AECL-9942

PASSIVE SAFETY FEATURES
FOR
NEXT GENERATION CANDU POWER PLANTS

by

A. Natalizio, R.S. Hart, J.J. Lipsett*
P. Soedijono, J.E. Dick

Paper Presented
at

International Workshop on
the Safety of Nuclear Installations
of the Next Generation and Beyond
1989 August 28-31, Chicago, Illinois, USA

Atomic Energy of Canada Limited
CANDU Operations
Sheridan Park Research Community
Canada L5K 1B2

---

* Atomic Energy of Canada Limited, Chalk River Nuclear
Laboratories, Chalk River, Ontario, K0J 1J0

PASSIVE SAFETY FEATURES FOR NEXT GENERATION CANDU POWER PLANTS

by

A. Natalizio, R.S. Hart, J.J. Lipsett
P. Soedijono, J.E. Dick

ABSTRACT

CANDU offers an evolutionary approach to simpler and safer reactors. The CANDU 3, an advanced CANDU, currently in the detailed design stage, offers significant improvements in the areas of safety, design simplicity, constructibility, operability, maintainability, schedule and cost. These are being accomplished by retaining all of the well known CANDU benefits, and by relying on the use of proven components and technologies. A major safety benefit of CANDU is the moderator system which is separate from the coolant. The presence of a cold moderator reduces the consequences arising from a LOCA or loss of heat sink event. In existing CANDU plants even the severe accident - LOCA with failure of the emergency core cooling system - is a design basis event. Further advances toward a simpler and more passively safe reactor will be made using the same evolutionary approach. Building on the strength of the moderator system to mitigate against severe accidents, a passive moderator cooling system, depending only on the law of gravity to perform its function, will be the next step of development. AECL is currently investigating a number of other features that could be incorporated in future evolutionary CANDU designs to enhance protection against accidents, and to limit off-site consequences to an acceptable level, for even the worst event. The additional features being investigated include passive decay heat removal from the heat transport system. A simpler emergency core cooling system and a containment pressure suppression/venting capability for beyond design basis events. Central to these passive decay heat removal schemes is the availability of a short-term heat sink to provide a decay heat removal capability of at least three days, without any station services. Preliminary results from these investigations confirm the feasibility of these schemes.

1. INTRODUCTION

The trend for the next generation of nuclear power plants is clearly towards installations that are safer, more reliable, simpler to construct and operate and less costly. The rationale for these objectives are elaborated in a companion paper presented at this meeting[1].

Given the need for change, how do reactor designers respond to that need? The response to date has been mixed and generally falls in one of two camps: the camp that promotes an evolutionary approach, and the camp that promotes a revolutionary approach by the introduction of radical, new designs. Atomic Energy of Canada Limited (AECL) has been following the evolutionary approach.

This paper outlines the evolutionary approach to safer and better reactors that is being pursued by AECL and also discusses some of the <u>passive design features</u> currently under investigation that would be implemented in future CANDU designs.

2. CANDU EVOLUTION

The CANDU design has evolved continuously and consistently since its inception in the mid 1950s. A constant theme of this evolution has been simplification, with resulting improvements in station performance and safety. Figure 1 illustrates the steady reduction obtained in station doses while maintaining a steady growth in the current high levels of performance.

2.1 Simplification

CANDU reactors feature a number of fundamental simplifications relative to other types of pressurized water reactors[2]. These include:

- Carbon steel heat transport system piping instead of stainless steel. It is more easily fabricated and inspected; it is ductile and immune to stress corrosion cracking.
- Pressure tubes instead of a massive pressure vessel.
- Easily replaceable pressure tubes, the only CANDU component subjected to a combination of high stress and high radiation.
- Short, simple fuel bundle design that is easily fabricated. The same bundle design is used for the entire core.
- Natural uranium, requiring no enrichment or burnable poison.
- No control devices in the high pressure reactor coolant circuit for reactivity control. They are located in the low temperature, low pressure moderator.
- Flexible irradiated and new fuel storage (no concerns over criticality regardless of storage configuration due to low reactivity of CANDU fuel).

Reduction in the number of components used has been a focus of CANDU evolution over the past 25 years. Tables 1, 2 and 3 illustrate the number of key components. The reduction in the number of these components is, of course, accompanied by a reduction in auxiliary components, including piping, cabling, instrumentation and support structures. These are not accounted for in the tables.

Table 1: Steam Generator Evolution

Station	Net Reactor Output (MWe)	MW(th) per SG	Area (m^2) per SG	No. of SG
Pickering	515	138	1850	12
Bruce	825	265	2415	8
CANDU 6	640	500	3200	4
Darlington	885	665	4760	4
CANDU 3	450	690	4200	2

Table 2: Reactor Coolant Pump Evolution

Station	Net Reactor Output (MWe)	Total No. of Pumps	No. of Pumps Operating	Motor Rating (kW)
Pickering	515	16	12	1420
Bruce	825	4	4	8200
CANDU 6	640	4	4	6700
Darlington	885	4	4	9400
CANDU 3	450	2	2	9400

Table 3: Valve Evolution

Station	Net Reactor Output (MWe)	No. of Valves	
		Packed	Bellows Sealed
NPD	22	1500	0
Douglas Point	220	2000	0
Pickering	515	175	570
Bruce	825	75	500
CANDU 6	640	90	300
Darlington	885	90	300
CANDU 3	450	50	200

Further simplifications and reductions in the number of components can only be achieved by changes in approach, as with the introduction of passive cooling methods.

2.2 Safety

The CANDU reactor uses natural uranium fuel and heavy water moderator and coolant. The fuel is contained in individual fuel channels that separate the coolant from the moderator. This reactor configuration, therefore, provides fundamental and inherent features that have a direct contribution to plant safety.

The combination of D_2O moderation and natural (or slightly enriched uranium fuel) gives:

- A CANDU fuel channel lattice that is optimized for maximum reactivity. Hence, any event that relocates the fuel reduces reactivity and shuts down the reactor. Criticality is impossible with light water or dilute heavy water in the channels, e.g., after emergency coolant injection.
- Power transients due to reactivity excursions are slow due to long neutron lifetime (about a millisecond).
- Ease of handling of new and irradiated fuel. No possibility for criticality regardless of storage configuration.

On-power refuelling results in:

- Very small and constant excess reactivity in the reactor at all times during station life.
- Low total worth of all reactivity regulation devices.
- Constant worth of reactor regulating system over the

life of the plant.

- Short fuel bundles limit the fission product source term per fuel element.
- Low radiation fields in the reactor coolant, due partly to on-line failed fuel detection and removal of fission products, and the absence of chemicals for reactivity control.

The cool low-pressure moderator, separate from the high pressure heat transport systems provides:

- a heat sink that can remove decay heat under severe conditions such as a loss of coolant coincident with a loss of emergency core cooling,
- a cool low pressure environment for all reactivity control devices, and
- a means to obtain comprehensive neutronic data for reactor control, facilitated by simple low cost detectors.

In building upon these fundamental and inherent safety features, CANDU also incorporated engineered safety and safety support systems to provide a high standard of safety for both plant personnel and the general public.

These engineered features include:

- two independent, fully capable, actively triggered, passively driven, shutdown systems that are diverse and functionally independent of the reactor regulating system,
- a shutdown cooling system that can be brought into service at full heat transport system temperature and pressure for decay heat removal, and
- discharge of coolant from valves connected to the heat transport system, such as pressure relief valves, is routed to a high pressure tank, which has relief devices set above the heat transport system operating pressure; hence the valve activation or failure of such valves to reclose after activation will not lead to a large inventory loss from the heat transport system.

Licensing requirements in Canada have also encompassed a relatively wide range of design basis events; these include the failure of any special safety system (including containment or emergency core cooling) coincident with major process failures (including a loss-of-coolant accident), and the failure of the reactor pressure vessel (the fuel channel).

It should be noted that fuel channel failure is not accompanied by disastrous consequences. In fact, the two fuel channel ruptures experienced in CANDU plants were catered to by normal process systems, without the initiation of any of the safety systems.

3. ADVANCED CANDU

The focus of the advanced CANDU design has also been on plant simplification and safety. This is evident from the design objectives established for the CANDU 3.

3.1 Design Objectives

Development of the CANDU 3 started in 1982 by identifying key design objectives[3,4]. These design objectives are listed below:

a. To improve traditional CANDU advantages, including safety, low radiation exposure, high capacity factor, ease of maintenance and low operating cost.

b. To reduce specific capital cost, construction schedule and unit energy cost.

c. To standardize the plant design such that it is suitable for any reasonable site, worldwide, without significant changes to the design.

d. To accommodate division among the plant structures and systems to facilitate a variety of shared financing, contractual arrangements, or partners with one or more organizations, without significant design or documentation changes.

e. To employ state-of-the-art technologies, including design, construction, operation and project management technologies, consistent with construction in the 1990s.

f. From a component design viewpoint, to:

   (1) maximize component life,
   (2) provide easy replacement at end of component life ("easy" replacement means quick and simple - without complex tooling or an extended outage, thereby minimizing radiation exposure),
   (3) minimize component cost, and
   (4) minimize component installation time and cost.

g. From a maintenance/in-service inspection viewpoint, to:

   (1) achieve a minimum of two years of station operation between scheduled maintenance/in-service inspection outages, which will not exceed 21 days, and
   (2) accommodate major equipment replacement (fuel channels, steam generators, etc.), major systems modification or modernization (control, computers, etc.), or major equipment refurbishing (reblading turbine, etc.) in a major maintenance outage not exceeding 90 days. Such a major main-tenance outage is expected to be required no more frequently than every 15 years.

h. From an operations performance viewpoint, to

   (1) achieve a lifetime capacity factor of 94% with less than one unplanned shutdown per year, and
   (2) provide the operator with modern information processing tools and methods to enhance human performance and to minimize the potential for plant upset due to error.

With the engineering of the CANDU 3 standard plant over 30% complete, we are confident that all of the above objectives will be achieved.

3.2 Safety

After reactor shutdown, decay heat removal from the fuel is the key to reactor safety. As with previous CANDU plants, the CANDU 3 follows an in-depth approach to heat removal.

Normal heat removal paths include the steam generators, which are supplied by two independent feedwater trains, and the fully capable shutdown cooling system, which is supplied with station services from two separate sources.

Should all normal heat removal paths be lost, the residual heat is rejected to the moderator system. Unlike other pressurized water reactor types, CANDU operates with the pressure vessel (fuel channels) surrounded by the cool low pressure moderator. Moderator volume is about 15 times the in-core coolant volume.

These multiple lines of defense result in a very low frequency of severe core damage for the CANDU 3.

In current CANDU designs, these heat removal systems are powered by pumps and controlled using valves. However, as discussed below, all of the decay heat removal systems can be made passive with built-in heat removal capability of at least three days.

4. NEXT GENERATION CANDU

Even as the engineering for the CANDU 3 is being completed, AECL is looking towards further improvements and evolution of this product. Some very challenging objectives and targets are being established for the next generation CANDU design. These include an expansion of the design basis set and stringent limits for off-site radiation doses and land contamination.

These, of course, are in addition to the objectives for further design simplification, improved constructibility, operability and maintainability, and lower plant cost.

To meet the above challenges, three principal design goals have been established:

a. to improve the overall capability of the plant so that it will have a higher level of resiliency to accident initiators.

b. to improve the capability of containment in coping with large releases of energy resulting from severe accidents, and

c. to improve the reactor design so that large reactivity transients can be eliminated,

A number of design studies have been identified and initiated to address the above goals.

The passive safety features currently under investigation, to address the above, are discussed below.

5. PASSIVE SAFETY FEATURES

The key feature of the passive cooling systems described below is the presence of a water source, close to the heat source, with sufficient capability to provide decay heat removal for at least three days, following a plant transient or accident. As shown in Figure 2, this concept effectively decouples the heat source from the normal heat sink by the introduction of a large thermal inertia between the two. This thermal inertia makes the plant more resilient and tolerant to disruptions or failures in the cooling water supply circuit.

5.1 Passive Safeguards for LOCA Events

The first line of defense against LOCA is the emergency core cooling system. The second line of defense is the moderator system. Design studies have been undertaken to simplify and improve the reliability of both systems.

Emergency Core Cooling System - This system is being considerably simplified so that the number of active components and automatic actions that have to take place after a LOCA are the absolute minimum. Core refill is achieved with two high pressure water tanks injecting into the reactor headers. Once the core is flooded, it is kept filled by recirculating water from the reactor building sump. The passive core refill system and the recirculating system are shown in Figure 3.

Moderator System - The moderator system is in operation during normal plant operation; therefore, its availability during a LOCA is assured. When the emergency core cooling system is available, the moderator provides cooling of the calandria tubes for those high power channels whose pressure tubes may expand into contact with the calandria tube. In that instance the moderator does not have a long-term function. However, in the case where the emergency core cooling system is unavailable, the function of the moderator is to remove decay heat for an indefinite period. In this instance it is desirable to rely on passive means for decay heat removal to ensure its long-term function.

Figure 4 illustrates one of several schemes being investigated for removing decay heat from the moderator using natural circulation. The operation of the system and the sequence of events is described with reference to Figure 5.

a) LOCA occurs at time zero. (AC power and the emergency core cooling system are assumed unavailable).

b) In ten seconds the power to the moderator is reduced to 10% of its nominal value.

c) At one minute, pressure tubes start to balloon or sag and contact the calandria tubes and at ten minutes all pressure tubes have contacted.

d) After contact is complete, the power transferred to the moderator rises to 65% of its nominal value and then follows the decay power curve.

e) Initially the moderator cooling system does not have adequate cooling capability and the moderator temperature rises until the heat transfer rate increases (due to boiling heat transfer in the heat exchanger) at about half-hour, as shown in Figures 5 and 6.

f) From then on, the moderator temperature increases slowly as the water in the tank heats up. The tank will be sized to provide adequate cooling, without operator intervention, for at least three days.

The studies performed to date have confirmed concept feasibility. The ongoing work is aimed at system optimization with respect to a number of design parameters, for example, inventory of heavy water in the moderator system, calandria design pressure and heat exchanger design.

5.2 <u>Passive Safeguards for Non-LOCA Events</u>

The first line of defense for non-LOCA events is the auxiliary feedwater system, which is automatically initiated. The second line of defense is the shutdown cooling system, and the third is the moderator.

Auxiliary Feedwater System - Further improvements to this system will not be required due to its short mission time and as a result of the enhancements to the shutdown cooling system described below.

Shutdown Cooling System - One of the options being considered for this system is shown in Figure 7. This scheme utilizes the same cooling water tank concept developed for the moderator system (Figure 4).

The shutdown cooling circuit has a check valve to prevent flow circulation as long as the heat transport pumps are running; hence no reactor power is lost to the water tank during normal operation. If electrical power is lost to the pumps then flow will be established in the circuit by natural circulation.

For the loss of AC power event the heat transport pumps will trip automatically. For other events, such as loss of feedwater or loss of service water, the heat transport pumps will be tripped on a steam generator "crash-cooldown" signal. As the pumps run down and the pump head decreases, the thermosyphoning head starts to build up and eventually natural circulation is established in the shutdown cooling circuit. Figure 8 illustrates the heat removal capability of this passive cooling circuit.

Moderator System - With a passive shutdown cooling system, a third line of defense is not really needed. Nevertheless, the moderator cooling circuit (discussed above) is available and is capable of removing decay heat for non-LOCA events as well.

5.3 Passive Safeguards for Containment

Although the other passive features discussed in this section reduce both the frequency and consequences of a severe accident, containment plays a special role in the safety of nuclear power plants. Because of this, it is important to ensure that containment integrity is maintained, regardless of the condition of the reactor core. This means that the isolation function must be performed with a high degree of reliability, and that the strength of the building must not be exceeded by internally generated pressure resulting from core damage.

Passive Isolation Devices - Figure 9 shows one of the passive isolation devices being evaluated for the reactor building ventilation system. The device is passively actuated by the internally generated pressure. As the cap is closed, a mechanical jaw (Not shown in Figure 9) is actuated to hold the cap closed even after the internal pressure is removed.

Pressure Suppression/Venting - The pressure suppression scheme shown in Figure 10 is being evaluated as a means for protecting containment integrity for events with severe core damage. The principle is simple. For events not leading to severe core damage, the pressure generated inside containment will be lower than the column of water in the standpipes. These events establish the design pressure of containment and do not require a relief capability. If, however, the design pressure is exceeded, the air/steam mixture inside containment is relieved through the standpipes. The steam in the mixture is condensed in the water pool, and the air is compressed in the air space above the water pool. Besides condensing steam, the water pool also cools the air escaping from containment, which also reduces the back pressure on the water pool and washes out fission products, which makes venting of the air space above the pool a possibility.

The event used to evaluate the feasibility of this concept is the early core disassembly scenario. In CANDU, this event has a very low frequency of occurrence ($<10^{-8}$ events/year). Nevertheless, it is selected because it is the absolute worst event and, if the concept works for this event, it will cover off all other severe accidents.

Early results from a preliminary investigation look promising and are shown in Figure 11. The results indicate that for a suppression volume of 5% of the containment volume, the peak pressure can be reduced by at least 15%, relative to the same containment without the pressure suppression capability.

This result is encouraging because it demonstrates that the pressure suppression scheme is at least three times more effective than increasing containment by the same volume; and, furthermore, it also provides the possibility of venting from the air space above the suppression pool to get further reductions in containment peak pressure, with only a fractional release to the environment.

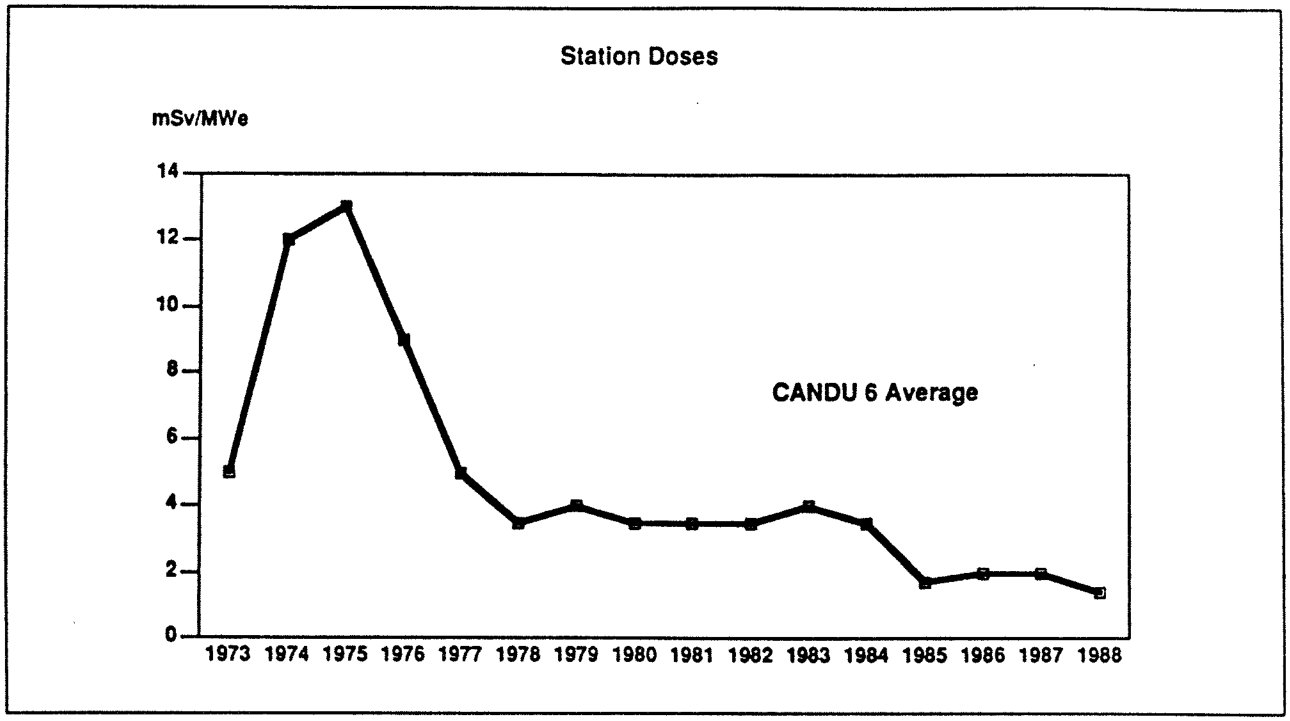
6.0 CONCLUSIONS

The CANDU 3 is the latest in the line of CANDU evolutionary nuclear power plants. Currently in the detailed engineering phase, the CANDU 3 meets the high level requirements established for the advanced LWR in all areas of design, construction and operation. For future designs, the passive cooling systems investigated to date for the moderator and shutdown cooling system are feasible and have the potential for significantly increasing safety and reliability, while reducing cost by eliminating redundant cooling water systems.

The containment studies are still in the early stages and further work is required to establish feasibility and costs. However, early results are encouraging.

References:

1. BROOKS, G.L.," Safety Aspects of Next Generation CANDU Reactors" paper presented at the IAEA Workshop on Safety of Nuclear Installations of the Next Generation and Beyond, Chicago, 1989 August.
2. HART, R.S., NATALIZIO, A. "CANDU - The Advanced PWR", Report AECL-9963, Atomic Energy of Canada Limited, CANDU Operations, Mississauga, Ont., (1989 August)
3. HART, R.S., "CANDU-3 - The Next Generation" AECL Report, Atomic Energy of Canada Limited, CANDU Operations, Mississauga, Ontario (1989 April).
4. HART, R.S., "Advances in Engineering and Construction", paper presented at the ANS/ENS International Conference, Washington, D.C., (1988, November).



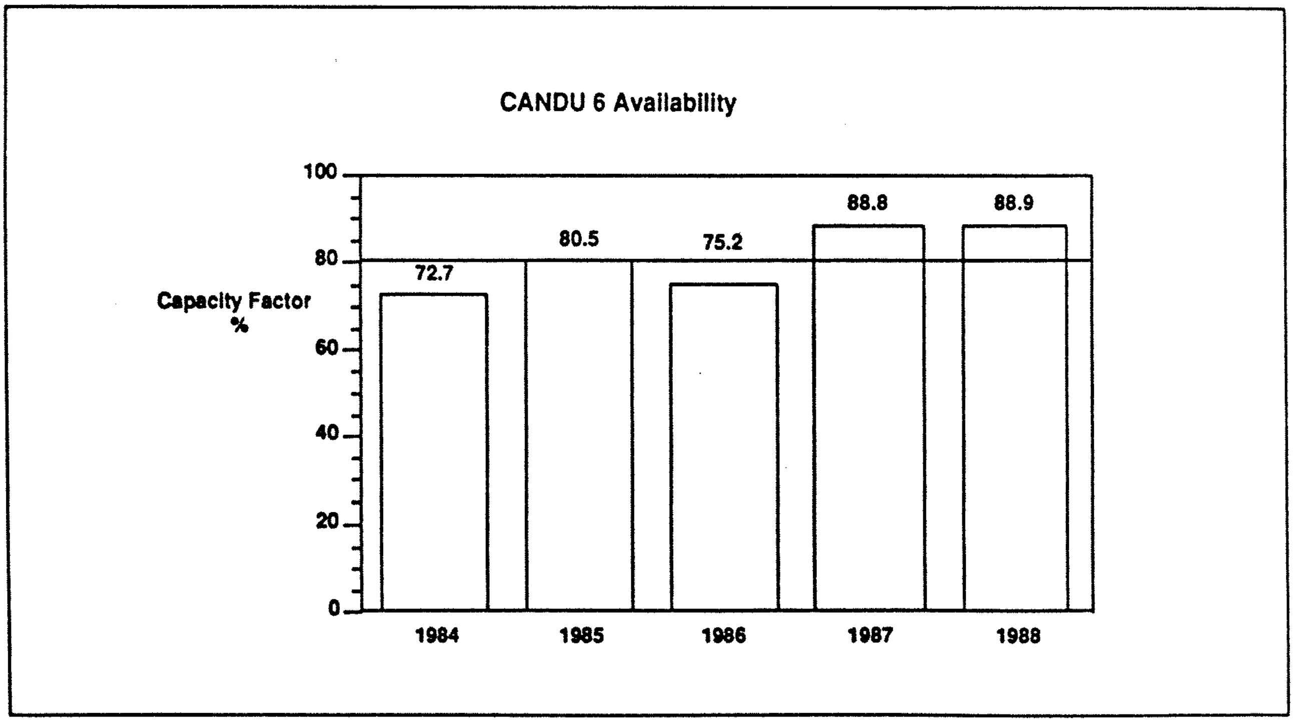
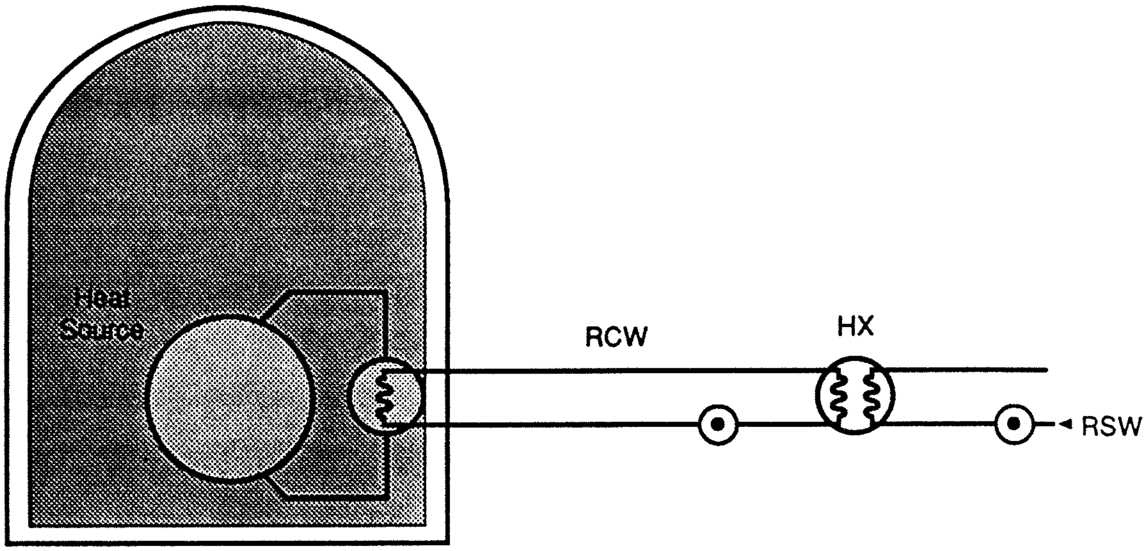
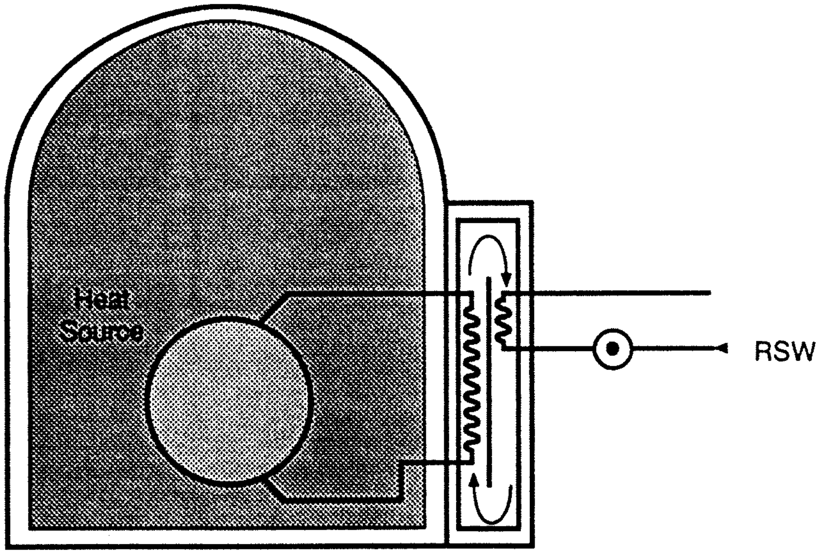


Figure 1 CANDU Performance



Conventional Approach



Passive Approach

[illegible]

FIGURE 2 Conventional and Passive Cooling Water Approaches

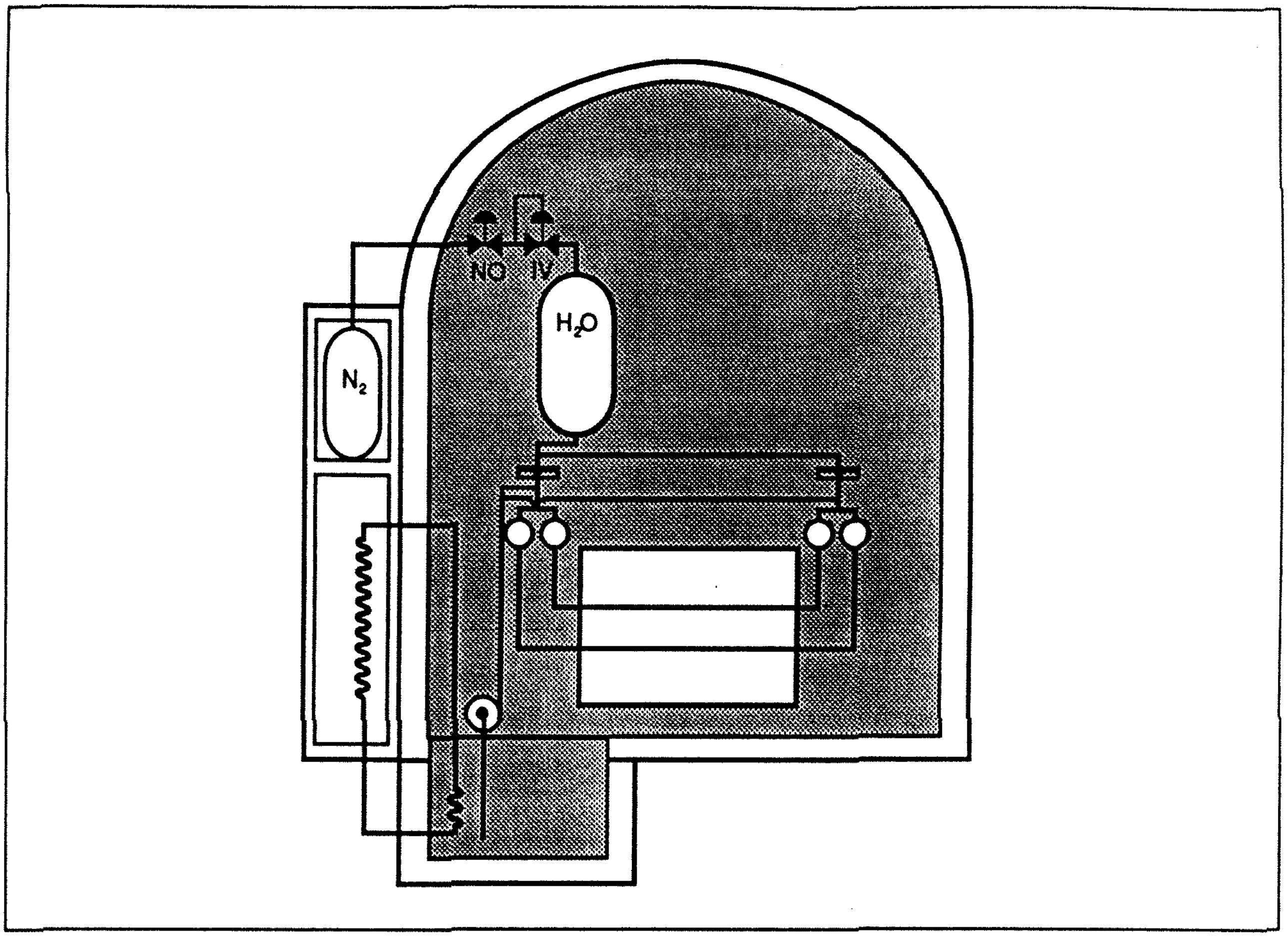
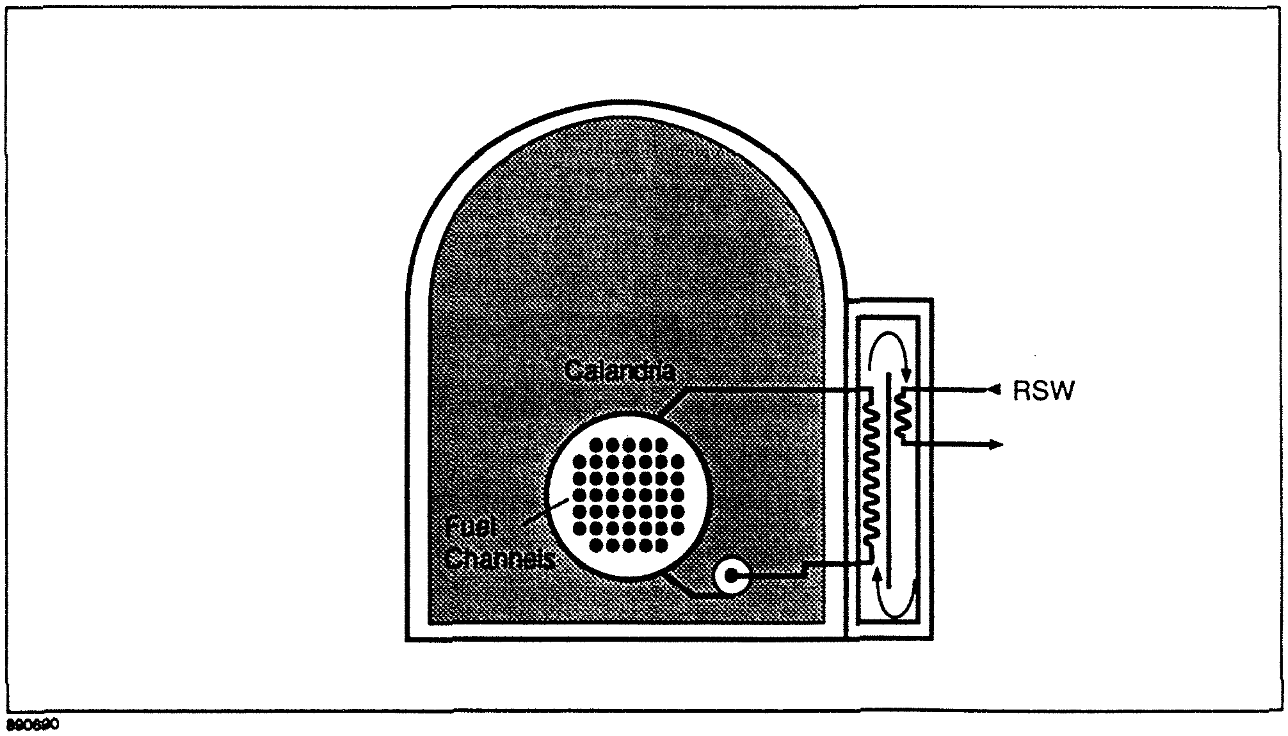


FIGURE 3 Simplified ECC System with Passive Refill Capability



890690

FIGURE 4 Passive Moderator Cooling System

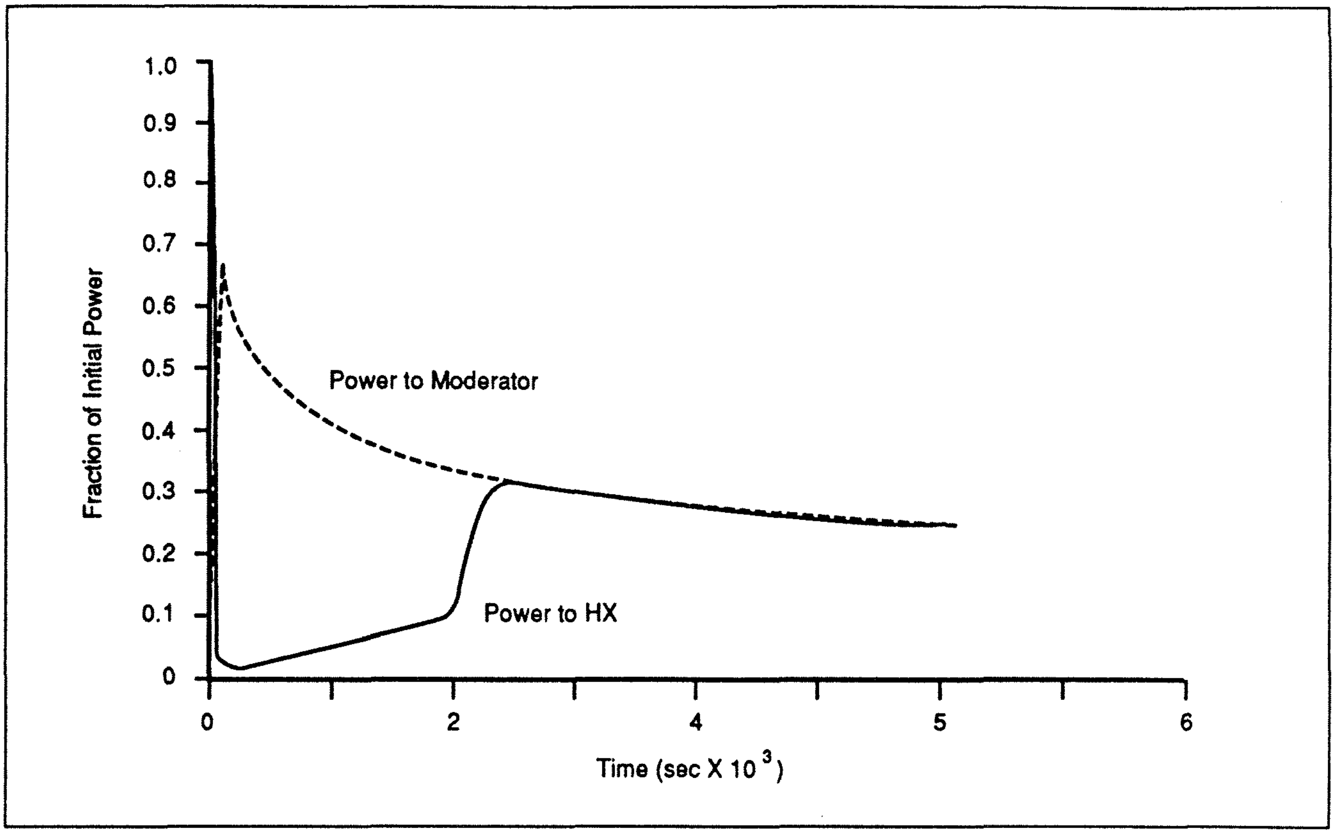
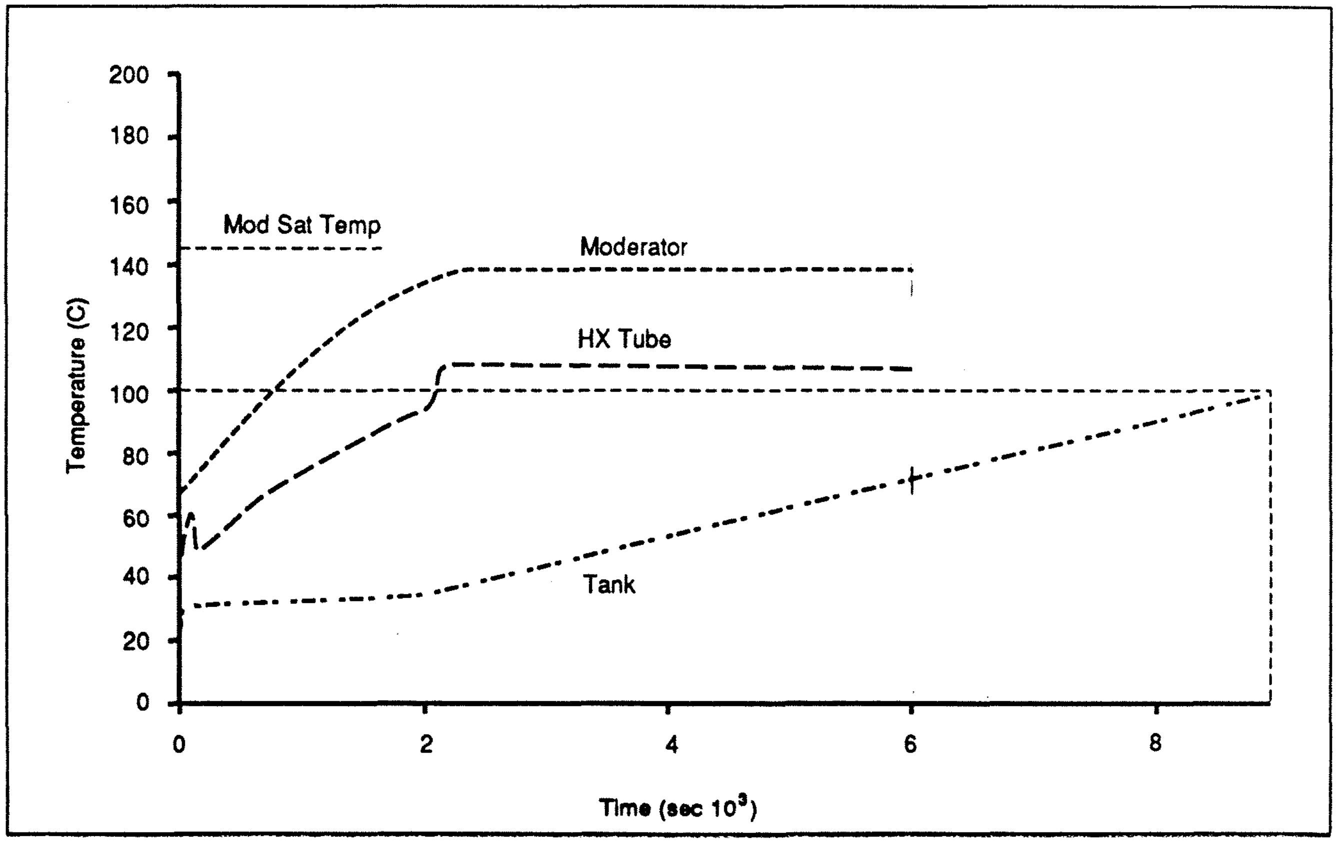


Figure 5 LOCA/LOECC Transient



890690

Figure 6 Moderator Cooling System Temperatures for LOCA/LOECC

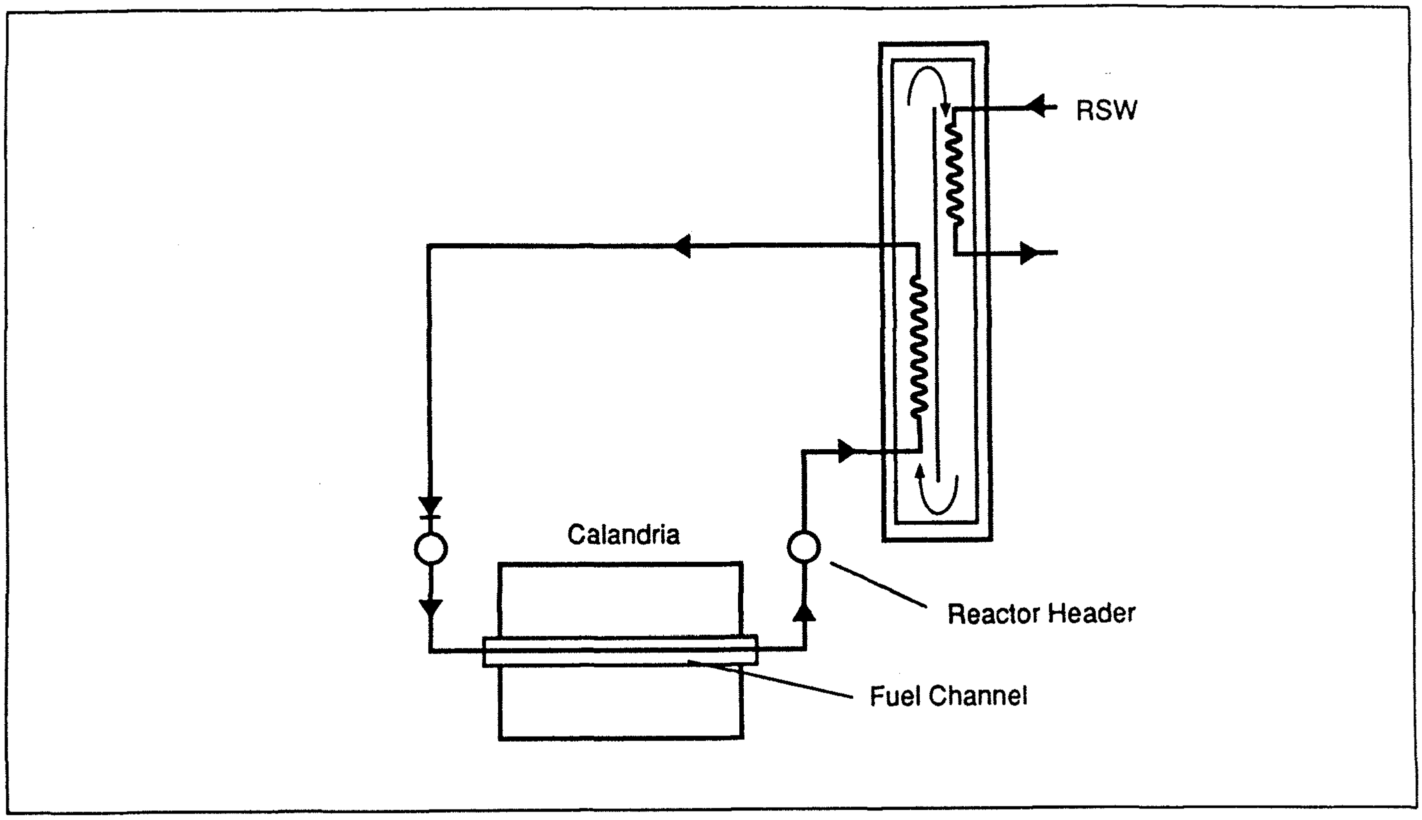
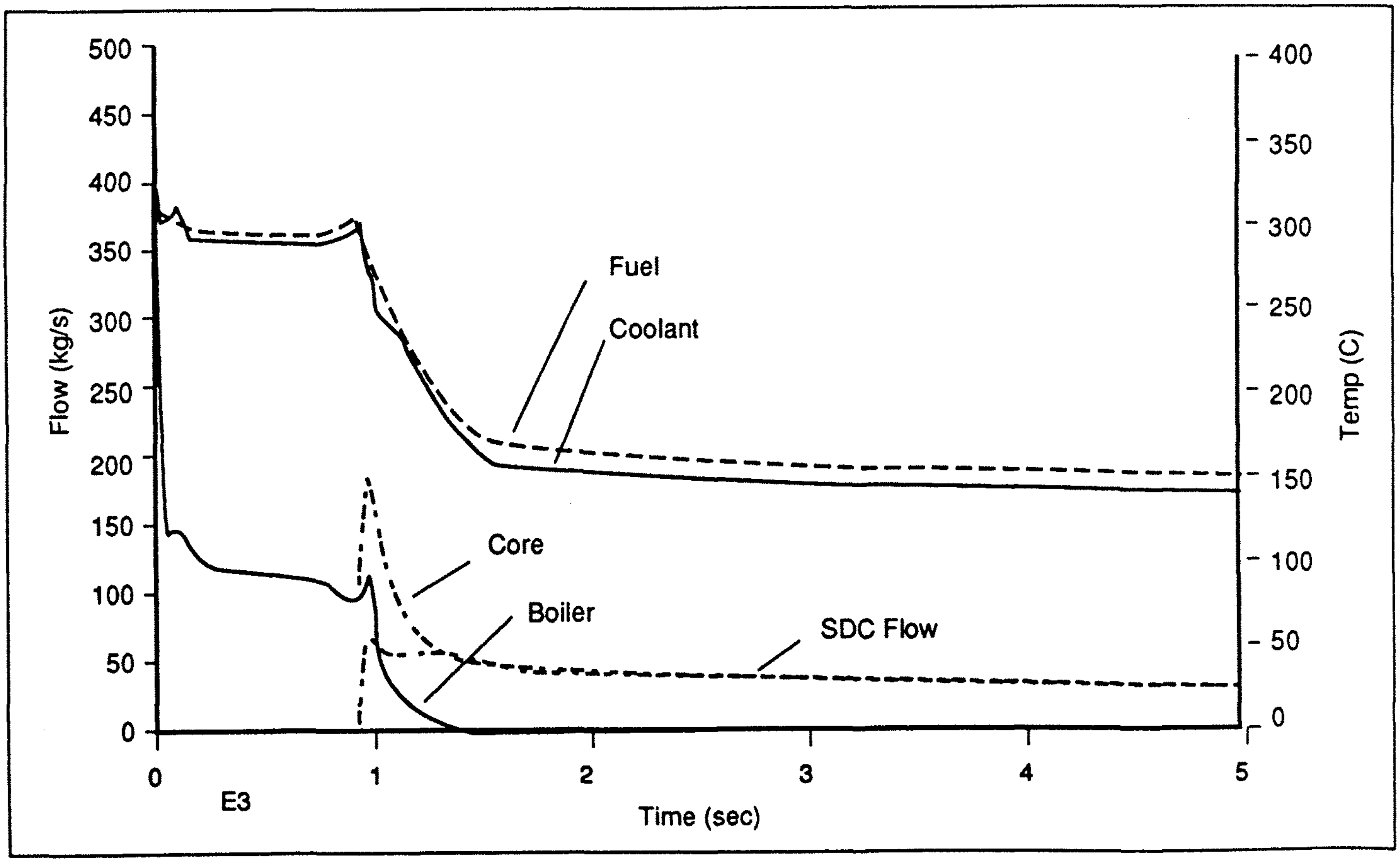


FIGURE 7 Passive Shutdown Cooling Loop



890690

FIGURE 8 Results for Loss of AC Power

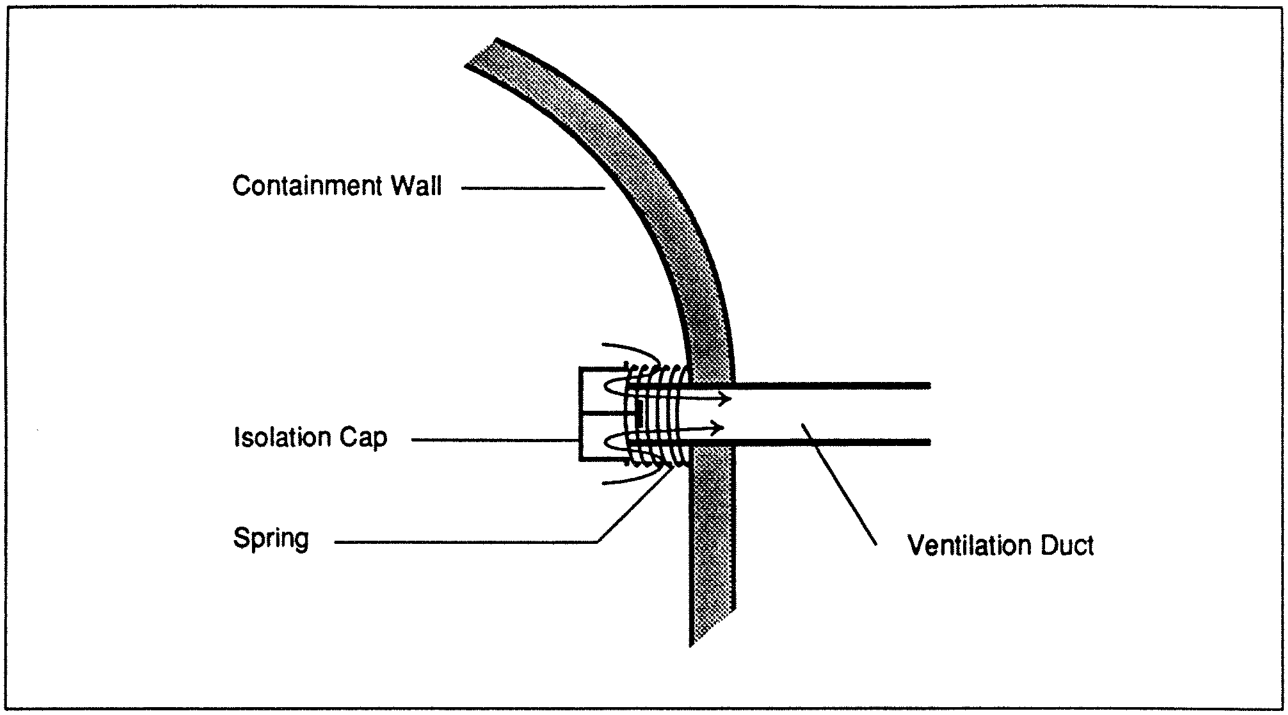


FIGURE 9 Passive Containment Isolation Device

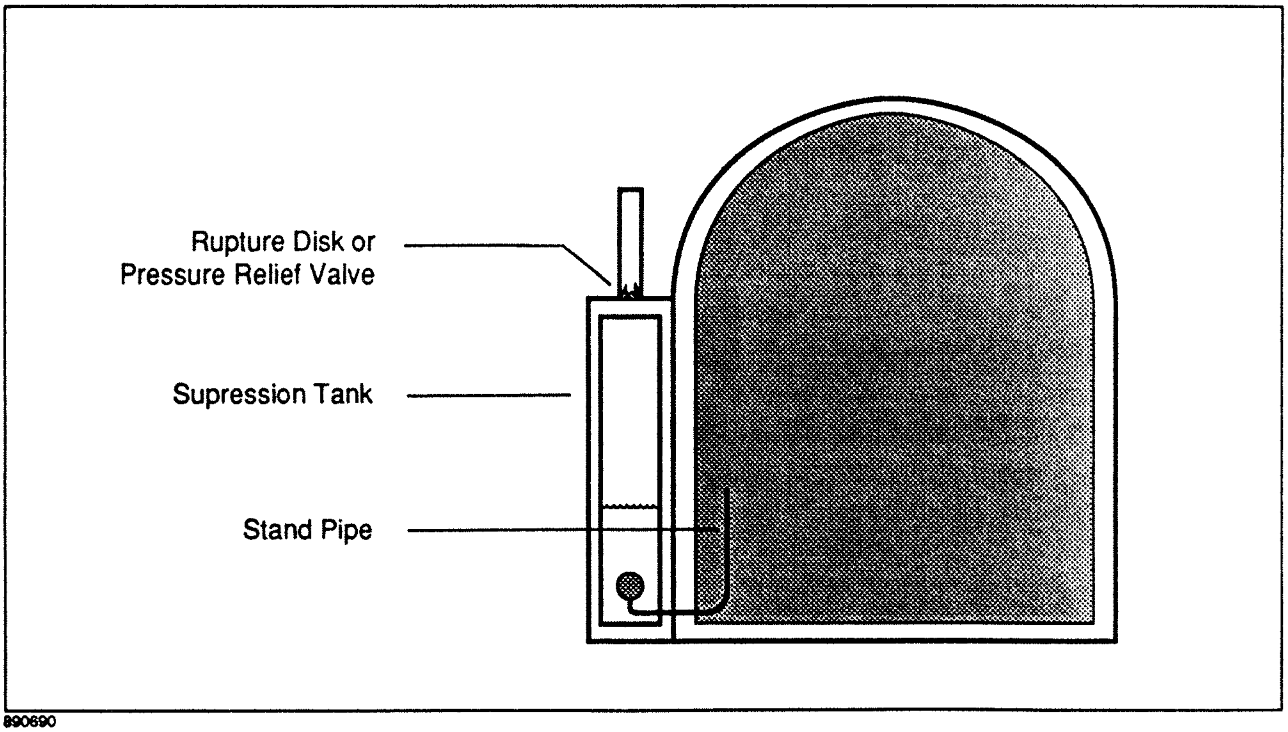
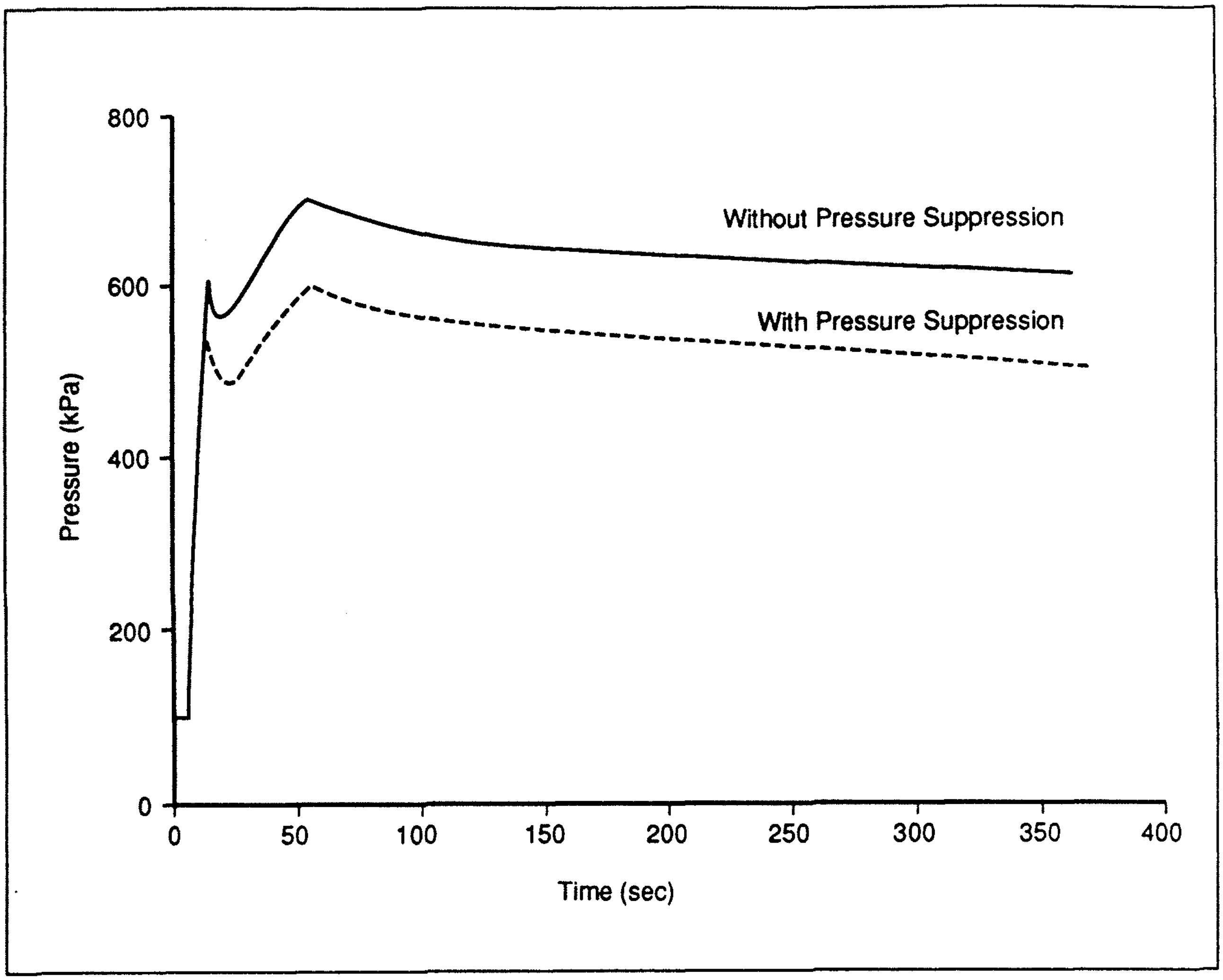


FIGURE 10 Passive Containmemt Pressure Supression/Venting Scheme



890690

FIGURE 11 Containment Pressure Transient for a Beyond Design Basis Event