ATOMIC ENERGY OF CANADA LIMITED
Power Projects, Sheridan Park, Ontario

Lecture 11

Nuclear power symposium

ACCIDENT ANALYSIS

J.D. Sainsbury
HEAD, SAFETY SECTION

ATOMIC ENERGY OF CANADA LIMITED
Power Projects

NUCLEAR POWER SYMPOSIUM

LECTURE NO. 11: ACCIDENT ANALYSIS

by

J. D. Sainsbury

1. INTRODUCTION

With respect to public risk, the nuclear industry's position is quite special; we are presumed guilty until we have proved our innocence. The Atomic Energy Control Board (AECB) in Ottawa sits in judgment as we present our defense, and a large part of this defense is the accident analysis - the subject of this lecture.

I'm going to begin this lecture in the same way as we begin our submissions to the AECB; by describing the safety features common to all CANDU reactors which are for the most part inherent to the reactor design as opposed to the specially engineered safety systems.

I will then review the series of failures we postulate in the accident analysis leading up to the pipe break or loss-of-coolant accident,which is most important (despite its low probability) because it has evolved as the design basis accident for all the engineered safety systems.

I will then describe these safety systems, explaining how we establish their required capability and how we demonstrate that they meet the requirements.

2. SAFETY FEATURES

2.1 Barriers to the Release of Fission Products

The hazards we consider in the accident analysis are those inherent in the radioactive materials produced by the reactor. Radioactivity can be produced in the coolant by the activation of impurities in the coolant. A radioactive form of hydrogen called tritium is produced in the heavy water moderator of all CANDU reactors and to a lesser extent in the heavy water coolant of the PHW type. However, the most significant to accident analysis is the radioactivity of the waste products of the fission process. The most significant of the fission products are the

noble gases such as Krypton and Xenon, and the isotopes of Iodine, Cesium and Strontium.

There are 5 barriers which prevent these fission products from reaching the public in any significant concentration:

(1) Fuel - diffusion resistant ceramic.

(2) Sheathing - sealed to vacuum technology standards.

(3) Heat Transport System - designed for and maintained to low leakage requirements.

(4) Containment - designed for and maintained to low leakage requirements.

(5) Exclusion Zone - provides atmospheric dilution of any fission product release.

I will now consider each of these in turn.

The uranium dioxide (UO_2) fuel is the first barrier to the release of fission products. UO_2 is a ceramic with a high melting point and is chemically inert in water. Most of the fission products remain trapped in the UO_2 matrix. Virtually all solid fission products are permanently retained even at operating temperatures, and only a small fraction of the gaseous fission products are released. For instance, only 5% of the Iodine-131 (the most significant isotope) gets free from the UO_2.

Each fuel element is sheathed with a zirconium alloy which forms the second barrier to fission product release. The sheath is designed to withstand the stresses resulting from UO_2 expansion and fission gas pressures, as well as external hydraulic pressures, and the mechanical loads imposed by fuel handling.

The coolant is contained in a closed heat transport system which forms the third barrier to fission product release. The carbon steel piping is designed to meet or exceed the relevant ASME Code regulations, and the zirconium-alloy pressure tubes (inside the core) are designed with a factor of about three between the working and ultimate stresses. This piping must fail before any fission products in the coolant could be released to the containment system.

The reactor and heat transport system are housed in a concrete containment system. This safety system is the fourth barrier to fission product release. There are two basic containment types used in Canada: the vacuum system used on multi-unit stations and the pressure

containment adopted for single unit stations. I will describe these two systems in some detail later; at this point it is sufficient to note that both systems attenuate any fission product release from the heat transport system by a factor of 10^6.

The public is excluded from a zone of 3000 feet radius from the plant. The atmospheric dilution between the plant and the boundary of this zone reduces the concentration of any fission product release from the containment system by a factor of 10^2 to 10^3.

This then is the five-layer defence between the public and the fission products produced in the fuel. Collectively they provide an attenuation of between 10^8 and 10^9.

2.2 Natural Uranium Fuel

All CANDU reactors use natural uranium fuel with heavy water moderator as explained by Dr. Pon in the first lecture, rather than the enriched fuel that is required in the reactors moderated with light water. Our combination of fuel and moderator has two significant safety advantages.

First, natural UO_2 fuel cannot be arranged in a critical array except in heavy water. For instance, the light water in the fuel storage bays where the fuel spends its retirement years does not have a sufficiently high moderating ratio to permit criticality. Secondly, the reactivity requirements in the reactor dictate a lattice geometry near the reactivity maximum and as a consequence lattice distortion or dispersion causes no positive reactivity transient. This is not the case, for instance, in the highly enriched breeder reactor being developed around the world. In these reactors the reactivity effect of fuel distortion is a serious concern in the safety assessment.

The oxide or ceramic form of the fuel has several advantages as well. The UO_2 does not react chemically with hot water and is therefore relatively tolerant to any sheath defects which might occur. UO_2 has a lower thermal conductivity than the metallic and carbide fuels which slows any feedback effects during transients. This slower response is an advantage to both the control and safety systems.

2.3 Reactivity Effects

The pressure tube concept (rather than pressure vessel) chosen for CANDU reactors also brings a safety advantage. All reactivity devices such as shutoff rods and control absorbers are outside the high pressure heat transport system, and are not therefore subject to ejection by any driving pressure. The pressure tube reactor has another even more important safety feature which I will point out when I discuss the loss-of-coolant accident.

The reactivity characteristics of the CANDU reactor are such that the control system does not require high response rates. The reactivity control devices are therefore mechanically limited to slow speeds which minimize the consequences of a control system malfunction.

3. SAFETY PHILOSOPHY

To understand the purpose of the activity we call "accident analysis" we must first understand the safety philosophy and requirements developed for Canada by the AECB.

The safety philosophy developed by the AECB is implemented by regulations and individual rulings on specific applications. General guidelines are published periodically covering the release and monitoring of radioactivity during normal operation and following accidents, and covering the design of the safety systems with respect to their reliability, redundancy, testability and independence. These guidelines establish the safety requirements which must be satisfied.

For the purpose of safety assessment, all systems in the plant are categorized as either process or safety systems. Process systems are those required for normal operation, and the safety systems are those provided to limit the release of radioactivity following failures in the process systems. An example follows:

Process Systems	Safety Systems
Heat Transport	Shutdown # 1
Control	Shutdown # 2
Turbine Plant	Emergency Cooling
Electrical Power Supply	Containment
etc.	

The Canadian safety philosophy recognizes that the risk people accept is dependent on the frequency of the event which puts them at risk. Thus the siting guidelines state maximum permissible radiation doses which must not be exceeded following two classes of event; the single failure in a process system and the much less frequent, single failure in a process system combined with the coincident failure of one of the safety systems. Thus we have single and dual failure dose limits.

Radiation Dose Limits for Failure Conditions

	Single Failures		Dual Failures	
	External Whole Body	Thyroid I-131	External Whole Body	Thyroid I-131
Individual	0.5 rem	3 rad	25 rem	250 rad
Population	10^4 man-rem	10^4 man-rad	10^6 man-rem	10^6 man-rad

The single failure dose limit would cause no measurable effect on public health. Even the dual failure dose limit causes only 40 fatalities per 10^6 population (from cancer) over a 10-20 year period compared to the annual death rate from cancer in the U.S. which is 1500 per 10^6 population or 15,000 deaths in the same 10-20 year period. The dose limits are truly conservative considering the frequency of the events that we class as single and dual failures and nuclear plants designed within these guidelines are indeed safe.

In addition to the dose limits the AECB siting guidelines state two requirements of the safety systems which are basic to the risk-frequency approach:

(a) The safety systems must be independent of the process systems and independent of each other. The single and dual failure approach is not valid, for instance, if a safety system failure occurs as a consequence of the initial process failure.

(b) Each safety system must have a demonstrated reliability greater than 0.997. This means that each safety system must be available to function properly 99.7% of the time.

These then are the safety requirements which have evolved from the Canadian nuclear safety philosophy. I will now discuss the accident analysis the designer does to demonstrate that the nuclear power plant meets the requirements.

4. ACCIDENT ANALYSIS

Each process system is considered in turn; component failures are postulated and the consequences assessed to demonstrate compliance with the single failure dose criterion. In these single failure cases we credit the operation of all four safety systems. Failures we postulate in the heat transport system include pump failure, pressure tube rupture, pipe rupture, end fitting failure, etc.

Failure of the control system is treated more simply. Since the control system is comprised of sophisticated control programs in a redundant twin computer system as well as a variety of reactivity devices, flow control valves, etc., it is almost impossible to single out all possible failure modes for analysis. Instead we identify the worst failure mode and assume that if we provide adequate protection against this we have covered all the other less serious failure modes. The worst failure is some combination of events which drives all reactivity devices positive at their maximum speeds. This produces the highest rate of reactivity increase possible from the control system.

Once we have analyzed the single process failures, we then postulate a coincident failure of each safety system in combination with each process failure to demonstrate compliance with the dual failure dose criterion. For instance, the worst failure mode of the control system is combined with coincident failure of shutdown system #1, then shutdown system #2, then emergency cooling, and finally containment. In each case the other safety systems are assumed to operate.

This systematic appraisal of single and dual failures does not lead to as many cases as first might appear since all four safety systems are not called upon for every process failure. For instance, a loss of control which causes a reactivity and hence power increase does not cause a loss of coolant from the heat transport system. The emergency cooling system is therefore not called on to operate, so postulating its failure following a loss of control is meaningless.

There is one type of accident which is much more severe than all the others. This is the loss of coolant resulting from a pipe rupture in the heat transport system. This postulated failure sets the design requirements for all four safety systems so that safety systems designed to these requirements are more than adequate for all other process failures.

4.1 Loss-of-Coolant Accident

A loss-of-coolant accident is the result of postulating a pipe failure somewhere in the heat transport system. The heat transport systems in CANDU-PHW reactors form a figure of eight (see Figure 1). The heavy water coolant is pumped through large pump discharge lines to the inlet header. Here the coolant is distributed to the fuel channels through small pipes called inlet feeders. After passing through the core the flow is directed through the outlet feeders to the outlet header, then through the heat exchangers to another set of pumps. This flow path is then repeated by another loop in series with the first and the total circuit forms a figure of eight. Most PHW reactors use two such figure of eight circuits in the heat transport system.

There are three basic consequences of pipe failure in the heat transport system:

(a) The break discharges flashing coolant which raises the pressure in the containment structure.

(b) Coolant is removed from the core section of the heat transport system and the reactivity of the core is increased.

(c) Heat transfer from the fuel to the coolant deteriorates and the temperature of the fuel sheaths increases.

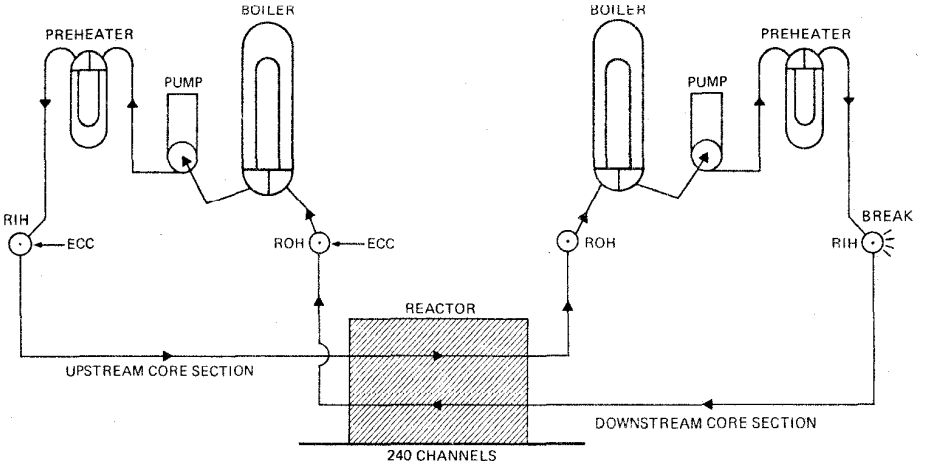

Figure 1 Primary Heat Transport System

The magnitude of these consequences is dependent on break location and break size. A brief description of these dependencies will demonstrate how we determine the particular pipe break which has become the design basis failure for all four safety systems.

The coolant at the inlet end of the reactor (pump discharge lines, inlet header and inlet feeders) is about 80°F cooler than the coolant leaving the outlet end of the core. Also the coolant pressure is highest at the discharge of the pumps. These two facts result in a larger specific discharge rate (lb/s-in^2) from breaks in the inlet piping (between pumps and core) than from breaks in the outlet piping. Therefore the pressure rise rate in the containment is largest following breaks in the inlet piping.

The removal of coolant from the core (core voiding) happens through the combination of two mechanisms; flashing of coolant due to general depressurization of the heat transport system, and additional boiling of coolant in the core due to the heat input from the fuel. A large inlet pipe break will stop the flow in the core and, if the break is large enough, will reverse the flow from the core to the break. The heat input from the fuel during this flow rundown and reversal causes rapid core voiding. A break in the outlet piping on the other hand increases the flow through the core and core voiding proceeds more slowly in response to depressurization. Core voiding (and hence reactivity addition) is fastest following breaks in the inlet piping.

The decreasing flow and high steam quality caused by a large break in an inlet pipe lead to dryout (explained in Lecture No. 8). The heat transfer during dryout is much less than normal and the fuel sheaths rise in temperature. Since the flow increases through the core following a break in the outlet piping the deterioration in heat transfer comes much later in the blowdown (when the power generation is low) and is less severe when it does come. For these reasons the sheath temperature transients are most severe following breaks in the inlet piping.

A break in the inlet piping is therefore our prime candidate for the design basis failure. The most severe break size is called the 100% break and has an area of twice the flow area of the pipe. Generally the largest pipe at the inlet end of the reactor is the inlet header. A 100% break in this header is therefore the design basis process failure in the CANDU reactor.

I will now take each safety system in turn and describe the requirements they must meet and how we demonstrate compliance with the requirements.

5. SAFETY SYSTEMS

5.1 Shutdown

A shutdown system puts a neutron absorbing material (poison) into the core to decrease the reactivity and turn off the power generation. Several systems have been developed for accomplishing this. Shutoff rods which gravity-drop into the core, shutoff rods which are gravity-drop assisted by springs, and liquid poison injection into the moderator, are the systems commonly used in recent designs.

Shutdown systems are not provided to protect the owner's investment but to safely stop any power excursion initiated by a process failure. Both loss of control and loss of coolant can increase system reactivity and start a power excursion. However, the reactivity rates following loss of coolant are much larger than the control system can provide and so the consequences of pipe failure set the delay and reactivity rate requirements of the shutdown system. Losing the coolant from the core also provides a larger total reactivity effect than the control devices can provide, so the loss-of-coolant accident also sets the total reactivity depth required of the shutdown system. Now we can define the specific requirements.

The postulated pipe failure violates our third barrier to the release of fission products. Failure of containment (our fourth barrier) must be postulated as a coincident event, and the fission product release must not exceed the dual failure limit. To meet this requirement we must demonstrate that the remaining working safety systems (shutdown and emergency cooling) limit the fuel sheath failures to a very small number. In fact we adopt a target for design purposes of no significant fuel sheath failures following the large failure of an inlet header. From this comes the specific requirement of the shutdown system. It must limit the overpower pulse and provide a sufficiently fast power rundown that the heat generated in the fuel can be removed by the discharging coolant and later by the emergency coolant without significant sheath failures. This then is the requirement. It remains to describe how we demonstrate compliance with this requirement.

The conditions in the core following the pipe break are calculated using a blowdown code which models the hydrodynamics, the fuel, and the neutron kinetics of the system. We have developed confidence in the model by numerous comparisons with experiments.

The core voiding which causes the reactivity increase is of prime importance when assessing the shutdown system capability. Figure 2 shows the voiding transient for each core section of a figure of eight

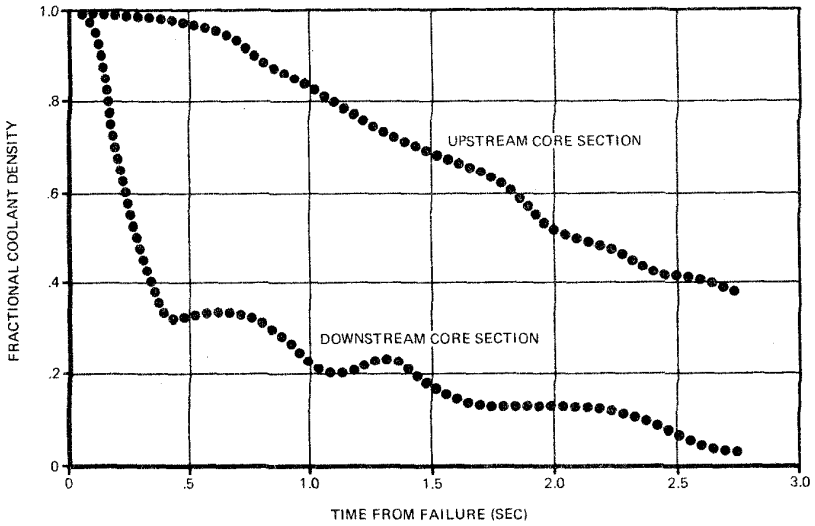

Figure 2 Coolant Density in the Two Core Sections Following Inlet Header Failure

heat transport system following the large break of one of the inlet headers. The coolant density as a fraction of the starting density is shown as a function of time after the break. The downstream core section experiences the fast flow reversal described earlier and voids quite quickly. If you look back to the circuit schematic of Figure 1 you see that an inlet header break appears to the upstream core section as a remote outlet end break. For this reason the core voiding in this part of the core is much slower.

These two core voiding transients together cause a positive reactivity transient like the one shown in Figure 3. (Figure 3 is a plot of all the reactivity components following a pipe failure in the Pickering reactor.) As long as the net reactivity remains positive the power increases so the shutdown system must counteract the positive void contribution fairly quickly to limit the overpower pulse. At this stage of the analysis the delay and reactivity rate requirements of the shutdown system are set. The delay has several components:

- time for the tripping parameter to reach the set point,
- time for trip signal to reach the shutdown device,
- delay inherent in shutdown device,
  - clutch de-energizing and inertia in shutoff rod system,
  - valve opening and transit time in liquid poison system.

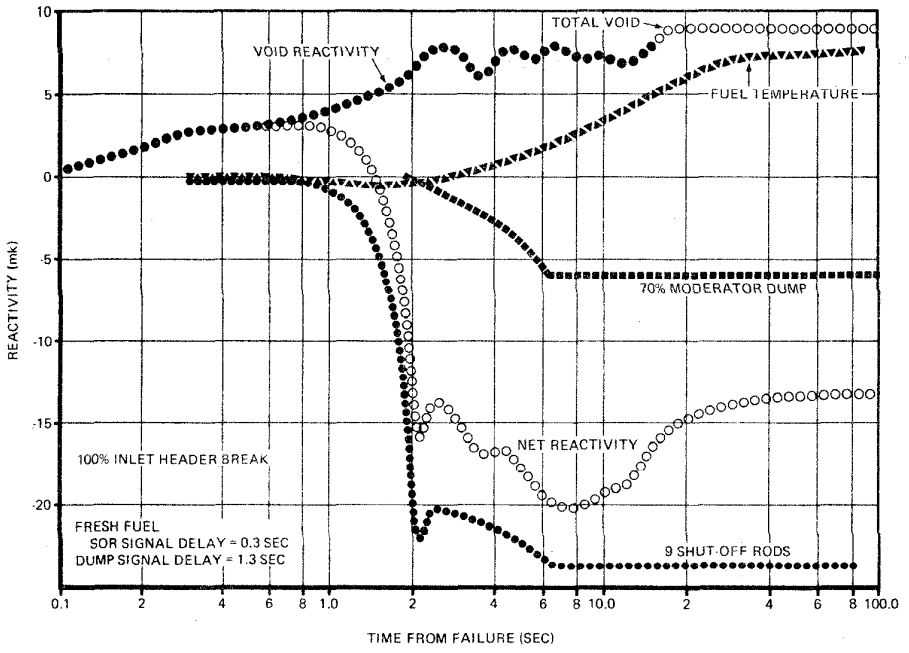

Figure 3 Reactivity Transients

The shutdown reactivity rate beyond this delay is a function of the type of shutdown device. Figure 3 shows the shutdown characteristic for nine gravity shutoff rods following a signal delay of 0.3 second. The net effect of the positive void reactivity and negative shutdown reactivity (confining ourselves now to the first two seconds in Figure 3) is an overpower pulse as shown in Figure 4.

The overpower pulse is only the first part of power generation which must be minimized by the shutdown system. The second part is the power rundown which is dependent on the reactivity depth of the shutdown system. The Pickering reactor uses a partial dump of the moderator to augment the depth of the shutoff rods. Therefore the shutdown depth in Pickering is 24 mk from the shutoff rods plus 6 mk from partial dump, totalling 30 mk. There is a second positive reactivity component shown in Figure 3. This is due to cooling down the fuel and is characteristic of new unirradiated fuel. As the fuel burnup proceeds this effect reduces to zero and for most of the reactor life the only positive reactivity is from coolant void. The combined effect of all these reactivity components is shown as the net reactivity of Figure 3. This net reactivity beyond 2 seconds determines the rate of power rundown.

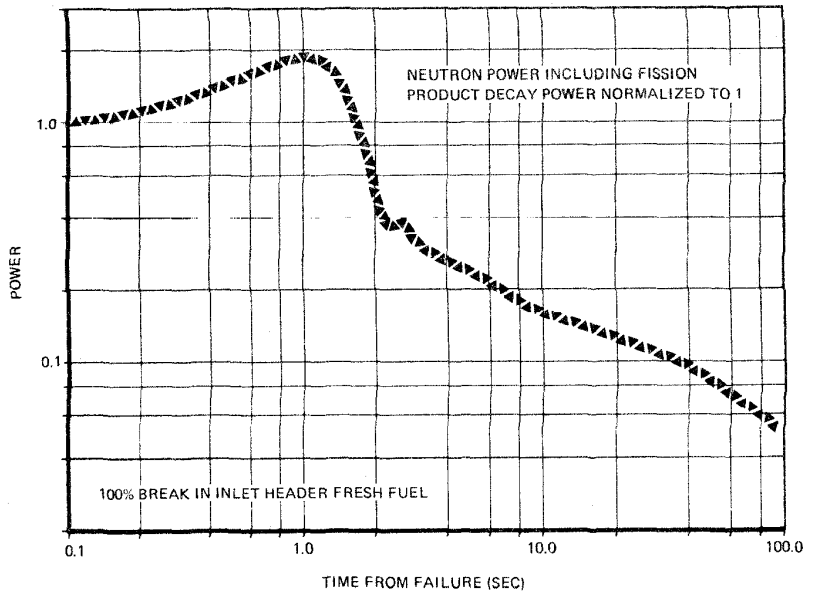

Figure 4 Neutron Power Transient

The integral of the power transient of Figure 4 is the quantity of heat added to the fuel during the blowdown (blowdown to atmospheric pressure occurs in about 100 seconds following the large header failure). The smaller the integrated power the lower the fuel sheath temperatures during blowdown. Thus the delay, reactivity rate and reactivity depth of the shutdown system is designed to limit the integrated power so that the sheath integrity is maintained during the blowdown. The shutdown characteristic is measured during the commissioning of the reactor and compliance with the required delay and rate is assured by periodic in-service testing.

Before I leave shutdown systems I want to describe an important recent development in the Canadian safety philosophy. Early Canadian reactors had one shutdown system, and one of the dual accidents analyzed in those reactors was a process failure which increased system reactivity (such as loss of control or loss of coolant) coincident with complete failure of the shutdown system. The object of this dual failure analysis was to demonstrate the capability of the containment to withstand the overpressure and to limit the release of fission products. However, the analysis of the consequences which involve core disassembly, pressure tube rupture and the discharge of coolant and fuel fragments into the moderator and ultimately a large heat release to the

containment, had a large uncertainty. The analytical uncertainty was compounded by the fact that the construction of the containment structure must begin early when the details of the reactor design (which influence the outcome of the postulated failure) are not finalized. Prevention of the accident is a much better solution than designing to live with it, and to that end we now provide two independent shutdown systems in our reactors. Each shutdown system has its own trip logic and signals and is capable of coping with the process failure even if the other should fail to operate. Thus the Bruce reactors have both a shutoff rod system and a liquid poison injection system.

5.2 Emergency Core Cooling

Previously I stated that following a header failure coincident with a failure of containment, the shutdown system and emergency cooling system together must prevent significant fuel failures. The requirement of one system is not independent of the capability of the other; they are two systems acting together to safeguard the fuel.

The mechanism of sheath failure following a loss-of-coolant accident needs explanation here to understand the fuel cooling analysis. Some of the fission products generated in the UO_2 by the fission process are gases. Some of these fission gases diffuse from the UO_2 and some get free through cracks that appear in UO_2 as it burns up. The effect of this release of gas from the UO_2 is a buildup of pressure inside the Zircaloy sheath. Deliberate gas spaces are provided in the fuel element to limit this gas pressure to values near the coolant pressure when the fuel is hot. In this way there is no pressure differential across the fuel sheath during normal operation.

However, during the blowdown following a pipe rupture, the coolant pressure drops (from 1200 psig to atmospheric in 100 seconds following the large header failure). Therefore the pressure differential across the fuel sheath is increasing during blowdown. This is of no consequence if the sheath remains near its operating temperature of 600°F, but unfortunately an increased sheath temperature is another consequence of the loss-of-coolant accident. Like all metals the strength of Zircaloy decreases with temperature. It is obvious from this that higher sheath temperatures can be accepted in the early portion of the blowdown when pressure differential is small than near the end of blowdown when the pressure differential is large. Thus the failure threshold for the sheaths is a function of both coolant pressure and sheath temperature for a given fuel design. If this threshold is exceeded the sheath can swell to block the coolant passages and prevent further cooling

or it can swell to rupture. Now that we understand the potential sheath failure mechanism we can go on to look at the sheath temperature transients and the role of the emergency cooling system.

The blowdown code that we use to predict coolant voiding also calculates the UO_2 and sheath temperatures throughout the blowdown. Figure 5 shows the sheath temperatures (upper curves) and average UO_2 temperatures (lower curves) during the blowdown in Pickering that we were discussing earlier. The rise of the UO_2 temperature in the first 2 seconds reflects the power pulse and the subsequent drop reflects the flow of heat to the outer portions of the fuel and the heat transfer to the coolant.

The sheath temperature transient is most severe in the downstream core section which experiences the flow reversal. The important point is that the high sheath temperatures occur early in the blowdown when the coolant pressure is still quite high. Beyond the initial rise the sheath temperature decays away slowly as the blowdown proceeds. This transient which is typical of a PHW blowdown does not exceed the sheath failure threshold. For this reason we do not require high pressure emergency cooling and the flow of emergency coolant into the heat transport system can wait until near the end of blowdown when the normal coolant is nearly all gone. The adoption of a low pressure emergency cooling system is dependent on a shutdown system with sufficient depth to limit sheath temperatures during the blowdown as in the analysis I have shown.

In our recent designs emergency coolant is supplied by gravity from a head tank. The injection pressure is about 40 psi. An important part of the system is the logic used to sense the location of the failure and direct the emergency coolant to the intact headers on the opposite side of the core. In this way we guarantee all the emergency coolant passes over the fuel on its way to the break. Also the core is the lowest point in the heat transport system of our PHW reactors and all the piping (except the small feeders) is above the core. This provides assurance that the core can be easily flooded by the incoming emergency coolant. These two features (logic and low core) eliminate the possibility of emergency coolant bypassing the core and going directly to the break, which is a serious concern at present in the U.S. pressure vessel reactors.

This discussion of emergency cooling leads directly to one of the most significant safety features inherent in the pressure tube reactor. The heavy water moderator is contained in a stainless steel calandria vessel and separated by the calandria tubes from physical contact with

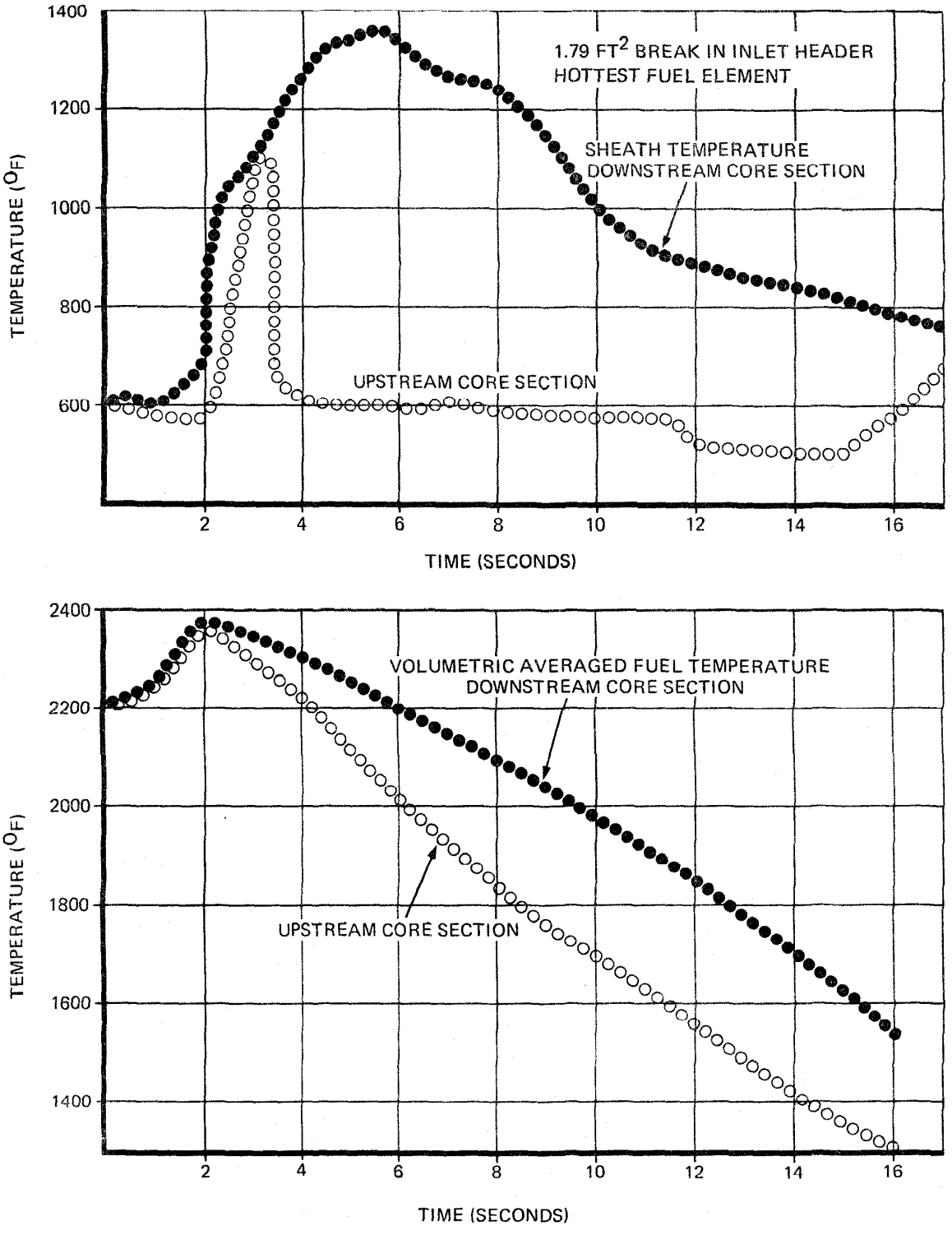

Figure 5 Fuel Temperatures

the pressure tubes. This design confines the high temperature coolant to relatively small channels. The heavy water moderator and reflector which surround these channels are at a relatively low temperature and the pressure is only a little above atmospheric. As a result, they act as a heat sink in the event of a reactor accident. This distributed heat sink in the core is an important safety feature of the CANDU reactor because failure of emergency core cooling does not lead to a core meltdown. This is not the case in pressure vessel reactors because both coolant and moderator are discharged through a pipe break. The very serious consequences of a core meltdown are a large part of the reason for concern about the reliability and effectiveness of emergency cooling systems in the pressure vessel reactors.

5.3 Containment

Containment, our fourth barrier to fission product release, is designed to withstand the overpressure created by a loss-of-coolant accident with little leakage to the atmosphere. In addition to the concrete structure there are several sub-systems which together form the containment system.

(a) Pressure Suppression System - In multi-unit stations a separate building normally isolated from the reactor buildings is maintained at a vacuum. In addition, this vacuum building has a water dousing system to condense incoming steam following a loss-of-coolant accident. The isolating of the vacuum building is accomplished by a bank of large self-actuating valves. Figure 6 is a schematic of this system. In single unit plants a water dousing system is provided in the reactor building to limit the peak pressure and minimize the period of overpressure following a loss-of-coolant accident. The containment for the Gentilly reactor shown in Figure 7 is an example of this type of system.

(b) Isolation - The containment structure is penetrated by ventilation ducts required to maintain humidity and temperature control in the reactor building. Since this system exhausts to atmosphere (either wholly or partially depending on the design) isolation dampers are provided which close automatically on signals of high pressure or high activity in the containment atmosphere.

(c) Other Heat Sinks - Fan-coil coolers are provided throughout the reactor building to control the temperature of the building atmosphere during normal operation. In some cases we credit their capability to condense steam following a loss-of-coolant accident to minimize the period of overpressure. When they are credited in this mode they become an essential component of the containment system.

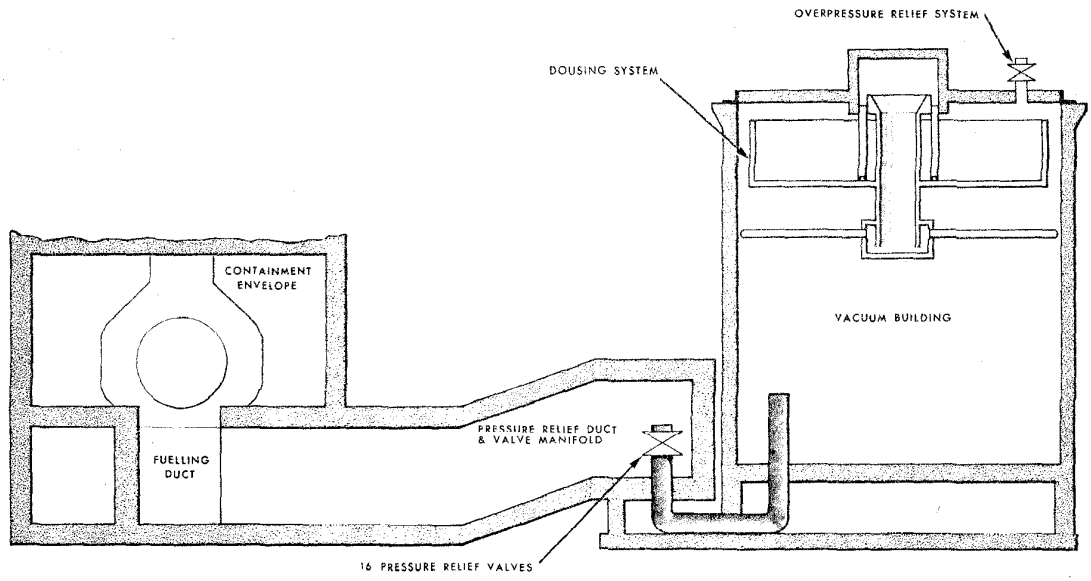

Figure 6 Vacuum Containment System

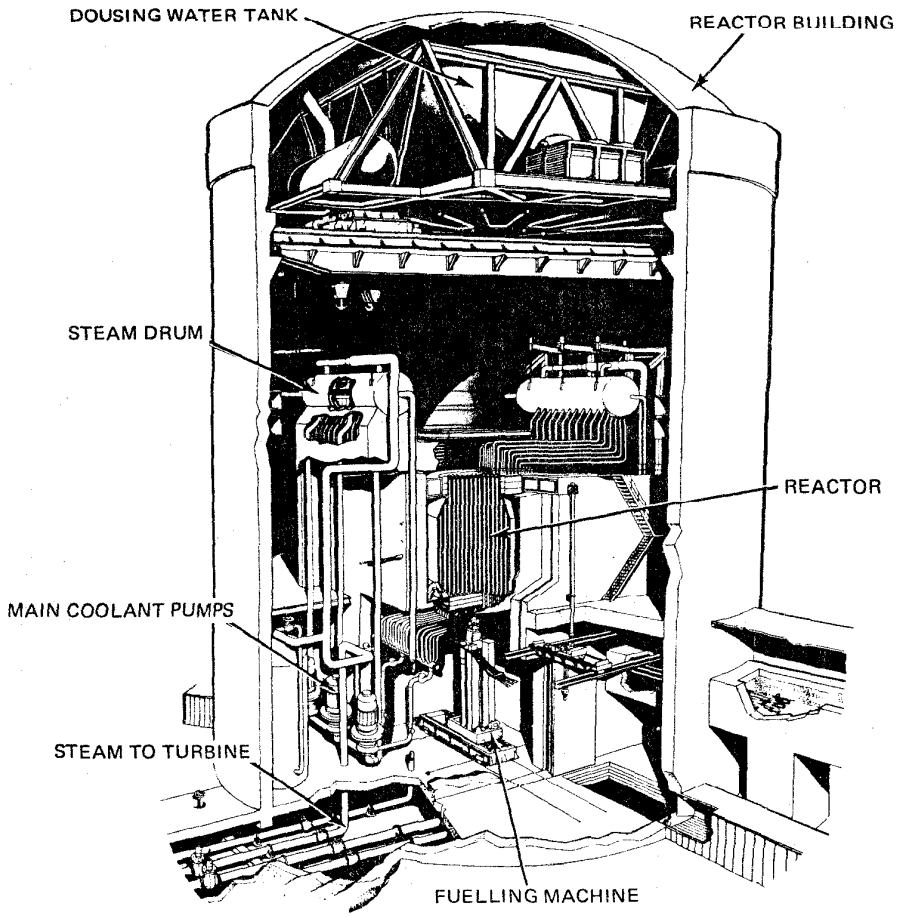

Figure 7 Gentilly Reactor Building

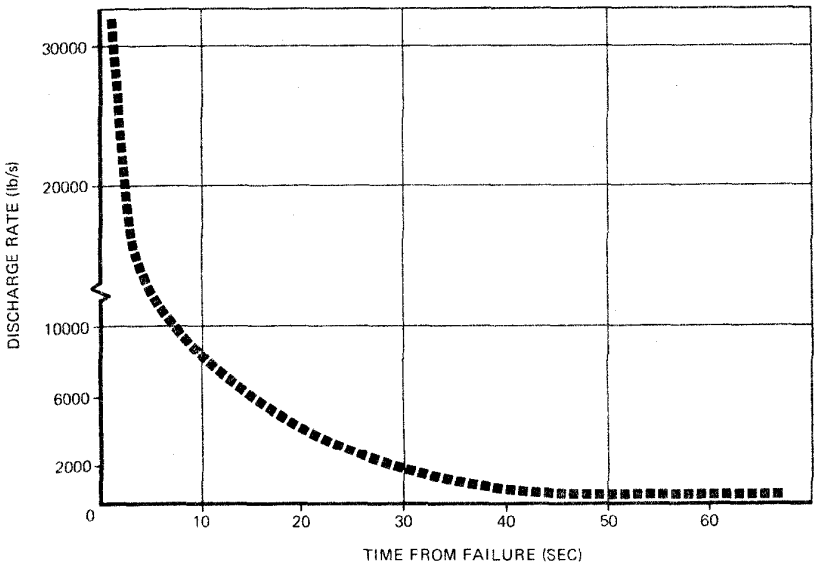

Figure 8 Coolant Discharge History
Following Inlet Header Failure

Since construction starts first on the concrete structures, the safety analyst must address the question of containment requirements early in the design phase. This requires a knowledge of the reactor design and geometry of the heat transport system. The largest pipe size at the inlet end of the reactor must be known to define the largest break size and hence largest discharge rate of coolant to the containment. Figure 8 shows the coolant discharge characteristic from a large break in a 22 inch inlet header. In addition to the heat stored in the coolant, heat stored in the piping and fuel is available to the containment atmosphere. Once the mass and energy discharge to the containment atmosphere is known, the peak pressure is calculated as a function of the characteristic of the pressure suppression system. This early analysis usually takes the form of a parameter survey since containment volume and the characteristic of the pressure suppression system can be varied to arrive at an economic minimum.

The pressure transients following a loss-of-coolant accident are quite different in the two containment types. The pressure rises quite quickly in the reactor building of a vacuum containment system (Figure 9) since the volume of the reactor building is relatively small. However, when the pressure reaches about 1 psig at the pressure relief valves they open and discharge first air, then steam and air into the vacuum building. The pressure peaks out in the reactor building

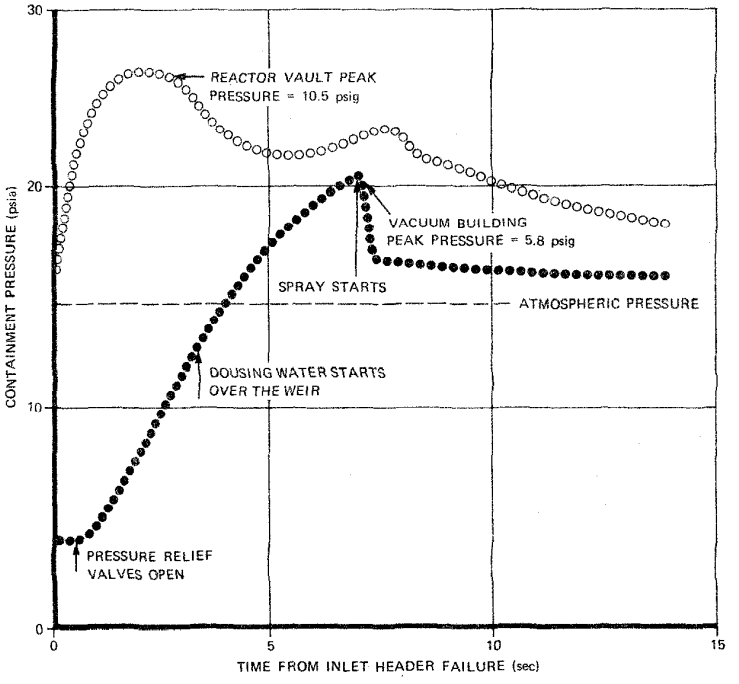

Figure 9 Vacuum Containment System Pressure Transients

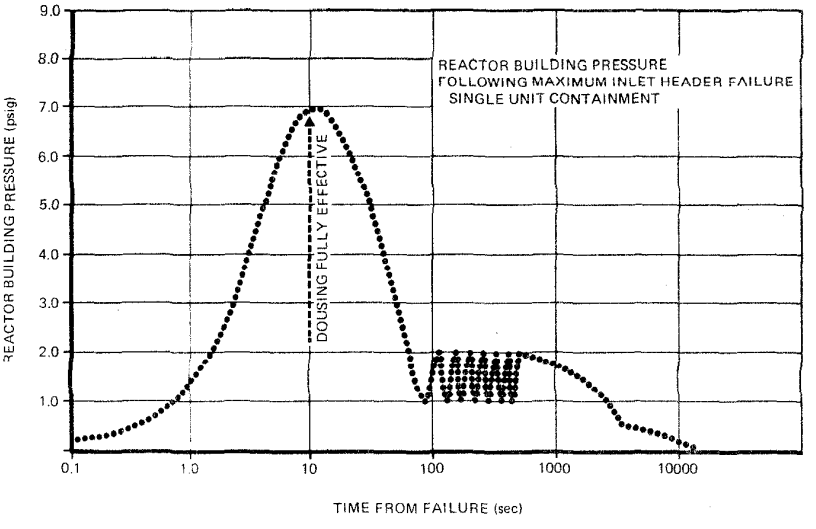

Figure 10 Single Unit Containment Pressure Transient

soon after the pressure relief valves open and decreases to less than atmospheric in a few tens of seconds.

The pressure transient in a single unit containment is more prolonged (Figure 10). The pressure rises slower initially because of the greater volume in the reactor building. When the pressure reaches about 2 psig the dousing system is signalled to start. The dousing action turns the pressure over and brings it down more slowly than the vacuum system and overpressure period is longer. Since the leakage from the containment is a direct function of the integrated overpressure, the building of a single unit containment must meet a tighter leak requirement than the buildings in a vacuum system.

6. SUMMARY

I have described the safety features inherent in the CANDU pressure tube reactor, and have discussed some of the analysis we do to set requirements for the engineered safety systems and to demonstrate compliance with these requirements. I have not been able to describe all the analysis nor the experimental programs that also are a part of the endeavour in the nuclear industry to provide a very high standard of safety.