences have been identified that have the potential to lead to damage to the core or the irradiation rigs. The purpose of this section is to investigate these sequences further with a view to defining an accident to be used for emergency planning purposes.

Seven BDBAs are identified for investigation:

1. PCS pump shaft seizure with failure of the FSS,
2. RSPCS pump shaft seizure with failure to detect the loss of flow,
3. Partial blockage of cooling channels in a Fuel Assembly,
4. Erroneous early removal of a U-Mo rig into the Hot Cell,
5. Control Bank withdrawal at nominal velocity during start up, and
6. Control Plate withdrawal during start up to low power operation with failure of the FSS and success of the SSS.
7. Total plant blackout for 10 days

They are included here as part of the demonstration of the robust design of the reactor.

In the case of partial blockage of cooling channels, it is assumed that some of the fuel plates melt. This assumption is highly conservative. Further, no credit is given for the possibility of flux perturbations causing a trip following the onset of nucleate boiling, which would occur long before melting.

16.19.1 Primary Cooling System Pump Shaft Seizure

Shaft seizure with failure of the FSS and success of the SSS has been analysed using RELAP 5. The sequence is more severe than that associated with actuation of the FSS.

This transient starts with the seizure of the shaft of a PCS pump. Failure of the FSS is assumed. This failure could be due to:

a) Failure to detect the flow reduction
b) Failure of the FSS itself

Failure to detect the flow reduction is considered unlikely, since the PCS flow and core pressure drop are both monitored by the RCMS (see Section 6.2). There are also signals on core coolant inlet and outlet temperature. The SSS has independent core pressure drop and high core outlet temperature signals that will detect the reduction of flow rate. It is assumed in the analysis that the actuation of the SSS is on low core pressure drop. The SRPS trip of the SSS sends an actuation signal to the FFAL (See Chapter 5). This insertion of the Control Plates is ignored. This is a very conservative assumption for a BDBA.

After the PCS pump shaft seizure, the forced circulation through the core is not interrupted. It is reduced from approximately 30% since the second PCS pump continues operating. Only the short-term response is analysed, since this is the time window of interest. Once the reactor has reached a safe shutdown state with one PCS pump operating, it can remain in this state until the operators shut off the second pump and natural circulation is established.

The SRPS trips the SSS when the pressure drop in the core reaches the analytical value for the set point. During the first seconds of the transient, the flow is governed by the abrupt seizure of the shaft of one of the pumps. Thereafter, the flow rate changes in accordance with new force balance between the torque of the remaining pump and the circuit friction losses.

As a result of the abrupt reduction in core flow, the postulated failure of the FSS and the delay in reactor shutdown by the SSS, channel temperatures start rising. The maximum cladding temperature reached is within safe limits. After the reactor is shut down by the SSS, temperatures fall to values that depend on the balance between the decay heat generated and the fluid heat removal capacity

The second undamaged pump is stopped by the operator by mistake a few seconds after the seizure and the flap valves open due to loss of forced circulation.

No core damage arises from this Beyond Design Basis Accident.

16.19.2 Reactor and Service Pool Cooling System Pump Shaft Seizure

A shaft seizure is postulated in the single operating RSPCS pump. It assumed that the flow detector fails to detect the loss of flow and the FRPS does not therefore trip the FSS on low RSPCS flow. There is no SSS trip signal associated to the loss of flow in the RSPCS. This results in the total loss of cooling flow to the irradiation rigs. The reactor continues to operate and the heat generated by the U-Mo rigs cannot be removed by natural circulation. The coolant in the rig channels boils and the CHFR goes below the safety limit for transients ($CHFR=q''/q''_{CHF}<1.5$). The U-Mo targets are then assumed to heat up to melting point, releasing their inventory of fission products into the pool water.

The main contributors to dose outside the Reactor Building are the noble gases that are formed as fission products in the Uranium-Molybdenum targets. The fusion of the complete inventory of U-Mo targets is postulated. There are three targets in each irradiation position, and twelve irradiation positions. Additional assumptions made are;

a) Initial release is via the stack.

b) Containment isolation is not initiated until 2 minutes after the detection of activity in the stack. This is a very conservative assumption that bounds the integration time of the stack activity monitors and the delay of the electronics.

c) Following containment isolation, fission product release occurs at ground level. During the first day, 3% of the volume of the containment is released. Of this release, one third (i.e., 1% of the containment volume) is released during the initial pressure transient following containment isolation. The remaining 2% is released due to the variation in barometric pressure outside the containment. Thereafter, a 2% release per day is assumed based on the barometric pressure variation. This assumes that the worst historical barometric pressure variation recorded at the Reactor site is maintained during the 100 days following the accident.

d) Following the assumptions made in ‘Application to ARPANSA for a Facility Licence, Site Authorisation, for the Replacement Research Reactor Facility’, the analysed sequence has been divided in five stages.

    (i) Prompt Period: Includes the first 2 minutes of the release of fission products through the stack. The venting rate during this period is one reactor building volume per hour and the release occurs at 45 m having been filtered. The filters are assumed to not retain noble gases.

(ii) Period 1: Lasts from the end of the prompt stage (120 s) to 12 hours (42300s). Due to the change in release flow rate, the P1 Stage has been divided in three sub-periods: P1A, P1B and P1C.

(iii) Period 2: Starts 12 hours after the beginning of the sequence and lasts 12 hours. The only change is in the atmospheric conditions, as shown in Table 16.19/1.

(iv) Period 3: Lasts 12 hours and it represents a return to meteorological conditions used in Prompt and P1 stages (see Table 16.19/1).

(v) Period 4: Lasts 98.5 days. Introduces a change in meteorological conditions, as shown in Table 16.19/1.

e) The environmental release is assumed to begin at the start of the least dispersive weather conditions, as this maintains a concentrated airborne plume, maximising the estimate of individual dose. These conditions are typical of night-time inversion conditions with Pasquill category F stability class and a low wind speed of 1 ms^{-1}. It is assumed that these conditions last for 12 hour periods over two consecutive nights. During the alternate 12 hours daytime period, Pasquill stability class D with wind speeds of 3 ms^{-1} is assumed. This is also assumed to be the average condition for the final period of release up to 100 days. Furthermore, it is also assumed that the wind remains constant in the direction of the most populated sector for the prompt and period 1 and 3 releases, but changes direction to the adjacent sector during periods 2 and 4.

f) Starting in P1 the deposition/plate out effects and nuclide radioactive decay produce a variation in the inventory inside the Reactor Building.

The release of fission products to the environment as a result of the melting of the U-Mo targets underwater is given in Table 16.19/2. The results are shown in terms of the releases corresponding to the above time periods. A full inventory of 36 targets is assumed to melt.

The release of fission products occurs underwater, therefore partition factors that represent the transfer up to the Reactor Building atmosphere are applied. The absence of coolant flow is assumed to result in the formation of steam surrounding the overheated rig. Bubbles will break out from this blanket. These bubbles will entrain fission products released from the damaged rig. The bubbles are small, of the order of a few centimetres in diameter[1]. The pool water above the irradiation rigs will be significantly subcooled, due to the large mass of water inside the pool. Thus, the bubbles will condense over a few centimetres and will not transport fission products to the pool top.

The degree of fission product retention in pool water has been studied experimentally [2 3.] Table 16.19/3 presents a summary of the partition fractions adopted in the calculations. Conservatively, no delay has been considered between the underwater release and the

[1] D. Bärmann et al., "Flow Oscillations in Two-Phase Flow, Their Characteristics and Effects on Burnout", Symposium on Two-Phase Flow Dynamics, 4-9th September 1967, EUR 4288 e.
[2] Dadillon, J., "An experimental Study of the Behaviour of Fission Products Following an Accident in a Swimming Pool Reactor", Bulletin D'Informations Scientifiques et Techniques Nº 112, February 1967, Translation to English AEEC-Lib/Trans-611.
[3] De Montaignac "On Site Releases of Noble Gases and Iodine in the Event of Core Meltdown in a Swimming Pool Reactor", CEA-SESR-N-07 23 March 1973. Translation to English AEEC-Lib/Trans 623

release into the Reactor Hall atmosphere. This is conservative as it neglects radioactive decay and the transit time through the pool water.

Deposition and plate out within the containment produce a reduction over time in the amount of fission products airborne in the containment. An exponential decay has been assumed, with an associated decay constant, λ_d. Table 16.19/4 shows the values of λ_d for different radionuclides.

Removal of air from the Containment due to leakage produces a reduction in the source strength that can be represented by an exponential decay with a decay constant λ_l, shown in Table 16.19/5 for different leakage rates.

Throughout the sequence, the iodine fraction of fixed to organic substances is conservatively taken to be equal to 5%.

The dose calculations were performed with PC-COSYMA. The dose obtained for an average person located at 1.6km from the reactor is given in the following table for the different periods. The calculations were performed assuming a prompt release at 45m (through the venting stack) with subsequent releases at ground level.

Distance	Prompt	Period 1	Period 2	Period 3	Period 4	Total
1600m	50μSv	16μSv	0.3μSv	0.5μSv	0.9μSv	67.7μSv

The collective effective dose for this scenario, calculated for the population within a radius of 22.5 km from the reactor is 0.99 Person-Sv, well below the 200 Person-Sv required by ARPANSA regulations.

Therefore, a total loss of flow in the RSPCS with subsequent failure of the FSS and assumed failure of all the U-Mo targets, would result in a dose to the public that is well below ARPANSA limits and require no emergency interventions or countermeasures.

16.19.3 Blockage of Cooling Channels in a Fuel Assembly

It is postulated that a small object may enter the PCS, bypass the different filters and block two fuel channels. Even though it is not credible to postulate the presence inside the PCS of an object large enough to totally block two channels, total blockage is assumed and no credit is given to the coolant flow that is in contact with the outermost faces of the two outer plates. All three fuel plates are assumed to melt and release their inventory into the Reactor Pool. Partition fractions, deposition and removal decay constants and leakage decay constants are the same used in Section 16.9.2. Atmospheric conditions during the analysed period (100 days) are also identical to those in Section 16.9.2. The release of the inventory of three fuel plates is presented in Table 16.19/6. The time periods over which the release occurs are set out in Section 16.19.2.

Calculations are performed with PC-COSYMA to determine the dose to an average person at 1.6 km. It is assumed that the, prompt release occurs at 45 m and all subsequent releases occur at ground level. The results are shown below.

Distance	Prompt	Period 1	Period 2	Period 3	Period 4	Total
1600m	5.5μSv	1.85μSv	0.04μSv	0.08μSv	0.15μSv	7.62μSv

The collective effective dose for this scenario, calculated for the population within a radius of 22.5 km from the reactor is 0.11 Person-Sv, well below the 200 Person-Sv required by ARPANSA regulations.

Therefore, a cooling channel blockage that could lead to the melting of three fuel plates would result in a dose to the public that is well below ARPANSA limits and require no emergency interventions or countermeasures such as evacuation and supply of iodine tablets.

16.19.4 Erroneous Early Removal of Irradiated U-Mo Targets into a Hot Cell

It is postulated that three U-Mo targets are erroneously removed from the decay rack in the Service Pool before having undergone adequate cooling and transported into the Hot Cell. It is further assumed that the interlock that inhibits the transport from the Service Pool into the HC cell on high activity has failed. The occurrence of this event requires sequential failures in adherence to operating procedures and the presence of an unrevealed mechanical failure. This is an unlikely sequence of events.

This event is assumed to result in the melting of the U-Mo targets when they leave the water and enter the HC. The heat dissipated by the targets by natural circulation to the air is assumed insufficient to prevent their melting.

The air inside the hot cells is circulated by means of a dedicated ventilation system (see Chapters 11 and 10). Five percent of the ventilation flow rate is sent to the stack to compensate the inward leakage of air from the containment into the hot cell. This results in a release to the atmosphere of 1440% of the volume of the cell. Both the recirculated and the vented air is filtered through absolute filters (to retain aerosols) and activated charcoal filters (to retain iodine). Subsequent to the release of fission products from the targets, 100% of the noble gases are assumed to be released and not retained by the filters. It is further postulated that the activated charcoal filters have a total degraded efficiency of 90% and that the absolute filters have a total degraded efficiency of 99.99%. The Containment is isolated after two minutes, and the cell ventilation system continues to recirculate the air in the hot cell. The negative pressure of the hot cell relative to the Containment is lost after Containment isolation. It is conservatively assumed that all the noble gases that remain within the cell after the prompt discharge (two minutes) are released into the Containment. After the transfer of the noble gases to the Containment, they are released to the atmosphere following the same pattern as the release for the accidents inside the Reactor Pool. Thus, during the first hour, the transient of the Containment conditions leads to a release of 1% volume. In addition, after the Containment isolation, a 2% volume per day release due to the variations in barometric pressure is assumed. Table 16.19/7 gives a summary of the assumptions adopted for the analysis of this accident. In addition, it is assumed that the performance of the filters, the plate out inside the cell and the Containment isolation with recirculation removes all the iodine and particulates. Therefore, iodine and particulates are released only during the prompt period and consequently, do not make a significant contribution to the dose once the Containment has been isolated, as can be seen in Table 16.19/8

Calculations are performed with PC-COSYMA to determine the dose to an average person at 1.6km. It is assumed that the, prompt release occurs at 45 m and all subsequent releases occur at ground level. The results are shown below.

Distance	Prompt	Period 1	Period 2	Period 3	Period 4	Total
1600m	11.8 μSv	0.8 μSv	0.012 μSv	0.031 μSv	0.059 μSv	12.7 μSv

The collective effective dose for this scenario, calculated for the population within a radius of 22.5 km from the reactor is 0.18 Person-Sv, well below the 200 Person-Sv required by ARPANSA regulations.

Thus, the removal of three molybdenum targets to the hot cell, before the predetermined decay time, would result in a dose to the public that is well below ARPANSA limits and requires no emergency interventions or countermeasures such as evacuation and supply of iodine tablets.

16.19.5 Total plant blackout for 10 days

Loss of Normal Power Supply initiates a reactor shutdown by the FSS. This protective action is not dependant on the operation of the FRPS since, on de-coupling of the CRD motors or de-energising of the CR electromagnets, the CRs fall into the core. In addition, the FRPS sends a signal to request the actuation of the FSS. Furthermore, if the SRPS detects a failure of two or more CRs to fully insert within a preset time after initiation of the FSS, actuation of the SSS occurs.

The sequence of events is as follows;

a) Interruption of Normal Power.

b) UPS units provide electric supply from batteries to the RCMS, the RPS, and the PAM system (for at least 30 minutes).

c) RPS produce alarms and warnings in the Main Control Room.

d) Loss of Normal Power to the FSS will de-energise the electromagnets and the motors, the pistons will de-couple from the control rod drive mechanism, and the CRs will fall into the core by gravity forces.

e) The FRPS sends a signal to request the actuation of the FSS and thus assisted control rod insertion.

f) If the SRPS detects a failure of two or more CRs to fully insert within a preset time after initiation of the FSS actuation of the SSS is initiated

g) Both Diesel Generators fail to start.

h) The PCS and RSPCS pumps coast down.

i) PCS and RSPCS flap valves open and natural circulation is established.

j) Decay heat from the core and the irradiation rigs is removed by natural circulation of the water contained in the Reactor Pool.

k) The RSPCS fails to function in Long Term Pool Cooling mode as the Standby Power System is not available.

l) Decay heat is removed by evaporation of the pool water without the use of the RSPCS for 10 days.

m) The Reflector Vessel will be heated by decay power only. This heat load can be removed by the pool water, no actuation of the Reflector Cooling System is necessary.

The behaviour of the PCS and the RSPCS has been analysed after a loss of electric power. Calculations have been made with the RELAP 5 code. The nodalisation used for the PCS and the RSPCS is presented in Section 16.3.

To calculate the increase in the pool water temperature, only the water between the top of the chimney and the bottom of the Transfer Canal has been considered. This volume is relatively small compared to the total volume of water in the pools. Thus, it represents a conservative assumption.

For the PCS calculations, the temperature of the coolant corresponds to the central node in the hot channel. The cladding temperatures correspond to the fuel node in that same channel.

The loss of power results in a loss of heat removal from the PCS via the heat exchangers (due to the shutdown of the SCS pumps) and the loss of flow in the PCS and RSPCS. The RSPCS and the PCS pumps stop and the flow coasts down according to the dynamics of the pumps.

The loss of power has been simulated numerically with successful actuation of the FSS and with failure of the FSS and actuation of the SSS. The reactor trip is triggered by a low flow signal in the PCS or RSPCS. Successful actuation of the FSS trips the reactor seconds after the blackout. This is a very conservative assumption, since the fail safe characteristics of the FSS are being ignored to introduce the delay. In reality, the actuation of the FSS is instantaneous and immediately follows the loss of Normal Power. Failure of the FSS and actuation of the SSS causes the reactor to trip. The RSPCS and the PCS have been treated separately, with connections through the pool water and the interconnection line flow. For the RSPCS calculations, the pool temperature and the interconnection flow rate come from the PCS calculations results.

The short term results are as those presented in Section 16.7. The interest in this Beyond Design Basis Accident is in the long term behaviour of the plant. On the basis of the decay heat generated during the ten days following the loss of power, a significant volume of water is evaporated from the pool. This evaporation leads to a reduction in the depth of water in the pool. The burnout heat flux for the conditions in the core following shutdown calculated with Fabrega correlation and assuming no subcooling is 20 Wcm^{-2}. After reactor shutdown, the reactor behaves as described in 16.7.5.3.2. During the period beyond that assessed in 16.7.5.3.2 the power decreases, the burnout ratio will increase and no burnout will occur in the core. Therefore, the core will remain in a safe shutdown state for the 10 days following the loss of power.

16.19.6 Control Rod Bank Withdrawal at Nominal Velocity

As shown in Section 16.8, this is a BDB event. Therefore, in accordance with International Best Practice, best estimate values have been used for some of the data adopted for the analysis of reactivity insertion accidents. The start up power has been taken as 50kW. Failure of the FSS has been considered and the SRPS trips the reactor on high neutron flux rate (low reactor period). Whilst the central rod moves slightly faster than the non-central plates the bank has been considered to move at the speed of the non-central plates. This has a minimal affect on the analysis as it is less than 20% of the worth of the bank. The rest of the assumptions presented in Section 16.3 and 16.8 have been maintained.

16.19.6.1 Start Up in the Physics Test State

The analysis has been performed with PARET. The total reactivity that can be inserted during the accident corresponds to the maximum cold core reactivity excess, without xenon. The analysis has been performed for the case with two control rods partially withdrawn and the reactor critical. A 20% uncertainty margin has been allowed and the analysis has been undertaken for reactivity insertion corresponding to the steepest insertion ramp.

The analysis established that the maximum clad temperature is within safe limits and follows power evolution with a small increase while the coolant temperature at hot channel outlet presents a maximum temperature of 51.9 ºC.

16.19.6.2 Start Up in the Power State

A Control Rod Bank withdrawal during start up in the Power state has been analysed. Failure of the FSS and trip of the SSS on High Neutron Flux Rate (low reactor period) has been postulated. This transient has been analysed with RELAP 5. The assumptions are the same as the ones used in Section 16.19.6.1.

The rate of insertion of reactivity by the whole bank is so large, that the high neutron flux rate (low reactor period) trip set point is reached almost immediately after the bank begins to be withdrawn. The total reactivity inserted is small, and almost half of it due to the delays involved in the stopping of the bank by SRPS (Figure 16.19/8). The analysis shows that the maximum core power reached is very low and that the coolant and cladding temperatures increase only slightly from their initial values.

16.19.7 Control Plate Withdrawal during Start Up in the Physics Test State with Failure of the FSS and Success of the SSS

The continuous withdrawal of a Control Plate at nominal velocity during start up in the Physics Test state with failure of the FSS is considered a BDBA. The combination of the short time the reactor operates in the Physics Test state with the low probability of failure of the FSS renders this scenario very unlikely. The event has been analysed as part of the additional analysis required by ARPANSA during the review of the application for a licence to construct the reactor facility. The transient has been analysed with PARET, using the same assumptions as in Section 16.19.6. At the moment point of generation of a trip signal plus the delay of the electronics, the plate withdrawal is stopped. The SSS is actuated upon failure of the FSS to respond. The analysis established that the maximum clad temperature is within safe limits and follows power evolution while the coolant temperature at hot channel outlet rises to a maximum value of 63.8 ^{o}C.

16.19.8 Conclusions

The analysis has shown that, of the Beyond Design Basis Accidents identified as being the most important in terms of their potential for fission product evolution, only three involve fission product release and, of those three, the worst consequences results in a dose of 68 μSv with a collective dose of 0.99 Person-Sv for the melting of the U-Mo targets in the reactor.

The Beyond Design Basis Accident “total plant blackout for 10 days” shows the robustness of the design in being able to cope with extended periods of natural circulation in the core.

The analysis of control rod bank withdrawal and control plate withdrawal during start up with SSS actuation shows that the reactor can cope with these BDB events with no challenge to the core.

It is concluded that the off-site consequences for Beyond Design Basis Accidents are minor and well within regulatory limits.

End of Section

Table 16.19/1 Summary of Conditions during the Beyond Design Basis Accident Sequences (Failure of U-Mo Targets under Water, Failure of Fuel Plates under Water)

Period	Time [s]	Release status		Meteorological Condition	Wind speed [m/s]
Prompt	0 to 120	normal (exhaust)	2400%/day	F (winter)	1 m/s
P1A	120 to 10^3	Isolated containment CERS	1% +(1/12)%is released during the first hour 2%day is released during the remainder of the period	F (winter)	1 m/s
P1B	10^3 to 10^4	Isolated containment CERS	2%/day	F (winter)	1 m/s
P1C	10^4 to 4.32 10^4	Isolated containment CERS	2%/day	F (winter)	1 m/s
P2	4.32 10^4 to 8.64 10^4	Isolated containment CERS	2%/day	D (winter)	3 m/s
P3	8.64 10^4 to 1.296 10^5	Isolated containment CERS	2%/day	F (winter)	1 m/s
P4	1.296 10^5 to 8.64 10^6	Isolated containment CERS	2%/day	D (winter)	3 m/s

Table 16.19/2 Radioisotope Release to the Environment following Melting of 36 U-Mo Targets Underwater

Isotope	Prompt/Bq	Period 1/Bq	Period 2/Bq	Period 3/Bq	Period 4/Bq
Xe-131m	7.15E+09	1.90E+10	1.08E+10	9.79E+09	8.96E+10
Xe-133m	2.69E+11	6.86E+11	3.35E+11	2.67E+11	8.74E+11
Xe-133	6.70E+12	1.76E+13	9.56E+12	8.37E+12	5.13E+13
Xe-135m	1.62E+12	7.04E+11	0.00	0.00	0.00
Xe-135	5.75E+11	1.18E+12	2.41E+11	9.06E+10	4.26E+10
Xe-138	8.24E+12	3.43E+12	0.00	0.00	0.00
Kr-83m	7.80E+11	8.91E+11	2.91E+09	2.89E+07	2.23E+05
Kr-85m	1.89E+12	3.14E+12	2.13E+11	3.12E+10	4.12E+09
Kr-85	7.77E+08	2.09E+09	1.22E+09	1.14E+09	1.67E+10
Kr-87	3.71E+12	3.58E+12	1.33E+09	1.79E+06	1.86E+03
Kr-88	5.07E+12	7.03E+12	1.40E+11	7.02E+09	2.84E+08
I-130	3.64E+06	5.67E+06	3.15E+05	7.02E+04	3.83E+04
I-131	3.65E+09	6.42E+09	7.50E+08	3.24E+08	1.88E+09
I-132	8.38E+09	8.99E+09	1.67E+07	1.71E+05	2.43E+03
I-133	1.47E+10	2.40E+10	1.83E+09	5.44E+08	5.51E+08
I-134	1.69E+10	1.26E+10	4.49E+04	0.00	0.00
I-135	1.36E+10	1.93E+10	5.32E+08	6.37E+07	1.34E+07
Te-125m	3.12E+00	7.92E+00	3.80E+00	0.00	0.00
Te-127m	1.10E+03	2.80E+03	1.35E+03	1.07E+03	3.28E+03
Te-127	1.27E+05	2.52E+05	4.34E+04	1.41E+04	5.29E+03
Te-129m	3.68E+04	9.33E+04	4.46E+04	3.50E+04	1.04E+05
Te-129	9.11E+05	8.32E+05	1.31E+02	0.00	0.00
Te-131m	5.94E+05	1.39E+06	4.86E+05	2.92E+05	3.47E+05
Te-131	3.63E+06	2.03E+06	5.45E-04	0.00	0.00
Te-132	5.61E+06	1.38E+07	5.89E+06	4.20E+06	8.35E+06
Te-133m	4.65E+06	3.82E+06	8.58E+01	0.00	0.00
Te-133	5.16E+06	2.01E+06	0.00	0.00	0.00
Te-134	9.80E+06	7.03E+06	7.36E+00	3.81E-05	1.51E-10
Cs-134m	3.41E+04	4.67E+04	8.35E+02	3.79E+01	1.39E+00
Cs-134	1.17E+03	2.96E+03	1.43E+03	1.13E+03	3.54E+03
Cs136	1.03E+05	2.59E+05	1.22E+05	9.40E+04	2.59E+05
Cs137	1.76E+05	4.47E+05	2.16E+05	1.71E+05	5.36E+05
Cs138	2.85E+08	1.80E+08	0.00	0.00	0.00
Rb-86	6.15E+03	3.98E+02	2.68E+02	2.42E+02	4.10E+02
Rb-88	5.01E+02	2.36E+02	0.00	0.00	0.00
Rb-89	1.48E+08	6.39E+07	0.00	0.00	0.00
Ru-103	1.54E+08	3.91E+08	1.87E+08	1.47E+08	4.41E+08
Ru-105	2.38E+08	3.82E+08	2.10E+07	2.56E+06	2.73E+05
Ru-106	2.21E+07	5.60E+07	2.71E+07	2.14E+07	6.68E+07

Table 16.19/3 Partition Fractions in Nuclide Transportation

Nuclide type	Release from fuel type source (F_{cp}) [%]	Release from pool water to containment (F_{pb}) [%]
noble gases (xenon and krypton)	100	100
iodine	30	0.5
caesium	30	0.01
rubidium	30	0.01
tellurium	1	0.01
ruthenium	1	0.01

Table 16.19/4 Deposition and Removal Decay Constant

Nuclide type	λ_d [1/s]	
noble gases (xenon and krypton)	0	
iodine	inorganic	3.85 10^{-5}
	organic	0
caesium	3.85 10^{-6}	
rubidium	3.85 10^{-6}	
tellurium	3.85 10^{-6}	
ruthenium	3.85 10^{-6}	

Table 16.19/5 Leakage Decay Constant

L/t_l		λ_l	Comments
100 %/h	$2.78\ 10^{-4}$ 1/s	$2.78\ 10^{-4}$ 1/s	Applicable to a ventilation exhaust flow of 10^4 m^3 per hour
3 %/day	$3.47\ 10^{-7}$ 1/s	$3.47\ 10^{-7}$ 1/s	Different leakage rates.
5 %/day	$5.79\ 10^{-7}$ 1/s	$5.79\ 10^{-7}$ 1/s	
10 %/day	$1.16\ 10^{-6}$ 1/s	$1.16\ 10^{-6}$ 1/s	
30 %/day	$3.47\ 10^{-6}$ 1/s	$3.47\ 10^{-6}$ 1/s	

Table 16.19/6 Radioisotope Release to the Environment Following the Melting of Three Fuel Plates Underwater

Isotope	Prompt/Bq	Period 1/Bq	Period 2/Bq	Period 3/Bq	Period 4/Bq
Xe-131m	6.12E+10	2.64E+10	2.53E+10	1.62E+10	4.06E+11
Xe-133m	3.55E+11	1.43E+11	1.21E+11	6.80E+10	3.72E+11
Xe-133	1.17E+13	4.94E+12	4.57E+12	2.82E+12	3.56E+13
Xe-135m	1.99E+12	2.58E+10	0.00	0.00	0.00
Xe-135	9.11E+11	2.62E+11	1.04E+11	2.76E+10	1.83E+10
Xe-138	1.03E+13	1.22E+11	0.00	0.00	0.00
Kr-83m	9.03E+11	8.61E+10	9.12E+08	6.37E+06	6.76E+04
Kr-85m	2.10E+12	4.19E+11	6.48E+10	6.66E+09	1.22E+09
Kr-85	1.54E+10	6.73E+09	6.64E+09	4.37E+09	3.72E+11
Kr-87	4.19E+12	2.79E+11	4.04E+08	3.83E+05	5.49E+02
Kr-88	5.94E+12	8.41E+11	4.47E+10	1.57E+09	8.78E+07
I-130	1.72E+08	3.04E+07	4.04E+06	6.36E+05	4.96E+05
I-131	8.15E+09	1.80E+09	4.58E+08	1.39E+08	1.92E+09
I-132	1.18E+10	9.86E+08	6.35E+06	4.58E+04	8.97E+02
I-133	1.78E+10	3.46E+09	6.10E+08	1.27E+08	1.91E+08
I-134	1.98E+10	7.79E+08	1.42E+04	0.00	0.00
I-135	1.66E+10	2.44E+09	1.76E+08	1.49E+07	4.38E+06
Te-125m	1.42E+03	5.70E+02	4.74E+02	2.63E+02	1.31E+03
Te-127m	3.26E+04	1.31E+04	1.09E+04	6.07E+03	3.09E+04
Te-127	3.51E+05	9.49E+04	3.27E+04	7.48E+03	3.93E+03
Te-129m	2.03E+05	8.13E+04	6.73E+04	3.72E+04	1.81E+05
Te-129	1.35E+06	8.01E+04	5.24E+01	0.00	0.00
Te-131m	6.96E+05	2.46E+05	1.56E+05	6.59E+04	1.15E+05
Te-131	4.61E+06	9.83E+04	0.00	0.00	0.00
Te-132	7.83E+06	3.00E+06	2.26E+06	1.13E+06	3.46E+06
Te-133m	4.93E+06	2.34E+05	2.45E+01	0.00	0.00
Te-133	6.56E+06	6.83E+04	0.00	0.00	0.00
Te-134	1.13E+07	4.04E+05	2.27E+00	0.00	0.00
Cs-134m	6.48E+06	8.93E+05	4.31E+04	1.38E+03	6.96E+01
Cs-134	4.48E+06	1.80E+06	1.51E+06	8.41E+05	4.35E+06
Cs-136	2.42E+06	9.62E+05	7.84E+05	4.26E+05	1.90E+06
Cs-137	3.88E+06	1.56E+06	1.31E+06	7.29E+05	3.78E+06
Cs-138	3.44E+08	9.47E+06	1.53E+00	0.00	0.00
Rb-86	2.45E+05	9.77E+04	8.03E+04	4.39E+04	2.04E+05
Rb-88	1.74E+08	2.62E+06	0.00	0.00	0.00
Rb-89	2.25E+08	2.87E+06	0.00	0.00	0.00
Ru-103	1.83E+08	7.34E+07	6.08E+07	3.36E+07	1.65E+08
Ru-105	8.18E+07	1.53E+07	1.97E+06	1.69E+05	2.49E+04
Ru-106	1.04E+07	4.21E+06	3.52E+06	1.96E+06	1.01E+07

Table 16.19/7 Summary of Conditions during the Beyond Design Basis Accident Sequences with Failure of U-Mo Targets in Air inside a Hot Cell

Period	Time [s]	Release status		Meteoro-logical Condition	Wind speed [m/s]
Prompt	0 to 120	normal (exhaust)	14400% hot cell volume/day	F (winter)	1 m/s
P1A	120 to 10^3	Isolated containment CERS	1%[1] +(1/12)%[1]is released during the first hour 2%day is released during the remainder of the period	F (winter)	1 m/s
P1B	10^3 to 10^4	Isolated containment CERS	2%/day	F (winter)	1 m/s
P1C	10^4 to 4.32 10^4	Isolated containment CERS	2%/day	F (winter)	1 m/s
P2	4.32 10^4 to 8.64 10^4	Isolated containment CERS	2%/day	D (winter)	3 m/s
P3	8.64 10^4 to 1.296 10^5	Isolated containment CERS	2%/day	F (winter)	1 m/s
P4	1.296 10^5 to 8.64 10^6	Isolated containment CERS	2%/day	D (winter)	3 m/s

1 Corresponds to percentage of volume of the containment

Table 16.19/8 Radioisotope Release to the Environment Following the Melting of a U-Mo Target in Air inside a Hot Cell

Isotope	Prompt /Bq	Period 1 /Bq	Period 2 /Bq	Period 3 /Bq	Period 4 /Bq
Xe-131m	4.00E+09	1.97E+11	1.46E+08	1.06E+05	7.67E+01
Xe-133m	1.501E+11	7.29E+12	4.74E+09	3.02E+06	1.92E+03
Xe-133	3.75E+12	1.84E+14	1.31E+11	9.16E+07	6.40E+04
Xe-135m	9.05E+11	7.73E+12	0.00	0.00	0.00
Xe-135	3.22E+11	1.41E+13	4.34E+09	1.30E+06	3.91E+02
Xe-138	4.61E+12	3.67E+13	0.00	0.00	0.00
Kr-83m	4.37E+11	1.32E+13	1.08E+08	8.54E+02	0.00
Kr-85m	1.05E+12	4.11E+13	4.91E+09	5.72E+05	6.67E+01
Kr-85	4.35E+08	2.15E+10	1.64E+07	1.22E+04	9.13E+00
Kr-87	2.07E+12	5.31E+13	5.95E+07	6.40E+01	0.00
Kr-88	2.84E+12	9.94E+13	4.08E+09	1.63E+05	6.49E+00
I-130	1.12E+08	2.14E+08	0.00	0.00	0.00
I-131	1.13E+11	2.15E+11	0.00	0.00	0.00
I-132	2.58E+11	4.80E+11	0.00	0.00	0.00
I-133	4.52E+11	8.63E+11	0.00	0.00	0.00
I-134	5.19E+11	9.22E+11	0.00	0.00	0.00
I-135	4.21E+11	7.97E+11	0.00	0.00	0.00
Te-125m	1.44E+02	2.76E+02	0.00	0.00	0.00
Te-127m	5.09E+04	9.74E+04	0.00	0.00	0.00
Te-127	5.88E+06	1.12E+07	0.00	0.00	0.00
Te-129m	1.70E+06	3.25E+06	0.00	0.00	0.00
Te-129	4.21E+07	7.61E+07	0.00	0.00	0.00
Te-131m	2.74E+07	5.24E+07	0.00	0.00	0.00
Te-131	1.68E+08	2.76E+08	0.00	0.00	0.00
Te-132	2.59E+08	4.95E+08	0.00	0.00	0.00
Te-133m	2.15+08	3.83E+08	0.00	0.00	0.00
Te-133	2.39E+08	3.41E+08	0.00	0.00	0.00
Te-134	4.53E+08	7.89E+08	0.00	0.00	0.00
Cs-134m	5.25E+04	9.81E+04	0.00	0.00	0.00
Cs-134	1.79E+03	3.43E+03	0.00	0.00	0.00
Cs-136	1.58E+05	3.03E+05	0.00	0.00	0.00
Cs-137	2.71E+05	5.18E+05	0.00	0.00	0.00
Cs-138	4.38E+08	7.42E+08	0.00	0.00	0.00
Rb-86	8.02E+02	1.53E+03	0.00	0.00	0.00
Rb-88	2.29E+08	3.55E+08	0.00	0.00	0.00
Rb-89	3.03E+08	4.53E+08	0.00	0.00	0.00
Ru-103	3.40E+07	6.50E+07	0.00	0.00	0.00
Ru-105	6.540E+07	1.23E+08	0.00	0.00	0.00
Ru-106	5.17E+05	9.90E+05	0.00	0.00	0.00

End of Tables

16.20 PROBABILISTIC SAFETY ASSESSMENT OBJECTIVES

The objective of the Probabilistic Safety Assessment (PSA) for the reactor is the quantitative evaluation of the risks associated with the operation of the Reactor Facility.

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

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

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

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

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

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

f) The comparison of the representative accident sequences risks with the regulatory objectives[1] .

The PSA was developed in parallel with the basic and detailed engineering phase of the RRR Project. The preliminary results were used as input to the design process, permitting improvements to be made to the design. The analysis was re-quantified with data from the detailed engineering.

16.20.1 The Probabilistic Safety Assessment and the Deterministic Safety Analysis

The safety analyses presented in previous sections of this chapter of the SAR considers a comprehensive range of postulated initiating events. It examines each of these postulated initiating events and determines which can be eliminated from further consideration on the basis of their low likelihood of occurrence, or plant design features that mean the event cannot credibly occur. The events that remain are considered design basis initiating events and are analysed using thermal-hydraulic and neutronics computer codes with very conservative assumptions. The analyses show that the safety features included in the design are effective in preventing the exceedance of safety limits.

In contrast to the deterministic safety analysis, the PSA asks “What if the postulated initiating event were to occur and more than one piece of equipment were to fail? What if several things were to go wrong?” The PSA attempts to determine all the possible combinations of how the plant could respond to an initiating event, group all the possible outcomes, obtain conservative estimates of the frequency (how likely), and bounding estimates of the consequences (the effect, usually expressed in the maximum effective radiation dose to a worst exposed individual member of the public). The frequency and consequence constitute the risk and can be compared against the safety objectives set out in the regulatory assessment principles.

[1] ARPANSA, “Regulatory Assessment Principles for Controlled Facilities”, Australia, October 2001.

16.20.2 Scope of the PSA

The risk evaluation was performed, taking into account internal events, internal hazards (eg fire) and external hazards (e.g., earthquakes) relevant to the plant. Sabotage and security related events are explicitly excluded from PSA.

The different PSA scopes are usually classified in three levels:

a) Level I: considers the development of accident sequence models to the point necessary to determine whether damage to the fuel assemblies and rigs has occurred, and the corresponding likelihood (expected frequency). The phenomenology of fission product release is not analysed, nor is the containment response to any release.

b) Level II: goes beyond Level I in the modelling of the phenomena associated with the release, transport and deposition of fission products from their original location (e.g., fuel) through the various plant systems to the containment. It examines the behaviour of the fission products in the containment environment and the degree to which they are released to the environment (the 'source term').

c) Level III: goes beyond level II in analysing the dispersion of radioactive material in the environment. It models the different paths that may exist for these radioactive materials to have an impact on members of the public.

The scope of the present PSA is Level I with some Level III aspects. The Level III aspects include the consequence analysis of a number of representative accident sequences. These accidents were selected on the basis of making a significant contribution to the overall frequency of damage to the plant. The comparison with ARPANSA requirements is made even taking into account the 95% confidence level provided by the uncertainty analyses. Even in this case, the calculated CDF fulfils the safety objectives.

In order to obtain risk-representative scenarios, several reactor utilisation accidents were selected. For the selected accidents, release fractions were derived using conservative assumptions and the containment response determined in order to obtain the source term for that sequence. The dose to members of the public was also calculated using conservative weather conditions.

The Level I PSA results provide estimates of the frequency of events that may cause damage to the fuel and other potential sources of radioactive material (eg heavy water). They also highlight the most important contributors to the risk of the plant from the frequency point of view, and they may help in the final definition of the safety systems parameters, configuration and set points.

The corresponding dependent failure analyses helped to verify the adequacy of the segregation and redundancy of safety functions.

The overall results, consisting of the representative accident sequences, their associated frequency and estimated doses, are compared against the regulatory requirements. The two main regulatory requirements in this respect are a total Core Damage Frequency of less than $1x10^{-4}$ per year and the meeting of the dose/frequency limits set out in Chapter 2 and repeated here below.

Maximum effective dose to most exposed individual off-site (mSv)	Total frequency, per controlled facility year	
	Safety limit	Safety objective
0.1 – 1	1	10^{-2}
1 – 10	10^{-1}	10^{-3}
10 – 100	10^{-2}	10^{-4}
100 – 1000	10^{-3}	10^{-5}
> 1000	10^{-4}	10^{-6}

The PSA includes consideration of all envisaged operating states of the Reactor Facility, and all expected radiation sources that may exist in the plant. These results demonstrate that there is no design basis accident or credible beyond design basis accident that could cause a sufficiently high dose to the worst placed member of the public such as to require countermeasures.

16.20.3 PSA Results – Core Damage Frequency

A very important result to be obtained from a PSA is the Core Damage Frequency. The Core Damage Frequency is the annual probability of occurrence of all accidents with the potential to cause significant damage to the reactor core. In the following discussion we consider the Core Damage Frequency arising from internal events and seismic events.

For the Reactor, the Core Damage Frequency obtained by the summation over all the frequencies of internal event sequences that may lead to core damage is:

Internal events CDF

Mean Core Damage Frequency: 1.4 10^{-7}/year

5^{th} Percentile Core Damage Frequency: 2.3 10^{-8}/year

95^{th} Percentile Core Damage Frequency: 3.4 10^{-7}/year

During screening of internal hazards, internal fire was identified as having the potential to cause core damage. The internal fire contribution was analyzed using the internationally accepted IAEA methodology, and several fire scenarios were calculated under a highly conservative approach, taking into account the particular layout of the RRR. The overall CDF due to internal fire initiated accidents is estimated to be:

Internal Fire CDF

Mean Core Damage Frequency: 1.4 10^{-8}/year

The contribution of the internal fire, under these conservative approach, is one order of magnitude less than the internal initiators CDF and is located well below the cut-off frequency of the regulatory requirements. Given this result, a more detailed (less conservative) evaluation of the internal fire contribution was not performed.

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

The first scenario considers the contribution to the Core Damage Frequency for those seismic events whose frequency is up to that stated for the SL-2 earthquake, that is, with a frequency higher or equal to 10^{-4}/year. This scenario examines the overall ability of the critical systems in the Reactor to withstand a seismic event of a magnitude for which they have been designed.

The second scenario considers the contribution to the Core Damage Frequency for all the seismic events above the SL-2 level as indicated by the hazard curve derived for the site. In this case, the ability of the critical systems to withstand a seismic event beyond their design basis is being considered. In this extreme scenario, the safety systems necessary to shutdown the reactor and prevent loss of coolant after a severe seismic event are treated as single systems whose performance can be degraded by vibration, damage or geometric distortion due to the high accelerations experienced. The seismic BDB events are not expected to occur; however, they are modelled in the PSA in order to evaluate their relative contribution.

The Core Damage Frequency obtained by the summation over all the frequencies of seismic event sequences (up to the SL-2 level) that may lead to significant core damage is:

SL-2 level seismic CDF

Mean Core Damage Frequency:	2.2 10^{-10}/year
5^{th} Percentile Core Damage Frequency:	1.7 10^{-11}/year
95^{th} Percentile Core Damage Frequency:	1.0 10^{-9}/year

These values, when compared with the contribution of internally initiated events, contribute less than 0.2% to the overall Core Damage Frequency. This value indicates that the design of the safety related components is sufficiently robust to withstand the seismic events that may be experienced at the Reactor Facility.

The Core Damage Frequency obtained by the summation over all the frequencies of seismic event sequences (for the full hazard curve) that may lead to core damage is:

Full hazard curve seismic CDF

Mean Core Damage Frequency:	3.8 10^{-7}/year
5^{th} Percentile Core Damage Frequency:	2.2 10^{-8}/year
95^{th} Percentile Core Damage Frequency:	6.3 10^{-7}/year

Note that the estimate of CDF arising from the full seismic hazard curve is about an order of magnitude higher than that provided in the PSAR due to improved modelling of the system fragilities.

The full hazard seismic values, when compared with the contribution of internally initiated events, indicate that extreme seismic events contribute approximately 75% to the overall CDF. Given the conservative assumptions for the calculations in these extreme cases and the fact that even for these cases the ARPANSA criteria are fulfilled, it can be concluded that the design of the Reactor Facility is very robust.

In the consideration of external events, all other initiators were screened out, including extreme winds and tornadoes. Two of the external events were aircraft crash and strike by military shell, with relatively high frequency contributions. Their estimated frequencies were 1.1×10^{-8}/year with an upper bound of 4.8×10^{-8}/year for the aircraft crash, and an upper bound of 1.0×10^{-8}/year for the military shell, respectively.

The total contribution of all accident sequences (initiated either by internal events, by internal fire, by external earthquakes, and other external events) is obtained by summing each of the above contributions. The mean value is obtained by the summation of the mean values (when they are available) or the upper bound estimations (when mean values do not exist). The uncertainty range is obtained assuming an uncertainty distribution for all contributors similar to the one obtained for internal events.

The overall core damage frequency is thus determined as:

Overall CDF (including seismic hazard up to SL-2)

Mean Core Damage Frequency:	1.7 10^{-8}/year
5th Percentile Core Damage Frequency	4.9 10^{-8}/year
95th Percentile Core Damage Frequency	4.1 10^{-7}/year

Overall CDF (with FULL seismic hazard)

Mean Core Damage Frequency:	5.4 10^{-7}/year
5th Percentile Core Damage Frequency	3.0 10^{-7}/year
95th Percentile Core Damage Frequency	9.1 10^{-7}/year

The regulatory requirement is that the Core Damage Frequency should be less than 10^{-4} /year.

It is thus concluded that those accidents involving core damage in the Reactor Facility have a very low likelihood of occurrence and well below the ARPANSA criterion.

It may also be concluded that those seismically initiated accidents with the potential to cause significant damage to the core pose a risk comparable to that posed by internal initiators to the public in the vicinity of the LHSTC.

16.20.4 PSA Results – Frequency/Dose Limits

As a consequence of the very low Core Damage Frequency of the Reactor, those accidents with a credible potential for radioactive release to the environment do not involve significant damage to the core but some involve damage to the irradiation rigs.

The purpose of performing this kind of analysis is, however, to demonstrate that even taking into account these extremely conservative assumptions, the regulatory requirements are fulfilled.

After screening of all possible accidents with the potential to cause radioactive releases, five release categories were established, and their associated annual frequencies calculated. The five categories described below.

Calculations were performed to determine the doses to individuals at the buffer zone boundary (1600m) using very conservative assumptions:

a) For the fuel and fuel plate events, the inventory was calculated for equilibrium (maximum) core and increased by 10% to take into account uncertainties.

b) Conservative retention factors for the water were assumed.

c) Radioactive decay was neglected during water transport.

d) The worst atmospheric conditions (Pasquill F with 1 m/s wind speed, winter season) were assumed during the first 12 hours followed by 12 hours of Pasquill at 3 m/s, another 12 hours of Pasquill F at 1 m/s and the final 98.5 days, Pasquill D at 3 m/s.

e) The “prompt” release would be at 45 m.

f) Containment closure would occur two minutes after the accident.

g) Subsequent release would be by leakage of the containment and this would be assumed to occur at ground level.

h) There is no exhaust filter retention of any kind.

i) The containment leak rate of would be 3% of the volume per day for the first day following closure of the containment (while pressure in the containment could be elevated) and 2% per day thenceforth, for up to 99 additional days.

j) The release continues for up to 100 days.

For the case of the targets melting in the hot cell, although the stack filter retention was again assumed to be zero, the cell recirculation filtering was assumed to be degraded. In the recirculation there are two charcoal filters and three absolute filters while in exhaust one charcoal and two absolute filters. The individual efficiencies were considered degraded (99% for each absolute filter and 90% for each charcoal filter).

These assumptions are realistic but conservative. For example, the containment would be expected to close within one minute of an accident.

The results obtained for each release category are:

Release category RC-B5 (corresponds to a local blockage of two flow channels):

Annual frequency: 1.3 10^{-6} /yr

Maximum individual effective dose: 0.0077 mSv

Release category RC-E3 (corresponds to the fall and subsequent break-up of a fuel element in transit under water):

Mean annual frequency: 3.0 10^{-3}/yr

Maximum individual effective dose: 0.00053 mSv

Release category RC-G1 (corresponds to the melting during irradiation of one U-Mo irradiation rig containing 3 targets):

Mean annual frequency: 1.2 10^{-5}/yr

Maximum individual effective dose: 0.0056 mSv

Release category RC-G2-FRPS (corresponds to the melting during irradiation of all twelve U-Mo irradiation rigs containing, in total, 36 targets):

Mean annual frequency: 7.2 10^{-5}/yr

Maximum individual effective dose: 0.0677 mSv

Release category RC-G3-RMI (corresponds to the melting in air of one U-Mo irradiation rig containing 3 targets):

Mean annual frequency: 6.9 10^{-5}/yr

Maximum individual effective dose: 0.0127 mSv

These values (with their 5% and 95% uncertainty bands) have been indicated in Figure 16.20/1. The mean core damage frequency shown on this graph includes seismic hazard up to SL-2. For clarity the sum of the frequencies in each dose band is not shown. There are at most, only two potential release categories in each band, so it can be seen that all of them fall below the regulatory safety objectives.

16.20.5 Conclusions

The PSA performed during the detail engineering stage for the Reactor has produced an estimate of the Core Damage Frequency and overall risk associated with the Reactor.

The assessed CDF of 1.7 10^{-7}/year for internal events, external events and seismic events up to SL-2 level compares well with the regulatory requirement of 1.0 10^{-4}/year.

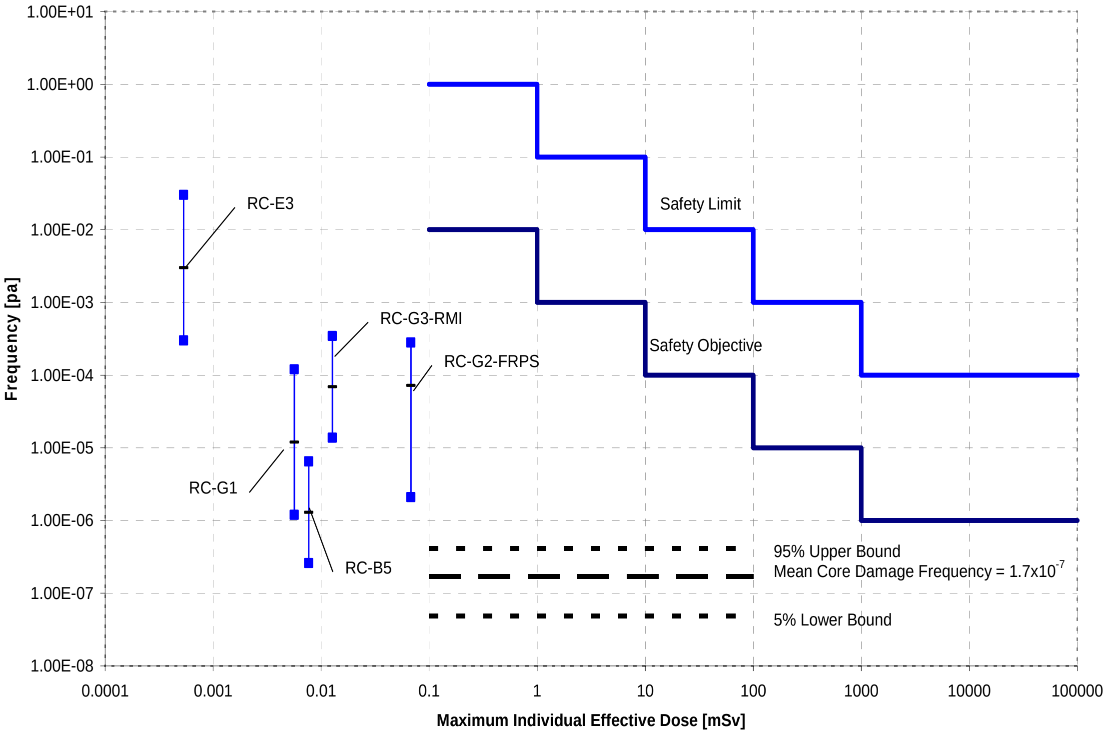
The estimated CDF of 3.8 10^{-7}/year for extreme seismic events indicates that even under these unexpected scenarios, the risk is low.

The representative accident scenarios for the Reactor do not involve significant core damage, being dominated by accidents occurring to the irradiation rigs. They pose very small risks to the surrounding population that meet the most stringent regulatory acceptance criteria.

The overall risk to the population in the vicinity of the LHSTC derived from the operation of the Reactor is sufficiently low that no need for external intervention (eg sheltering or evacuation) is necessary.

End of Section

Figure 16.20/1 Probabilistic Safety Assessment Results and Comparison to Safety Limits and Objectives



End of Figures

16.21 COMPARISON OF INCIDENTS THAT HAVE OCURRED IN OTHER POOL TYPE REACTORS AGAINST THE REPLACEMENT RESEARCH REACTOR DESIGN

16.21.1 Introduction

The objective of this Section is to review those incidents that have occurred in Pool Type Research Reactors around the world, consider their root causes and either show that the event is not applicable to the Reactor design or that it would adequately cope with the event.

The analysis applies to the behaviour of the core, PCS, FSS, CRDs and SSS.

The descriptions of the incidents have been obtained from IAEA TECDOC “Experience with Research Reactor Incidents”, 1995. The comparison is presented in a table format.

16.21.2 Comparison of Incidents with the Design

Reactor	Incident	Root Cause	RRR Design Provision
ISIS, Saclay, France	Reactivity insertion during experimental rig extraction. Mechanical damage to fuel assemblies. Dose to operator: 0.35mSv External dose: none	Control Rods not fully inserted; erroneous reading of control rod position.	RPSs’ power reading from neutron flux measurement and not from rod position. Rod position detector indicates effectiveness of FSS SSS actuates on failure of FSS.
University of Michigan Ford Research Nuclear Reactor, Michigan, USA	Removal of fuel assembly from reactor while critical.	Human error Violation of operational procedures Lack of indication of control rod position in reactor bridge.	FE cannot be removed unless reactor is shutdown.
Engineering Test Reactor, USA	Coolant flow blockage by foreign object. Spike in N16 primary water recorder, ignored due to previous erratic behaviour of monitor. Radiation alarm sounded, reactor scrammed manually. Melting of small portion of six fuel assemblies.	Clear plastic sight box used during maintenance for core observation through water left in the reactor, sunk down onto core blocking coolant flow.	Upward flow would remove any lightweight object on reactor core. Chimney grille provides protection against foreign objects falling into the core. No clear plastic objects allowed in the Reactor Hall.
Materials Testing Reactor, USA	Coolant flow blockage by rubber debris	Seal gasket of the tank floating roof deteriorated and	Incident not applicable to open pool design. No gaskets in Reactor

Reactor	Incident	Root Cause	RRR Design Provision
	Reactor at full power. Fuel assembly differential pressure monitor showed reduced difference between pitot tube total pressure and static pressure. CRD servo moved erratically. N16 detector sounded alarm. Low differential pressure trip initiated scram. Partial melting of fuel plates.	rubber debris blocked water flow to several fuel plates.	Pool. Thorough flushing of PCS during commissioning using temporary filters in pump suction pipe. Heat exchangers act as coarse filters. No gaskets downstream of heat exchanger. Lower plenum diffuser and core grid act as inlet filters to the core. Upward flow would remove any lightweight object on reactor core.
ORR, Oak Ridge, USA	Coolant flow blockage by foreign object Visual inspection of core at 6MW, no abnormal observations. Power rise. Power fluctuations at 12MW, ignored by operator. At 24MW radiation monitor of PCS sounded, Reactor scram. Maximum radiation level inside the building: 20R/hr Outside the building: 2R/hr. Radiation back to normal values 20 hr after shutdown. One of the fuel plates in a fuel assembly was partially melted	Large neoprene gasket slipped off an inner fixture in the reactor tank and lodged on top of the fuel. Fuel assembly outside the scope of viewing port.	No gaskets in Reactor Pool. Thorough flushing of PCS during commissioning using temporary filters in pump suction pipe. Heat exchangers act as coarse filters. No gaskets downstream of heat exchanger Lower plenum diffuser and core grid act as inlet filters to the Core. Upward flow would remove any lightweight object on reactor core.
Siloe, France	During overpower testing fuel plate partially melted, either due to coolant flow redistribution or a foreign object blocking coolant flow. Meltdown of 6 fuel	Presumably, a foreign object blocked several channels in the fuel assembly and disappeared later on during the accident. Could have been a	No paint or painted objects inside the reactor tank. Grille on top of the reactor chimney. Grille on top of the Reflector Vessel and

Reactor	Incident	Root Cause	RRR Design Provision
	plates. 55000Ci of fission products released into the Reactor Pool 2000Ci released to the stack within two days of the accident (most of it noble gases) No personnel irradiation. Insignificant release to the environment.	piece of dry paint peeled off the Reactor Pool walls.	irradiation rigs. Upward flow through the core would remove any lightweight object.
BR-2 Mol, Belgium	Automatic scram during power rise by high fission product contamination signal in PCS. Fuel plate partially molten. Radiation level in heat exchangers: 100R/hr, decreasing with a half life of 40 days	Screwdriver fell into reactor tank during shutdown and partially blocked coolant flow through a fuel assembly.	Protective grille on top of chimney. Upward flow through the core would remove any lightweight object. Strict administrative procedure regarding lightweight objects at Reactor Pool top Zippered and velcro'd clothes in protective clothing
University of Michigan Reactor, USA	Leak due to horizontal beam thimble break.	A long shielding plug was inserted inside the air filled thimble, which faced the Core lattice. The short thimble was ruptured and water started to rush out from the pool around the edge of the plug and onto the experimental floor.	Double barrier for pool water: thimble and metallic plate on outer face. No objects placed inside neutron beam guides.
University of Virginia Reactor, EEUU	Leak due to piping break	Separation of a screwed fitting in plastic piping in the demineraliser room.	All unions are flanged and sealed. Short stretches of piping rigidly supported. Large safety margins in piping specifications. Mechanical design and stress analysis of the PCS to ensure that it will withstand the SL-2 seismic event.

Reactor	Incident	Root Cause	RRR Design Provision
			Siphon breaker will terminate leak. Leak detectors on floor.
Texas Agricultural and Mechanics College Reactor, USA	Water flowing from tank access hole to hot sump. By the time the operator entered the Reactor Building and found the fault, the water level had dropped eight feet. Pool water had an activity of 43μCi/ml. No serious consequences resulted.	Failure of gasket in demineraliser tank access-hole from where it overflowed, letting most of the water spill onto the ground. From there it went to a dry gully.	Pool cannot be drained to demineraliser tank, only to refilling pool. Permanent connections only up to siphon breaker level No permanent connections below siphon breaker level. Drainage only through insertion of portable submersible pump into Reactor Pool. Level indicator with alarm in demineraliser tank. Leak detectors on floor.
Siloe, France	Leak at the bottom of the Reactor Pool. Operator discovered an increase in the amount of water added periodically to the pool to compensate losses due to evaporation. Contamination of underground water (max activity 170,000Bq/l of tritium)	Slight degradation of tightness at bottom of pool (pool wall made of ceramic tile joined with epoxy resin)	Stainless steel pool. Leak detectors in basement level.
Pulstrar, North Carolina State University, USA	Leak in primary coolant system, accelerated during the weekend. Leak estimated as 378 l/day (≅16 lt/hr).	Not clear in description of incident	Short stretches of piping rigidly supported. Large safety margins in piping specifications. Mechanical design and stress analysis of the PCS to ensure that it will withstand the S2 seismic event. Siphon breakers in all lines. Leak detectors on floor.

Reactor	Incident	Root Cause	RRR Design Provision
Materials Testing Reactor, Idaho Falls, USA	Overexposure due to mishandling of an activated component. Highly radioactive reactor component placed in a position where it was not adequately shielded due to lowered water level.		Radiation monitor at pool top area gives alarm when objects are moved to a height with inadequate shielding. Administrative procedures and staff training in handling of active elements.
BR-2, Mol, Belgium	Leakage of UO_2 – PuO_2 capsule in a hydraulic rabbit Burnout of a CEB-5 capsule Burnout of a UO_2 rod in a hydraulic rabbit Burnout of a UO_2 capsule in a thimble tube		Temperature measurement in pneumatic irradiation position. Indication of coolant flow. Trip signal due to unavailability of pneumatic irradiation channels cooling system. QA system for target preparation and control.
BR-2, Mol, Belgium	Tellurium capsule burnout in a thimble tube. About 10Ci of I-131 was liberated in the thimble tube, the Reactor Pool and the Reactor Building. I-131 inhalation by two operators during a transfer of the thimble tube after the incident. Doses accumulated by thyroid: 80mrem 50mrem. Release to the environment: 0.5mCi of I-131. Maximum thyroid dose to a 6 month-old infant exposed by milk consumption: 1mrem	Not available in accident description	QA System for target preparation and control. Protection of irradiation tubes by caps to prevent blockage by objects that may fall into the pool. Irradiation facilities cooled by forced flow. Temperature measurement in irradiation positions. Indication of coolant flow and shutdown requested if requirements are not met.
BR-2, Mol, Belgium	Fuel-element cladding failures. Slow increase of primary water activity	Impurity grains present in raw aluminium before rolling or introduced in the cladding during	QA of fuel fabrication process. On-line failed fuel detection.

Reactor	Incident	Root Cause	RRR Design Provision
	during fuel cycle. Periodic shutdown to check fuel assemblies; some fuel assemblies had to be rejected before attaining the burn-up allowed by specifications.	plate fabrication process.	
EWA Reactor, Poland	Several significant defects were discovered in the primary cooling system joints, including the welded joints under the reactor tank, whose rupture could lead to a LOCA	Lack of radiographic testing of welding during construction.	Inspection of welding according to QA plan during installation. Siphon breakers in all lines. Leak detection on weld lines.
EWA Reactor, Poland	Fuel assembly break during spent fuel transfer from the reactor core to the spent fuel storage pool. The transfer tool had not properly gripped one of the fuel assemblies, due to a mechanical problem, and released it during the horizontal movement of the tool. The fuel assembly fell down and broke into two parts. Total release of fission products into the pool was 1.8 10^9Ci. The accident did not cause any exposure of personnel to radiation.	Mishandling of transfer tool. Alarm went off due to poor adherence to the tool, but did not give time for any reaction.	Adequate tool design qualified by tests. Teaming of operators.
BR-2, Mol, Belgium	Over exposure of operators due to mishandling of a transport container with capsules of irradiated uranium. At a certain moment during the transport, the shielding plug of	Procedural deficiency: using two cranes simultaneously. Non adherence to written procedures.	The proposed design minimises the need to enter hot-cells on a regular basis. Health physics instrumentation located in potential risk areas. Loading of targets and

Reactor	Incident	Root Cause	RRR Design Provision
	the container was lifted.		design of transport containers based on ANSTO's 40 year experience in radioisotopes production
University of Massachusetts, Lowell, USA	Operation without one flow bypass basket installed. Operator immediately shutdown the reactor when he became aware of the condition.		Flow restriction in irradiation channels will be locked into place. U-Mo rigs design will prevent their placement into Ir positions.
Ohio State University, Columbus, Ohio, USA	Stuck shim safety rod. While attempting a normal shutdown, the operator noted that shim safety rod Nº 1 failed to scram.	Short circuit between two wires, enhanced by high air humidity. Deficient preventive maintenance programme.	Qualification of control rod drive through design analysis and control drive testing. Outcome of systematic FMEA of CRD incorporated to the design to identify potential for failure and operational errors. SSS shuts down the reactor when two or more control plates fail to reach the end of run
University of Virginia, USA	Reactor operated for approximately five hours at maximum power (2MW) with power level scrams, intermediate-range period scrams, low primary coolant flow scrams, loss of power to primary pump scram, range switch scram and key switch scram inoperable. Because of recent history of spurious automatic scrams, the senior reactor operator (SRO) interchanged two logic drawer modules while trouble shooting the RPS problem. The SRO discovered the problem when he	Interchange of two non-identical modules and non-performance of a scram operability test prior to restart of the reactor following the exchange of the modules.	Manual by-pass of RPS signals not allowed by system design.

Reactor	Incident	Root Cause	RRR Design Provision
	attempted to insert a period scram at the conclusion of the operating day.		
MNR, McMaster University, Canada	A power excursion, which caused a reactor trip on overpower, occurred during refuelling. After the replacement of a shim rod, the fuel assembles were being returned to the core. After loading the fifth fuel assembly, the shim safety rods were withdrawn to verify that the reactor was not critical. The rods were then driven to the 85% withdrawn position instead of the required 40% (safeguard position). On insertion of the sixth fuel assembly, a blue glow was seen and the reactor tripped on overpower. The Log N trip had been bypassed to avoid spurious trip. No personal injuries or equipment/fuel damage occurred.	Violation of core change policies and procedures. Inadequate review of procedures. Failure to consider the hazards and potential consequences of the work. Violation breached licence condition.	Refuelling with fully inserted safety absorbers. Maintenance operations of performed with drained Reflector Vessel. Strict operating procedures.

16.21.3 Conclusions

The Reactor has sufficient and adequate design provisions to prevent, avoid and protect the facility against all the initiating events collected in the IAEA database.

End of Section

16.22 CONCLUSIONS

This chapter of the SAR has presented the safety analysis for the Reactor. It has assessed a comprehensive range of postulated initiating events in order to determine those applicable to the design of the Reactor. It has shown that:

1. The inherent safety features and robust design are very effective in preventing accidents and in mitigating the impact of any failures of plant systems.
2. No credible external event has the potential to affect the safety of the Reactor Facility.
3. The plant will safely shutdown, even for very severe seismic events with a return period of once in 10,000 years and beyond.
4. For all design basis initiating events, no significant core damage occurs to the Reactor and the plant is safely shutdown.
5. For irradiation rig design basis accidents, the consequences of failures are either benign or minor.
6. The occurrence of a ‘fast LOCA’ leading to uncovery of the core is not credible owing to the high quality of the design and many design provisions.
7. The reactor safety system performance exceeds all regulatory requirements for reliability.
8. Even for those accidents that are so unlikely as to render them beyond the design basis, the consequences are sufficiently minor as to not require any off-site response or any off-site countermeasures.
9. For those beyond design basis accidents that can potentially damage the core, the analysis has shown that their total likelihood is over two orders of magnitude below the regulatory limit.

It is concluded that the Reactor meets all regulatory safety requirements and presents a minimal risk to the operators and the surrounding population.

Specific points worth noting include;

- Operator action is not required in any transient to ensure safe shutdown.
- The reliability of the FRPS renders the failure to shutdown the reactor with the FSS very unlikely.
- The two independent shutdown systems ensure that failure to shutdown the reactor is not credible.
- The pool is capable of being cooled by natural circulation without operator intervention for over 10 days before requiring coolant make-up.
- The reactor is capable of coping with a full break in the main PCS line.
- The passive siphon breakers ensure the cessation of any pipework leak.
- The reactor can cope with the most severe losses of flow in the PCS and RSPCS with no damage to the fuel or rigs.
- Design provisions render core blockage not credible.
- Design provisions and administrative procedures regarding handling of objects at the Reactor Pool top render blockage of an irradiation position very unlikely.

- Reactivity insertion transients are moderate.
- Failure of the Cold Neutron Source does not affect the reactor core.
- The reactor can cope with the continuous extraction of a control plate during reactor start up with failure of the First Shutdown System.
- Losses of heat sink lead to benign transients with no adverse impact on the core or rigs.

End of Section