To: Collins, NRR
cys: EDO
DEDMRS
DEDR
DEDM
AO
RES
ACRS 1P

OFFICE OF THE SECRETARY
CORRESPONDENCE CONTROL TICKET

Date Printed: Jul 08, 2003 17:06

PAPER NUMBER:	LTR-03-0440	**LOGGING DATE:**	07/08/2003
ACTION OFFICE:	EDO		
AUTHOR:	John Polcyn		
AFFILIATION:	MD		
ADDRESSEE:	Nils Diaz		
SUBJECT:	Safety characteristics of the advanced CANDU reactor design ACR-700		
ACTION:	Appropriate		
DISTRIBUTION:	RF, ACRS, OIP...Encls to: EDO		
LETTER DATE:	07/07/2003		
ACKNOWLEDGED	No		
SPECIAL HANDLING:			
NOTES:	OCM #3248		
FILE LOCATION:	Adams		
DATE DUE:		**DATE SIGNED:**	

Template: SECY-017

E-RIDS: SECY-01

3248

AECL
TECHNOLOGIES INC.

CHAIRMAN REC'D
03 JUL -8 PM 3:16

July 07, 2003

Our File: 108US-013210-021-001
Your File: Project No. 722

The Honorable Nils J. Diaz, Chairman
U.S. Nuclear Regulatory Commission,
Washington, D.C. 20555

Dear Chairman Diaz:

AECL is engaged with the NRC in the pre-application review of the ACR-700 nuclear plant design with a targeted completion of late summer 2004. AECL, through AECL Technologies, intends to submit an application for Standard Design Certification (SDC) for the ACR-700 in late 2004. AECL believes that the introduction of the ACR-700 to the United States will greatly enhance the competitive choices available to American utilities for safe, cost-effective, future nuclear power generation.

The timely introduction of the ACR-700 to the US hinges on NRC's success in efficiently and rationally applying U.S. regulations developed for light water reactors to a different type of reactor design, grounded in a pressure tube technology, whose maturity and safety have been demonstrated by the successful operation of CANDU-type reactors in seven countries throughout the world encompassing over 450 reactor-years of operations. While there are a number of differences in the regulatory requirements, the basic approach to nuclear safety in both the United States and Canada is the same. Significant progress in understanding the technical and regulatory bases of ACR safety is occurring through the co-operative discussions currently being held between the NRC and the Canadian Nuclear Safety Commission (CNSC). We appreciate the openness shown by the NRC to work with the CNSC in this regard.

To highlight the similarity in approach to nuclear safety and to introduce the safety characteristics of the ACR-700 to the Commissioners, the ACRS and the senior NRC staff, AECL requested an overview report from two former senior regulators with broad experience: Dr. Kenneth Rogers, former NRC Commissioner, and Mr. John Waddington, former Director-General of the CNSC. AECL asked them to summarize the safety of the ACR-700 at a level which would be useful to senior regulators in both countries. Their report, entitled "Safety Characteristics of the Advanced CANDU Reactor Design ACR-700", is attached for your information. I believe the report will prove a useful overview for your future deliberations on the ACR-700.

481 North Frederick Avenue, Suite 405, Gaithersburg, MD, 20877 U.S.A., Tel. 301-228-8240, Fax. 301-417-0746

AECL
TECHNOLOGIES INC.

If you have any questions on this letter and/or the enclosed report please contact either of us at 301-228-8409, and (905) 823-9060 extension 2005, respectively.

Yours sincerely,

John Polcyn
President
AECL Technologies, Inc.

Dr. Ken Hedges
Vice President
AECL – ACR Business Unit

cc.

E. McGaffigan, Jr. (USNRC)
J. Merrifield (USNRC)
W. Travers (USNRC)
S. Collins (USNRC)
A. Thadani (USNRC)
W. Borchardt (USNRC)
J. Lyons (USNRC)
M. Gamberoni (USNRC)
B. Sosa (USNRC) – 20 copies
ACRS Secretariat
L. Keen (CNSC)
K. Pereira (CNSC)
J. Blyth (CNSC)
I. Grant (CNSC)

481 North Frederick Avenue, Suite 405, Gaithersburg, MD, 20877 U.S.A., Tel. 301-228-8240, Fax. 301-417-0746

Safety Characteristics of the Advanced CANDU Reactor Design ACR-700™

J.G. Waddington & K.C. Rogers
June 2003

SAFETY CHARACTERISTICS

OF THE ADVANCED

CANDU REACTOR DESIGN

ACR-700

J.G. Waddington and K.C. Rogers

June 2003

This paper was prepared by J.G. Waddington and K.C. Rogers at the request of Atomic Energy of Canada Ltd. J.G. Waddington was a Director General of the Canadian Nuclear Safety Commission (formerly the Atomic Energy Control Board) from 1991 to 2002. Dr K.C. Rogers was a Commissioner of the United States Nuclear Regulatory Commission from 1987 to 1997.

PREFACE

This report has been prepared as an introduction to the Advanced CANDU Reactor (ACR™-700) design for use by professionals familiar with conventional pressurized light water reactors, but unfamiliar with a pressure tube reactor which uses heavy water for moderation, light water for heat removal and which refuels on-power.

It describes the main features of the ACR™*, how they have evolved from operational and design experience derived from the fleet of CANDU reactors over more than three decades, and how they relate to the safety and security of a functioning reactor. It also describes those safety characteristics of the reactor which are significantly different from those seen in PWRs, and discusses briefly the safety principles that have been developed in Canada to deal with them.

The terminology used in the report has been chosen to be as close as possible to that employed by the U.S. Nuclear Regulatory Commission. However, there are some aspects of the reactor that are not well described with that language. The report seeks to identify these and provide helpful clarification for readers accustomed to U.S. technical and regulatory terminology.

The report focuses on design issues related to operational safety. By intent, it does not discuss comparative costs or economics.

The report aims to provide the reader with a broad overview of the ACR together with sufficient technical detail to illustrate the design from the standpoint of public health, safety and protection of the environment.

---

* ACR™ (Advanced CANDU Reactor™) is a trademark of Atomic Energy of Canada Limited (AECL).

TABLE OF CONTENTS

SECTION		PAGE
1.	GENERAL DESCRIPTION	1-1
1.1	Historical Evolution and Design Intent	1-1
1.2	Overall Plant Layout	1-1
1.3	The Reactor and Moderator	1-2
1.4	CANFLEX® Fuel	1-3
1.5	Reactor Coolant System	1-3
1.6	Shutdown Systems	1-3
1.7	Emergency Core Cooling	1-4
1.8	On-power Refuelling	1-4
1.9	Reactivity Control	1-4
1.10	Electrical Distribution System	1-5
1.11	Instrumentation and Control Systems	1-5
1.12	Earthquakes and Tornados	1-5
1.13	Exclusion Zone	1-6
2.	SAFETY DESIGN PRINCIPLES	2-1
2.1	Potential Failures of the Plant	2-1
2.2	Safety Goals	2-1
2.3	Void Coefficient of Reactivity	2-1
2.4	Power Coefficient of Reactivity	2-1
2.5	Control Rod Ejection	2-1
2.6	Safety Margins	2-2
2.7	Response to Upset Conditions	2-2
2.8	Incorporation of Past Experience	2-2
3.	DEFENSE IN DEPTH, REDUNDANCY AND RELIABILITY	3-1
3.1	Separation of Process and Safety Systems	3-1
3.2	Reference dose limits.	3-1
3.3	Use of Serious Accidents in Plant Design	3-2
3.4	Two Shutdown Systems	3-2
3.5	Computer Controlled Shutdown	3-3
3.6	Reliability of Shutdown System Software	3-3
3.7	Safety System Reliability	3-3
3.8	General Reliability Principles	3-4
3.9	Use of Independent Lines of Defense	3-4
3.10	System "Divisions"	3-4
3.11	Emergency Power	3-4
3.12	Fourth Line of Defense	3-5
4.	PRESSURE BOUNDARY DESIGN	4-1
4.1	Natural circulation	4-1
4.2	Horizontal Pressure Tubes	4-1

TABLE OF CONTENTS

SECTION		PAGE
4.3	Annulus Gas System	4-2
4.4	Rolled Joints	4-2
4.5	Feeders	4-2
4.6	Feeder Weld Integrity	4-2
4.7	Reactor Coolant System Headers	4-3
5.	CANFLEX FUEL	5-1
5.1	Fuel Bundles	5-1
5.2	Critical Heat Flux	5-1
6.	ON-POWER REFUELLING	6-1
6.1	Reactivity Holdup	6-1
6.2	Reactor Coolant System Integrity	6-1
6.3	Defective Fuel	6-1
7.	OPERATIONAL CONSIDERATIONS	7-1
7.1	Reactor Control	7-1
7.2	Transient Physics Behaviour	7-1
7.3	Start-up Time for Emergency Power	7-1
7.4	External Electrical Supply System Vulnerabilities	7-1
7.5	Human Factors Principles	7-1
7.6	Quality Assurance	7-2
8.	SAFETY ANALYSIS	8-1
8.1	Analyzed Events	8-1
8.2	Large Loss of Coolant Accidents	8-3
8.3	Small Loss of Coolant Accidents	8-3
8.4	Single Channel Flow Blockage	8-3
8.5	Pressure Tube Failures	8-4
8.6	Emergency Core Cooling	8-4
8.7	LOCA Plus LOECC	8-4
8.8	Fuelling Machine Failures	8-5
8.9	Containment Failures	8-5
8.10	Loss of Reactivity Control	8-6
8.11	Loss of Heat Sinks	8-6
8.12	Earthquakes	8-6
8.13	Operator Action	8-6
8.14	Post Accident Management	8-6
9.	SERIOUS CHALLENGES	9-1
9.1	Severe Accidents (Severe Core Damage Accidents)	9-1
9.2	Loss of Offsite Power and Station Blackout	9-1
9.3	Passive Heat Removal	9-2

TABLE OF CONTENTS

SECTION		PAGE
9.4	Offsite Considerations and Source Term	9-2
10.	PROBABILISTIC RISK ASSESSMENT	10-1
11.	SUPPORTING RESEARCH AND COMPUTATIONAL PROGRAMS	11-1
11.1	Computer Models and Codes	11-1
11.2	Audit Codes	11-1
12.	SAFEGUARDS AND SECURITY	12-1
12.1	Safeguards and Proliferation Resistance	12-1
12.2	Security	12-1
13.	INSPECTIONS AND TESTS	13-1
14.	REFERENCES	14-1

APPENDICES

Appendix A	Identification and Classification of Failures	A-1

TABLES

Table A-1	Classification of Events	A-2
Table A-2	Event Class Probability Ranges	A-3
Table A-3	Reference Dose Limits	A-4

FIGURES

Figure 1-1	ACR-700 Overall Plant Flow Diagram	I-1
Figure 1-2	Nuclear Steam Systems	I-2
Figure 2-1	ACR Two-unit Plant Layout	I-3
Figure 2-2	Reactor Building Section	I-4
Figure 3-1	Fuel Channel Components	I-5
Figure 3-2	ACR Calandria & Shield Tank Assembly	I-6
Figure 3-3	Moderator	I-7
Figure 3-4	Reactor	I-8

TABLE OF CONTENTS

SECTION		PAGE
Figure 3-5	ACR-700 Reactivity Control Units	I-9
Figure 4-1	CANFLEX Fuel	I-10
Figure 4-2	CANDU Fuel Components	I-11
Figure 4-3	CANFLEX Bundle	I-12
Figure 5-1	Reactor Coolant System	I-13
Figure 5-2	Reactor Coolant System	I-14
Figure 6-1	Shutdown Systems	I-15
Figure 7-1	Emergency Coolant Injection System	I-16
Figure 7-2	Long Term Cooling	I-17
Figure 8-1	ACR Fuel Handling Equipment	I-18
Figure 8-2	Fuelling Machine on Reactor	I-19

1. GENERAL DESCRIPTION

1.1 Historical Evolution and Design Intent

The Advanced CANDU Reactor (ACR) is a pressurized water reactor of quite a different design concept from PWRs licensed in the U.S. It is a design that has evolved from thirty-one earlier CANDU®* reactors developed in Canada and licensed to operate in Canada and several other countries. World wide, twenty CANDU units are currently in operation, six are being refurbished, one (Qinshan 2) has gone critical and is being commissioned, and one (Cernavoda-2) is under construction. These CANDUs are pressurized water reactors using heavy water for both neutron moderation and for heat removal, and that burn natural uranium (0.72% U^{235}) UO_2 fuel. Fuel rods, arranged in bundles, are aligned horizontally within several hundred individually cooled tubes through which flows pressurized heavy water (D_2O) coolant. Each of these pressure tubes resides within a slightly larger coaxial tube (the calandria tube). These are arranged in a cylindrical array and enclosed within a large cylindrical vessel (the calandria) containing the D_2O heavy water moderator at essentially atmospheric pressure. Reactor coolant water that has passed through the core is collected and fed to steam generators similar to those in conventional light water PWRs. The balance of the plant resembles other PWRs. A fundamental feature of the CANDU design is on-power refuelling that does not require reactor shut down to remove spent fuel and introduce fresh fuel. Moreover a pressure tube (or its contained fuel) can be inspected when the reactor is shut down, without defuelling any more than the single affected channel.

The Advanced CANDU Reactor, ACR-700 design is an evolution of the CANDU 6. The intent is to produce a simplified design that requires fewer people to operate and is easier and economical to maintain; that has significantly improved safety margins, lower emissions and more passive backup systems than existing CANDUs; that will operate for 60 years at an average capacity factor of 90% with one major refurbishment at 30 years, and that can be built in 48 months for a repeat unit at a capital cost that is competitive with a natural gas fuelled plant. The ACR replaces the heavy water coolant in previous CANDUs with light water, replaces the natural uranium fuel with slightly enriched (~2.1% U^{235}) uranium fuel and modifies the core to produce overall operating improvements. The improvements have been based on more than three decades of operating experience and the use of PRA in design. Improvements also include increased thermal margins, no overpower transients in a loss of coolant accident and enhanced reactor stability. Each ACR unit is designed to provide a nominal gross output power of 731 MWe with a net output of approximately 680 MWe. The overall plant flow diagram and nuclear system are shown in Figures 1-1 and 1-2.

1.2 Overall Plant Layout

The ACR-700 is intended to be one of a matched pair of reactors at a plant site as shown in Figure 2-1. The reactor building and reactor auxiliary building, which are seismically qualified, house the nuclear steam plant, safety systems and the majority of the safety related systems. The main steam safety valves and isolation valves are located in a seismically qualified and protected enclosure in the top of the reactor auxiliary building. The safety support systems are located in

---

* CANDU® (CANada Deuterium Uranium) is a registered trademark of Atomic Energy of Canada Limited (AECL).

the reactor auxiliary building, the raw water system (RWS) pump house, and in the main control building. Areas housing the safety support systems and all essential equipment within them are seismically qualified, and protected against external events. The plant layout minimizes the potential for common cause events that could impact both units at the same time. It further ensures that either or both units can be safely shut down for such events. For each unit, two (redundant) divisions of safety support systems are located in physically separated areas. The main control room, located in the main control building, is shared between two units. A secure route is provided for the operator to move from the main control room to the seismically qualified secondary control building, located remotely from the main control and reactor auxiliary buildings, should an event occur that causes a loss of operability or habitability of the main control room.

Each reactor is enclosed within a dry steel-lined prestressed concrete containment structure (Figure 2-2).

1.3 The Reactor and Moderator

The reactor core contains 284 horizontal fuel channels approximately 20 feet long. For neutron economy, the portions of the fuel channel and the supports for the reactivity control devices inside the calandria vessel are made out of zirconium materials. Each fuel channel consists of a Zircaloy-4 calandria tube 6.14" (156 mm) outside diameter surrounding a pressure tube of 4.36" (117.05 mm) outside diameter made from extruded, cold-worked Zr-2.5 wt% Nb seamless tubing. CO_2 gas flows through the 0.67" (17 mm) annular gap between the pressure and calandria tubes. Twelve fuel bundles, each 19.24" long, are located within each horizontal pressure tube and held in place with removable shield plugs. At each end of the pressure tube is a steel end fitting to which the feeders that provide cooling water to the channel are welded. The end fittings are sealed to the calandria tubes by a bellows to contain the gas in the annular gap. The end fittings also allow the refuelling machines to connect to the channel. Figure 3-1 illustrates the main fuel channel components.

The calandria tubes that surround the pressure tubes are immersed in a steel tank (the calandria) 17.2' (5250 mm) in diameter, which is filled with heavy water that acts as a neutron moderator and reflector. The calandria in turn is enclosed within a 32.7' (9966 mm) diameter shield tank filled with light water. The D_2O in the moderator removes 5% of the heat generated in normal operation (from neutron moderation, heat transferred to the calandria tubes from the pressure tubes, and heat transferred from reactor structures), through its own circulation and heat exchanger system. The moderator is also used to disperse chemicals to control reactivity in the reactor core or shut down the reactor, and serves as a back up heat sink following severe accidents. The shield tank, which also has its own circulation and heat exchanger system, provides thermal and biological shielding, and serves as an additional back up heat sink following severe accidents. All reactivity control devices function within the moderator. Figure 3-2 illustrates the calandria and shield tank assembly. Figures 3-3, 3-4 and 3-5 illustrate the moderator and reactor components.

1.4 CANFLEX®* Fuel

In refuelling, two fuel bundles are introduced into the core through the upstream end of the fuel channel, and two spent fuel bundles are withdrawn from the opposite end of the channel. Each CANFLEX fuel bundle contains 43 fuel rods 19.24" long assembled between end plates to form the fuel bundle. Forty-two rods contain ~2.1 wt% U_{235} while the central rod is natural uranium plus a small percentage of dysprosium, a burnable neutron absorber. This combination gives the core its small negative void coefficient of reactivity. Depending on its position in the bundle, each fuel rod contains either 45 or 30 UO_2 high-density fuel pellets within a Zircaloy-4 tube cladding 0.016" thick. To reduce neutron absorption, the sheaths are thin. This also allows the cladding to collapse onto the surface of the pellet under the force of the 12.5 MPa reactor coolant pressure. This improves heat transfer. A graphite coating is applied to the inside of the cladding as a protection against failures arising from power manoeuvring ramps and fission product damage. A cross section of a fuel bundle is shown in Figure 4-1 and fuel bundle assemblies in Figures 4-2 and 4-3.

Fuel burn-up is projected to be in the range of 20,000 MWd/T. Typically PWR fuel burn-up is 50,000 MWd/T or greater.

1.5 Reactor Coolant System

The major components of the reactor cooling system are arranged with one steam generator and two pumps at each end of the core. Reactor coolant flows through half the fuel channels and feeders to an outlet header, through one steam generator and two pumps. It returns to the core through an inlet header to the other half of the fuel channels in which flow is in the opposite direction. The coolant then flows to an outlet header at the other end of the core, the second steam generator and the other two pumps and back to the first inlet header to complete the circuit. The system thus forms a single figure of eight loop. Steam generators are located above the headers to promote removal of decay heat by natural circulation. There are no large pipes at or below the core level, and no valves in the reactor coolant system flow loop. The system is designed to permit rapid power manoeuvring (0 to 100% power within 8 minutes) and heat up or cool down (5 deg F/minute). Figures 5-1 and 5-2 illustrate the reactor coolant system.

1.6 Shutdown Systems

The reactivity control devices operate within the low pressure moderator. Their mechanisms do not penetrate the high pressure reactor coolant system pressure boundary, and hence are not subject to large pressure differentials. Control or shutoff rod ejection from the core by reactor coolant pressure is not possible.

There are two fully independent shutdown systems. SDS1 drops 20 shutoff rods into the core under gravity on a reactor trip signal, inserting -50 mk of reactivity in ~2 seconds. SDS2 injects a gadolinium nitrate solution into the moderator from pressurized accumulators through nozzles traversing the calandria in the upper and lower reflector regions. SDS2 is also designed to inject -50 mk of reactivity in ~2 seconds, to a total of -150 mk of reactivity as mixing progresses,

---

* CANFLEX® is a registered trademark of AECL and the Korea Atomic Energy Research Institute (KAERI)

which keeps the reactor shut down under any circumstance. The shut down systems layouts are illustrated in Figure 6-1.

1.7 Emergency Core Cooling

Emergency core cooling after a loss of coolant accident (LOCA) is also performed by two separate systems; emergency coolant injection (ECI) and long term cooling (LTC).

The ECI operates through the passive injection of high pressure cooling water from large pressurized accumulators into the two reactor inlet headers, following the opening of a one-way rupture disk at a differential pressure in the forward direction of less than 75 psi (0.52 MPa). Just prior to this, the two outlet headers are interconnected to assist in establishing an effective cooling path through all the channels in the core in the event of an inlet header break. ECI actuation is designed to meet a minimum availability target of 0.999. The emergency coolant injection system is shown in Figure 7-1.

LTC provides fuel cooling in the recovery stage of a LOCA and also removes long-term decay heat for all conditions when the reactor coolant pressure boundary is intact. It has two redundant divisions located in separate areas of the reactor auxiliary building. LTC pumps are supplied with power from the seismically qualified Class III electrical system described in Section 1.10.

The LTC system also provides the shutdown cooling after a normal shutdown. The long term cooling system is shown in Figure 7-2.

1.8 On-power Refuelling

On-power fuelling is carried out remotely by two fuelling machines which act in tandem at opposite ends of the reactor core. On-power fuelling is used to keep the reactor critical and controls the global power distribution in the reactor core and the fuel discharge burn up. It also allows on-power removal of defective fuel and (when the reactor is shut down) pressure tube inspection. Since the coolant flow in adjacent channels is in opposite directions, adjacent channels are also fuelled in opposite directions to maintain a uniform neutron flux throughout the core. When the loading and unloading operation is completed, the downstream fuelling machine travels to its spent fuel port and discharges its bundles. The typical fuelling scheme consists of changing two of the twelve bundles in each channel and on average twenty-one channels each week. This requires 4 hours/day fuelling if done every day, or 6 hours/day if performed 4 days per week. The fuelling machines incorporate many years of experience and improvement in their latest design. Figure 8-1 shows the ACR fuel handling equipment, and Figure 8-2 is a photograph of the fuelling machine on reactor. Note that the feeders are hidden from view behind the thermal shield cabinets which cover the reactor face.

1.9 Reactivity Control

The ACR core is characterized by moderate negative reactivity feedback coefficients and simplified active control.

The fuel and moderator design results in an inherent characteristic of a long (0.33 millisecond) prompt neutron lifetime relative to LWRs so that the rate of rise of power following a change in reactivity is relatively slow. The void coefficient is the only source of fast reactivity change. It is small and negative. The small absolute value reduces the requirements on shutdown system

speed. With light water reactor coolant and heavy water in the calandria, the ACR core lattice is slightly under-moderated.

Reactivity control in normal operation and upset conditions is carried out by two types of devices. Normal operation is controlled by nine control rod assemblies. Each assembly consists of two independently adjustable control rod segments. In upset conditions, four separate control absorber rods, normally held out of the core, are used; they can be driven (setback) or dropped (step back) into the core to reduce power automatically should a plant transient occur. The nine control rods and four control absorbers are separate from the rods used in SDS1. The negative void and fuel temperature reactivity coefficients make the core stable and make routine reactivity control simple.

1.10 Electrical Distribution System

The electrical distribution system is divided into four classes of power. Class IV provides AC power for normal operation of the plant, and all non-safety related loads. The main coolant pumps, feed water pumps and condenser pumps are examples of loads powered by this system. Class IV receives power from the turbine generator or the grid. The loads on this system can tolerate long-term interruption of power without endangering safety. The system is divided into two independent, redundant divisions to improve reliability.

Safety related loads are provided by Classes III, II and I. Class III power supplies all those AC loads that can be interrupted for a short period, such as the pumps providing cooling water to safety related heat exchangers. During normal operation, Class III draws its power from the Class IV system. In emergencies, Class III is powered by the standby diesel generators. Class II supplies AC power to those safety related loads that should not be interrupted. Class I supplies DC power to safety related, uninterruptible loads such as instrumentation. It is backed up by batteries, and through inverters, supplies Class II in the event of an emergency. Class III is divided into two independent, redundant divisions. Class II and I each have three independent divisions, supporting the triplicated instrumentation and two-out-of three-trip logic. Classes I, II, and III are seismically qualified. For increased reliability, Class III can be cross-connected from one reactor unit to the other.

1.11 Instrumentation and Control Systems

The control and monitoring systems apply modern distributed digital control, display, and network communication technologies. The distributed control system and plant display system significantly reduce the need for relay logic and analog control loops, commonly used in older plants. This simplification also improves reliability and improves the operator/system interface, thus reducing the frequency of operator error. Improved information and data communications systems facilitate awareness of the operational state of the plant and detection and diagnosis of faults. Safety systems generally use separate instrumentation from the process systems which is different from PWR practice.

1.12 Earthquakes and Tornados

The design basis earthquake has a peak horizontal acceleration of 0.3 g. The layout and structures are designed to accommodate tornados up to level F5 on the Fujita scale as defined in USNRC Regulatory Guide 1.76.

1.13 Exclusion Zone

Provision is made in the plant design for an exclusion zone of 500 m radius.

2. SAFETY DESIGN PRINCIPLES

2.1 Potential Failures of the Plant

In Canadian safety practice, the designer identifies all the potential failure modes of the plant that could lead to the release of fission products from the fuel through a formal, systematic design review of all plant systems. The review uses, amongst other techniques, Probabilistic Risk Assessment and the review of 470 unit years of operating experience from 31 CANDU plants, and looks at multiple system failures as well as failures of single components. A preliminary systematic review has been performed for the ACR design and a set of 74 initiating events at full power and 6 events from the shutdown state has been derived from the preliminary review. Design Basis Accidents are then derived from this set. The process is discussed further in Section 8.

2.2 Safety Goals

The ACR is designed to meet the USNRC Safety Goals of a probability per reactor year of 10^{-5} for severe core damage, and 10^{-6} for a large release of radioactivity to the environment.

2.3 Void Coefficient of Reactivity

The ACR is designed to have a small, negative coolant void reactivity (CVR) in order to give the core inherent power reduction characteristics in the event of a loss of coolant accident (LOCA). Coolant void reactivity is a combined effect resulting from a loss of neutron absorption which increases reactivity, and a loss of moderation which decreases reactivity. The net effect is negative in the ACR core, and the reactor immediately begins to shutdown following a LOCA.

The magnitude of the reactivity that arises from the voidage of a full core (CVR) is about -7.2 mk. In normal operation there is a small amount of coolant boiling at the exit of each channel. The small absolute value of the CVR means that for accidents which could collapse this void (e.g. steam main break), the potential positive reactivity insertion is quite small also.

2.4 Power Coefficient of Reactivity

The ACR is designed to have a negative power coefficient of reactivity to give an inherently stable core and easily controllable neutron flux, and to minimize the number of reactivity control devices necessary.

The spacing between the individual pressure tubes and the annular gap between each pressure tube and its calandria tube have been chosen to give a power coefficient of reactivity that results in an reactivity increase of about 8 mk as the reactor changes from zero to 100% power. Incipient oscillations in the neutron flux are inherently self-correcting with this value. Nine control rod assemblies are provided to control the fission reaction in normal operation, supplemented as noted previously by four control absorbers to reduce power in upset conditions.

2.5 Control Rod Ejection

Reactivity control devices are mounted in low pressure areas of the core, outside of the reactor coolant system, to avoid forces that could accidentally eject them.

All control and shutoff rods operate in the moderator, which is at slightly above atmospheric pressure. The maximum rate of withdrawal of the rods is governed by the mechanical drive, as

there are no other significant forces acting on the rods. The only interaction between reactor coolant pressure and these rods would be from the rupture of a fuel channel (i.e. failure of a pressure tube and its surrounding calandria tube). Such an event cannot eject rods. It could, however, result in limited damage to nearby control and SDS1 rods, which would not prevent either shutdown system from performing its function.

2.6 Safety Margins

Safety margins of the reactor are increased over those achieved in previous CANDU designs.

The positive void coefficient of reactivity has been replaced with a small negative coefficient; all sources of fast positive reactivity change have been removed; fast shutdown is not required following a LOCA; the reactor has negative reactivity feedback characteristics in a number of potential accident situations, including LOCA and loss of Class IV power; and failure of a fuel channel leads to shutdown because of injection of light water into the moderator.

The maximum linear heat rating of the fuel pins is about 10% less than in CANDU 6; the critical heat flux (defined in Section 5.2) has been increased by between 10 and 20%; and the rate of increase of the fuel clad temperature under fuel dry out conditions has been reduced.

Stress levels in the pressure tubes have been reduced by about 20% compared to CANDU 6; the time for an operator to respond in most accident situations (excluding multiple independent failures) has been extended to 8 hours; and additional passive heat sinks have been added.

2.7 Response to Upset Conditions

The plant is designed to respond slowly to upset conditions. The migration distance for thermalizing neutrons in heavy water is significantly longer than in light water. This gives rise to a long prompt neutron lifetime for the ACR of 3.3×10^{-4} s (a typical figure for a PWR plant is 5×10^{-5} s). Power changes following reactivity changes are therefore comparatively slow. The total thermal mass of the water in the reactor coolant system, calandria, shield tank and reserve water tank is 3254 metric tons. (Figures 5-1 and 2-2) As a result, reactor coolant system and fuel temperature transients tend to be comparatively slow to develop and boil-off times in severe accidents comparatively long.

2.8 Incorporation of Past Experience

The lessons learned from previous design and operating experience are incorporated in the ACR design in a systematic manner.

A thorough formal review of past experience has been carried out within each engineering discipline resulting in 475 feedback issues to review, and 1175 suggestions for improvement. Many design changes resulted from the process. The three most significant of these were a change in material for the lower feeders to protect against thinning of the feeder wall from erosion/corrosion; design criteria and modifications leading to a steel lined pre-stressed concrete containment design; and the provision of a passive source of make-up water to the moderator to improve the plant response to LOCA combined with a failure of the ECC system and unavailability of moderator cooling.

3. DEFENSE IN DEPTH, REDUNDANCY AND RELIABILITY

3.1 Separation of Process and Safety Systems

The ACR is designed to meet Canadian regulatory requirements for separation and independence. The Canadian Nuclear Safety Commission (CNSC) requires that the shutdown, emergency core cooling and containment systems are separate and independent from those systems that are used in normal operation (termed "process systems") and whose failure would require operation of these safety systems. These safety systems should also be independent of each other (References 1, 2, 3). These principles were developed in the 1960s to provide a defense against common mode or cross linked failures ("sneak paths"). These are likely to be the dominant failure modes when seeking to keep the probability of a large release down to around 10^{-6} per year (Reference 4). The CNSC has accepted some practical limitations to these principles, particularly where the number of devices measuring the same parameter became excessive, or where there was one type of instrument that was significantly more reliable than others. The number of these instances has been small.

3.2 Reference dose limits

"Reference dose limits" are set by the CNSC as a means of judging the adequacy of the overall design. The failures that challenge the systems important to safety (identified by the process described in Section 2.1) are grouped into five classes, based loosely on their expected probability of occurrence. A reference dose limit is set for each event by the CNSC; the lower the expected probability of occurrence of the event, the higher the reference dose limit. Deterministic safety analysis of each failure mode must predict a dose to the most critical member of the public which is less than the appropriate reference dose limit (Reference 5). If the predicted dose is greater than the reference dose limit, the engineered performance of the safety systems must be strengthened. A reference dose limit is defined therefore as a dose (to the most exposed member of the population) that the safety analysis for an event predicts will not be exceeded. Given that safety analyses are required to be very conservative, doses that might actually occur in the event of an actual accident are expected to be substantially less than those predicted.

Tables which define the five classes, the reference dose limits for each class, and a sample of the failure modes that are assigned to each class, are shown in Appendix A. The examples of failure modes in the table have been taken from Reference 5. The examples and the understanding of their likelihood that led to the assignment of a particular failure mode to one of the five classes, was based originally on a probabilistic assessment of the Darlington nuclear generating station. The reference doses were chosen by the CNSC on a "risk informed" basis in 1981. A limit of 25 rem (250 mSv) was chosen for Class 5 accidents to be consistent with the "dual failure" reference dose limit set in 1964, which was set at that time so that a risk of observable harm to a member of the public from serious accidents would be an order of magnitude lower than the risk posed by serious accidents in other conventional industrial activities. It is consistent with the figure of 25 rem used in 10 CFR 50.34 and, as with that figure, is not intended to imply that 25 rem is an acceptable limit for an emergency dose to the public under accident conditions. In CANDU plants it is used for analysis of accidents which include impairment of the ECC function, and for which the source term must be calculated, as well as for a number of other "multiple failures" such as containment impairments. This compares to US practice where ECC

impairment is implied by requiring the licensee to assume a much larger source term than would occur if the ECC was working as expected. Both the US and Canadian approaches have the effect of ensuring that a very high level of leak tightness is required of the containment design.

The limit of 0.5 rem (5 mSv) for Class 2 is the same as that for normal operation, and was set on the basis that events with this likelihood are expected to have no greater impact on the public than normal operation of the reactor. The rest of the reference doses in the table were set to reflect the principle that risk is defined as a probability multiplied by a consequence. The values in the table therefore form a coherent set of risk considerations. The values are also set to recognize "risk aversion" - that is the public's aversion to events that have the potential for high consequences, even though they are expected to be of very low probability. Hence the product of probability and consequence is smaller for higher consequence events than for lower consequence events.

3.3 Use of Serious Accidents in Plant Design

The CNSC requires that the plant must be designed to deal with all the events that appear in an agreed table of events. The events are derived by identifying those failure modes of the plant that provide the greatest challenge for each design parameter of the safety systems intended to mitigate against plant failures. Appendix A shows part of the table that was developed after the licensing of Darlington nuclear generating station to illustrate the process. A revised table of the events to be analyzed for the ACR will need to be presented to the CNSC and agreed upon by them as part of the licensing process for the ACR in Canada. The events to be analyzed for the ACR will be based on the process described in Section 2.1 and reflect the specific design of the ACR. The topic is discussed further in Section 8 on Safety analysis.

The safety systems and other systems important to safety must be designed such that the predicted dose to the public from each of the events in the table does not exceed its reference dose limit. Events in the table are not limited to the failure of a single component or system. The events in classes 4 and 5 in the table include events that will result in limited core damage. Canadian licensing practice requires a designer to not only provide an engineered defense against initiating events but also against an initiating event followed by the failure of the safety system that is designed to mitigate the effects of that initiating event. These events typically include an initiating event, together with the failure of one of either of the shutdown systems, or the ECC system, or the containment. Failure of a shutdown system is taken to mean complete failure. Failure of the ECC is taken to mean complete failure of high pressure injection. Failure of containment is taken to mean failure of any specific subsystem of containment, such as the ventilation system. The design must show that other systems will be available and capable of limiting the potential dose to the public to below the reference dose limit. This is discussed in more detail in Section 8.

3.4 Two Shutdown Systems

Recognizing that shutdown is critical in accident protection, the ACR has two fast acting shutdown systems that use diverse means of actuation, which are spatially separated, and have independent means of monitoring reactor conditions (Figure 6-1). Shutdown System 1 uses 20 mechanical rods that enter the reactor from the top. They are independent from the 4 control absorbers and 9 control rods used to control reactivity in normal operation. Shutdown System 2 uses poison injection, and enters the reactor from the side. Each shutdown system has its own

instrumentation. The result is to ensure that the probability of complete failure to shut down is extremely small (the equivalent of the USNRC requirement to consider anticipated transients without scram (ATWS).

3.5 Computer Controlled Shutdown

All trip decisions, with the exception of manual trip, are embedded in safety-critical software which is developed and tested in accordance with the most rigorous international standards, and proven in earlier designs. Each shutdown system has three separate, independent channels for the instrumentation and trip logic, and each channel has its own trip computer. The voting logic between the three channels that initiates the shutdown system is through hard wired relays. The software developed for each shutdown system uses different software design principles. The reliability has been sufficient (see below) that there is no need for hard-wired backup.

A Test Computer is also provided to improve the reliability of Shutdown System testing and reduce the probability of operator error. Monitor Computers, buffered from the trip computers, identify to the operator those component and system failures which might contribute to parameter or system unavailability.

3.6 Reliability of Shutdown System Software

Software control of the trip function has been found to give an opportunity to achieve very high reliability of more sophisticated trip algorithms than is possible with traditional hard wired systems. To realize this opportunity, however, the software controlling the shutdown systems has to have high reliability designed in from the start. There must be no "bugs" in the software that would prevent the shutdown system from operating correctly when it is required. To achieve very high reliability, a rigorous process is followed from the start to the finish of the development of the software. Formal specifications are written in mathematical terms for the requirements of the system, the software, the design of the code, and the verification of each of the steps in the development process. The software is kept simple: safety related code is separated from non-safety related code, and interactions between subroutines are minimized to maintain simplicity. Reliability of the safety critical software is demonstrated through trajectory-based random testing. This type of testing assigns a random, within range value to every input to the software, and allows the software to complete the calculation of the appropriate output, and repeats the process very many times. The executable code is tested to demonstrate conformance to the system level requirements. Software engineers working on code development are independent from those working on review and verification, and formal verification and testing is built into the process. The software for the two shutdown systems is developed by two independent teams. These principles and a high level standard have been published in References 6 and 7. Detailed standards, procedures and guides have also been developed to support them. The standards and guides are based on research and on experience, including the development and review of the shutdown software for the Darlington and Qinshan stations.

3.7 Safety System Reliability

The reliability of each shutdown system, ECC and containment must meet a value (specified by the CNSC) defined as an unavailability of 10^{-3} years/year. The value was chosen to ensure that the likelihood of a large release of radioactive material, due to an accident with failure to shutdown, was extremely low. Formal reliability analysis of each system is required at the

design stage to demonstrate the adequacy of the design, followed by tests throughout operation to demonstrate that the required reliability is being maintained.

3.8 General Reliability Principles

A recent policy by the CNSC (Reference 8) requires all systems important to safety (i.e. not just shutdown, ECC and containment) to have defined reliability targets. The designer will identify explicitly all systems important to safety, the minimum performance required from each system, and set a reliability target required of each minimum performance in order to meet the overall safety goals of the plant. Reliability targets are derived from a design-assist PRA. The ACR uses the safety goals developed by Electric Power Research Institute (EPRI) for this purpose which are consistent with the USNRC Safety Goals. The designer demonstrates by formal reliability analysis of each system that it can meet its reliability target in operation as designed. In Canada, plant owners are required to demonstrate that the reliability is maintained in operation by a combination of testing programs and by comparison of observed component failure rates and modes with those assumed in the reliability analyses.

It is expected that reliability targets for each system important to safety that are developed directly from overall safety goals will form a sound technical basis for the development of improved technical specifications to meet the expectations of Reg Guide 1.117 (Reference 9).

3.9 Use of Independent Lines of Defense

The long standing CNSC requirement to look at the effects of failure of safety systems in addition to initiating events (discussed in 3.1, 3.2, and 3.3) has had a significant effect on the design of CANDU plants. The approach has required the designer to identify specifically those systems that must operate in the event of safety system failure, and hence provide an independent third line of defense. For a loss of coolant accident, the third line of defense (assuming the ECC system has also failed) is the moderator system together with the recirculating cooling water system that cools the moderator heat exchangers. The basic geometry of the core is expected to be maintained under these conditions, with the pressure tubes sagging onto the calandria tubes to maintain a predictable path to transfer heat from the fuel to the moderator. The designation of a specific third line of defense, together with the requirement to meet a specific reliability target for the ECC system, has meant that multiple trains of ECC have not been considered necessary by the CNSC as they have been in other jurisdictions. Nevertheless, the ECC system in the ACR has two separate trains. The ECC system for the ACR-700 is also designed to meet the USNRC single failure criterion defined in 10 CFR 50 Appendix A (Reference 10).

3.10 System "Divisions"

The long term cooling system, the raw service water system, the recirculating cooling water system, and the electrical systems are replicated into two "divisions" to provide high reliability for heat sinks and electrical power. A division provides essentially the same function as a replicated "train" in other jurisdictions.

3.11 Emergency Power

Four 100% emergency diesel generators are provided for a twin-unit plant to provide the high reliability of Class III power to essential loads that is required to meet the overall safety goals The diesel generators all start automatically; the first to start is loaded. The redundant generators

will continue to run unloaded until shut down by the operator. They have the capability of supplying either reactor unit. Inter-unit ties enable a stricken reactor unit to be supplied with power from its neighbour.

Batteries provide backup electrical power to the essential safety loads on Class I and II.

3.12 Fourth Line of Defense

In addition to its roles of providing structural support to the fuel channel lattice, acting as the vessel to contain the moderator, and acting as an active heat sink as discussed in 3.9 above, the calandria, together with the shield tank, provides a passive thermal mass as a fourth line of defense. This role is discussed further in Section 9.

4. PRESSURE BOUNDARY DESIGN

4.1 Natural circulation

The basic layout of the reactor coolant system with the steam generators above the core, Figure 5-1, allows the reactor coolant system to dissipate heat through natural circulation, if all electrical power to the reactor coolant pumps fails. Tests have been carried out to confirm this capability. The tests also showed that decay heat could continue to be rejected even when the reactor coolant system had lost about 10% of its inventory.

4.2 Horizontal Pressure Tubes

The 284 horizontal tubes form the reactor coolant pressure boundary inside the core. They are made from an alloy of Zirconium and 2.5 wt% Niobium in which trace elements, particularly chlorine, copper and iron, are closely controlled. The material is recognized by the Canadian Standards Association, and standards have been developed for it which are consistent with the intent of the ASME code. It has not yet been recognized by the ASME code itself. The material has been chosen for its low neutron absorption, and its response to the mechanical, chemical and radiological environment. 150,000 years of full power operating experience of pressure tubes has been gained in CANDU plants. Since 1986, no failures have occurred in 100,000 full power pressure tube operating years.

Over the 30 year expected lifetime of the tubes, they will be subject to radiation induced creep, both diametrally and axially; the effects of hydrogen absorption; and radiation embrittlement. The weight of the fuel will also tend to make the tubes sag slightly. Diametral creep will cause the tube diameter to increase by up to 4.5%, increasing the proportion of the coolant flowing around the outside of the fuel bundle. Axial creep will lengthen the fuel channel by up to 7.3" (190 mm) over the 30 year life. One end of the channel "floats" on bearings where it is supported by the calandria vessel end shields to allow for this.

Zirconium's ability to absorb hydrogen from its surroundings can lead to embrittlement. If sufficient hydrogen is absorbed such that it exceeds the solubility limits of the zirconium, platelets of zirconium hydride will form which can lead to cracking of the material. Zr-2.5%Nb has been shown to be much less prone to these problems than other zirconium alloys. A through-life inspection program of every pressure tube is followed to ensure the material properties and behaviour of all tubes are monitored and controlled to remain within prescribed limits. The material of individual pressure tubes can be sampled without removing the tube or defuelling the core.

The pressure tube material is at reactor coolant system temperature - about 572°F (325°C). Spacers keep the outside surface of the tube at a distance of 0.67" (17 mm) from the calandria tube which surrounds it, and which is at moderator temperature of about 176°F (80°C). The annulus between the two provides thermal insulation. If the pressure tube sags into contact with the calandria tube, a "cold spot" occurs on the pressure tube, at which, over a period of time, zirconium hydride "blisters" can form and cause material cracking, which is then a potential source of tube failure. The position of the spacers is therefore important, together with the degree of tube sagging between the spacers that occur over years of operation. Formal "Fitness for Service Guidelines" have been developed to control these parameters. Periodic inspection of pressure tubes keeps track of the parameters in order to demonstrate that tubes continue to operate within their specifications and to ensure corrective action is taken if any individual tube

approaches the limit of its specifications. Corrective action can include replacing the tube. Operating CANDU reactors have replaced some tubes during the life of the reactor, and some stations have replaced all the tubes as part of a major refit. All the tubes in the ACR are expected to be replaced once to achieve a 60 year reactor lifetime.

The water chemistry of the reactor coolant system is also specified and controlled to limit the degree of hydrogen available for absorption in the pressure tubes. Pressure tubes and feeders are essentially thin walled tubes, and thermal shock is not expected to be an issue for this type of component, as it can be for thick walled pipes or vessels.

4.3 Annulus Gas System

The annulus gas system recirculates CO_2 in all the gaps between the pressure tubes and the calandria tubes, and controls the gaseous environment surrounding the pressure tubes. It is monitored for the presence of water vapour, which could indicate a leak from a pressure tube. The tube would then need to be replaced. The material properties and stress levels are such that pressure tubes are expected to leak before breaking, and a formal assessment of the critical crack length is done to check this. The overall reactor safety analysis assumes, however, that a guillotine "double-ended" break could occur. This is an "in-core LOCA" and is discussed in Paragraph 8.5.

4.4 Rolled Joints

The end fittings are attached to the pressure tube by a rolled joint, rather than by a weld between dissimilar metals. The inside of the pressure tube is rolled to squeeze tube material into three grooves on the inside surface of the end fitting. Rolling must be precisely controlled to ensure a strong leak tight joint with the correct profile of stresses in the tube material. There are over 20,000 rolled joints in use in CANDU plants around the world. Though improper rolling was a contributory factor in a small number of early fuel channel leaks, rolling techniques were corrected through design and other changes in the 1970s and early 1980s. No leaks have occurred in the rolled joints since 1982.

4.5 Feeders

Each pressure tube is attached to an inlet and outlet feeder pipe. The diameters of the feeders are sized to balance the reactor coolant flow rate of each channel to its heat output, based on the position of the channel in the core. The lower part of the feeders in the ACR is made from stainless steel to minimize flow assisted corrosion; the upper part is made of carbon steel where the feeder diameters are larger and flow assisted corrosion is not a concern. Some feeders are fitted with orifices to measure coolant mass flow. Failure of a feeder is considered in the safety analysis. It represents a small LOCA, and is discussed in Section 8.3.

4.6 Feeder Weld Integrity

There are on average seven welds in each feeder, three of which are between dissimilar metals (stainless to carbon steel, or stainless to Inconel). Two of the carbon steel to carbon steel welds in each feeder are made on-site during construction. All others are shop welds. On manufacture, all welds are volumetrically inspected using radiography and inspected for surface defects using dye penetrant. They will also be volumetrically inspected using ultrasonics to provide a baseline for in-service inspection. The close proximity of the feeders and the large number of welds

means that it is difficult to inspect many welds during operation. An in-service inspection program to meet the requirements of the Canadian standard CSA-N285 is being developed for welds that have high stresses or are dissimilar metal welds. The standard is based on the inspection of a sample of welds every 10 years. Section XI of the ASME code also requires inspection of all dissimilar and high stress welds within a 10 year period, and samples within 5 years. The code requirements are being reviewed to develop an inspection program that meets the intent of the code, and that also recognizes the practical difficulties presented by the feeder configuration.

4.7 Reactor Coolant System Headers

The feeders are welded to two inlet and two outlet headers. (Figure 5-1 and 5-2). The headers are carbon steel forgings, and are built to the ASME code for nuclear pressure vessels. A guillotine break of a header is considered in the safety analysis as a large LOCA. This is discussed further in Section 8.2. Headers have been designed for the thermal transients associated with the rapid cooling that occurs when the main steam safety valves (MSSVs) are opened to cool the reactor coolant system. The carbon steel used (SA 106 grade C) is a very malleable material, and is designed for the thermal shock arising from the rapid cooling. The water in the pressurized water accumulators that supply the emergency core cooling system is maintained at 77°F (25°C). The accumulators are located within the reactor building as shown in Figure 7-1.

5. CANFLEX FUEL

5.1 Fuel Bundles

The defect rate of CANDU fuel is 2 defects per million rods, with 2 million bundles irradiated. The CANFLEX fuel designed for the ACR is a development of the fuel used in existing CANDU reactors. The basic construction of the fuel has not changed; the end caps of CANFLEX fuel are resistance welded to the fuel cladding, the end plates are resistance welded to the end caps, and spacers (which keep the fuel rods apart) and bearing pads (which keep the rods away from the pressure tube) are brazed to the cladding in the same manner as for existing fuel (Figure 4-2 and 4-3). As with current fuel, a very thin layer of graphite covers the inside surface of the cladding. The cladding is filled with unpressurized helium and air before the end cap is welded on to improve leak testing and pellet-to-clad heat transfer. The fuel pellets are chamfered at both ends to reduce inter-pellet stresses on the fuel cladding, and dished to provide a larger volume for fission gases. The fuel bundle has been tested in existing power reactors using natural uranium, and a Design Qualification program is in progress for ACR fuel.

5.2 Critical Heat Flux

The critical heat flux from the fuel is that heat flux at which the surface of the fuel first departs from nucleate boiling- i.e., a film of steam first appears on the cladding surface. The reactor coolant of a CANDU reactor is at saturation conditions at the exit from most channels. The effects of exceeding the critical heat flux (CHF) from the fuel under these conditions are quite different from those seen in conventional PWRs. CANDU fuel responds to a critical heat flux condition in a controllable manner. The surface temperature of the fuel does not rise almost instantaneously as it does in a sub-cooled reactor such as a PWR. The fuel can dry out to some extent without significant ill effects, and dry out is predictable. A 10% increase in heat flux above critical typically produces a 50°C rise in the surface temperature of the fuel. Hence a regulatory rule requiring a Departure from Nucleate Boiling Ratio (DNBR) of 1.3 to be observed has not been necessary for licensing CANDUs in Canada and elsewhere. The limits that are used for heat flux from the fuel have been based on CHF and post dry-out research.

CANFLEX fuel has been designed with special buttons brazed to the rods at two planes to increase the turbulence in the channel and enhance the CHF and post-dryout behaviour. Additional full scale CHF tests are planned to extend the existing CHF database to ACR conditions.

6. ON-POWER REFUELLING

6.1 Reactivity Hold up

When the ACR core goes critical for the first time, the fuel has a slightly lower enrichment. After a year's operation, and on-power refuelling to compensate for reactivity depletion during that year, the distribution of fresh and burned fuel in the core has reached equilibrium conditions. Hence, the ACR will be operated at equilibrium conditions for more than 90% of its lifetime. Without refuelling, the ACR reactor will shut itself down after about 7 to 8 days of full power operation. The amount of excess reactivity in the core when the core is first loaded with fuel is about +20 mk, dropping to about +5 mk under equilibrium conditions. This is significantly less than in a typical PWR which has an excess reactivity of more than +100 mk after refuelling that is normally held down with boron in the coolant. The additional reactivity inserted by two new fuel bundles in a channel is very small (about 0.2 mk).

6.2 Reactor Coolant System Integrity

To refuel, two fuelling machines lock on to either end of the same fuel channel. One of the fuelling machines carries two new fuel bundles in its magazine. The magazine of the other machine will receive two spent bundles during the refuelling process. Both machines are pressurized to reactor coolant system pressure. Pressure seal plugs in both machines and in the two end fittings of the channel must be removed so that the fuelling machines become part of the reactor coolant system pressure boundary during the refuelling process. The fuelling machines retain the pressure boundary using passive pressure activated locks which make sure that reactor coolant pressure boundary is maintained while the fuel channel closures are removed. The fuelling machines are designed to ASME standards with special features, like the safety locks, governed by CSA standards. The basis of the channel closure design is a flexible metallic ring that makes a face seal against an edge in the end fitting. At operating pressures, the design relies on reactor coolant hydrostatic forces to assist in the sealing operation. The channel closures are locked in place by safety locks and tested for leakage each time they are reinstalled, before the fuelling machine is unlocked from the fuel channel.

There have been no failures of the reactor coolant system pressure seals in the channel end fittings in CANDU operating experience.

6.3 Defective Fuel

Fuel that becomes defective during operation is detectable, and can be removed by the fuelling machines with the reactor at power. This helps to minimize the amount of radioactive material that could be in the reactor coolant system.

7. OPERATIONAL CONSIDERATIONS

7.1 Reactor Control

As the excess reactivity hold-up in the fuel is small (about 20 mk), the reactivity worth of the devices for reactivity control can also be small. The worth of each control rod assembly is 1 mk or less, and the most reactive absorber assemblies are worth 3 mk. The reactor can be made sub-critical by the control system acting alone, without the operation of either shutdown system. The neutron flux in the core is stable, as the negative power coefficient of -8 mk (from zero to full power) is expected to self-correct any potential neutron flux oscillation from Xenon transients. Flux oscillations due to Xenon will not occur on the ACR reactor.

7.2 Transient Physics Behaviour

There are no major sources of excess reactivity in the ACR. In normal operation, the maximum rate of reactivity insertion arises from the maximum mechanical rate of withdrawal of the 4 control absorbers from the core. This is larger than that arising from the malfunction of a control rod assembly (1 mk).

Rapid cool down transients, such as a guillotine break of the main steam line, also do not introduce significant reactivity increases. As noted in Section 2.3, there is a small amount of reactor coolant boiling at the exit of each channel in normal operation. The small value of the negative void coefficient of reactivity means that if sudden collapse of the voids from this boiling should occur, the positive reactivity insertion is small also. Since the core is only slightly under-moderated, the reactivity insertion from rapidly reducing the reactor coolant system temperature is also small.

7.3 Start-up Time for Emergency Power

In a two unit ACR-700 plant, the four 100% standby generators are common to the two units. All four generators start automatically within 20 seconds following loss of Class IV (i.e. normal) electrical power, and hence failure of power to the Class III buses and their safety related loads. The first generator to start is fully loaded within 180 seconds.

7.4 External Electrical Supply System Vulnerabilities

The design of the safety related electrical power systems (Classes I, II and III) has been based on a design PRA that uses the EPRI overall Safety Goals. It assumes a grid reliability of one failure per 3 years based on Canadian experience. The design of the normal power supplies and the distribution system can also withstand the transient that would follow a complete and sudden loss of the switchyard as a result of external events.

7.5 Human Factors Principles

Human factors principles are incorporated systematically in the design of the ACR through a formal program. Few operator actions are required in the field during normal operation as testing of most safety systems is done from the control room. The control room is designed to meet modern human factors principles and the requirements of the CNSC policy on human factors (Reference 11). On-line refuelling is carried out from a separate panel in the control room and does not interfere with the control of the reactor.

7.6 Quality Assurance

The whole of the design process follows a quality assurance program and quality management principles that are outlined in Canadian standard CSA-N-286. These standards are consistent with the IAEA Safety Series on Quality Assurance (Reference 12), 10 CFR 50 Appendix B (Reference 13) and also meet ISO 9001 requirements (Reference 16).

8. SAFETY ANALYSIS

8.1 Analyzed Events

Events that are analyzed in safety analyses and are submitted to the Canadian regulator (CNSC) have evolved to recognize the specific design and safety characteristics of CANDU reactors in general. The intent of these safety analyses is the same as that for all jurisdictions; to ensure the likelihood of a large release of radioactive material to the environment is extremely low.

The safety analyses for the ACR reflect this evolution. The analyses examine four different types of event, compared with three that are considered in the United States and elsewhere. Traditional PWR safety analyses concentrate on:

1. Design basis accidents (DBAs) such as LOCA,
2. Specific licensing basis events such as source term analyses, station blackout and anticipated transients without scram, and
3. Severe core accidents.

The ACR safety analyses examine:

1. Design basis accidents (DBAs) such as LOCA,
2. "Limited core damage accidents" (LCDAs),
3. Station blackout, and
4. Severe core accidents, which are called "severe core damage accidents" (SCDAs) in ACR terminology.

The definition of a DBA for the ACR is essentially the same as that used by the USNRC, that is an initiating event that demonstrates that offsite dose requirements will be met, and the design of key engineered safety features, in particular shutdown systems, ECC and containment, is adequate. There is one significant difference in the definition used for the ACR that makes it more demanding for a designer to meet. Initiating events assume the total failure of the system or component. "Total failure" means the complete failure of the system to provide its stated function, not just the single failure of an active or passive component of the system. Initiating events cover those of moderate frequency (expected to occur several times in a plant lifetime), infrequent events (may occur once during the lifetime of a plant), and limiting faults.

The second type of events, LCDAs, are of a lower probability than DBAs, and are divided into three subsets; i) those high temperature accidents which are arrested at the channel boundary; ii) severe single channel events which could result in small quantities of molten material being released into the moderator; and iii) loss of all heat removal events, which are terminated by a few channel failures, and which then use the moderator as the heat sink.

Events in subset (i) are arrived at by assuming that a "traditional" DBA has occurred, and, in addition, one of the safety systems designed to mitigate the consequences of the DBA has also failed. An example of this is a LOCA followed by the assumption that the high-pressure emergency core injection system has also failed (LOECC). Another example is a complete loss of reactor control (LOR) followed by a complete loss of a shutdown system (LOSDS). Consideration of these types of "dual failures" in formal safety analysis ensures that an independent third line of defense is available for all DBAs. The safety analyses of these types of events recognize and utilize the capabilities of other safety related systems in the plant such as the moderator and the moderator cooling system. Subset (i) also includes events that are

equivalent to USNRC licensing basis accidents. A LOCA plus LOECC results in a large source term within containment, and LOR plus LOSDS is equivalent to a transient without scram. Given that CANDU reactors have two independent shutdown systems, events which assume the loss of a shutdown system have no consequence, as the other independent shutdown system is available to shutdown the reactor.

Events in subset (ii) are severe, very specifically defined events of low probability that involve a single channel. There are two; a single channel flow blockage of greater than 99.7%, and "feeder stagnation" break accidents. They are discussed further in Sections 8.3 and 8.4.

Events in subset (iii) are derived from probabilistic risk assessments, and are beyond design basis accidents which assume that both the primary and secondary engineered heat sinks fail. They are designed to ensure that adequate heat sinks are available as a third, independent line of defence.

Station black-out analyses are identical to those carried out in the US and are discussed further in Section 9.2.

Severe core damage accidents (SCDAs) are those events which result in widespread loss of the core and channel geometry, and are directly equivalent to severe core accidents in the US. They are discussed further in Section 9.1.

Examples of typical events that are analyzed and the reference dose limits that apply to them are given in Appendix A.

The identification of initiating events to be analyzed in the safety analysis is both formal and thorough. Events are derived from a list of potential failure modes that are identified by a systematic review of all the ways in which fission products could potentially be released from the fuel. Most of the events identified have no releases. The review, as discussed in Section 2.1, uses probabilistic risk assessment (PRA) techniques and experience from the design and operation of previous CANDU plants, and has identified 74 initiating events at full power and 6 shutdown events. The engineering specifications for the design parameters of each safety system are derived from these initiating events - usually from several of them. For example, the required ECC injection pressure is set partly by a small loss of coolant such as a break in a feeder pipe, since the rate of fall of reactor coolant system pressure is comparatively slow, and the break itself is not an adequate heat sink. The initiation time for ECC, however, is set by a large loss of coolant, such as a break in a header. For this accident, the ECC system needs to start refilling the reactor coolant loop as soon as possible. LCDA events discussed above are also analyzed in the safety analysis and, under Canadian licensing rules, must meet the reference dose limits for classes 4 and 5, as discussed in Section 3.3. LCDA events also influence engineering specifications for safety systems. For example, the ECC system must also be capable of limiting the release of fission products from the core in a large LOCA when there is a leak in the containment arising from a postulated failure to isolate properly. The containment must deal with the fission product and pressure load arising from a loss of coolant combined with failure of the emergency core cooling system (LOCA + LOECC), with the moderator providing the heat sink. The moderator must be effective under these conditions. The systems used to mitigate these low probability events may operate at higher allowable stresses and lower engineering margins than in normal operation. The Canadian regulatory process places a burden of proof on an applicant for a license to demonstrate that this process is as complete as possible.

8.2 Large Loss of Coolant Accidents

The largest postulated break in the system is assumed to be a break of one of the 19.5" (495 mm) diameter headers. The break area is assumed to be twice the cross sectional area of the header. Breaks of both the inlet and outlet headers are analyzed as the thermal hydraulic response of the core is different for the two cases. The two outlet headers are connected by a normally closed line which opens in the event of a LOCA (Figure 7-1). The line is designed to ensure good, predictable cooling of the core should one of the inlet headers break. The fuel cladding temperature is not expected to exceed 2030°F (1110°C) as a result of a large LOCA followed by ECC injection.

8.3 Small Loss of Coolant Accidents

Small LOCAs are defined as those for which the heat loss through the break itself does not provide sufficient cooling of the fuel, and for which it is necessary to depressurize the reactor coolant system by opening the main steam safety valves (MSSVs) to inject emergency core cooling water more quickly. For breaks that are up to 0.07% of the flow area of a large header break, the reactor coolant system make-up provides sufficient flow to maintain the inventory of the reactor coolant system. Analysis of small LOCAs is usually performed up to a break size of 2.5% to cover breaks in the largest feeder and postulated complete failures of a single pressure tube. In a single-channel LOCA (e.g. a feeder break or pressure tube break), fuel or cladding temperature excursions are not expected in any of the other channels of the core or in the affected one, with one exception.

A very specific feeder break size exists for which the thermal hydraulic forces in the feeder and channel result in no net flow in the channel itself. This is termed a "feeder stagnation break". In this event, fuel and cladding overheating could be severe in the affected channel and the fuel cladding and the pressure tube of that channel are expected to fail. Fuel in the rest of the core remains well cooled for both this event and feeder breaks in general. Feeder stagnation breaks are considered very low probability and are therefore in the category of Limited Core Damage Accidents (LCDA).

8.4 Single Channel Flow Blockage

If a feeder pipe becomes blocked for any reason when the reactor is operating at power, the reduction in flow could result in increasing temperatures of the fuel and the pressure tube in the affected channel. The temperature transient, and the sequence of events that could occur, depend on the extent of the blockage. For a wide range of possible blockages, (up to 98.7 %) the pressure tube will contain the fuel without failing. A number of fuel elements may fail, as the cladding of fuel may be operating at higher temperature than normal for some time. For blockages of between 98.7 % and 99.7 % of the cross sectional area (a flow reduction of between 88 % and 94 %,) the pressure tube will heat up due to heat transfer from the hot fuel, begin to lose its strength, and will strain and rupture. The calandria tube is not expected to fail. Failure of the pressure tube causes high pressure in the annulus gap (Figure 3.1) which causes the bellows at the ends of the channel to fail. The event then becomes a small LOCA, and the fuel in the affected channel regains its cooling. Blockages up to 99.7% are Design Basis Accidents (DBAs). In the worst case, (blockages >99.7%) the fuel cladding may melt before the pressure tube fails. If this occurs, the calandria tube will also likely rupture. Molten cladding and a eutectic of zirconium and uranium dioxide would then be ejected into the water of the moderator

at high pressure. The effect of ejecting a small amount of molten material into the moderator has been studied at length by the CNSC and Canadian industry. It is not expected to lead to significant further damage to the core. Experimental programs at Chalk River Nuclear Laboratories and Argonne National Laboratory are in progress to validate the expected behaviour. The program is overviewed by an international panel. A blockage of 99.7% or more is considered to be highly improbable, and this accident is considered to be a Limited Core Damage Accident (LCDA).

8.5 Pressure Tube Failures

The safety analysis assumes that a pressure tube can fail instantaneously, with an assumed break area of twice the cross sectional area of the tube. For the ACR design, the calandria tube is not expected to fail under these circumstances, and a failure of a pressure tube will not propagate to other pressure tubes. With an intact calandria tube, the two halves of a channel that has broken are retained by the fuel channel restraints fastening the end fittings to the outer wall of the end shields. The bellows at the ends of the channel that seal the gap between the pressure tube and the calandria tube will fail as a result of the pressurization of the gap, and reactor coolant will escape into the containment. The plant and the ECC system respond as for a small LOCA.

8.6 Emergency Core Cooling

On receipt of a LOCA signal, the Emergency Cooling Injection (ECI) system is initiated by opening 100% duplicated isolation valves in the line from the pressurized water accumulators to each inlet header. The water in the accumulators is kept at a pressure of 711 psig (4.9 MPa(g)) during normal operation by nitrogen gas at the top of each accumulator. One-way rupture discs in each line form part of the reactor coolant system pressure boundary during normal operation, and rupture open when the differential pressure across them exceeds about 75 psi (0.52 MPa) in the ECI to RCS direction. High pressure water then injects into each of the inlet headers. The ECI lines up to and including the injection valves are designed for full reactor coolant system pressure and temperature. The LOCA signal also opens the main steam safety valves (MSSVs) and a line that connects the two outlet headers together. Opening the MSSVs cools down the steam generators rapidly and hence depressurizes the reactor coolant system. This enhances the effectiveness of ECI. The interconnect line between the outlet headers is designed to provide good predictable cooling for inlet header breaks. Low level in an ECI accumulator initiates the associated Long Term Cooling (LTC) System by closing the ECI injection valves and opening the LTC isolation valves in that train. The LTC recirculation pumps pick up water from the containment sumps, and after cooling, re-inject it into the reactor coolant system inlet header.

Analysis of ECC performance covers a full range of potential break sizes of the reactor coolant system, in many different locations. The analysis codes used and their validation are discussed briefly in Section 11.

8.7 LOCA Plus LOECC

Under the current Canadian regulatory process, a designer is expected to analyze the effects of, and to have a specified defense for, a loss of reactor coolant followed by the complete failure of the ECC system to inject high pressure water when required. The accident is a Limited Core Damage Accident (LCDA) in class 5, and is taken account of in the design of the containment. The containment must be designed such that the dose, predicted by deterministic safety analysis,

which could be received by the most exposed member of the public as a result of this event, does not exceed 25 rem. The designer is expected to identify and assess the phenomena that would occur in the core during such a transient, including the behavior of fission products released from the fuel, and to determine the fission product inventory that would be released into containment. In Canadian licensing practice, this is used as the source term for predicting public doses with the containment operating as designed. As the steel-lined containment of the ACR has a very low leakage rate and double isolation, this requirement is expected to be met with a large margin of safety.

Should such an event occur, the reactor power will start to fall immediately as a result of the negative void coefficient. Both shutdown systems and the power reduction function of the control system are triggered. As coolant is lost from the core and not replaced, the fuel heats up from decay heat and heats up the pressure tubes. Once the pressure tubes reach about 750°C, they are expected to sag onto their calandria tubes. The timing and the number of tubes that reach high temperature is very dependant on the break size assumed, and hence on how long it takes for reactor coolant system pressure to fall and the reactor coolant system to empty. Heat is rejected from the fuel into the moderator by radiation heat transfer through the walls of the pressure and calandria tubes, and by conduction through the walls of both tubes where they are in contact. The moderator is cooled by pumped flow through the moderator heat exchangers. An extensive database of tests exists for this event sequence for current CANDUs; additional experimental tests are planned to confirm the expected behaviour of the ACR channel geometry in this accident.

This accident generates hydrogen from the chemical reaction that occurs at high temperature between steam and the zirconium in the fuel cladding and pressure tubes. The containment is fitted with passive autocatalytic hydrogen recombiners to control the concentration of hydrogen below detonation limits. Analysis, supported by experimental data, is expected to show that there are no local pockets of high concentration of hydrogen that could cause local detonation.

8.8 Fuelling Machine Failures

Postulated failures of the fuelling machines include the machines coming off a channel inadvertently, and failure of the coolant hoses when the fuelling machine is off-reactor. The first is equivalent to a small LOCA; the second can result in overheating of the bundles in the magazine. The machines are prevented from coming off a channel by mechanical passive locks to guard against a small LOCA, and the coolant hoses are fractions of an inch in diameter, with appropriate isolation, to reduce the size of potential leaks from hose failure to a very small value.

8.9 Containment Failures

The designer is required by the CNSC to examine the effects of failures of subsystems of the containment system such as the ventilation system, or the vault cooler system. The containment of the ACR is designed to have a double isolation system on the ventilation system to reduce the likelihood of failure to isolate when required. Containment's steel liner is designed to give a very low leakage rate.

The CNSC requires that a deterministic safety analysis must show that the dose predicted to be received by the most exposed member of the public should a containment subsystem failure occur will be less than 25 rem. The ACR containment is designed to meet this requirement.

8.10 Loss of Reactivity Control

The ACR safety analysis assumes that the reactor control system adjusts all reactivity devices at the maximum rate possible. It also assumes that both the power reduction functions of the control system (the setback and step back functions outlined in Section 1.9) and the first shutdown system to respond to the event have failed to operate, and the transient is brought under control by the second shutdown system reacting to the second signal that would trigger it, not the first. These requirements form part of the design bases for the shutdown systems. No fuel failures are expected in this event.

8.11 Loss of Heat Sinks

These events include loss of the steam generators through steam and feed line breaks, loss of feed water pumps, and spurious closure of feed water valves. All are analyzed to ensure there are adequate alternate heat sinks for each accident. Generally, two alternative means of cooling the fuel are provided for all Class 1 and 2 events.

8.12 Earthquakes

The ACR is designed for a safe shutdown earthquake (SSE) with a peak horizontal acceleration of 0.3 g. All the systems required to shutdown, cool, contain and monitor the reactor during and after a design basis earthquake are seismically qualified including SDS1, SDS2, the containment, and long term cooling. Both the main control room and the secondary control room are qualified, together with the instrumentation associated with essential safety functions, and the sources of electrical power or compressed air needed for their control. Batteries provide sufficient power for all these systems to operate for one hour after the earthquake. Air tanks are also sized to provide compressed air to valves and other safety loads for one hour. There is sufficient fuel onsite for the diesels to provide electrical power for seven days.

All the structures that contain seismically qualified systems are also qualified, including the reactor building, the reactor auxiliary building, the spent fuel storage bay, the diesel generator building, the RSW pump-houses, the control building and secondary control building.

8.13 Operator Action

The plant response for almost all accidents caused by a single initiating event is automatic for the first 8 hours, and operator action is not required. This does not prevent the operator from taking corrective action to deal with the cause of the event, and stabilizing the situation and hence terminating the event earlier than might otherwise be the case.

8.14 Post Accident Management

Batteries have sufficient capacity to support post accident monitoring for 8 hours, assuming there are no other sources of power available. The passive thermal mass of the moderator, shield tank and reserve water tank provides the operator with many hours to stabilize the situation. Emergency procedures will be available for operations to guide post accident management.

9. SERIOUS CHALLENGES

9.1 Severe Accidents (Severe Core Damage Accidents)

The sequence of events that would result in severe core damage and loss of predictable geometry to the ACR core is different from that for a PWR, and the nature of the corium that could be postulated is also likely to be different. For this reason, these events are called "Severe Core Damage Accidents" (SCDAS) in ACR terminology. The sequence starts as a LOCA plus LOECC as discussed in Section 8.7. This event could be expected to terminate with the moderator providing a heat sink to a core which consists of discrete pressure tubes full of fuel which have sagged onto their calandria tubes. However, if the cooling to the moderator heat exchangers is also postulated to be unavailable, a rupture disc at the top of the calandria tank will open when the moderator begins to boil, and the pressure in the calandria tank rises. The calandria is fed passively by the reserve water tank in the roof of the containment building for tens of hours. As the water in the calandria tank eventually boils off, the fuel, pressure tubes and calandria tubes would collapse slowly and progressively towards the bottom of the calandria as the water level in the calandria tank falls. The shield tank now becomes the heat sink. If nothing is done to maintain water in the shield tank (which can also be filled passively from the reserve water tank,) it too will eventually boil off. The collapsed core debris will be maintained within the shield tank as it is cooled by the water that has accumulated during the accident around the outside of the shield tank (i.e. in the reactor vault).

The full sequence of events is likely to take a considerable period of time, given that the total volume of water in the reactor coolant system, moderator, shield tank and reserve water tank that must be boiled off is over 3200 metric tons. Rapid fuel melting that could produce "lava flows" is not expected to occur.

The resulting corium debris would likely be primarily a combination of fuel and zirconium oxide from the pressure and calandria tubes with structural material added. The likelihood of a severe accident of this nature actually occurring is extremely small.

9.2 Loss of Offsite Power and Station Blackout

If both Class IV power divisions of a unit fail, offsite power is lost, all four 100% standby diesels fail to start, and the dedicated inter-unit ties between the Class III buses of the two stations also fail, a station blackout as defined by 10CFR 50.63 will result. The plant response for the first 8 hours in the event of a station blackout is automatic. Emergency feed water initiation and other valve openings do not require operator action. The plant would likely respond as follows: The reactor shuts down and the core initially cools by natural circulation with the steam generators as the heat sink. As the steam governing valves and the feed water to the steam generators are lost, (as a result of loss of electrical power), the secondary side will heat up and the main steam safety valves will open almost immediately. Once the secondary side pressure is reduced to close to atmospheric pressure, the reserve water tank near the top of the containment provides passive emergency feed water to the steam generators to maintain the heat sink for up to three days. The batteries continue to provide power for up to 8 hours to the steam generator level control. If water can be pumped into the reserve water tank from an external source as a result of operator action, this mode of cooling can continue indefinitely.

As the reactor coolant system cools, it shrinks. The water in the pressurizer is currently sized to make up the shrinkage from full power to zero power. The core will continue to cool by natural

circulation even with some void in the reactor coolant system. If the reserve water tank is not replenished, the steam generators would eventually dry out, and this heat sink would be lost. The reactor coolant system would reheat, and eventually the liquid relief valves on the system would lift. When the fuel channels start to dry out, a few pressure tubes could fail, converting the accident from a loss of heat sink at high pressure, to one at low pressure. The moderator then becomes the heat sink and, if no corrective action is taken to maintain moderator cooling, the accident progresses in the same way as for the severe core accident described in Section 9.1.

9.3 Passive Heat Removal

The layout of the plant with the steam generators above the core is conducive to natural circulation. The ability of the reactor coolant system to maintain heat rejection by natural circulation even if it has lost some of its inventory has been shown by experiment and analysis. The reserve water tank in the top of the containment is a passive emergency water source which can be used to supply the secondary side of the steam generators, the make-up system for the reactor coolant system, the moderator, and the shield tank, to maintain their capacities as heat sinks in a variety of situations.

9.4 Offsite Considerations and Source Term

The source term that has been used in previously licensed Canadian designs has been based on the results of calculations of the amount of fission products that could be released into containment in both the large LOCA, and LOCA plus LOECC analyses. Given the leak tightness of the steel lined containment, the design is also expected to accommodate the US standard source term used to calculate off-site doses defined in NUREG 1465 (Reference 14).

10. PROBABILISTIC RISK ASSESSMENT

AECL has developed several methods over a number of years to assist the development of probabilistic risk assessment (PRA).

PRA techniques are used in the design process to ensure the design takes account of all the failure modes of interest, and is well balanced. A well balanced design is one in which there is no single factor that stands out as a major contributor to the predicted core damage frequency, and in which the reliability required of all the systems important to safety is within reasonably easily achievable targets using well established engineering principles. The "design assist" PRA is undertaken at an early stage, and is updated as the design progresses to realize these principles.

PRA is also used to meet the requirements of the CNSC for safety analysis (Reference 5) to determine the appropriate class and hence reference dose limit for a particular type of accident. The level 1 PRA also generates the plant damage states that are used for the level 2 PRA that examines the capability of containment.

A PRA for internal as well as external events will be performed, as well as PRAs for both full power and shutdown states.

11. SUPPORTING RESEARCH AND COMPUTATIONAL PROGRAMS

11.1 Computer Models and Codes

A suite of computer codes has been developed by AECL over the last 40 years specifically for the physics, thermal hydraulics and materials analysis of CANDU reactors. For a number of years, Ontario Hydro (now Ontario Power Generation) developed a separate suite of safety analysis codes. For the most part, these have now been integrated with the AECL-developed codes to produce an Industry Standard Toolset (IST) for CANDU safety analysis. A wide range of research facilities at Chalk River and Whiteshell Laboratories supported by other laboratories in Canada and around the world, have developed experimental data to support these codes. Experimental data has been developed to understand the neutron kinetics of the core, fuel behaviour, the material properties of fuel channels, the physical phenomena involved in the full range of potential accidents and many other issues. Many of these phenomena are similar to those found in other types of reactors such as PWRs, and can be compared with international data. Some, particularly associated with natural uranium cores with high neutron efficiencies, and the behaviour of horizontal Zr-2.5 wt% Nb pressure tubes fuel channels in both normal and accident situations, are unique to the CANDU reactor.

Computer codes that model these phenomena are developed to provide as close a prediction as possible to the real physical processes that take place. This approach requires a thorough understanding of the details of the physical processes but makes the subsequent validation of the code more systematic.

Code validation is treated as a completely separate exercise from code development and follows a very formal process. Significant phenomena in each accident sequence are identified in a Technical Basis Document (Reference 17). Validation matrices for each major technical discipline (e.g. physics, system thermal hydraulics, fuel and fuel channel containment) are developed, in which a suite of experiments of both separate and integrated effects is identified which is used to test the predictive capability of each code, and its limit of applicability. The validation program also uses experiments that are available as international test comparisons. The validation program is subject to detailed regulatory scrutiny by the CNSC.

To ensure the safety analyses are highly conservative, the input assumptions to the codes used for formal safety analyses, submitted to support a license application, are very conservative. They are generally set at the outside limit of the possible operating envelope, even when limits for different parameters in the same analysis do not normally exist together. Starting points for transient analyses may also assume a prior malfunction in the reactor control system. For example, the starting point for the loss of regulation accident assumes that the reactor control system has incorrectly introduced a significant neutron flux tilt in the core and that the setback/step back functions have not operated.

11.2 Audit Codes

The CNSC has not developed its own independent codes for the analysis of loss of coolant accidents. This contrasts with the position taken by the USNRC. The CNSC approach has been to hold the licensee responsible for the accuracy of code predictions, and review their codes to ensure that they include all the physical phenomena that can be expected to affect the outcome, and to insist on, and review in depth, the validation of the phenomena both as separate effects and as integrated into the model of the reactor behaviour as a whole.

The CNSC is using codes (HELIOS and NESTLE) which are independent of the Canadian nuclear industry to assist in the regulatory review of the nuclear physics of CANDU reactors.

12. SAFEGUARDS AND SECURITY

12.1 Safeguards and Proliferation Resistance

The International Atomic Energy Agency (IAEA) has successfully applied safeguards to CANDU reactors since the 1980s. Experience gained over this period has been fed back into the design process to facilitate IAEA inspection, instrumentation and sealing, the need for near real time accounting and remote monitoring, and to enhance the ACR proliferation resistance. The design includes space for a dedicated IAEA safeguards instrumentation room; a serial number on each fuel bundle; appropriate power, lighting, cable penetrations and space for anticipated IAEA instrumentation, and layout features to address potential diversion paths and simplify safeguards monitoring. The path that spent fuel follows from the fuelling machines to the spent fuel bay has been designed to take into consideration the requirements of the IAEA for the additional safeguards protocol. The ACR has better proliferation resistance than previous CANDUs through its use of slightly enriched fuel. This fuel results in a lower fuelling rate than for previous CANDU designs, and less spent fuel per megawatt hour of energy produced. The higher burn up spent fuel is also less attractive, from a proliferation perspective, because of its higher radiation field and lower quality plutonium (higher ratio of Pu-240 to Pu-239).

12.2 Security

Protection against major external and internal events has been fully considered in the layout and design of ACR. The use of widely separated divisions and systems to perform the same safety function gives a robust defence against local events. The reactor building, particularly the containment structure, provides a hardened barrier to mitigate the effects of intentional impact of a large commercial aircraft. The main control room is located near the centre of the building complex, limiting external access routes and to ensure the plant can be shutdown, cooled, monitored and maintained in a safe shutdown state. The secondary control room is separated horizontally and vertically from the main control room to reduce the possibility of a common event affecting both. A protected pathway exists between the two control rooms. The Reserve Water Tank has the ability to cool the core for many hours without reliance on systems outside the containment building.

13. INSPECTIONS AND TESTS

As discussed in Sections 3.7 and 3.8, under Canadian regulatory requirements, the designer is required to define explicitly the minimum performance required from every system important to safety, and the reliability with which that performance must be delivered. For the shut down, ECC and containment systems, the designer defines the specific functional tests and their frequency that the operator should use to demonstrate that the required availability will be met in operation. This information should provide a sound technical basis for the development of a set of inspection, tests, analyses and acceptance criteria (ITAAC) that will be required during the construction inspection program (Reference 15).

14. REFERENCES

1. CNSC (formerly known as AECB), "Requirements for Containment Systems for CANDU Nuclear Power Plants", Regulatory Document R-7, February 1991.
2. CNSC (formerly known as AECB), "Requirements for Shutdown Systems for CANDU Nuclear Power Plants", Regulatory Document R-8, February 1991
3. CNSC (formerly known as AECB), "Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants", Regulatory Document R-9, February 1991
4. D.G. Hurst and F.C. Boyd, "Reactor Licensing and Safety Requirements", AECB-1059, June 1972.
5. CNSC (formerly known as AECB), "Requirements for the Safety Analysis of CANDU Nuclear Power Plants", Consultative Document C-6 Rev 1, September 1999.
6. Norman M Ichiyen, "IAEA Symposium on Evolutionary Water Cooled Reactors: Strategic Issues, Technologies and Economic Viability", Software in Safety Applications, Seoul, Korea, Nov 30 - Dec 3 1997
7. Ontario Power Generation and Atomic Energy of Canada "Standard for Software Engineering of Safety Critical Software", CE-1001-STD. Rev 2. Dec 1999
8. CNSC, "Reliability programs for Nuclear Power Plants", Standard S-98, December 2001.
9. USNRC, "An approach for risk informed decision making: Technical Specifications", Regulatory Guide 1.117, Aug 1998
10. 10 CFR 50, Code of Federal Regulations, Title 10, Part 50, "Domestic Licensing of Production and Utilization Facilities - Appendix A – General Design Criteria for Nuclear Power Plants: Definition of a Single Failure".
11. CNSC, "Policy on Human Factors", Policy P-119, October 2000.
12. IAEA, "Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations", Safety Series 50-C/SG-Q.
13. 10 CFR 50, Code of Federal Regulations, Title 10, Part 50, "Domestic Licensing of Production and Utilization Facilities -Appendix B - Quality Assurance Criteria for Nuclear Power plants and Fuel Reprocessing Plants".
14. USNRC, "Accident Source Terms for Light Water Nuclear Power Plants", NUREG-1465.
15. 10 CFR 52, Code of Federal Regulations, Title 10, Part 52 "Early Site Permits; Standard Design Certifications; and Combined Licenses For Nuclear Power Plants - , Subpart C - Combined Licenses -10 CFR 52.97 paragraph (b) (1)".
16. International Organization for Standardization, "ISO 9001: 2000 Quality Management systems – Requirements".
17. Atomic Energy of Canada, "Technical Basis for the Validation of Computer Programs used for Safety Analysis for the ACR Design", 108 US-03500-TBD-001, Rev 0, May 2003.

Note:

Regulatory documents published by the Canadian Nuclear Safety Commission can be viewed on the CNSC website (www.nuclearsafety.gc.ca) or prints can be ordered from:

Communications and Information Management Division
Canadian Nuclear Safety Commission
PO Box 1046, Station B
280 Slater St, Ottawa, Ontario, K1P 5S9

or by e-mail: publications@cnsc.ccsn.gc.ca

Appendix A

Identification and Classification of Failures

Reference: CNSC Consultative Document C006 Rev 1 - Safety Analysis of CANDU Nuclear Power Plants.

This appendix outlines some of the failure modes that the Canadian Nuclear Safety Commission (CNSC) expects to be analyzed to demonstrate the safety of a CANDU plant, and the reference dose limits that the consequence analysis of each safety analysis should meet. Consultative document C-006 (Reference 5) gives a more complete treatment of the subject. This document is the result of considerable discussion between the Canadian nuclear industry and the CNSC on the best way to carry out a thorough analysis of all the ways in which a CANDU plant could fail, and to develop design criteria for the systems that defend against, and mitigate the results of, those potential failures. The onus is on the designer to ensure the list of failure modes and the list of defensive systems is complete, and the analyses are sufficiently conservative that a specific minimum performance required of each of the defensive systems can be derived from them.

Table A-1 lists examples of the description of the types of failure modes that are assigned to the classes in the Table as well as examples of the failure modes themselves. The examples are taken from the tables in C-006 Rev 1. Examples are given for each of the five classes of events. Within each class, many more modes than the examples given have been analyzed. One of two alternative methods has been used to assign a failure mode to a class. The primary method used to assign the failure modes in the table is deterministic. The CNSC has assigned a set of "specified initiating events" to classes 1, 2 and 3, and the table shows some of these. The assignment is based loosely on the expected probability of the event. Class 1 events are expected to be of moderate frequency (expected to occur several times in a plant lifetime); Class 2 are infrequent events (they may occur once during the lifetime of a plant), and Class 3 are unlikely to occur in many plant lifetimes. They are traditional Design Basis Accidents.

A second method of assigning events to a class which is available to a designer is probabilistic, and can be based on PRA. For a design with a significant number of new design features such as the ACR, it is expected that the designer will review and propose a new or revised list to the CNSC based on the results of a preliminary PRA, and confirm them from the results of the final PRA that is completed at the end of the design process.

Events in the table can be of three different types: 1) an initiating event; 2) an initiating event followed by another initiating event some time later; and 3) an initiating event followed by the failure of a system intended to mitigate the effects of the initiating event. These can be either systems that are used in normal operation and have a second, safety related duty, or safety systems whose sole function is the mitigation of an accident. There are four systems of this latter type in a CANDU reactor: shutdown system 1, shutdown system 2, high pressure emergency core cooling, and containment. Examples of all three types of events are included in the table.

Table A-1 Classification of Events

Note: These examples are taken from the tables in Reference 5.

Class	Examples of Failure types	Examples of Failure descriptions
Class 1	Initiating event: failure of an active system	Bulk loss of reactivity control Steam generator pressure control Reactor coolant pressure control Steam generator feed flow A single steam generator tube Moderator system Installation of channel closure seal Service water system Fuelling machine cooling system Partial loss of Class IV power
Class 2	Initiating events: i) failure of a non-nuclear standard passive component ii) failure of one of many similar nuclear standard passive components Multiple event: Class 1 event + failure of a mitigating system (that is also used in normal operation for another task) to respond	Piping, causing loss of service water Seizure of a main coolant pump Calandria tube causing loss of moderator Flow blockage in a fuel channel (up to 98%) Pressure tube/calandria tube intact Piping, causing a small loss of reactor coolant (e.g. feeder pipe) Loss of reactivity from distorted flux shapes Total loss of Class IV power Reactor coolant pump seizure
Class 3	Initiating events: Failure of a nuclear standard passive component Multiple event: Class 1 + failure of a standby emergency system to respond Class 1 + failure of a shut down system Class 2 +single failure in a SDS, or ECC or Containment	Piping, causing a large loss of reactor coolant Multiple steam generator tube rupture Steam generator feed water plus auxiliary feed water Pressure tube/calandria tube failure

Class	Examples of Failure types	Examples of Failure descriptions
Class 4	Initiating event: Failures of very low probability Multiple events: Class 1 event + failure of a SDS, or ECC or Containment	Steam generator feed water plus a shutdown system Small LOCA plus loss of ECC 98%-100% blockage of a fuel channel
Class 5	Initiating event: Failures of extremely low probability Multiple events: Class 3 event + failure of a standby emergency system Class 3 event +single failure of a SDS, or ECC or Containment	Large LOCA plus loss of high pressure ECC Loss of Class IV and Class III power Large LOCA plus failure of containment isolation

When the table is revised for a new design such as the ACR using PRA analysis, the events, both singles and multiples, can be assigned to the five classes using the expected annual event probabilities in Table A-2.

Table A-2 Event Class Probability Ranges

Event class	Annual event probability
1	More than 10^{-2}
2	10^{-2} to 10^{-3}
3	10^{-3} to 10^{-4}
4	10^{-4} to 10^{-5}
5	10^{-5} to 10^{-7}

The CNSC has set reference dose limits for each of the classes in Table A-1. A deterministic, conservative safety analysis of each of the failure modes in the table must predict a dose to the most exposed member of the public which is less than that relevant value defined in Table A-3 below.

Table A-3 Reference Dose Limits

Requirement	Event Class				
	1	2	3	4	5
Effective dose (mSv)	0.5	5	30	100	250
Lens of the eye (mSv)	5	50	300	1000	1500
Skin (mSv, averaged over 1 cm^2)	20	200	1200	4000	5000

Other, more detailed acceptance criteria for each event class are developed by the CNSC and the designer to provide further guidance to the development of the design. Examples of these are the use of B, C, and D service levels defined in the General Requirements under Section III of the *American Society of Mechanical Engineers Boiler and Pressure Vessel Code* (ASME code) for different classes.

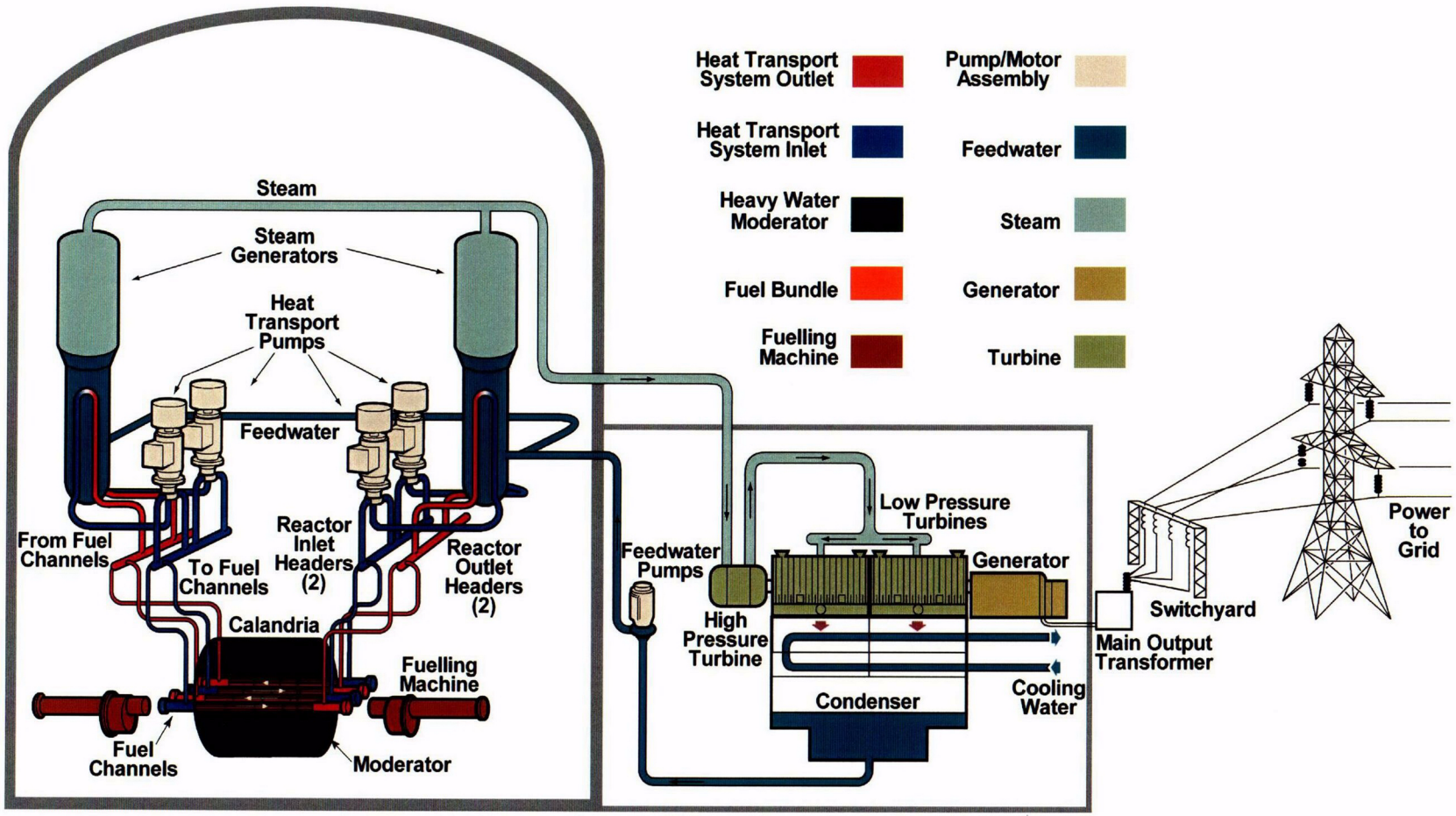

Figure 1-1 ACR-700 Overall Plant Flow Diagram

C01

Major nuclear systems

STEAM

FEEDWATER

LIGHT WATER COOLANT

HEAVY WATER MODERATOR

1 MAIN STEAM PIPES
2 PRESSURIZER
3 STEAM GENERATORS
4 HEAT TRANSPORT PUMPS
5 HEADERS
6 CALANDRIA
7 FUEL
8 MODERATOR PUMP
9 MODERATOR HEAT EXCHANGER
10 FUELING MACHINES

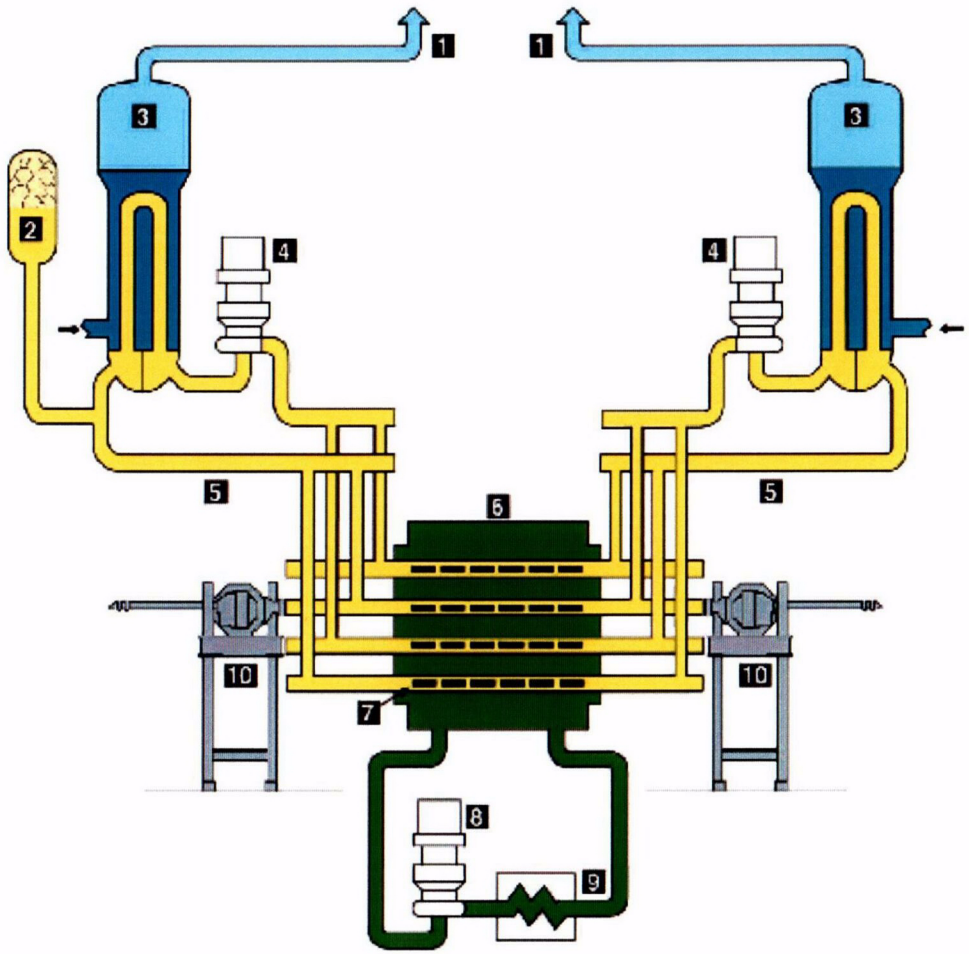

Figure 1-2 Nuclear Steam Systems

C02

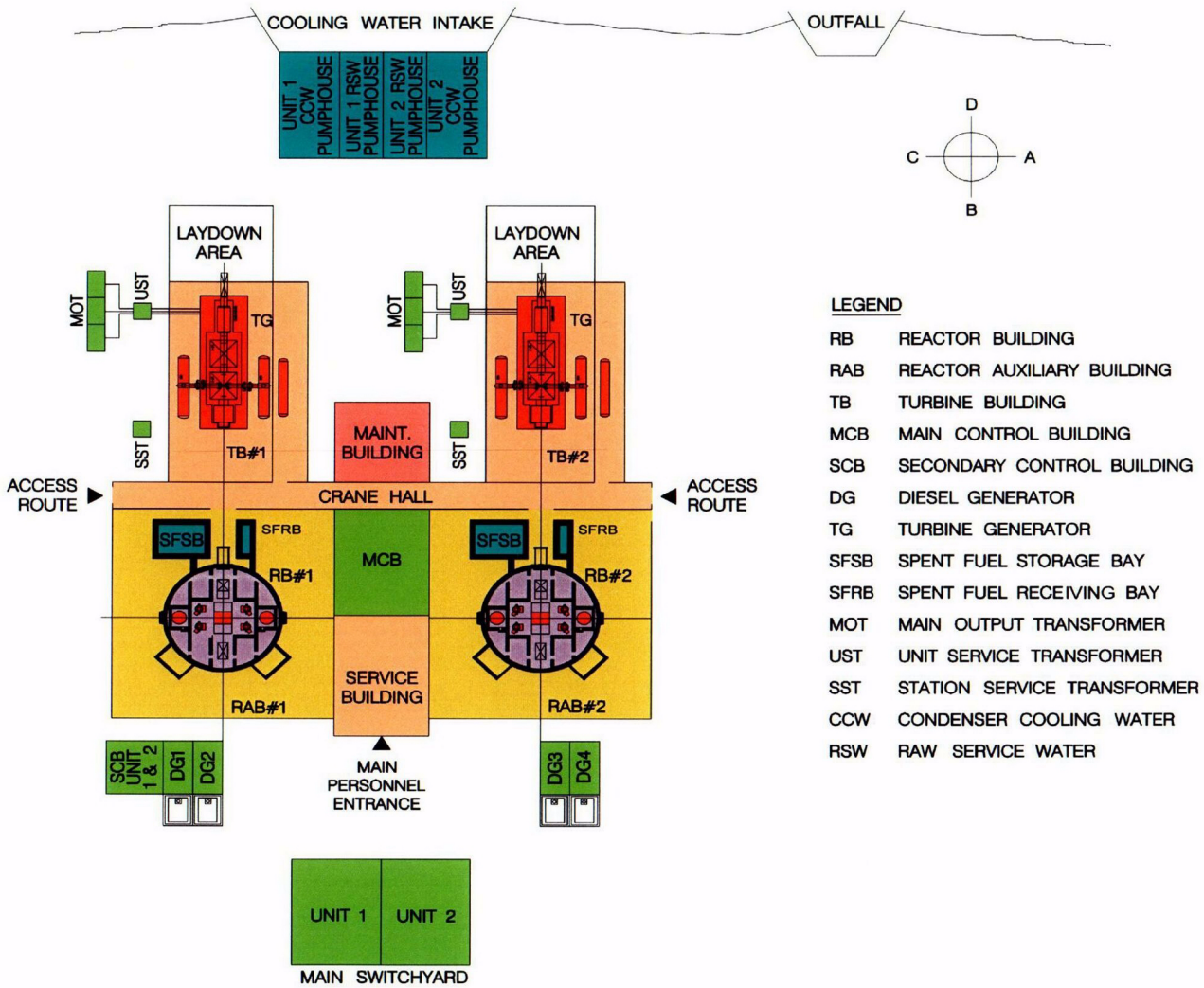

Figure 2-1 ACR Two-unit Plant Layout

C03

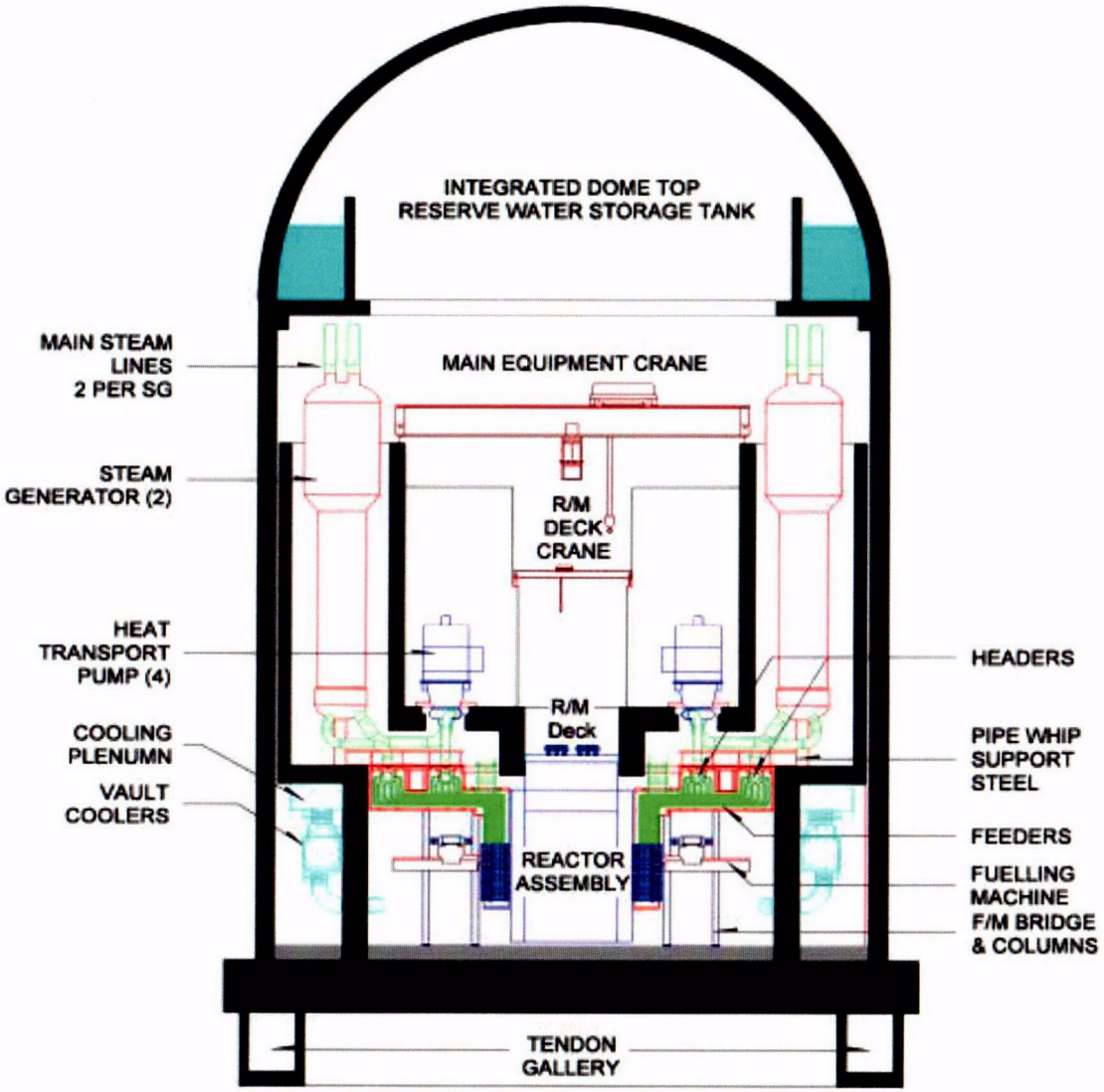

Figure 2-2 Reactor Building Section

C04

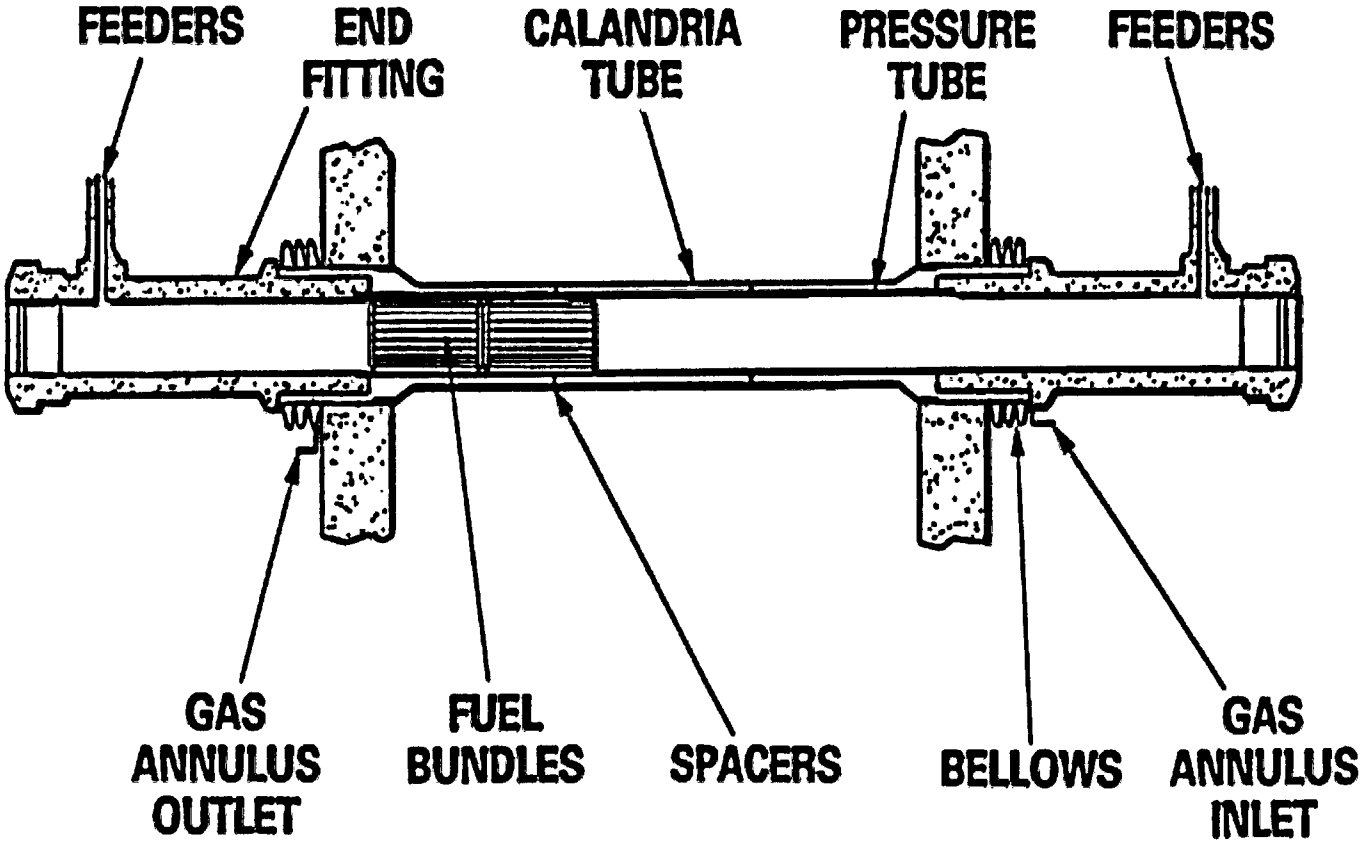

Figure 3-1 Fuel Channel Components

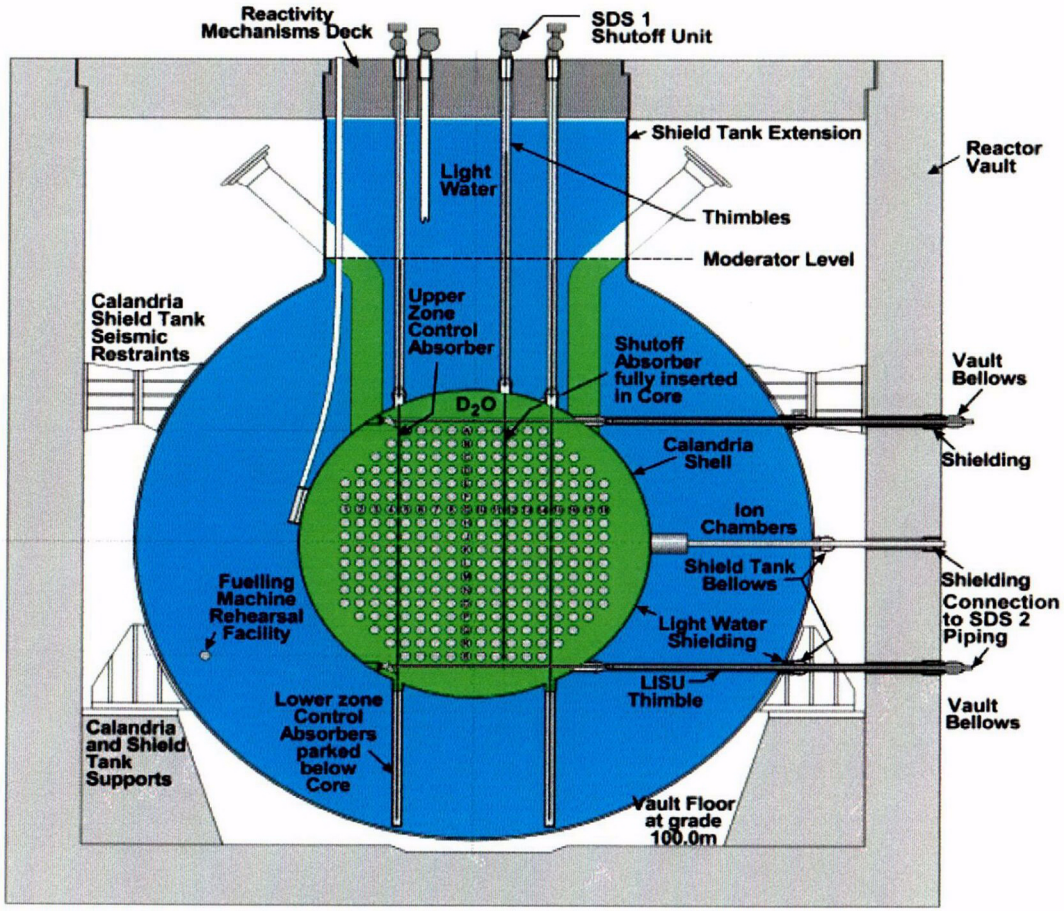

Figure 3-2 ACR Calandria & Shield Tank Assembly

C05

- **Cool, low-pressure heavy-water moderator**
- **Removes~5% of the fuel heat in normal operation, similar to decay heat shortly after shutdown**
- **Absorbs energy from a postulated channel failure**
- **Long-term emergency heat sink for LOCA with loss of ECCS**
  - **No melting of the UO_2fuel; preserves channel integrity**
  - **Backed up by light water shield tank – slow and graceful progression of severe core damage**

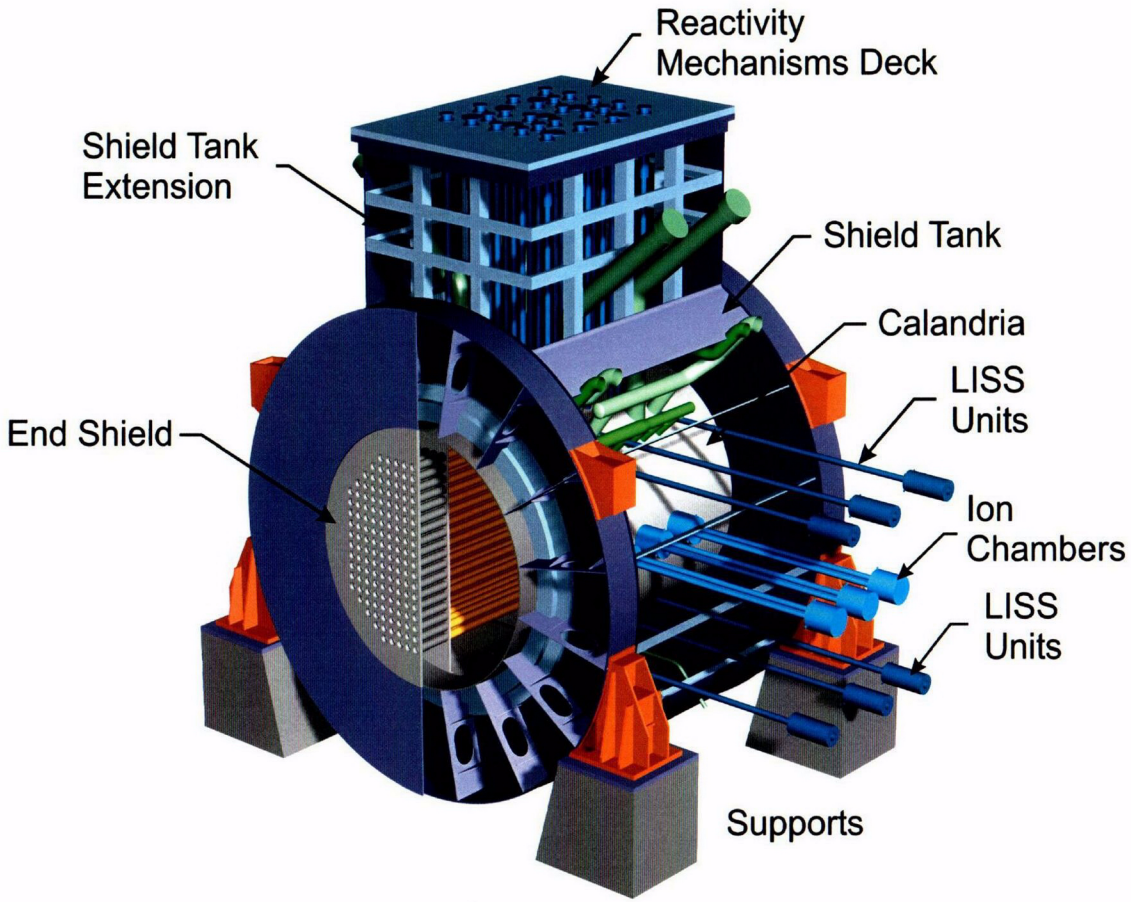

Figure 3-3 Moderator

C06

- Horizontal fuel channels surrounded by low temperature, low pressure moderator
- Steel calandria contains moderator & supports fuel channels
- Shield tank surrounds calandria and contains light water for thermal & biological shielding
- All reactivity devices in moderator

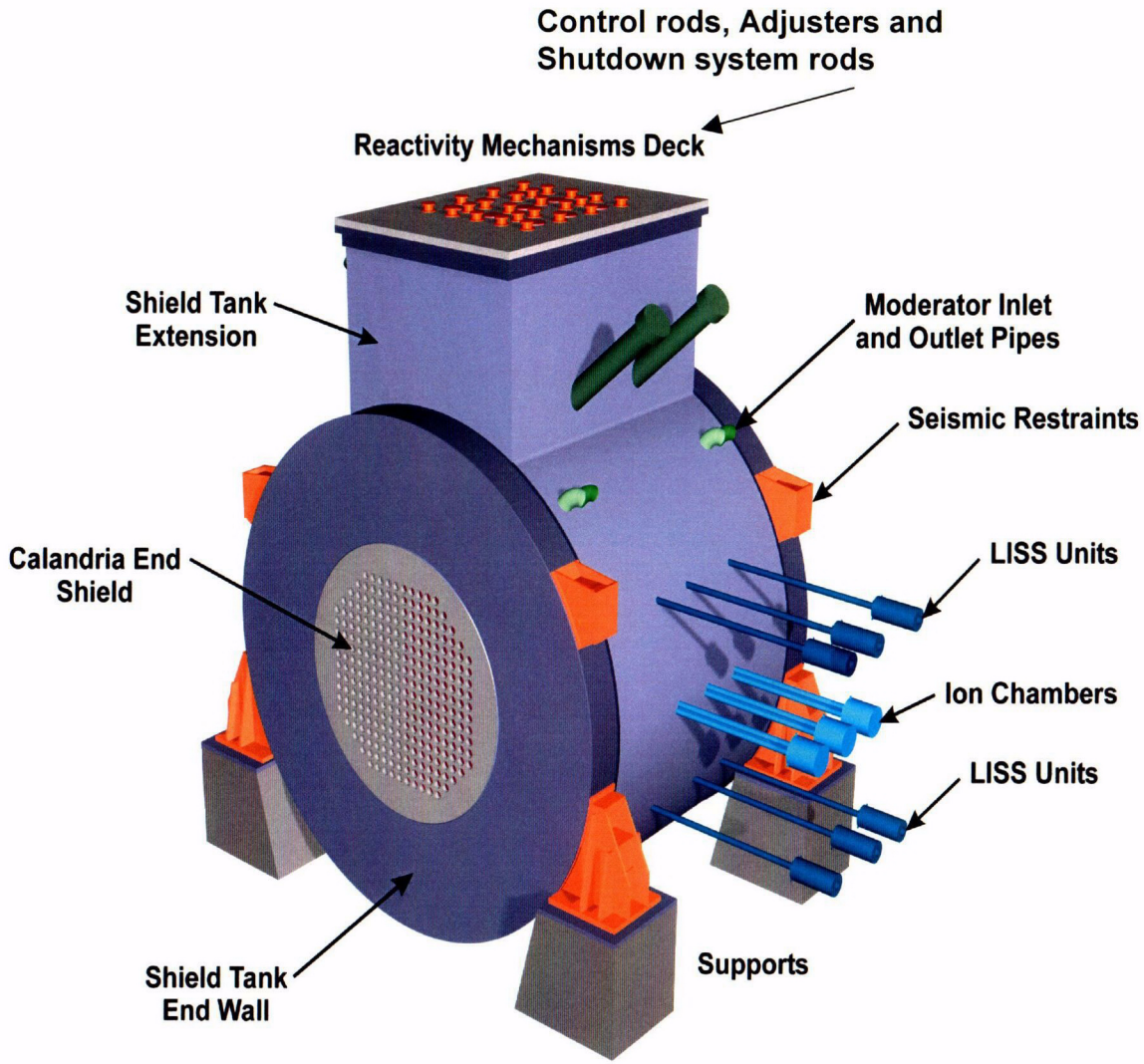

Figure 3-4 Reactor

C07

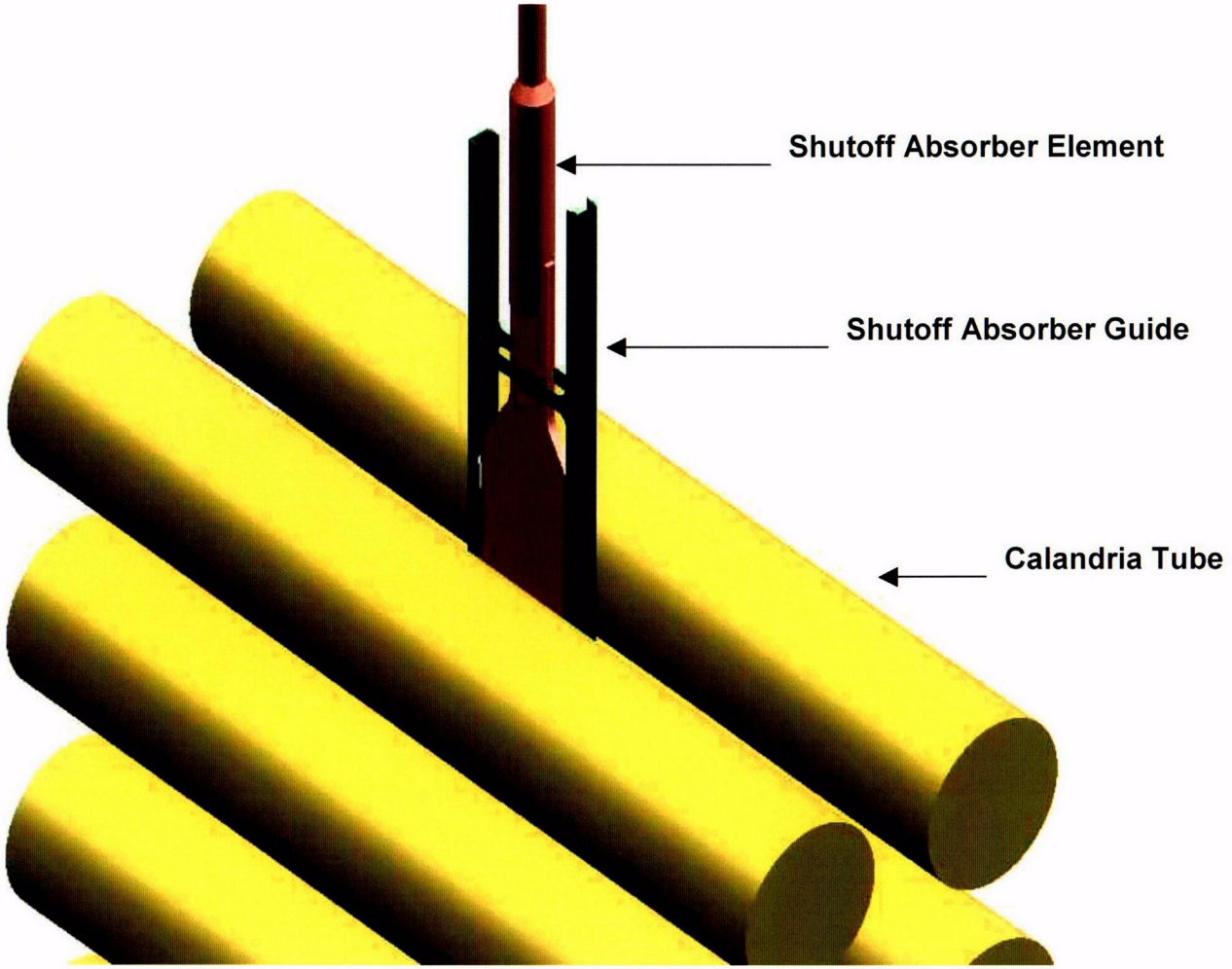

Figure 3-5 ACR-700 Reactivity Control Units

C08

- 43 elements, 2 pin sizes
  - 8 central elements 13.5 mm (0.53") in diameter
  - 35 outer elements 11.5 mm (0.45") in diameter
- ~20% lower peak rating than for 37-element fuel
  - facilitates achievement of higher burnup
- CHF-enhancing buttons
  - increase coolant turbulence
  - higher operating margins

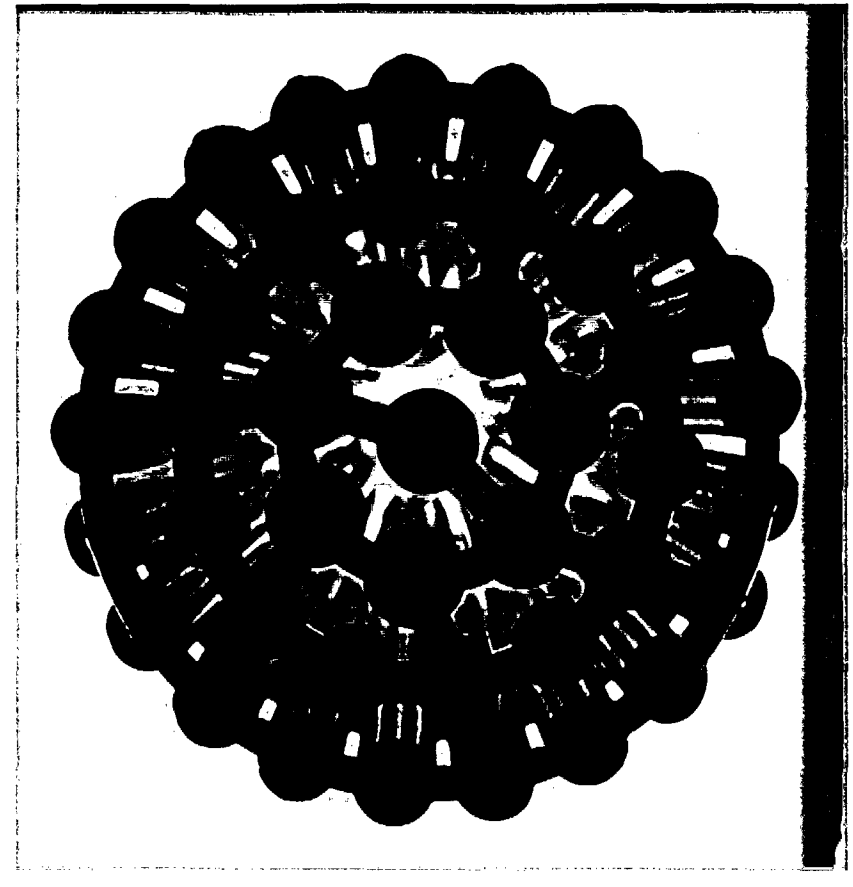

Figure 4-1 CANFLEX Fuel

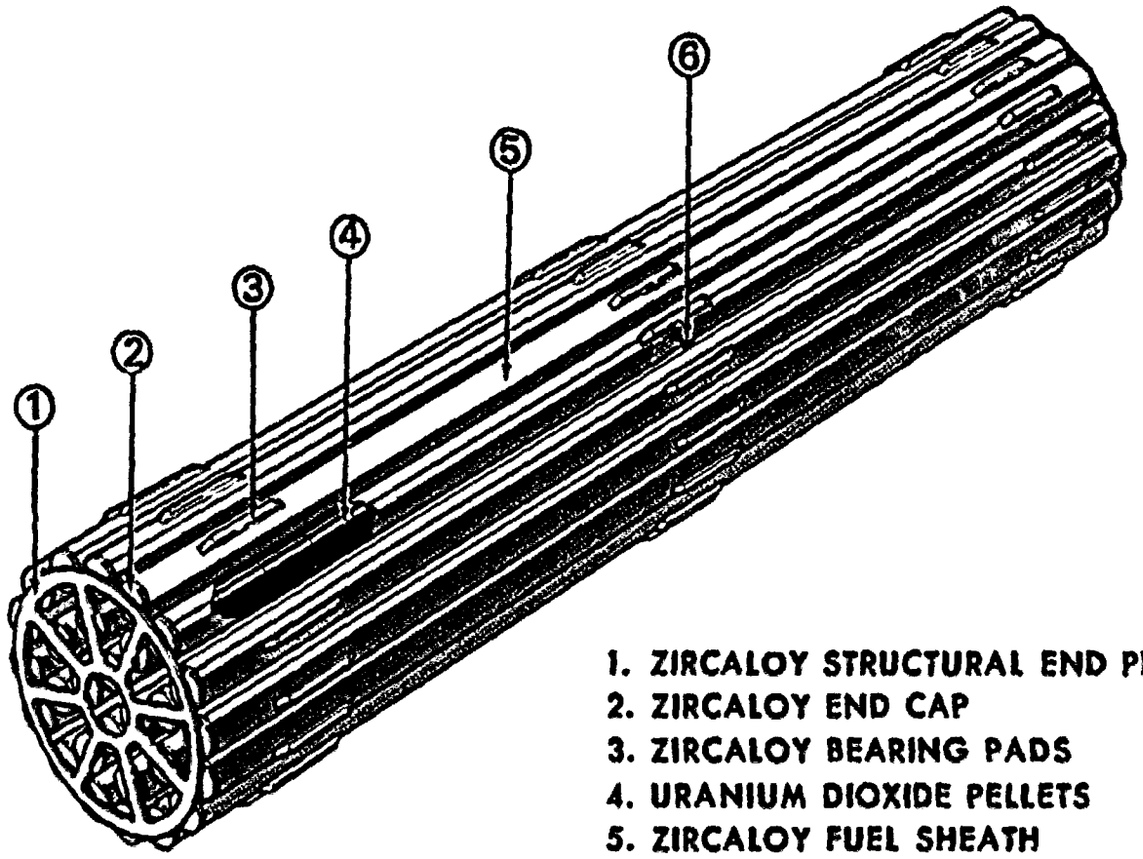

Figure 4-2 CANDU Fuel Components

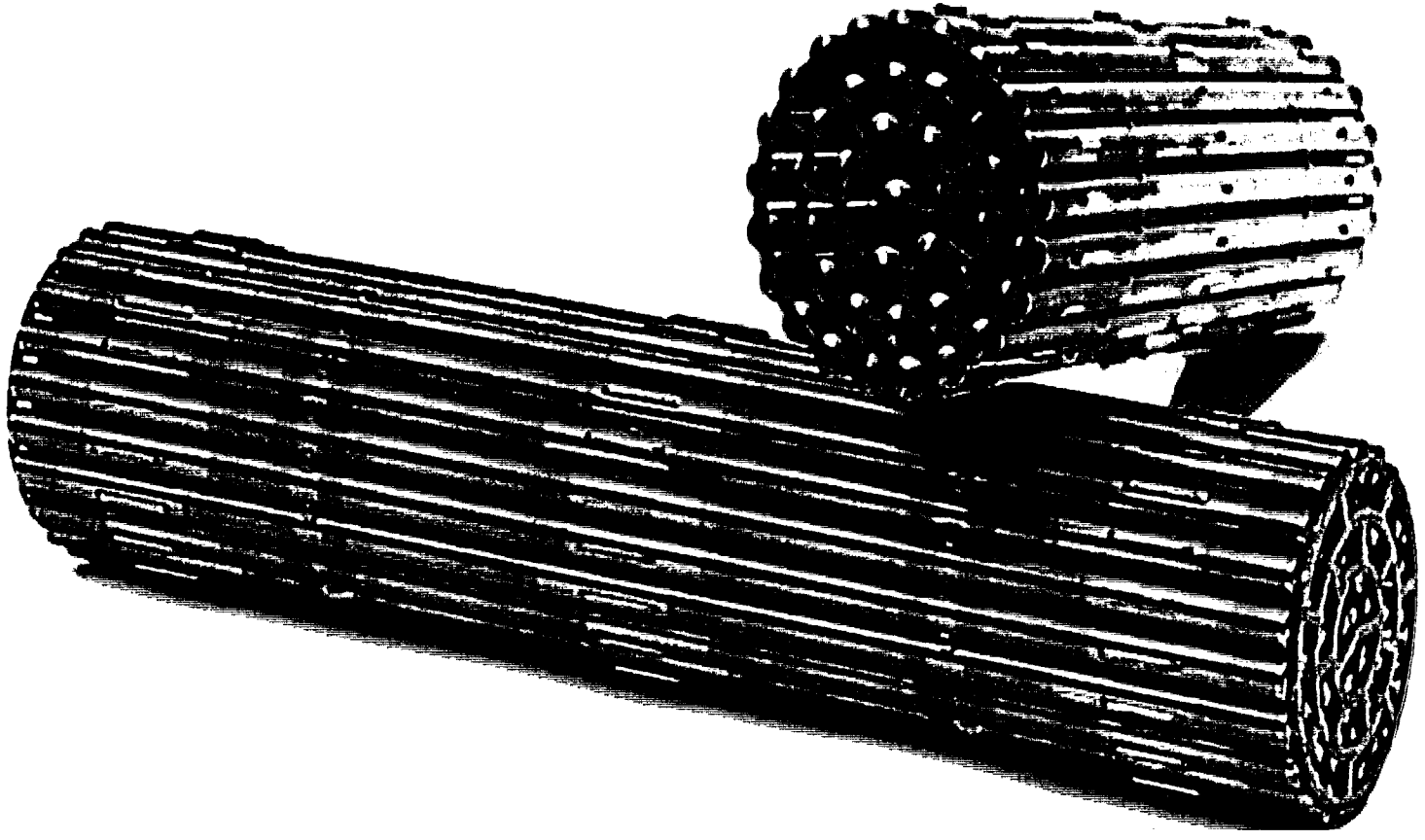

Figure 4-3 CANFLEX Bundle

Above the reactor – similar to PWRs

- Steam generators above the reactor
  - promotes thermosyphoning at decay power
- Each channel individually connected to collectors (headers) above the core
- No large RCS piping at or below core level

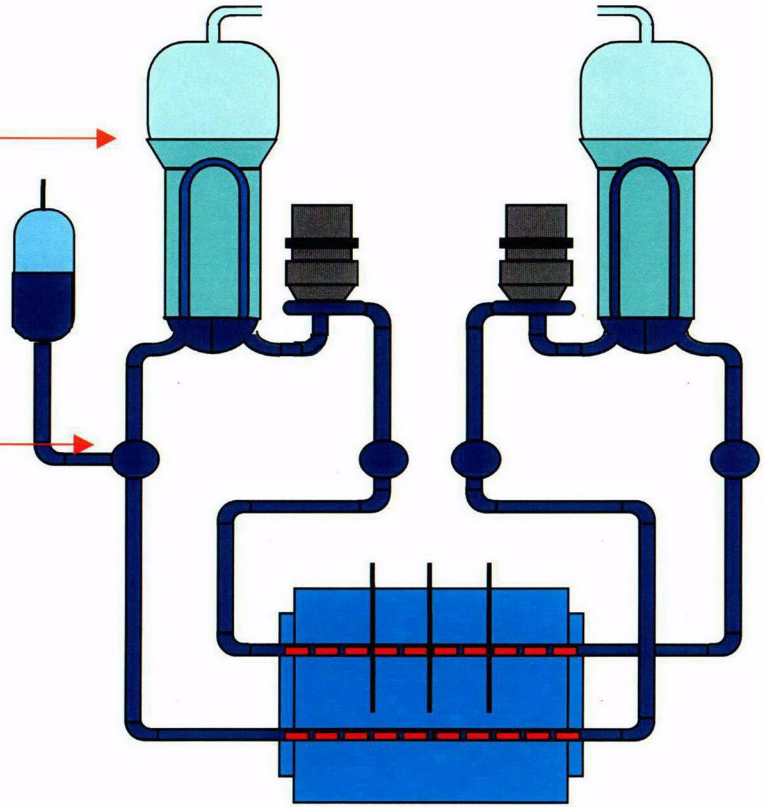

Figure 5-1 Reactor Coolant System

C09

- Each channel is connected at its inlet and outlet by small (feeder) pipes to headers, above the reactor
- Above headers – similar to PWRs
- No large pipes at or below core level
- Tolerates pump seizure
- Natural circulation, even with some void

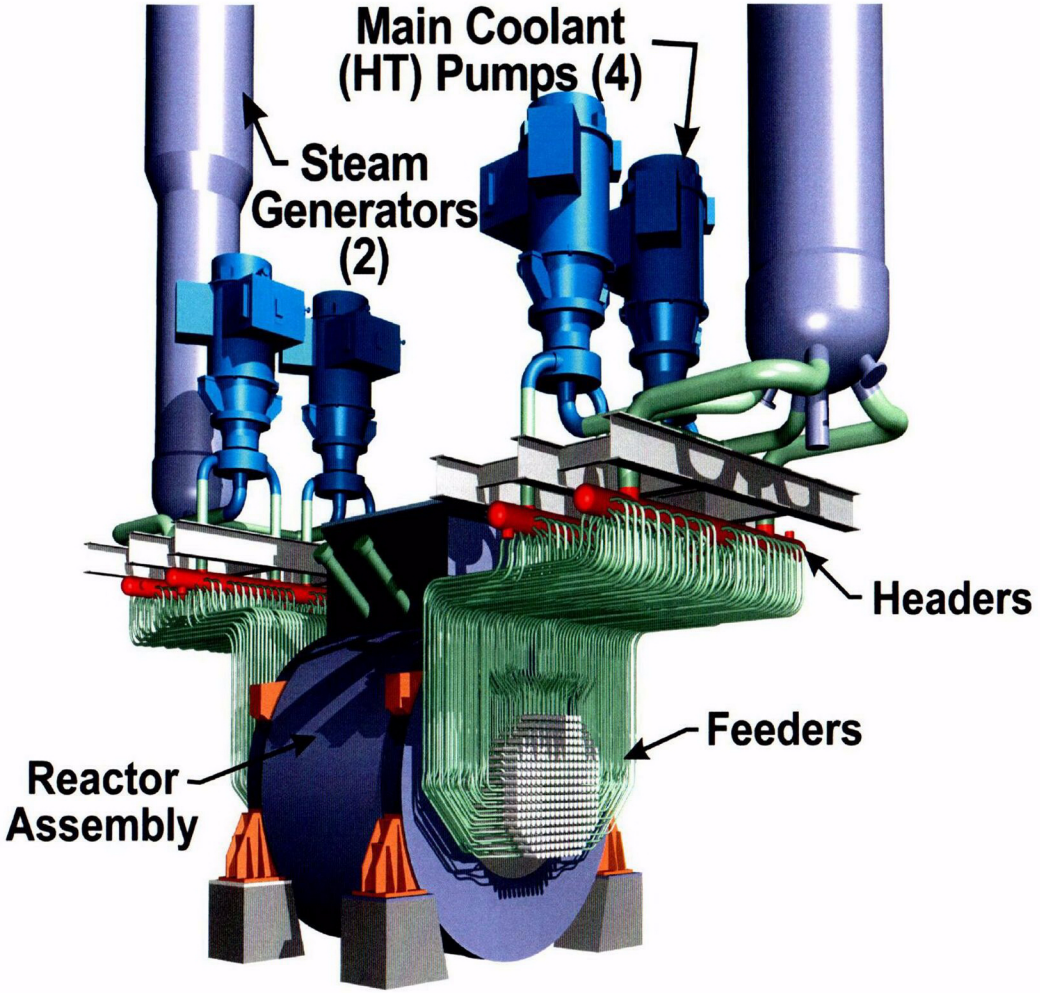

Figure 5-2 Reactor Coolant System

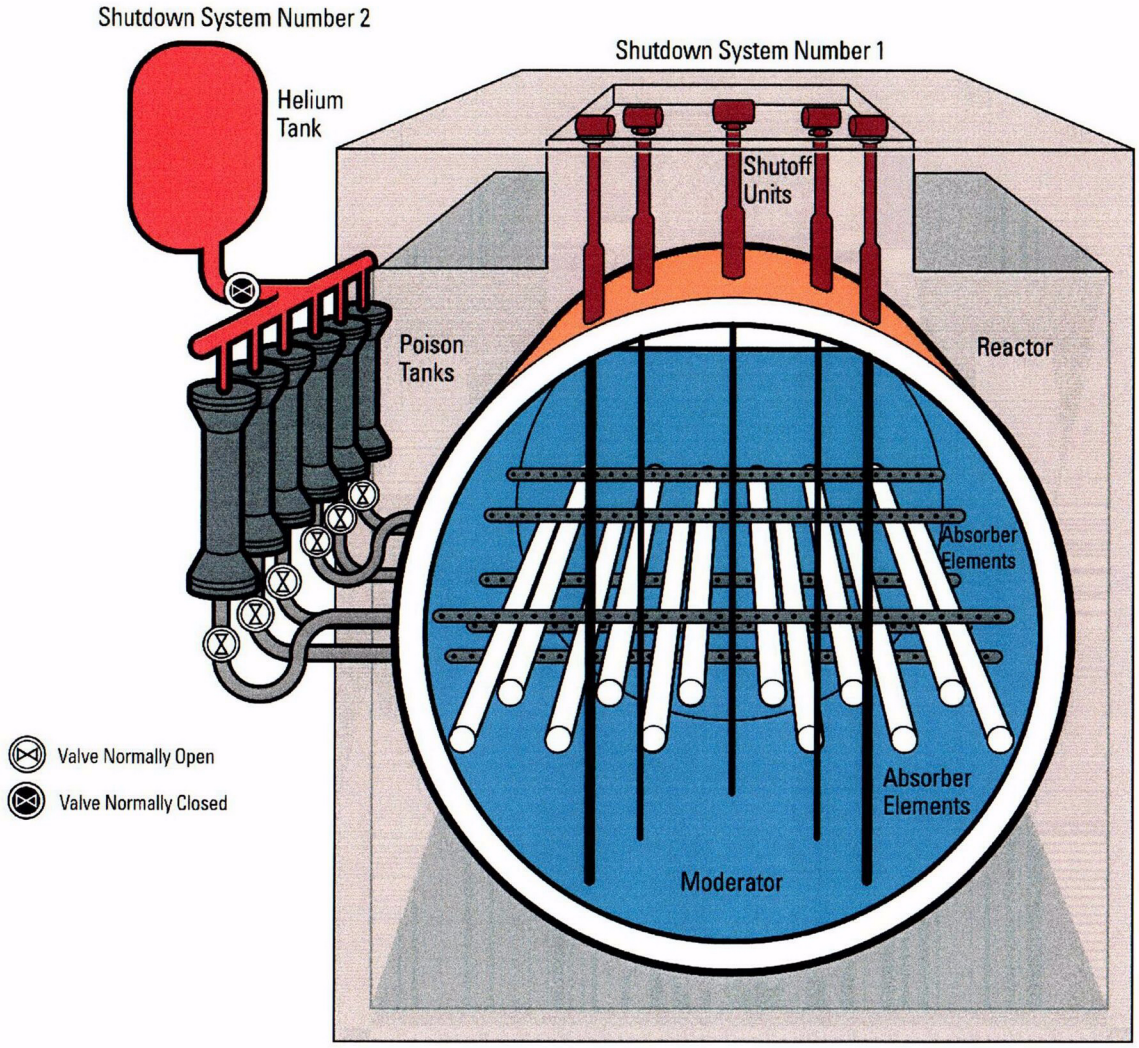

Figure 6-1 Shutdown Systems

C11

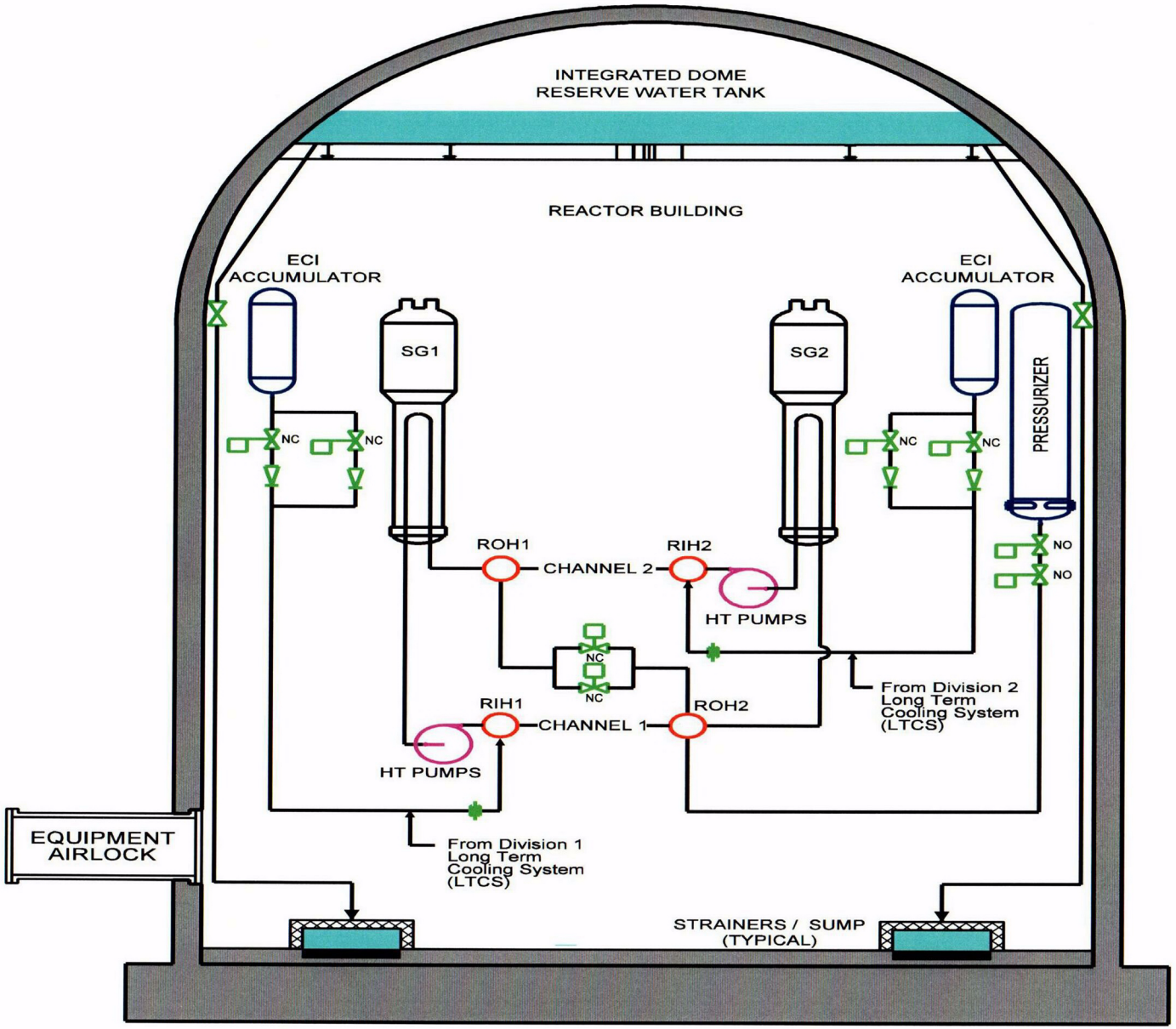

Figure 7-1 Emergency Coolant Injection System

C12

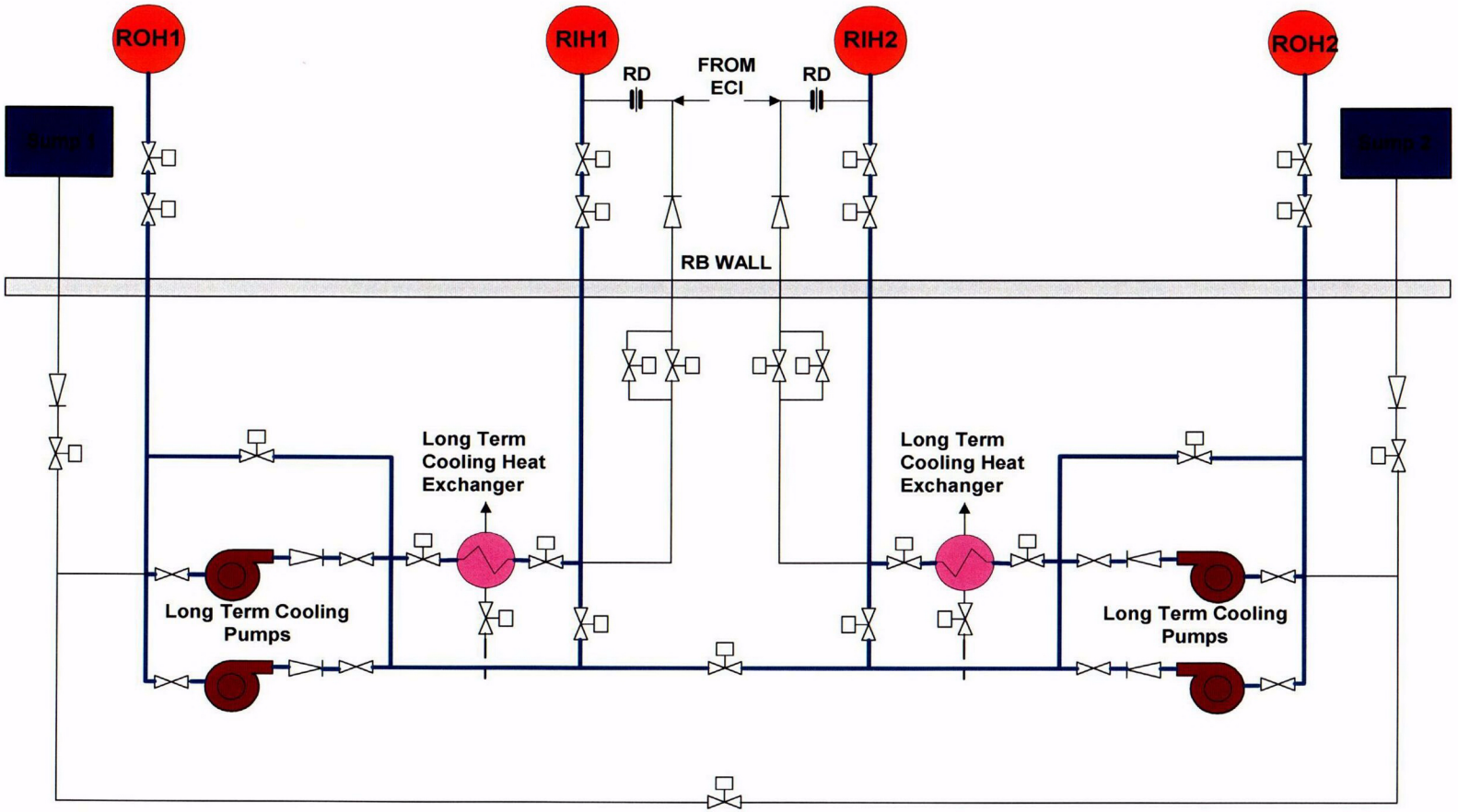

Figure 7-2 Long Term Cooling

C13

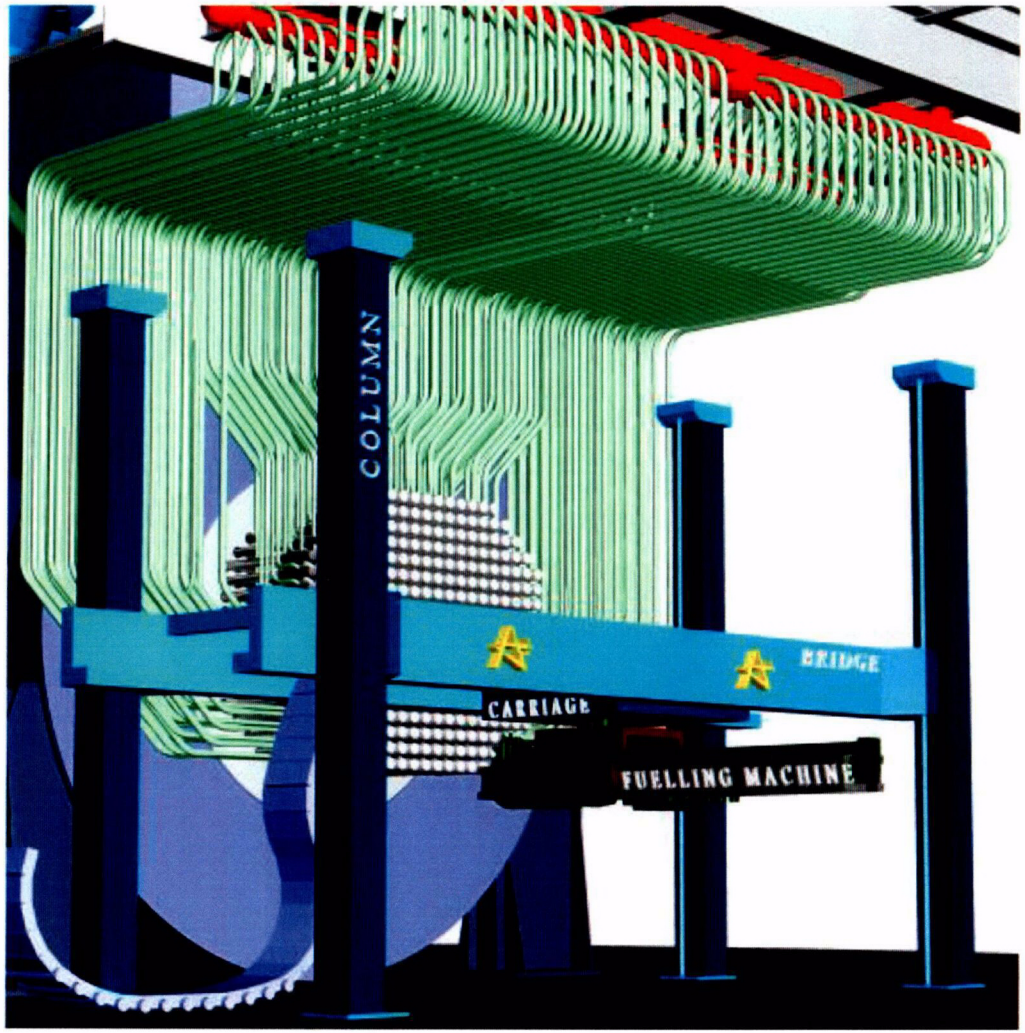

Figure 8-1 ACR Fuel Handling Equipment

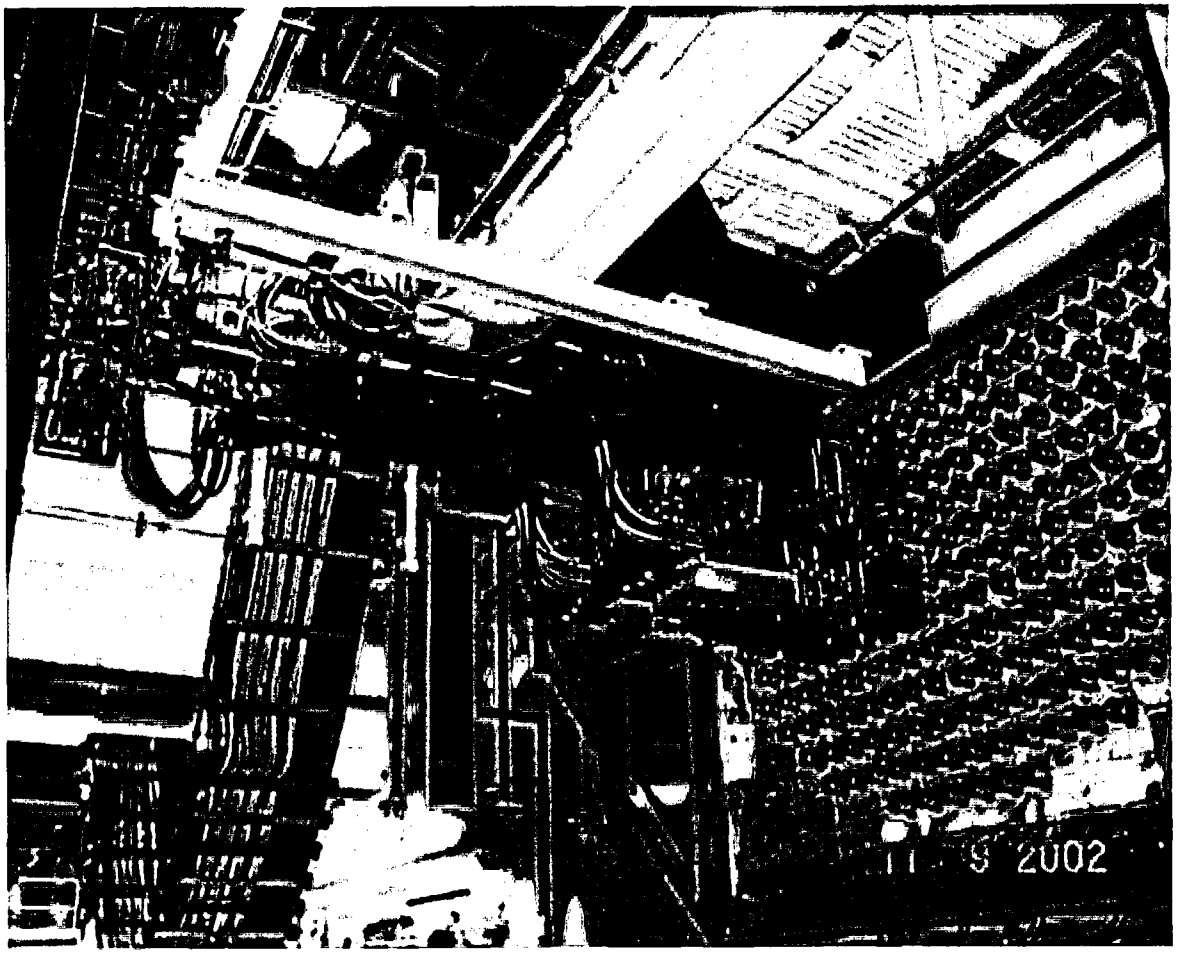

Figure 8-2 Fuelling Machine on Reactor