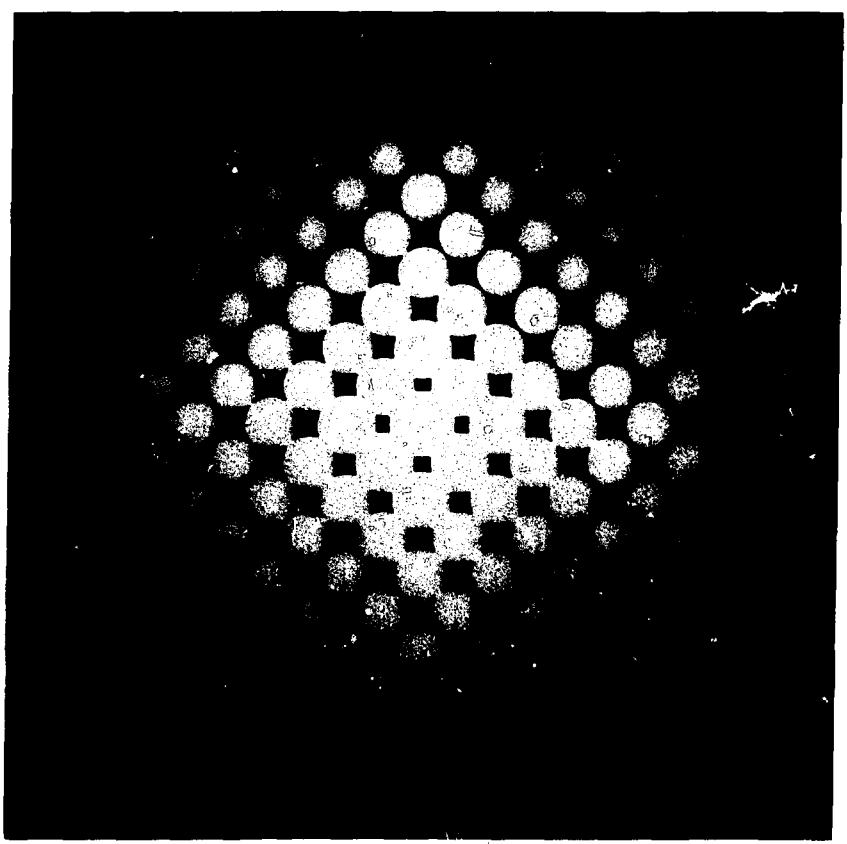
Safety of CANDU Nuclear Power Stations

by V.G. Snell

AECL - 6329



Safety of CANDU Nuclear Power Stations

by V.G. Snell

Dr. Snell heads a section within the Safety Branch of the Reactor Performance Engineering Group, Engineering Company, AECL, Sheridan Park, Ontario. A high energy physicist by training, Dr. Snell has had several years' experience in safety analysis of nuclear power systems.

November 1978

AECL-6329

ABSTRACT

A nuclear plant contains a large amount of radioactive material which could be a potential threat to public health. The plant is therefore designed, built and operated so that the risk to the public is low. Careful design of the normal reactor systems is the first line of defense. These systems are highly resistant to an accident happening in the first place, and can also be effective in stopping it if it does happen.

We back up the normal systems with special independent and redundant safety systems. Their sole purpose is to minimize the effects of an accident, or to stop it completely. They include shutdown systems, emergency core cooling systems, and containment systems. We also show that massive impairment of any one safety system, together with an accident, can be tolerated. This "defense in depth" approach recognizes that men and machines are imperfect and that the unexpected happens. The nuclear power plant need not be perfect to be safe. To allow meaningful judgments, we must know *how* safe the plant is. The Atomic Energy Control Board guidelines give one such measure, but there are several reasons why these may over-estimate the true risk. We interpret the guidelines as an upper limit to the total risk, and trace their evolution.

RESUME

Une centrale nucléaire contient une grande quantité de matériaux radioactifs qui pourraient menacer la santé du public. Par conséquent, la centrale est conçue, construite et exploitée de telle façon que le danger encouru par le public soit faible.

Une conception soignée des systèmes normaux du réacteur est la première ligne de défense. En premier lieu, ces systèmes résistent fortement à un accident et sont en outre capables de l'arrêter si l'accident a lieu.

Les systèmes normaux sont renforcés par des systèmes de sûreté spéciaux, indépendants et redondants. Leur but unique est de réduire au minimum les effets d'un accident ou de l'arrêter complètement. Ils comprennent des systèmes d'arrêt, de refroidissement d'urgence du coeur et de confinement.

Le rapport indique également que la défaillance massive d'un des systèmes de sûreté coïncidant avec un accident, peut être tolérée.

Cette "défense en profondeur" reconnaît que l'homme et ses machines ne sont pas parfaits et que l'inattendu peut se produire. Mais il n'est pas nécessaire que la centrale nucléaire soit parfaite pour être sûre.

Afin de pouvoir prendre de bonnes décisions, il faut connaître le degré de sûreté de la centrale. Les directives de la Commission de contrôle de l'énergie atomique en donnent une certaine mesure, mais il existe plusieurs raisons qui disent que le vrai danger a peut-être été surestimé. Le rapport interprète ces directives comme une limite supérieure du danger total et retrace leur évolution.

NATURE OF RISK

- No activity is without some measure of risk.
- Most industrial activity involves some public risk.

Some of this risk is chronic, such as the continuous release of toxic chemicals by trucks, foundries and coal-burning power plants, and the continuous release of small amounts of radioactivity by nuclear power plants. Society limits the amounts of these releases to various degrees. For nuclear plants, the Atomic Energy Control Board sets limits which minimize the risk to public health[1].

Some risk is acute (accidents), e.g. large releases of toxic chemicals, explosions, dam failures, collapse of structures. The only difference between these postulated accidents and a postulated accident in a nuclear plant is that the public risk from the latter is radiological rather than chemical or physical. A nuclear plant has no large inventories of toxic, easily-dispersed chemicals, and simply cannot explode like an atomic bomb. Only accidents which can potentially release large amounts of radioactivity pose a risk to public safety.

The words "measure of risk" are important, and we shall devote the second half of this paper to attaching numbers to the risk. The first half will describe where the risks come from, and what we do (in a qualitative sense) to limit them.

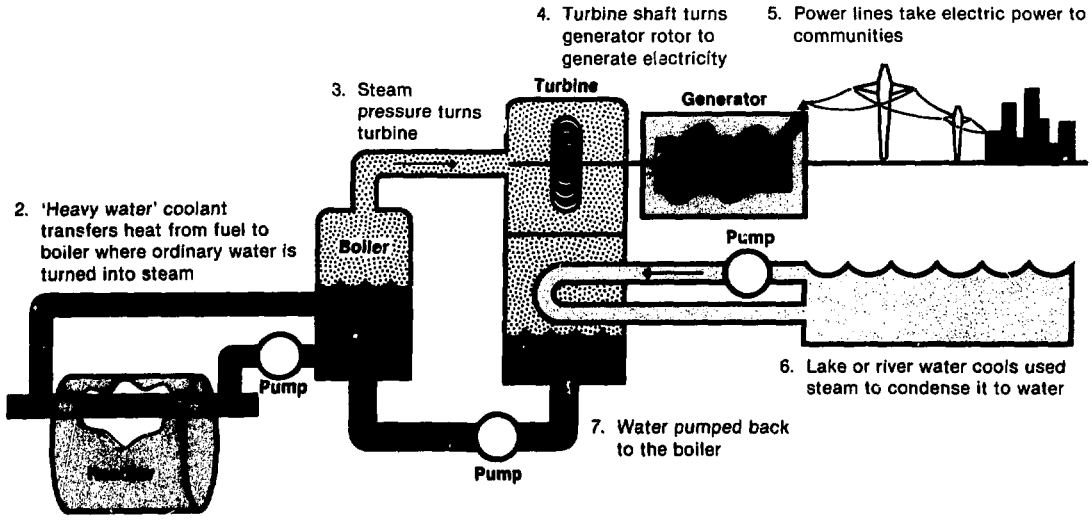
SOURCES OF RADIOACTIVITY — BARRIERS TO RELEASE

Figure 1 shows the basic pieces of a CANDU* power plant. Fissioning uranium fuel in the nuclear reactor produces heat. This heat is carried to boilers by a "heavy water" coolant under pressure, which is then pumped back to the reactor core; the entire circuit is called the primary heat transport system. In the boilers the heavy water gives up the heat to ordinary water, which is turned into steam. The steam runs turbines, which power electrical generators.

As uranium fissions or "burns", it produces radioactive fission products. These fission product "ashes" contain over 99% of the radioactivity in a nuclear power plant, and are located both in the nuclear reactor itself, and in the bay where spent fuel is stored. In each location, several physical barriers lie between the radioactivity and the public, and prevent its escape.

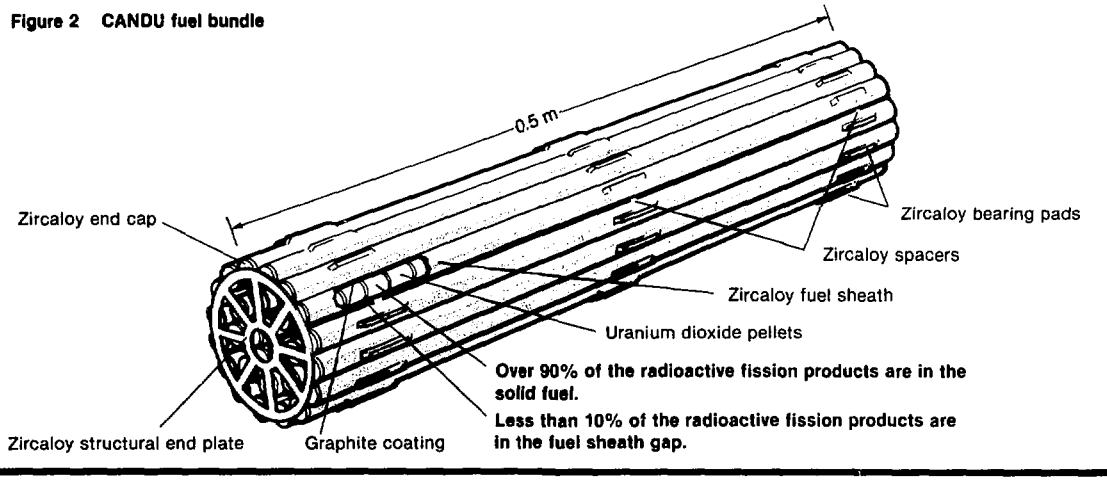
In the *reactor* most of the fission products are locked inside the solid uranium dioxide *fuel.* They cannot escape unless the fuel becomes very hot. The fuel and the remaining fission products are sealed in metal *sheaths.* Figure 2 shows an assembly of sheaths, called a fuel bundle. All the fuel bundles lie inside a closed *heat transport system,* and the entire reactor is surrounded by a massive *containment* building. Finally, no

Figure 1 CANDU pressurized heavy water nuclear power process



* Canada Deuterium Uranium

Figure 2 CANDU fuel bundle



member of the public may live within an *exclusion zone* extending for 1 km around the reactor (Fig. 3).

So before any radioactivity from the fuel could escape in an accident, the barriers formed by the fuel, the sheath, the heat transport system, and the containment would have to be perforated. Beyond that, the exclusion zone allows dilution of any release before it could reach a member of the public.

In the *spent fuel bay*, the first two barriers are again the solid fuel and the fuel sheath. The fuel bundles lie in large tanks of water. The tanks[2] are of double-walled reinforced concrete construction with an interspace between the walls. The interspace is monitored to detect and collect any leakage of water out of the bay. The bay water is also monitored to measure its temperature and to detect any leakage of radioactivity from the stored fuel (Fig. 4). The exclusion zone again allows dilution of any release.

Figure 3 Barriers to release of radioactivity (Reactor)

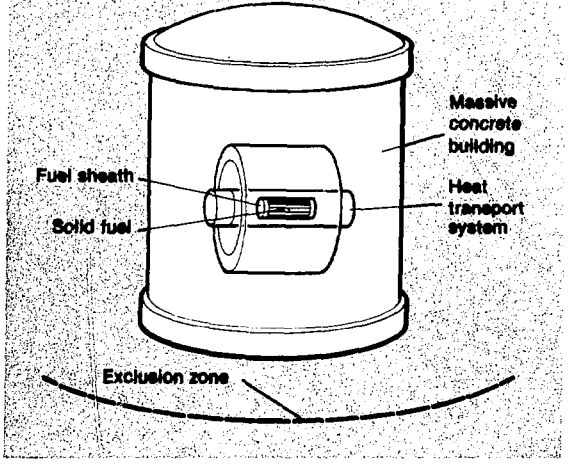
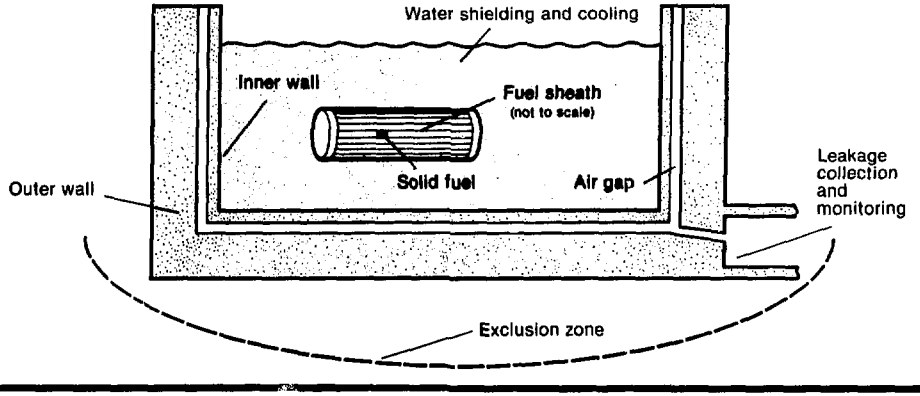


Figure 4 Barriers to release of radioactivity (Spent fuel bay)



ACCIDENTS — POTENTIAL CAUSES OF RELEASE

Like most metals, fuel sheaths weaken at high temperatures. Sheath integrity is therefore at risk if the cooling of the fuel is reduced relative to the power it produces.

One can imagine the following accidents causing such a mismatch:

1. The cooling remains normal, but the power rises (loss of power control).
2. The power is initially controlled, but the cooling deteriorates. This can happen:

   — if there is a break in the piping of the primary heat transport circuit (loss of coolant).

   — if the coolant flow over the fuel or the steam removal from the boilers is reduced (loss of cooling).

The sheath can withstand a range of abnormal temperatures and loads, and even sheath failure by itself does not imply a release of radioactivity to the public, because of other barriers which remain. We aim, where possible, to restore appropriate power — cooling balance. How we achieve this is discussed in the next section.

Sheaths may also fail from mechanical damage, e.g. dropping a fuel bundle, during transfer from the reactor to the spent fuel bay. This can only happen to a few bundles at a time. Containment and the exclusion zone give retention and dilution for such events.

In the spent fuel bay, the power in a fuel bundle is hundreds of times lower than what it was in the reactor. It comes only from the radioactive decay of the fission products formed while the fuel was in the reactor, and cannot increase. In fact, each bundle power is continuously decreasing with time. Loss of cooling of these fuel bundles could occur by:

1. failure of bay water cooling systems, or
2. loss of bay water itself through leaks in the bay walls*.

The station operator would be alerted to the event by the monitoring systems described in *Sources of Radioactivity — Barriers to Release*. Because the decay power is so low, both the loss of cooling and any deterioration of the sheaths would proceed very slowly [3] (days to weeks), allowing ample time for the operator to correct the situation.

PROTECTION — DEFENSE IN DEPTH

In an earlier section, we described the barriers to release of radioactivity. In practice, good design ensures that an accident is unlikely to occur in the first

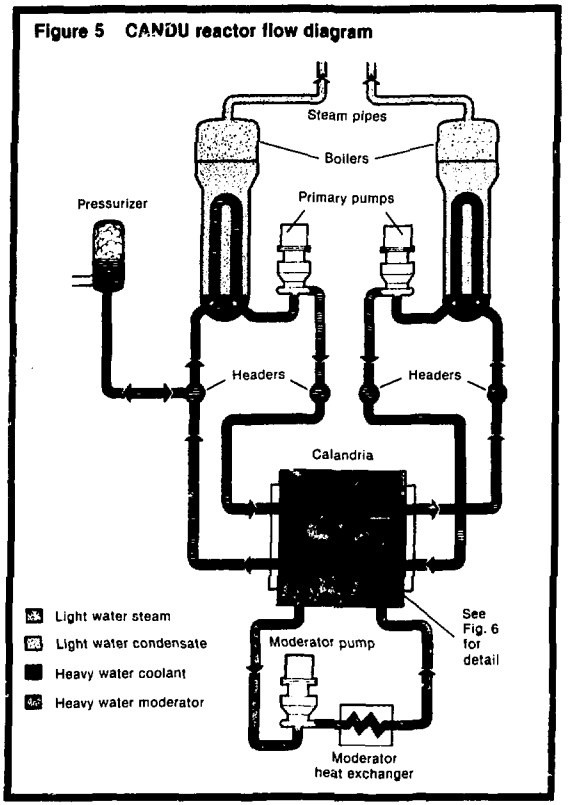


Figure 5 CANDU reactor flow diagram

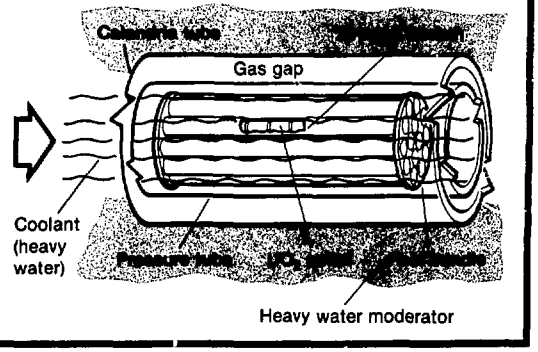
place. This is coupled with strict quality control during manufacture and installation, and with periodic inspection of the major components during the lifetime of the plant[4]. Public safety is not the only motivation: an accident which takes a plant out of service costs money for replacement electricity. So there are also sound economic incentives for accident prevention, particularly for potentially frequent accidents.

Even if an accident occurs, the reactor process systems (the normal systems which are used to keep the plant running) can often stop its course or mitigate its effects. Backing these up are separate safety systems. These have one purpose: to handle accidents. They are independent of the process systems and of each other both logically and physically, and are not used in the day-to-day operation of the plant. They can, if needed, shut down the reactor (shutdown systems), refill the reactor core with coolant and remove residual or "decay" heat from the fuel (emergency core cooling system) and prevent release to the environment of radioactivity which may escape from the reactor (containment systems).

This safety approach — accident prevention, accident mitigation, and accident accommodation — is called *defense in depth*. It is characteristic of the design of the entire plant[5].

* Catastrophic failure of the bay appears highly unlikely. For example, it is designed to stay intact during any earthquake likely to occur in the plant lifetime. Further, large objects, such as fuel transfer flasks which may be moved over the bay have "cushions" provided, designed to absorb the impact energy and prevent damage should they be accidentally dropped into the bay.

Figure 6 Separation of coolant and moderator



The approach recognizes that failures occur, and that systems and human beings are not perfect. The plant design tolerates such failures and imperfections. It need not be perfect to be safe.

We digress briefly with a thumbnail description of the reactor core. The fuel and its heavy-water coolant are contained in hundreds of horizontal zirconium alloy tubes called pressure tubes, arranged in a lattice. A horizontal, cylindrical vessel (the calandria) surrounds the pressure tube array, and contains the moderator (Fig. 5). A calandria tube, and a gas gap, insulate each pressure tube from the moderator (Fig. 6). The moderator and coolant systems are therefore separate. This is different from most other reactor types — for example, in U.S. light water reactors, one water circuit does both moderation and cooling.

The reactor control and shutdown devices are located in the moderator, but do not cross the coolant pressure boundary. They run between columns or rows of calandria tubes (Fig. 7).

With this background, we return to the three levels of defense for the classes of accidents we imagined in *Accidents — Potential Causes of Release*[5].

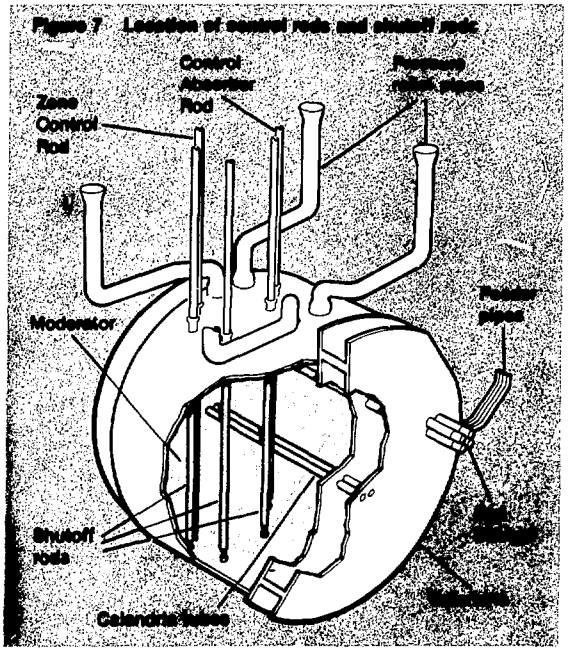
LOSS OF POWER CONTROL

Care is taken in designing the actual devices which control reactor power (e.g. light-water-filled zone compartments; absorber, adjuster and booster rods) (Fig. 7). Since they are not within the coolant pressure boundary, they cannot be expelled by coolant pressure loads. Further, they are inherently slow devices, so that maximum possible rates of power rise are modest.

Redundancy in the control system is the key to preventing an uncontrolled power rise. All important sensing instruments are duplicated, for assurance against wrong measurements. The main control computers are also duplicated. Either can, by itself, operate the plant. A continual and sophisticated system of self-checking looks for computer faults, transferring control to the standby computer if one computer fails, and shutting down the reactor if both computers fail.

Further diversity in preventing loss of power control is obtained by subsystems of the power control system, largely independent from the rest of it, whose only function is to reduce power under abnormal circumstances.

They are backed up by the shutdown systems, which are entirely independent of the power control system. They are an additional and decisive way of shutting down the reactor.



LOSS OF COOLANT

Rupture of a pipe without warning is an uncommon event in any industry. We expect that nuclear piping, with its higher standards for fabrication and inspection, will be better than average[7]. If there is a defect in a pipe, we would expect warning of pipe failure before it occurred; our tests on deliberately predefected tubes show that they leak before they break[8]. Such leaks would be detected by instruments which sense moisture in the atmosphere of the reactor vault and in the gap between the pressure tube and the calandria tube, radioactivity in the steam flow to the turbine, and water on the vault floors. So in most cases appropriate defensive measures would be taken to prevent or minimize the effect of pipe rupture.

In our safety analysis, however, we assess the response of the reactor to the instantaneous failure (at any location) of any pipe, from the largest to the smallest.

The reactor systems must do two things in such an accident:

1. Stop the power rise that is caused by coolant escaping from the fuel channels, and shut down the reactor *(See Safety Systems).* The power increases because the coolant affects the energy of the neutrons so as to make them slightly less effective in causing fission.
2. Assure a supply of cooling water over the fuel.

For rather small breaks, the normal process systems can do both: the power control system shuts down the reactor, and coolant makeup systems maintain cooling. Naturally they are backed up by the safety systems.

For large breaks, the power rise and the loss of coolant are such that the safety systems are needed. Shutdown systems stop the power rise and shut down the reactor, and an emergency core cooling system restores fuel cooling. Containment is a backup, in case any fuel sheaths should fail and release radioactivity. (Heat can also be rejected by an independent route — to the bulk moderator. Fuel damage could be severe, if this were the only way of removing heat from the core, but the containment barrier would remain. Such a backup cooling route is unique to the CANDU design, because the moderator is at low temperature, and unaffected by a loss of coolant.)

LOSS OF COOLING (Intact Primary Circuit)

A loss of cooling in an intact primary circuit is inherently less severe than a loss of coolant due to a pipe break, since the heat transport system piping remains an effective barrier to radioactivity release. An example is loss of the electrical power which drives the main pumps.

Reactor power reduction is affected by the power control system, backed up by the shutdown systems. Heat is rejected by the auxiliary cooling systems (such as the shutdown cooling system) and/or by natural convection to the boilers.

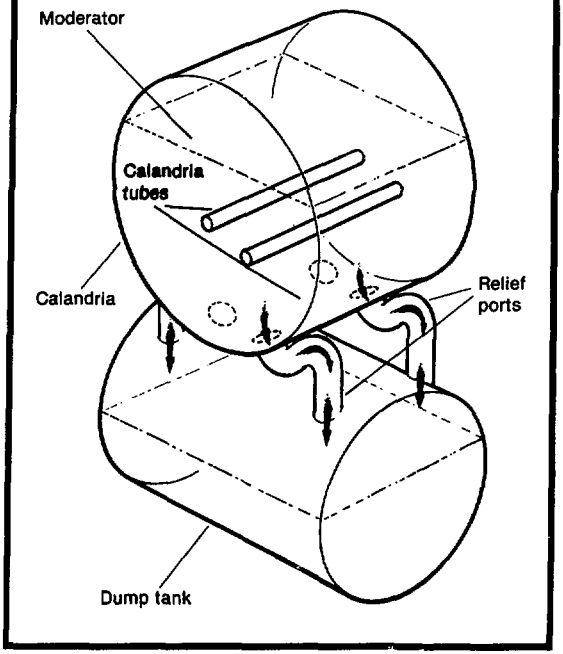
SAFETY SYSTEMS

In this section, we describe the safety systems and their capabilities[9] [10].

Shutdown Systems

CANDU reactors have used three types of shutdown mechanisms. Moderator dump (draining the moderator out of the calandria) shuts down the chain reaction by removing the fluid which slows down the neutrons (Fig. 8). For the recent larger cores, we used solid shutoff rods (falling in from the top under the action of gravity,

Figure 8 Shutdown systems: moderator dump



and sometimes assisted by springs) and injection of liquid "poison" through tubes directly into the moderator water (Fig. 9). The rods and poison stop the chain reaction by absorbing the neutrons.

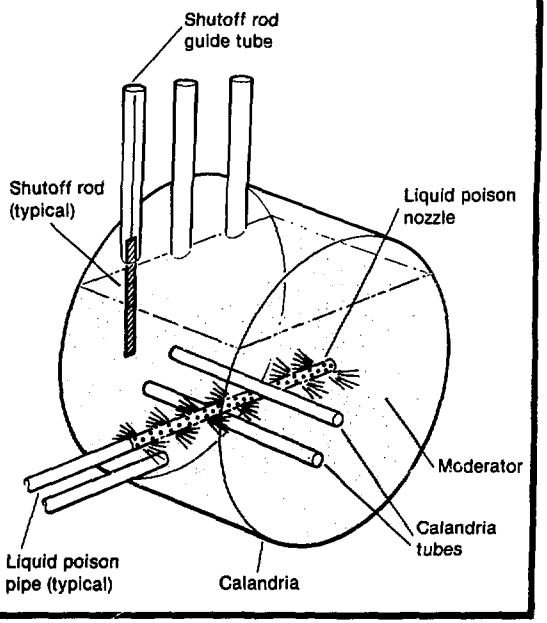
How quickly the shutdown systems must act, and how strong their neutron absorbing power must be, come from these requirements:

1. They must be able to overtake accidental power rises. This requirement largely sets the instrumentation delay that can be allowed and the speed of shutdown actions needed.
2. They must reduce post-shutdown power to decay levels consistent with available cooling. This requirement determines the amount of neutron absorption or "reactivity depth" needed.

As noted earlier, malfunction of the reactor power control system can produce only slow power rises. Its total reactivity range (which determines the amount of neutron absorption needed to stop the accident) is also modest — because CANDU reactors use natural uranium, long-term reactivity control is by on-power refuelling, not by reactivity devices. Control system malfunctions do not, therefore, set the requirements for the shutdown system speed or depth.

The power increase caused by a loss-of-coolant is the only type which would be assisted by the coolant pressure. A large pipe break causes the fastest power rise, but even this cannot be developed instantly since

Figure 9 Shutdown systems: shutoff rods and liquid "poison" injection



the coolant takes time to escape. In technical terms, the break could typically develop a "reactivity"* of 8 milli-k per second. The rate of power rise is further reduced by the relatively slow rate at which neutrons multiply in heavy water reactors. The multiplication rate in the U.S. light water reactor is about ten times faster than in CANDU's. Thus, even for large breaks, a delay of about half-a-second for the shutdown system to react to a signal, a shutdown system capable of reducing reactivity by 50 milli-k, and at a rate of about 30 milli-k per second are adequate. This performance is readily achievable.

The shutdown systems penetrate the moderator but not the coolant pressure boundary. Since all large coolant pipes are cutside the core, the shutdown systems would not be subject to the hydraulic forces due to a large pipe break, so giving confidence in their performance for such events.

Within the reactor core, where the pressure tubes are the pressure boundary, the maximum break size is small, and the consequences are limited. We would not expect any significant damage to other in-core components such as shutdown systems or other pressure tubes[11]. Also the pressure tubes are arranged to give maximum reactivity (a consequence of using natural uranium fuel) so that almost any accident which damages the core would tend by itself to shut the reactor down.

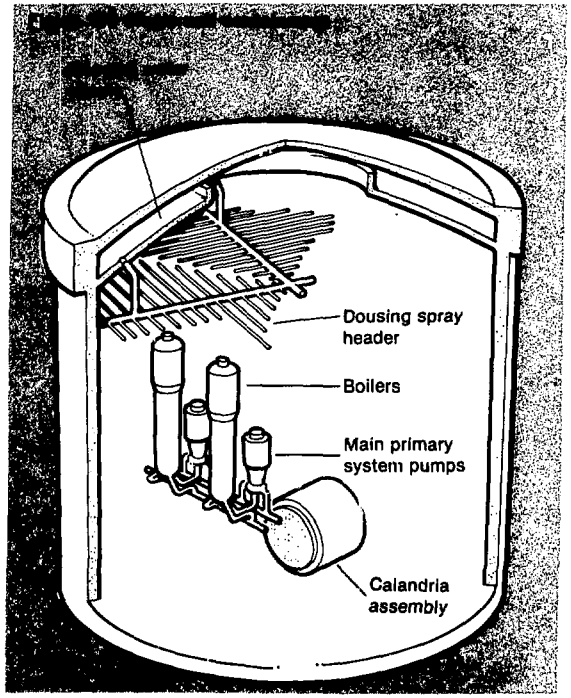
The shutdown system characteristics are therefore set by the large pipe breaks.

Canadian regulatory practice requires the analysis of accidents assuming the impairment of any safety system. In particular, one must assume that an entire shutdown system is unavailable. This analysis of power rises for which shutdown is not credited is difficult but has been done in the past. More recently, a second independent shutdown system has been added to the design, and is now in fact a regulatory requirement[12]. At this level of protection, there is no practical purpose in analyzing reactor power rises without shutdown, nor is it required.

Emergency Core Cooling System

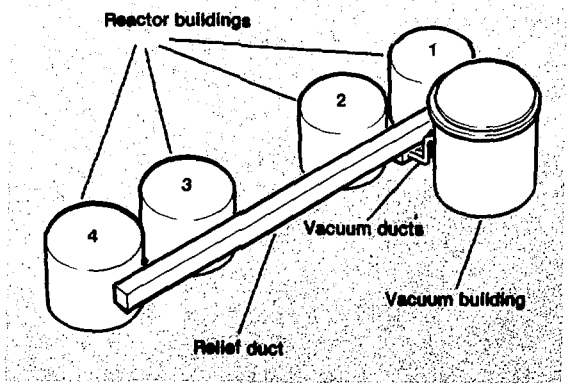
The emergency core cooling system (ECCS) would reestablish fuel cooling following a loss-of-coolant-accident.

For very small breaks in the primary circuit (around 6 cm², or 0.2% of maximum) the normal coolant makeup system can prevent net loss of fluid from the circuit. The ECCS serves only as a backup supply. For slightly larger breaks (up to a percent or so), safety valves on the boilers are opened; the heat absorbed, as the ordinary water boils and escapes through these valves, cools and depressurizes the primary coolant system down to ECCS pressure before very much primary coolant has escaped from the break. The ECCS serves here as a coolant makeup system. For large breaks (up to the maximum of about 0.5 m²) the ECCS provides enough flow to reflood the core, regardless of break location.



* Reactivity measures the driving force behind a chain reaction. A reactor holds a steady power at zero net reactivity, increases in power if the reactivity is positive, and decreases if the reactivity is negative.

Figure 10b Multi-unit containment



The major features of the ECCS are the water supply, injection points, pressure and heat removal pathways.

The ECCS water supply comes from either the heavy water moderator or, in recent plants, an ordinary water storage tank.

The injection points are at the reactor headers. These headers are large pipes to which every fuel channel is connected. They are at either end of the core, and above all the fuel channels (Fig. 5).

The injection system has a relatively low pressure supply, driven by pumps or gravity. We are also considering adding a higher pressure supply, driven by pumps or pressurized gas accumulators. This source could, among other things, reduce the risk of expensive cleanups for small breaks.

Decay heat would be removed by the boilers, special coolers for water which is recovered from the floor and re-injected into the core, air coolers in the containment building, and condensation on the containment walls; the dominant heat removal path would depend on break size.

Generally speaking, a loss-of-coolant accident could damage fuel sheaths[9]. The damage would be minimal at the small end of the break spectrum, somewhat larger at the large end, and larger in between. We are not granted foreknowledge of break size or location, so we design ECCS systems which give a good overall response across the break range. For breaks where fuel damage would occur, containment and the exclusion zone would be effective in limiting radioactivity releases to the public.

In addition to the ECCS, we noted earlier that the cool, low-pressure moderator is available as a backup means of heat removal, since a heat transfer path exists from the fuel, through the pressure tube and its surrounding calandria tube to the moderator fluid and the moderator heat exchangers (which can remove the reactor decay power) (Fig. 5).

Containment

The functions of the containment system (following a pipe break) are to:

- cool the escaping coolant and thereby suppress any pressure surge
- contain the activity release, if any, for the duration of the pressure surge
- provide a means of long-term control of radioactivity release using coolers and filters.

In a single unit plant, the reactor has its own independent containment building which includes both an initial means of pressure suppression (water dousing from overhead sprays) and a long-term means of pressure suppression (air coolers and a filtration system). Its leak rate is typically 0.1% of its volume per day at its design pressure (Fig. 10a).

In multi-unit containment[13], each reactor vault is connected by a duct through banks of self-actuating valves to a common dousing system (Fig. 10b). This is inside a separate building kept at reduced pressure (the vacuum building). Such an approach is economic on multi-unit plants and is very effective in pressure suppression. Consequently, the tolerable leak rate is larger (1% of its volume per hour at design pressure).

MEASURE OF RISK

This section describes the *amount of risk* implied by the operation of a nuclear power plant[14].

Before we protect against particular accidents, we must decide how safe we want the plant to be. Nothing can be made absolutely safe, and the "safer" we try to make the plant, the more it costs in terms of safety devices and reduced output. Indeed, beyond some point the improvements in "real" safety may be illusory.

Without numbers for risk, it is as hard to compare the safety of competing energy technologies as it would be to compare their economics without knowing their cost. Sometimes such quantitative studies give surprises. It is hard to see much risk in solar power, and perhaps easier to see risk in nuclear power. Yet Inhaber[15], who studied both in an exploratory analysis, claimed the reverse: he claimed that the public risk of death and of man days lost is higher for solar power than nuclear. The main reason is the enormous amount of materials needed for the "benign" technology — these must be manufactured and transported and that is where most of the risk lies. This type of analysis is still in its infancy, but the exercise is instructive.

Usually, risk is defined as the probability or frequency of an event multiplied by its consequences. The measure of frequency is usually "number of times per

year". The measure of consequence for nuclear safety is usually "radiation dose received by the public". This measure can be put in terms of public health effects, or of radiation released from the station. Nuclear energy is one of the few industries which has had during its development and deployment an extensive risk assessment. Perhaps as a consequence, we can take pride in lower risks than for most other industries. Modern commercial power reactors have an excellent safety record. There have been accidents, as in any industrial operation, but the consequences have been minor; in particular there have been no radiation injuries.

The risk numbers can also be used within a single technology to ensure that the design efforts are used most effectively. They can put into perspective numerous "what if" questions, most of which arbitrarily assume multiple failures. What is important here is not only the consequences (which may be spectacular) but also how often such failures may be expected. If the answer is "very infrequently", as is usually the case for nuclear safety, the actual risk is probably small.

In short: we cannot make a human activity absolutely safe. We can improve its safety. This requires social resources. At some point society must judge when the level of safety is good enough, so it can use these resources elsewhere.

As an example, for a long time, the people of Ontario by and large accepted the risk of driving cars without wearing seatbelts. This risk gradually became to be considered unacceptable, so car manufacturers were required to install seatbelts in every car and people were required to wear them. (Seatbelts are a good example of a safety system.) Wearing a seatbelt reduces the consequences (but not the probability) of an accident and therefore the total risk. Reducing risk by reducing the probability of an accident ever occurring is another route to the same goal. We could accomplish this, if we wished, by better road design and improved driver training. Using both seatbelts, highway improvements and driver education would be an example of "defense-in-depth".

In safety analysis, we are at liberty to hypothesize any arbitrary accident. To be useful, these hypotheses should strike some balance between the probability of an accident and its consequences. For a given reactor design, our emphasis on preventing an accident, or on building systems to stop it, is set both by how likely the accident is, and how severe its effects could be if unterminated. This approach is followed in setting numerical risk targets by those countries which have pioneered nuclear energy.

The United Kingdom assesses its designs with the Farmer[16] risk criterion. (The licensing authority accepts analysis based on this criterion, but judges on a case-by-case basis.) Farmer used "curies of iodine-131 released" as his measure of consequences. His risk

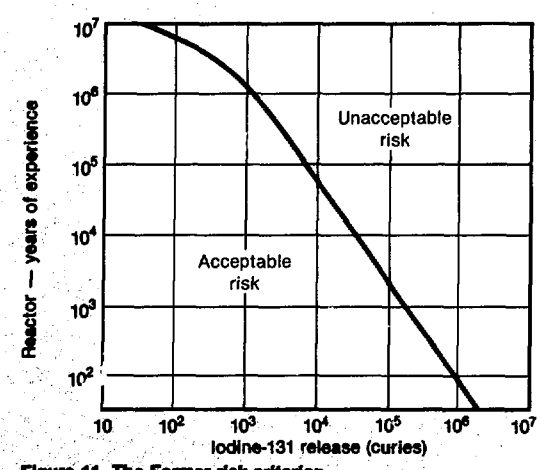


Figure 11 The Farmer risk criterion

criterion is a continuous curve of maximum release versus frequency of occurrence (Fig. 11).

United States designers used a stepped risk target. Events (including normal operation) are put in one of four categories, depending on their expected frequency. In each category, a limit is set for the amount of fuel damage or the release of radioactivity. The regulatory authority states in great detail how to calculate the damage, but again licenses on a case-by-case basis.

In Canada the Atomic Energy Control Board (AECB) is empowered[17], among other things, with the licensing of nuclear power plants. The AECB sets numerical guidelines for the frequency and consequences of accidents, but also licenses on a case-by-case basis. Events are postulated to fall into one of two classes[18]:

1. Single failures, where a normal reactor system (process system) is assumed to fail completely.
2. Dual failures, where a process system is assumed to fail simultaneously with the unavailability of any one safety system.

This classification grew from the design principle of logical and physical separation of control and safety systems, and of each safety system from any other.

The AECB limits the frequencies to once in 3 years for single failures and once in 3000 years for dual failures (Table 1). Consequences are interpreted as radiation dose to the public and are listed in Table 1.

This gives a stepped approach to public risk, roughly consistent numerically with the risk in Farmer's continuous approach. The AECB does not, however, prescribe how the analysis is to be done[19]. So it avoids sitting in judgement on its own methods, and leaves the design responsibility with the designers, where it properly belongs.

The AECB also sets exposure limits for normal operation[18]. These are essentially the same as those

Table 1 AECB Guidelines for Accident Conditions

Situation	Maximum Frequency	Individual Dose Limit	Total Population Dose Limit
Single Failure	1 per 3 years	0.5 rem* whole body 3 rem thyroid	10^4 man-rem whole body 10^4 thyroid rem
Dual Failure	1 per 3000 years	25 rem whole body 250 rem thyroid	10^6 man-rem whole body 10^6 thyroid rem

* A rem is a measure of the effect radiation has on the human body.

recommended by the International Commission on Radiological Protection[20], namely:

Individual dose limit — 0.5 rem/year whole body
3 rem/year thyroid

Population dose limit — 10^4 man-rem/year whole body
10^4 thyroid rem/year

In practice, these dose limits are translated into radioactivity emissions limits (Derived Release Limits or DRL). The DRL's are based on the most critical pathway for exposure of an individual due to radioactivity released from the station. In fact, the plants are designed to achieve an emissions target of 1% of the DRL for the radioactive elements generally emitted, and this target is usually met[9] [21].

In gaining an appreciation of what risk AECB guidelines actually imply, it must be realized first of all that reactors do not operate at the guidelines. Indeed, neither frequency nor consequence guidelines are approached in practice. For example, a large loss-of-coolant accident every ten years, while perhaps not too frequent to jeopardize public safety, would be an economic disaster for the plant owner. So the "allowed" frequencies for the more severe failures are never approached in actuality. The consequence guidelines too are usually upper bounds. Whereas they "allow", for example, all loss-of-coolant accidents to cause the specified public doses, in practice the only ones which come near are large breaks in a particular location, whose size is a particular fraction of the pipe area. Most of the breaks would cause small or zero radioactive releases from the plant. The failures (single or dual) which can release significant radioactivity are therefore a very small fraction of the total number of failures.

In addition, the dose calculations intentionally involve very pessimistic assumptions, which increase the predicted consequences. For the pipe break, it is assumed that:

- the effect of coolant void on reactivity is larger than it really is; and that the shutdown systems are slower and less effective than in reality, i.e., the power rise that would occur is overestimated;
- none of the process systems helps out, although they may be able to; it is assumed that only the safety systems do anything to mitigate the accident;
- the weather is that which maximizes population dose (atmospheric inversion with a light wind blowing in the direction of highest population density), even though such inversion occurs less than 10% of the time;
- the dose calculated is that for the most susceptible individual, e.g., a six-month old baby at the plant boundary for iodine-131.

These assumptions impose large margins. For example, just using the most likely weather at the Bruce 'A' nuclear power plant, rather than the worst occurring 10% of the time, reduces the individual dose due to iodine-131 by a factor of six, and using an average adult at the nearest populated site combined with average weather gives a factor of around fifty.

There are, of course, accident scenarios which do not fit neatly into single- or dual-failure pigeonholes. For these, a risk analysis may be done outside the guideline framework for consideration by the AECB. There are also other accidents which can be postulated, but which are of such low probability that higher releases than the guidelines allow may be tolerated. By and large, the guidelines are used but judgment both inside and outside their framework is sometimes necessary, and licensing is always done on a case-by-case basis. In short, the guidelines are an upper limit to the total overall risk, as described below.

For single failures, recall that the consequence guidelines for whole body doses (similar analyses apply to thyroid doses) are 0.5 rem for an individual, and 10^4 man-rem for the population. The frequency guideline is one event per three years. Doses as low as 0.5 rem have no detectable early effects, though a slight increase in the risk of delayed cancer (less than one in ten thousand) may result. The 10^4 man-rem would on average produce 1½ cases of fatal cancer over the entire exposed population, plus one case of curable cancer[1]. (It could also cause perhaps three cases of hereditary

disease, within a factor of five either way.) The total risk from the collective whole-body doses to the population would thus be in the vicinity of 2½ cases per three years per reactor, or roughly one case a year *at the guideline value*. If, for example, a 1000 MW(e) reactor serves a population of 10^6 people (1 kWe per capita) the 1½ cancer deaths per three years may be compared with some 4500 cancer deaths from other causes per three years in the same population.

For dual failures, recall that the frequency guideline is once per 3000 years. Whole-body dose guidelines are *25 rem for an individual and 10^6 man-rem for the population*. The individual dose would be associated with a risk of cancer death 50 times that for the 0.5 rem, i.e., about 0.5%. With the linear dose hypothesis[1], the population exposed to 10^6 man-rem could experience 250 cases of cancer (150 fatal) and 300 hereditary diseases, within a factor of five either way. When allowance is made for the infrequency of a dual failure, the average annual risk becomes 1/10 of a case for cancer and hereditary disease, *at the guideline value*. These are one tenth the values for single failures.

This calculation does not imply that these time-averaged risks are acceptable, simply because they are low. That is a social and political decision. Other factors also intervene. For example, people are less tolerant of single large accidents than many smaller ones, even if the average annual consequences are equal[22]. We do not attempt to include such a weighting in our numbers.

How do we know Safety Targets are met?

Our confidence that we can achieve low target risks is based on several factors. First, for frequency:

— In about 50 reactor-years of Canadian operating experience with power reactors, no member of the public has ever been killed or injured, and no worker in the plants has suffered a radiation injury. There have been no dual failures, and few single failures, all of which were in fact terminated without harmful radioactive release. That is enough data to establish that the target frequencies of single failures are being achieved. All data available internationally for civilian power reactors above 30 megawatts give fifteen hundred reactor-years without a large activity release*. There have been accidents in research reactors, and such mishaps have occurred regardless of reactor type. Trying to apply such experience to modern power reactors is misleading. Research reactors are used to gain information: both their design and their mode of operation are different from those of power reactors. In any case, most accidents in research reactors happened over ten years ago and none caused any major consequences to public health. The NRX accident in Canada was no exception[23][24].

— No dual failure has ever occurred, so we can only estimate the expected frequency. This can be done without having to wait until the systems are called upon in an accident. In-service testing of individual components and systems gives us a measure of availability in as little as a year of operation. The expected dual failure frequency can then be estimated by multiplying the observed single failure frequency by the safety system unavailability demonstrated by tests. The targets, inferred from AECB guidelines, are that the safety systems should be available at least 999 times out of a thousand tries; in other words, for all but 8 hours a year*. If the targets are not met in practice, the utility takes the appropriate corrective action to improve the availability to the target level.
In multiplying the single failure frequency by the safety system unavailability it is assumed that the risk contribution of common mode failures (one event causing several failures) is small; later on, we justify this assumption.

— Fault-tree analysis can combine logically the individual failure rates of various components to calculate failure rates for the whole system. This is useful in assessing the design process and provides further evidence that the design can meet reliability targets.

On the consequence side, past history will not indicate whether the dose guidelines for serious accidents are in fact achievable, since there have not been any in power reactors whose designs are being licensed. So we must calculate. These calculations use mathematical descriptions of components and their physical behaviour. Methods of individually verifying the "models" include:

— heating and pressurizing fuel sheaths to verify our model of deformation;

— making intentional breaks in circuits ranging from single pipes to complex loops to verify our hydraulic models;

— bursting predefected pressure tubes to verify the leak-before-break principle;

— studying the behaviour of fuel under severe conditions.

A comprehensive technical review[25] of this subject is available.

Event-tree analysis identifies the various possible accident sequences following a given event. When combined with fault-tree analysis, population-density distributions and frequency of weather types, it can give a good estimate of the actual risk, as opposed to the upper limit of risk, to the public of a nuclear power plant. To do a thorough job of this requires considerable

* International Atomic Energy Agency Annual Report, 1977.

* This depends somewhat on the reactor — see *Evolution of Canadian Safety Philosophy*.

resources of skilled professional manpower; the United States Reactor Safety Study (RSS) took 70 man-years of effort.

For licensing calculations, such a comprehensive analysis is unnecessary. The separation of the plant into process systems and independent protective systems allows the use of pessimistic assumptions to compute in detail the consequences of fewer, but more stylized, accident sequences. As a result, the estimated values set upper limits to the actual risk.

Sequences which cannot be quantified *a priori* — for example, common mode failures — inherently occur very rarely. In Canada it has long been believed that such events make a relatively small contribution to public risk when care is taken in the design and operation of the plant. To avoid common-mode failures, as noted, we separate the safety systems and the process systems from one another both logically and physically. In current designs this goes as far as building two control areas, from either of which different systems can shut down the reactor and remove decay heat. Where possible, the two safety systems employ totally different principles — for example, the first shutdown system uses solid absorber rods falling vertically into the core, the second uses liquid absorber injected into the moderator through horizontal pipes. Also, where possible they are designed to be "failsafe" — loss of power to the shutoff rod clutches, for example, lets the rods drop into the reactor, shutting it down.

The general approach was spelled out and practised in the early days of CANDU technology.

Laurence in 1962[26] said: "Simultaneous damage in the process equipment, the protective devices, and the containment provisions by one common cause must also be considered. Unlike the independent faults, the probable frequency of this happening is much too small to determine from past experience. We can do no more at present than reduce the probability of the three-fold damage from a common cause by careful design and cautious operation so that we have confidence that this risk is acceptably small. We are unable to support this confidence by direct evidence. That fact does not detract from the importance of establishing by the methods described that the risk of a bad accident resulting from the casually independent failures is also acceptably small."

The frequency of a common-mode failure can never be greater than the frequency of the initiating event. By itself this can sometimes give acceptably low bounding risks. For example, suppose a large loss-of-coolant always caused a loss of injection of emergency core coolant. A realistic frequency for the first event alone is perhaps 10^{-4} to 10^{-5} events per year[27] which would be below AECB guidelines for the frequency of a dual failure.

The same belief was expressed by Laurence in 1972[28]: ". . . the Reactor Safety Advisory Committee set very low limits for the frequency of faults in the process equipment, and for unreliability in the protective devices and the containment provisions, and has insisted that the three parts of the plant be functionally independent so that there is little chance that faults in the process equipment can damage the protective devices and the containment provisions also."

We referred earlier to the United States RSS. Their estimates for the risks of early fatalities and illnesses (Tables 2a and 2b) showed that the public risk from US reactors is low[29]. This study is not used in the licensing process in Canada (or in the US). We note, however, that:

- a large portion of the risk assessment in the RSS depends on population distributions and weather conditions which are independent of reactor design;

- all water-cooled reactors have a high pressure heat transport system and the frequency and consequences of failures in this system should be comparable;

Table 2a Individual Risk of Early Fatality by Various Causes
(U.S. Population Average 1969)

Accident Type	Total Number for 1969	Approximate Individual Risk: Early Fatality Probability/year*
Motor Vehicle	55,791	3×10^{-4}
Falls	17,827	9×10^{-5}
Fires and Hot Substances	7,451	4×10^{-5}
Drowning	6,181	3×10^{-5}
Poison	4,516	2×10^{-5}
Firearms	2,309	1×10^{-5}
Machinery (1968)	2,054	1×10^{-5}
Water Transport	1,743	9×10^{-6}
Air Travel	1,778	9×10^{-6}
Falling Objects	1,271	6×10^{-6}
Electrocution	1,148	6×10^{-6}
Railway	884	4×10^{-6}
Lightning	160	5×10^{-7}
Tornadoes	118**	4×10^{-7}
Hurricanes	90***	4×10^{-7}
All Others	8,695	4×10^{-5}
All Accidents	115,000	6×10^{-4}
Nuclear Accidents (100 reactors)		2×10^{-10}†

* Based on total U.S. population, except as noted.
** (1953 — 1971 avg.)
*** (1901 — 1972 avg.)
† Estimated, based on a population at risk of 15×10^{6}.

Table 2b Average Annual Risk of Illness from Various Accidents in the U.S.

Accident Type	Individual Risk: Injury Probability/Year
Motor Vehicles	2×10^{-2}
All non-nuclear accidents — average person	3×10^{-2}
Very risk-average person	3×10^{-4}
Nuclear Accidents*	1×10^{-6}

* Estimated, based on early and latent illness involving the approximately 15 million people located within 25 miles of nuclear power plants.

— most water-cooled reactors use ceramic (uranium dioxide) fuel, in zirconium-alloy sheaths, so the causes and effects of fuel damage are comparable.

We therefore, believe that the results of the RSS are very roughly applicable to most water-cooled reactors (including CANDU reactors), and in this sense confirm the judgment that the risks defined by the regulatory authority are pessimistic.

EVOLUTION OF CANADIAN SAFETY PHILOSOPHY

The Atomic Energy Control Board and Atomic Energy of Canada Limited were set up as administratively and financially independent organizations reporting to the Minister of what is now called Energy, Mines and Resources. They have retained this separation through the years. *Safety analyses* for specific license applications have always been prepared by the designer (or owner). They are subsequently examined by the AECB, which has the necessary expertise to determine whether the technical issues are adequately treated. The *underlying philosophy* has been evolving in public for the last twenty years, with contributions from both AECL and the AECB.

We summarize the key publications:

As early as 1954, Siddall[30] studied predictions of failure rates in the NRU reactor and described a basis for in-service testing. In 1959[31] he extended this in an early attempt to quantify the risk from nuclear power and to compare it with other industrial operations. He assumed *a priori* that nuclear plants could be five times safer than coal-fired plants, and derived the required reliabilities of the nuclear plant's control and safety systems.

Laurence[32] arrived at similar numbers by requiring that large releases of radioactivity (from what we would now call a triple failure) have a frequency less than 10^{-5} per year. He believed this risk was both less than other industrial risks and achievable in practice. His target implied the separation of reactor systems into three types, each with a target failure rate which could be demonstrated:

— process systems (10^{-1} failures per year)
— protective systems (1 failure per 100 demands)
— containment systems (1 failure per 100 demands)

He refined these somewhat a year later[26] to 0.3 per year for process failures, and 3×10^{-3} for protective and containment system unavailabilities.

Dose guidelines for what we now call a dual failure (of the process and protective systems) were noted in a paper in 1964 by Laurence et al[33]. They suggested the exclusion zone should be large enough to limit the dose to a member of the public to 25 rem whole-body and 250 rads to the thyroid except under extremely infrequent weather conditions.

Boyd[34] added single failures in 1967. He accepted Laurence's 1962 frequency guidelines. For dose guidelines he proposed for normal operation, values in line with ICRP recommendations; and for accidents:

— single failure of a process system:
  — to an individual, 0.5 rem whole-body
    3 rem thyroid
  — to the population, 10^4 man-rem whole-body
    10^4 rem thryoid

— dual failure of a process and protective or containment system:
  — to an individual, 25 rem whole-body
    250 rem thyroid
  — to the population, 10^6 man-rem whole-body
    10^6 rem thyroid.

In calculating accidental doses, the worst weather conditions occurring 10% of the time were to be used.

In 1972, Hurst and Boyd[18] removed the separate classification of containment as opposed to other safety systems. Any process system failure would now be analyzed with any safety system failure as part of the dual-failure matrix. A second shutdown system could be considered a separate entry in this matrix if it was independent, in design and operation, of both process and safety systems and if it was capable of accommodating any serious process failure. At the same time, because of larger fission product inventories of later reactors and the large accident matrix, the unavailability targets for the safety systems were reduced to 10^{-3}, and the process system failure frequency of 1 in 3 years was interpreted as a total, combined failure rate of all such systems. This is close to where we are now. Of course, the details will continue to change, but the basic approach has remained notably consistent.

The evolution of safety requirements poses an interesting question: what about reactors which were satisfactorily licensed under then-current guidelines, but which do not necessarily meet newer ones? Are they unsafe? Not really — the risk per reactor has

always been small, and what is important is the total risk from all reactors. Guidelines which become more stringent with time reflect more the larger number of reactors than a judgment as to the adequacy of any particular one.

Of course, older reactors may be reassessed if significant new information or better analytical techniques become available. A judgment is then made as to whether the original estimate of public risk is still valid. Such a judgement relies on both the results of the accident analysis and on the probability of the initiating event. The latter often dominates, so that the total risk is not too sensitive to changes in the details and scope of the accident analysis. An AECB view on this question has been presented by Beare and Duncan[35].

Similarly, the designer (even in a constant regulatory climate) may on his own improve the design in a manner that decreases public risk. This does not imply that he feels the older designs have become unsafe, although such criticisms have been levelled. As noted by Pease[36], to counter such a criticism decisively the designer would have to refuse to change his design beyond the first licensed reactor — hardly a constructive position.

Large Consequence Events

There is considerable public preoccupation with large consequence events. In fact, catering to specific "disasters" is unlikely to change public risk by a significant amount. This may seem surprising at first sight, but it follows from the very low frequency of such events.

It has already been noted that the average public risk under the AECB guidelines is less for dual failures than for the milder single failures, because of the lower frequency. Going beyond the guidelines, one can infer a maximum triple failure frequency of (1 process failure per 3 years) x (1 safety system failure per 1000 demands)^2 of 1 in 3 million years.

To estimate the consequences approximately, we can take those for the less frequent one-in-ten-million-year event of the RSS[29], which has 110 early and (at most) 18,000 delayed deaths. This approximation yields an average of 18,110/(3 x 10^6) or 0.006 deaths per year. (Even assuming the consequences of the one-in-a-thousand-million-year event occur in a triple failure, the consequences are only 0.02 deaths per year on average.) This calculation, admittedly crude, suggests the average risk decreases with increasing accident severity. There is no law of nature that says this must be so. However, it parallels human experience in other fields.

Laurence and Boyd[37] have put it well. Defending the Canadian regulatory practice to an international audience, they said: "The misleading use of hackneyed phrases is deplored; for example, the expression "maximum credible accident" may lead to oversight of some bad accidents that are not a negligible risk for very large nuclear power stations in very densely populated areas." At that time Canada was almost alone in the world in requiring analysis of failure of any safety system. Indeed, in 1961, when first setting up reliability targets for the three plant divisions (process, protective and containment systems), Laurence[32] said: "Emphasis on the worst credible accident has distracted interest from the less serious accidents which may be a more important risk because they are more probable. The usefulness of the concept is limited also by the vagueness of the world 'credible' to describe the probability of an occurrence in the life of the plant. It does not lead, therefore, to a recognizable standard for safety approval. A standard of acceptance that is expressed in more quantitative terms is needed to guide the designer."

CONCLUSION

The past safety record of CANDU reactors is impressive. Continuing care in design and operation, in this highly safety conscious industry, should keep it so.

REFERENCES

(1) **H. B. Newcombe,** *Nuclear Power: The Canadian Issues,* a submission from Atomic Energy of Canada Limited to the Royal Commission on Electric Power Planning. Atomic Energy of Canada Limited, Report AECL-5800, "Public Health Aspects of Radiation", Chap. 3 (April 1977).

(2) *Generation - Nuclear,* a submission from Ontario Hydro to the Royal Commission on Electric Power Planning, 1977 Final Hearings (June 1977).

(3) *Reactor Safety Study. An Assessment of Accident Risks in US Commercial Nuclear Power Plants,* United States Nuclear Regulatory Commission, Report WASH-1400, Appendix 1, Sect. 5 (October 1975).

(4) *CSA Standards N285.4,* "Periodic Inspection of CANDU Nuclear Power Plant Components" (February 1975).

(5) **G. A. Pon,** *Nuclear Power Reactor Safety,* Atomic Energy of Canada Limited, Report AECL-5694 (October 1976).

(6) **V. G. Snell,** *Nuclear Power: The Canadian Issues,* Atomic Energy of Canada Limited, Report AECL-5800, "Safety of CANDU Reactors", Chap. 2 (April 1977).

(7) **W. S. Gibbons and B. Hackney,** *Survey of Piping Failures for the Reactor Primary Coolant Pipe Rupture Study,* GEAP-4574 (May 1964).

(8) **P. A. Ross-Ross et al.,** *Experience with Zirconium Alloy Pressure Tubes,* Atomic Energy of Canada Limited, Report AECL-4262 (August 1972).

(9) **L. Pease and R. Wilson,** *Pressurized Heavy-Water Reactor Safety.* A paper presented at the Session on Heavy-Water Reactors, Canadian Nuclear Association 16th Annual Meeting, Toronto, Ontario, 13-16 June 1976. Atomic Energy of Canada Limited, Report AECL-5520 (September 1977).

(10) **L. Pease and V. G. Snell,** *Safety of Heavy-Water Reactors.* Paper IAEA-CN-36/181 presented at the IAEA International Conference on Nuclear Power and its Fuel Cycle, Salzburg, Austria, 2-13 May 1977. Atomic Energy of Canada Limited, Report AECL-5709 (May 1977).

(11) **P. A. Ross-Ross,** *Experiments on the Consequences of Bursting Pressure Tubes in a Simulated NPD Reactor Arrangement,* Atomic Energy of Canada Limited, Report AECL-1736 (February 1963).

(12) *Atomic Energy Control Board Licensing Document 13,* "The Use of Two Shutdown Systems in Reactors" (January 1977).

(13) **E. W. Fee and G. E. Shaw,** *Vacuum Containment Systems for Multi-Unit Nuclear Power Stations,* Societé Française de la Radioprotection, VIIme Congrès International sur le Confinement de la Radioactivité dans l'Utilisation de l'Energie Nucléaire, Versailles (May 1974).

(14) **J. A. L. Robertson,** *AECL's Final Argument Relating to Nuclear Energy Before the RCEPP,* Atomic Energy of Canada Limited, Report AECL-6200 (March 1978).

(15) **H. Inhaber,** *Risk of Energy Production,* Atomic Energy Control Board, Report AECB-1119 (March 1978).

(16) **F. R. Farmer,** *Siting Criteria - A New Approach.* Proceedings of IAEA Symposium on the Containment and Siting of Nuclear Power Plants, Vienna, pp. 303-329 (April 1967).

(17) *Atomic Energy Control Act, 1946,* Chap. 37, Sect. 1, as amended in Chap. 47 (1953-1954).

(18) **D. G. Hurst and F. C. Boyd,** *Reactor Licensing and Safety Requirements,* Paper 72-CNA-102. Presented at the 12th Annual Conference of the Canadian Nuclear Association, Ottawa (June 11-14, 1972).

(19) **G. Hake, P. J. Barry and F. C. Boyd,** *Canada Judges Power Reactor Safety on Component Quality and Reliable System Performance,* A paper presented at the 4th United Nations International Conference on the Peaceful Uses of Atomic Energy, Geneva, 6-16 September 1971. Atomic Energy of Canada Limited, Report AECL-3974 (September 1971).

(20) *Recommendations of the International Commission on Radiological Protection,* ICRP Publications 9 (1966) and 26 (1977).

(21) *Generation - Environmental,* Submission from Ontario Hydro to the Royal Commission on Electric Power Planning with respect to the Public Information Hearings (March 1976).

(22) *Reactor Safety Study. An Assessment of Accident Risks in US Commercial Nuclear Power Plants,* United States Nuclear Regulatory Commission, Report WASH-1400, Appendix 1, Sect. 2.2 (October 1975).

(23) **W. B. Lewis,** *The Accident to the NRX Reactor on December 12, 1952,* Atomic Energy of Canada Limited, Report AECL-232 (July 1953).

(24) **D. G. Hurst,** *The Accident to the NRX Reactor, Part II,* Atomic Energy of Canada Limited, Report AECL-233 (October 1953).

(25) **L. Pease and S. Sawai,** *Heavy-Water Moderated Pressure Tube Reactor Safety.* Presented to the International Conference on World Nuclear Power; American Nuclear Society/European Nuclear Society, Washington, November 1976. Atomic Energy of Canada Limited, Report AECL-5856 (August 1977).

(26) **G. C. Laurence,** *Operating Nuclear Reactors Safely.* Proceedings of Symposium on Reactor Safety and Hazards Evaluation Techniques I, Vienna (1962).

(27) **S. H. Bush,** *Reliability of Piping in Light Water Reactors,* International Symposium on Application of Reliability Technology to Nuclear Power Plants, International Atomic Energy Agency, Vienna (October 1977).

(28) **G. C. Laurence,** *Nuclear Power Safety in Canada.* Presented to the Meeting of the Niagara-Finger Lakes Section of the A.N.S. (January 26, 1972).

(29) *Reactor Safety Study. An Assessment of Accident Risks in US Commercial Nuclear Power Plants,* United States Nuclear Regulatory Commission, Report WASH-1400, Main Report pages 112-113 (October 1975).

(30) **E. Siddall,** *A Study of the Serviceability and Safety in the Control System of the NRU Reactor.* Atomic Energy of Canada Limited, Report AECL-399 (1954).

(31) **E. Siddall,** *Statistical Analysis of Reactor Safety Standards.* Nucleonics Week, Vol. 17, pp. 64-69.

Atomic Energy of Canada Limited, Report AECL-498 (1959).

(32) **G. C. Laurence,** *Required Safety in Nuclear Reactors.* Atomic Energy of Canada Limited, Report AECL-1923 (1961).

(33) **G. C. Laurence, F. C. Boyd, J. H. Jennekens, J. B. Sutherland and P. E. Hamel,** *Reactor Safety Practice and Experience in Canada.* Presented to the Third International United Nations Conference on the Peaceful Use of Atomic Energy, Geneva 1964, Session 3.6, p. 318. Atomic Energy of Canada Limited, Report AECL-2028.

(34) **F. C. Boyd,** *Containment and Siting Requirements in Canada.* Proceedings of IAEA Symposium on the Containment and Siting of Nuclear Power Plants, Vienna, April 1967. Atomic Energy Control Board, Report AECB-1018.

(35) **J. W. Beare and R. M. Duncan,** *Siting - The Means by Which Nuclear Facilities are Integrated into a Canadian Community.* Presented to the IAEA-NEA Symposium on the Siting of Nuclear Facilities, Vienna, December 9-13, 1974. Atomic Energy Control Board, Report AECB-1079.

(36) **L. Pease,** *Transcripts of the Royal Commission on Electric Power Planning,* Debate Stage Hearings, Toronto, Ontario. Vol. 174, p. 25,597 (November 22, 1977).

(37) **G. C. Laurence and F. C. Boyd,** *Trends in Reactor Safety - A Canadian View.* Presented to the International Nuclear Industries Fair, Basel (October 6-11, 1969).

Note: The report cited in Reference (29) should be read in the context of a recently published review (U.S. Nuclear Regulatory Report — NUREG/CR-0400) by an ad hoc review group, H.W. Lewis, Chairman (September 8, 1978).

Atomic Energy of Canada Limited
L'Énergie Atomique du Canada, Limitée

AECL-6329
November 1978

La présent publication est également disponible en français

Printed in Canada