AECL EACL

AECL CANDU EACL CANDU

Chernobyl – A Canadian Perspective

by
Dr. V.G. Snell and J.Q. Howieson

AECL EACL

Chernobyl – A Canadian Perspective

by
Dr. V.G. Snell
Licensing Manager, SES-10
Local Energy Systems

and

J.Q. Howieson
Manager, Safety
CANDU 3 Program

Revised August 1991

Contents

What This Brochure Is All About

Before April, 1986, if the name ‘Chernobyl’ had been mentioned to a Western scientist, chances are that he or she would have no idea what it was. It was nonetheless one of the largest and most successful nuclear power stations in the Soviet Union, producing about 4000 million watts of electrical power, about the same size as the combined Pickering A and B CANDU stations near Toronto, and enough to fill the electrical needs of millions of Soviets. The Soviets said that Chernobyl (pronounced Cher-NO-bill) was considered a model plant, recently-built and trouble-free. On April 26, 1986, it was also the location of the largest accident in the history of peaceful nuclear power. When it was over, one reactor had been destroyed, 31 people had died, the surrounding area had been badly contaminated by radioactive particles, and studies had begun to predict what might happen to people in the long-term.

Four months later, on August 25, 1986, hundreds of nuclear scientists and engineers converged on the offices of the International Atomic Energy Agency (IAEA), in Vienna, Austria. For the first time since the Chernobyl nuclear power station accident, we were to find out from the Soviets themselves what had really happened. The answers went beyond what most of us had ever guessed (Reference (1)). Yet tantalizing holes in the story still remained. Now, thanks to intensive work in Canada, the U.S. and other Western countries, as well as in the Soviet Union, many of these holes have been filled in, and we believe we know in detail what went wrong. The Canadian work in discovering the most likely root cause of the accident has been accepted by most of the Western world and acknowledged by the Soviet Union.

First, however, we will go back into the nature of the Soviet nuclear program, look critically and fairly at the design of the Chernobyl plant, and describe the sequence of events that night of April 25-26. Like all accidents, it resulted from a combination of human error and design weakness; like all accidents, it could have been stopped at a number of places and would never have been heard of.

This brochure then looks at the Canadian CANDU (CANada Deuterium Uranium) reactor to see how it stacks up in its ability to tolerate the sorts of mistakes that were made at Chernobyl. One of the reasons the CANDU **is** more tolerant of error is that in Canada we *had* a severe accident in a research reactor in 1952. Although the accident caused much less damage (since the reactor was very much smaller), some hard lessons were learned and applied in the Canadian power reactors later on.

Finally we’ll look at the lessons that are being learned from Chernobyl by both the Soviets and ourselves.

1. Chernobyl — The Place and the Plant

1.1 The Chernobyl Site

Chernobyl itself is a small town of 12,500 people in the Ukraine region of the Soviet Union (Fig. 1 (a) & (b)). It is located about 105 km north of Kiev, the major city of the Ukraine with 2 1/2 million people. Chernobyl town gave its name to the nearby Chernobyl nuclear power station, 15 km to the north-west, which by 1986 had four of the most recent of the Soviet RBMK-type reactors in full operation, and two more being built. Three kilometers away from the reactors was the town of Pripyat, with 45,000 people. The Pripyat River flows through the area on its way to the Kiev reservoir.

1.2 The Soviet Program

The initials RBMK are a Russian acronym which translates roughly as "reactor cooled by water and moderated by graphite". It describes one of the two types of reactors the Soviets have built for power production, the other being simi-

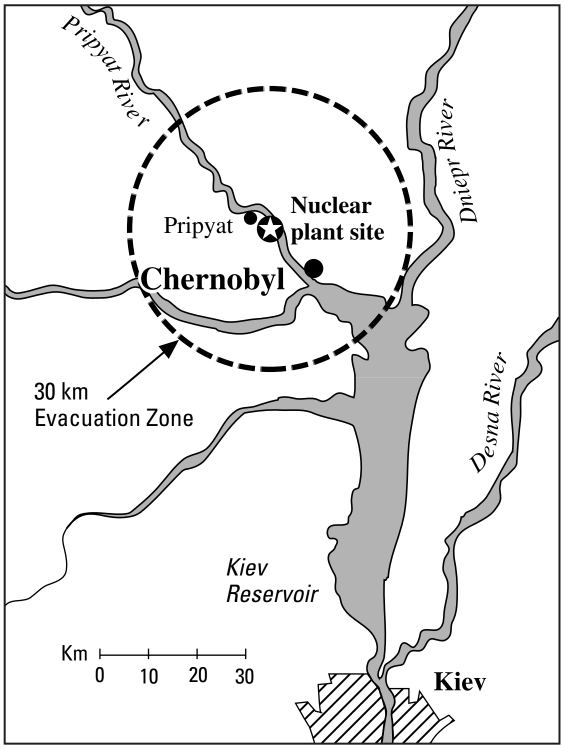


Figure 1(b) Area nearby the Chernobyl reactor site

Figure 1(a) Chernobyl reactor location

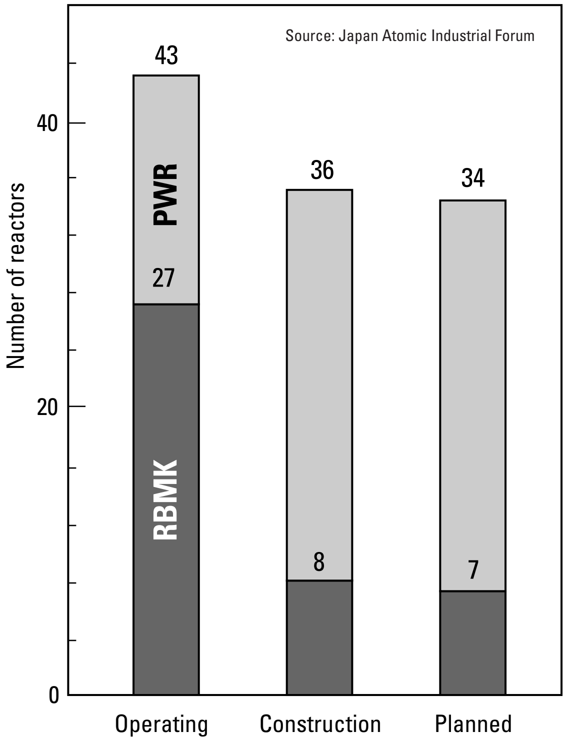


Figure 2 The Soviet Reactor Program (10% of the world's nuclear program)

lar to the United States pressure vessel reactor. The RBMK type is the older of the two designs. The Soviets developed it, by themselves, from early models which had been first used to generate plutonium for weapons, and to produce heat for district heating.

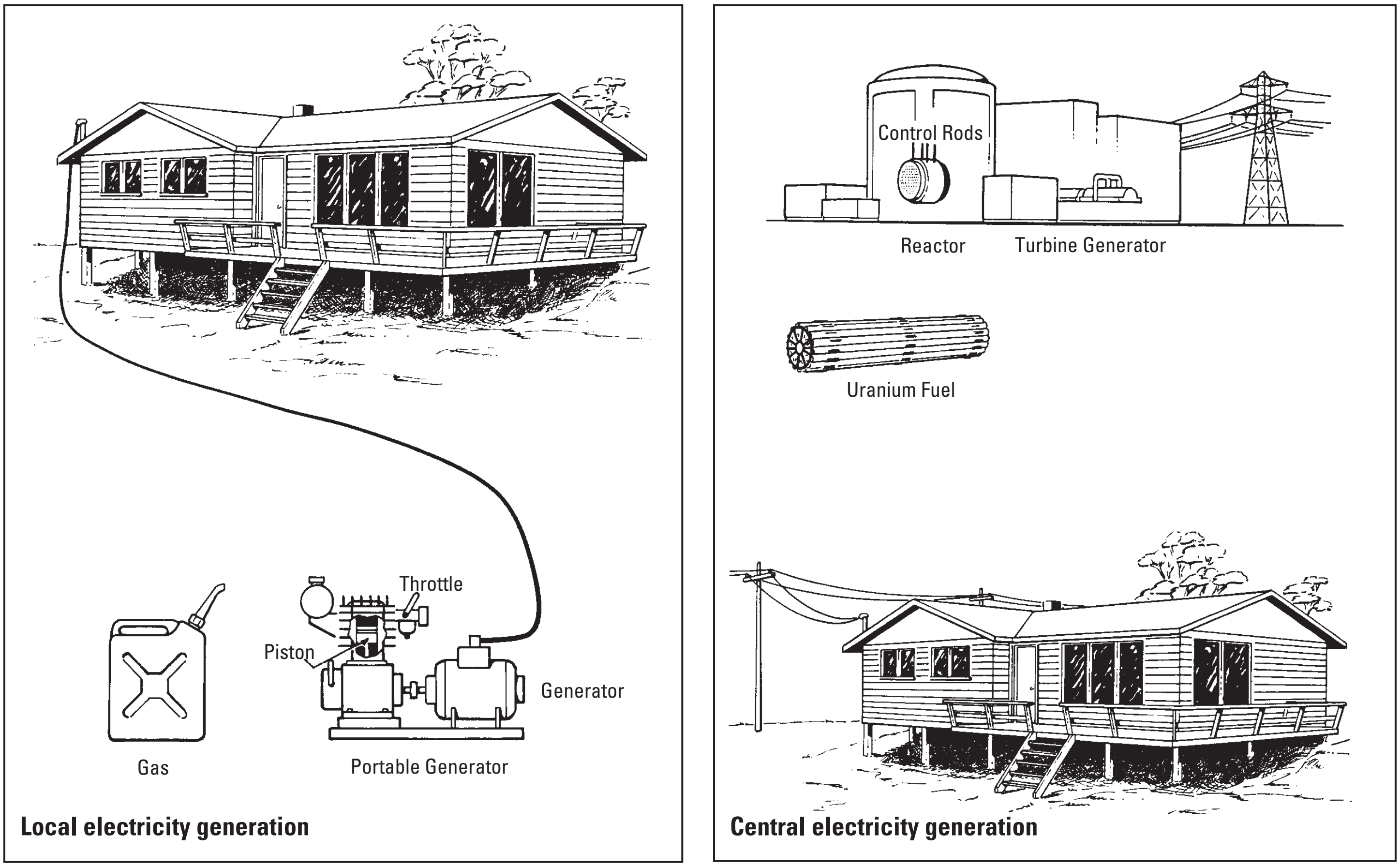
The Soviets have a strong and growing nuclear power program. At the time of the accident they generated about 10% of the world's nuclear power from 43 operating reactors, a total of 27 thousand million watts of electricity. They had under construction another 36 reactors representing 37 thousand million watts, and had planned another 34 reactors or 36 thousand million watts. Figure 2 shows the split by type of reactor as of January, 1986. Even then, there was a big shift in future plants **away** from the RBMK-type of reactor and **toward** the pressure-vessel (PWR) type of reactor. This was a recognition, we believe, that the RBMK reactors were becoming obsolete, and were not economic compared to modern pressure-vessel and modern pressure-tube concepts.

1.3 How a Reactor Works

Before we describe the RBMK reactor and the accident, it's worth reviewing the major parts of a nuclear generating station. Let's start by comparing it with a simple gasoline-powered portable generator that people use in cottages and on trips (Figure 3). The motor burns gasoline, and uses the energy of the hot gases produced to move pistons. Since the pressures from the burning gasoline are high, the engine encloses the "reaction" in strong cylinders. The pistons turn a crankshaft, which in turn spins an electrical generator. The electricity in turn can be used to run lights, work a refrigerator, etc. You control the power of the engine by a throttle which varies the rate at which gasoline is fed into the engine.

The basic principles are: using a fuel to heat up a fluid (gas), and then using the energy of the fluid to spin a generator. The **same** principles are used in a nuclear power reactor — of course the scale is vastly different. The fuel is uranium. Small particles called neutrons split the uranium atoms; this produces heat, and more neutrons, which keep the reactor going. The heat turns water to steam, and the energy of the hot steam spins a turbine (it's more efficient than a piston) which in turn spins an electrical generator. Since the hot steam is at high pressure, it must be kept in a strong container. You control the power of the reactor by changing the number of neutrons. The power is steady if the number of neutrons produced exactly matches the number used up. If more are used up than produced, the reactor shuts down; if more are produced than used up, the power increases. There are lots of materials which are very good at absorbing neutrons, for example boron (found in household borax), and these are used in making reactor "throttles". Usually they are formed into rods, and by moving these **control rods** in or out of the reactor, you can move the power down or up.

We mentioned that a strong container is needed to hold the uranium and the hot water. In the RBMK reactors, the containers consist of about 1600 small (4 inch diameter) pipes, called pressure tubes. In the other type of Soviet reactor, the container is a single huge pressure vessel, containing **all** the uranium and hot water in a large pot. Both concepts are used elsewhere — Canada, Korea, Argentina, Japan, the United Kingdom, India, Pakistan and Italy all have experience with pressure tube reactors of one sort or another, and the U.S., France, Germany and many other countries have built pressure-vessel reactors.



Local electricity generation

Central electricity generation

Figure 3

1.4 How an RBMK Reactor Works

1.4.1 Getting the Right Conditions

If you just put blocks of uranium together, and tried to split uranium atoms, you would find that the neutrons moved **too fast** and would miss the uranium atoms too easily. So all of today's commercial nuclear power stations have a way of slowing the neutrons down, by making them pass through a material called a **moderator**. In Canadian reactors, this moderator is a special type of water, called **heavy water** (it *is* 10% heavier than ordinary water); in U.S. pressure-vessel reactors, it is an extra supply of ordinary water; in the RBMK reactor, it is a solid called graphite. It's the same graphite that you write with when you use a pencil, except purer — both reactor graphite and pencil graphite are forms of carbon, which is what is burned as briquettes in a charcoal barbecue.

So the heart or *core* of an RBMK reactor consists of a huge container, about as big as a Canadian house, filled with graphite blocks. The blocks are pierced by about 1660 vertical holes, in which the pressure tubes and the throttles, or control rods, fit (Figure 4). As neutrons split the uranium atoms, the uranium fuel gets hot. Water is pumped from the bottom of the pressure tubes over the fuel. It removes the heat from the fuel, turns to steam in the process, and leaves the reactor core at the top. From there it goes through pipes and gives up its energy to spin *two* large turbines, in an adjacent building (Figure 5). The turbines in turn spin electrical generators, and the cooled water goes back into the reactor again. All the reactor itself does is the mundane job of boiling water.

As in all pressure tube reactors, some (about 5%) of the heat produced by the uranium leaks out to the moderator. In the CANDU reactors, where the moderator water is separate from the cooling water, the moderator heat is removed by an independent moderator cooling circuit, consisting of special pumps which circulate the moderator water through coolers, and pump it back into the reactor core — like a transmission oil cooler in a car. The coolers keep the moderator temperature at about 70°C, or the same as

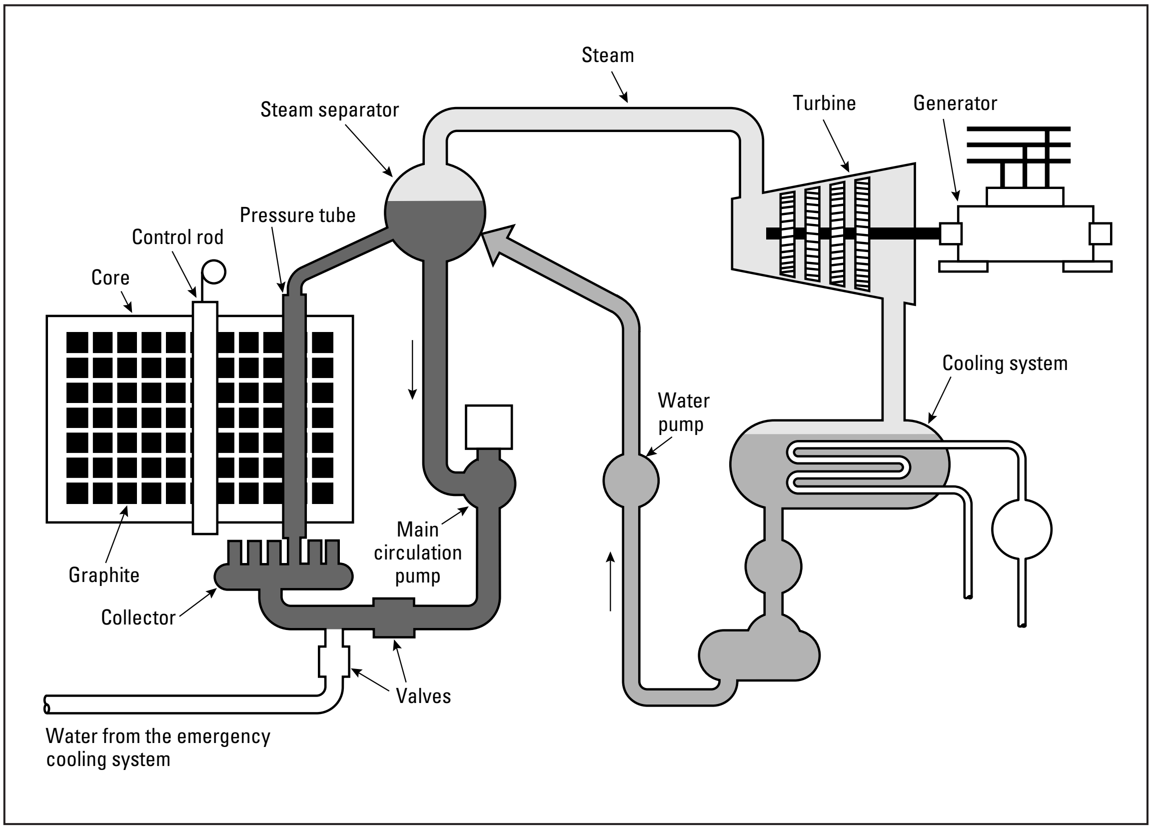


Figure 4
Schematic diagram of the RBMK-1000

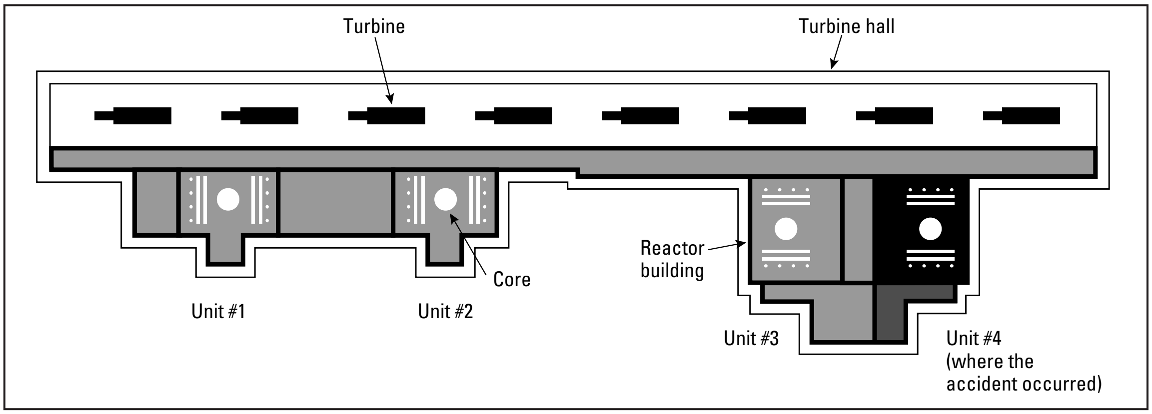


Figure 5
Layout of four reactor units

from a hot tap. Obviously you can't do that with solid graphite. In the RBMK design, the graphite operates at a high temperature — about 700°C — and if you could see it, it would be glowing faintly red-hot. This heat flows slowly from the graphite back through the pressure tubes, and is finally taken away by the boiling water. Now the problem with graphite at high temperature is that if exposed to air, it will burn slowly, just like the charcoal briquettes on a barbecue. So it's **very** important in the RBMK design to keep air away from the graphite. To do this, the Soviets put their entire core in a sealed metal container (Figure 6), and circulate a mixture of inert gases, helium and nitrogen, which do not react with graphite, inside the container. The container was built so it could withstand the failure of a pressure tube without bursting and letting in air.

1.4.2 Containing an Accident

The rest of the structure in Figure 6 is just shielding, to reduce the levels of radiation around the reactor while it is operating. Shielding is used in all reactors so that people can work in the buildings the reactors are in without getting overexposed to radiation. On the sides of the RBMK reactor are shields made of water, sand, and concrete; on the bottom is a concrete shield; and on the top another concrete shield. **All** the pressure tubes and control rods are attached to this top shield, and it played a key role in the accident.

The reactor itself is placed inside a building. Now in any reactor, if a pipe carrying the water which cools the uranium were to break, several things could happen:

a. mildly radioactive steam would escape from the pipe and contaminate or damage the plant;

b. since the uranium has lost its cooling water, it would get too hot, and would be damaged;

c. radioactive material normally safely contained inside the uranium could escape to the rest of the plant and to the outside.

This is an unacceptable risk both from a public safety and an economic point of view. To reduce the chances of escape of radioactive material, designers of nuclear reactors normally provide several "lines of defence":

- Exceptionally high-quality piping, plus inspection of the piping in-service to see if it is deteriorating unexpectedly. This follows the old adage of **prevention** being better than cure.
- Normal control systems which, if a pipe break does occur, can shut the reactor down and, in most cases, replace the water that is being lost without damage to the fuel. This **mitigates** an accident after it has occurred so that both *safety* and *economics* are respected.
- Special *safety systems*, which act only in an accident, and back up the normal control systems. They can shut the reactor down, and replace water as fast as it is lost from *any* pipe break. (The system which replaces lost water is called an Emergency Core Cooling system or ECC.) The main function of these special safety systems is public and worker safety, so they are mitigating systems.
- Strong leak-tight buildings surrounding the pipes so even if they do break, and even if radioactive material is released, the steam and

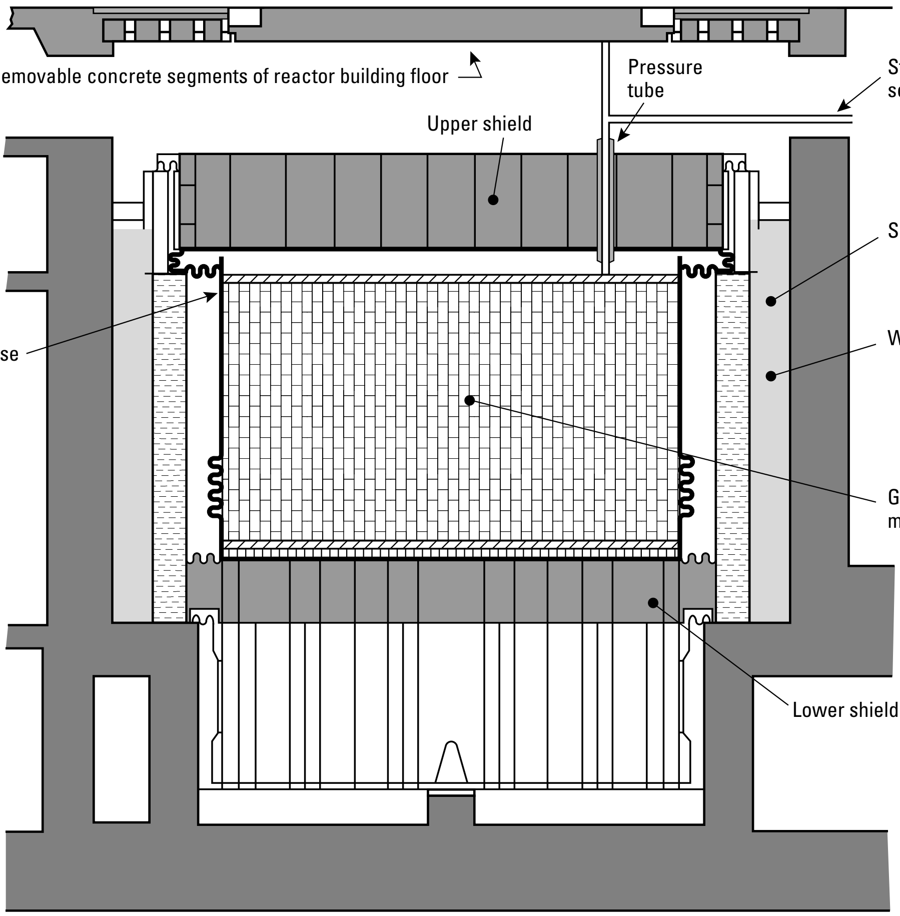


Figure 6
Cross sectional view of reactor vault

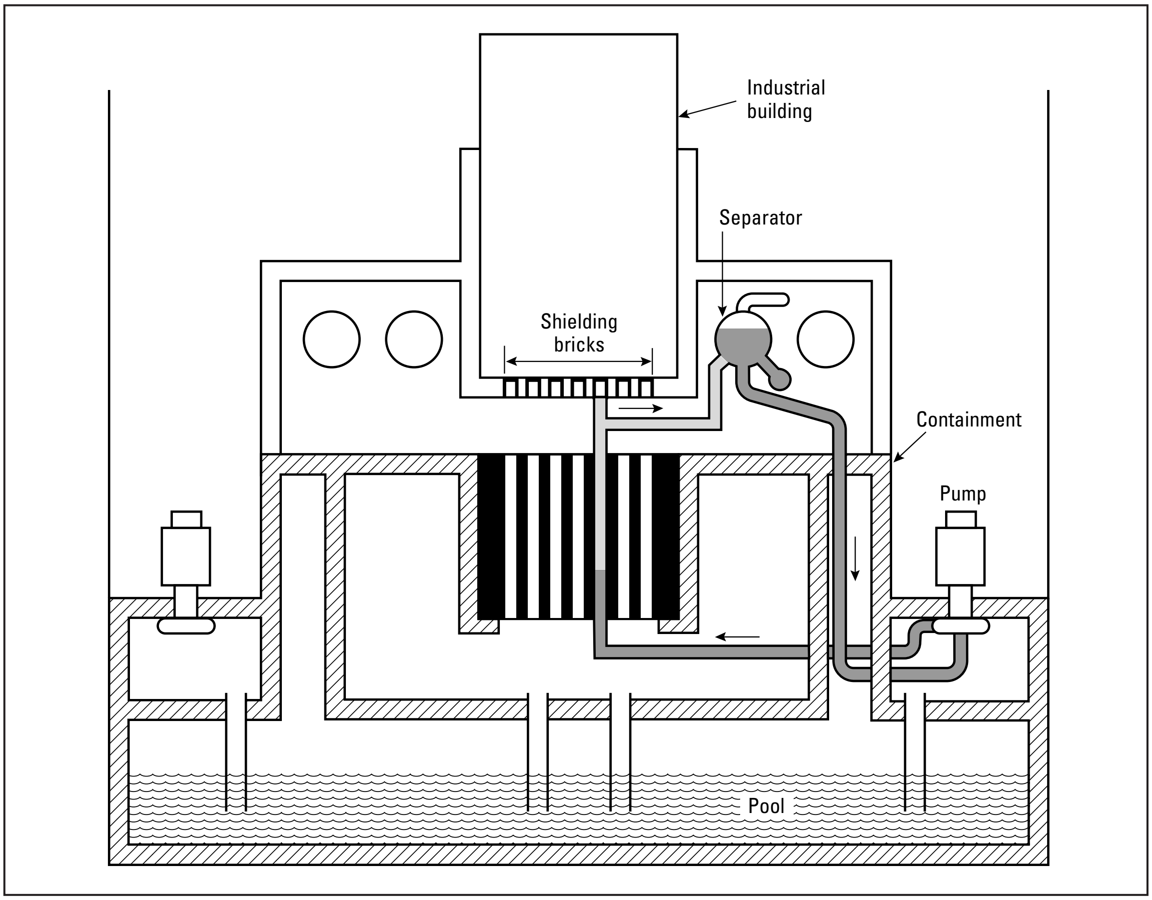


Figure 7
Chernobyl containment

the radioactivity are *contained* by the buildings. This does not prevent plant damage, but protects the public by **accommodating** an accident. These structures are normally called *containment* and are a safety system.

The Chernobyl unit 4 reactor had shutdown and emergency core cooling, as we shall discuss later, but had only a **partial** containment. The pipes *below* the reactor core were inside what the Soviets called "leak-tight boxes". These boxes were connected to a huge pool of water under the whole building — the "bubbler" pond, as the Soviets named it. If one of the pipes in the boxes broke, the steam would be forced into the pond, where it and any radioactive particles it contained would be trapped in the water, and the leak-tight boxes would hold. But all the steam pipes **above** the core were inside *ordinary industrial* buildings (Figure 7). Thus if one of these pipes broke, particularly if the break were large, a release of radioactive steam would occur. The amount of radioactivity released would depend on how effective the other systems — shutdown and emergency cooling — were in preventing damage to the fuel. At first this seems hard to understand — why not build containment around the whole reactor and all its piping?

Earlier versions of the RBMK reactors, for example the 4 units at Leningrad, do not even have a partial containment. The Soviet philosophy at the time these were built relied on accident prevention and mitigation, and neither their RBMK reactors nor their U.S.-style pressure-vessel reactors had containment. The accident at the U.S. Three Mile Island plant in 1979 caused a thorough review of safety in all countries, including the USSR. While the Soviets may have already started to add containment to reactors near cities, it is likely that as a result of Three Mile Island, they confirmed that containment buildings were justified at other locations. But the RBMK is a huge reactor — there is a tall fuelling machine at the top that replaces the uranium as it is used up, so the building above the reactor is large — about 71 meters high. The Soviets felt that to put all this in a containment is difficult and costly. To put the bottom pipes in containment is easier, and this was done. So Chernobyl unit 4 represented a compromise.

2. The Accident on April 26, 1986

Much of the information on the accident sequence comes from Soviet official sources (References (1) and (2)). The Soviets have published reactor design information, in open literature, providing the key characteristics of the RBMK, and sometimes discussing weaknesses with exemplary frankness. Can it be checked? Yes. In Canada scientists can and have checked the consistency of the Soviet information on the accident sequence and the design using our own mathematical reactor models, and confirmed that the Soviet information is consistent. We also discovered important omissions from the Soviet presentation in Vienna — they had left some clues, but because there were design weaknesses, they were not highlighted. We have now filled in the blanks, and AECL's interpretation of the accident cause (Reference (6)) is now accepted by many countries, and has been confirmed as plausible by independent assessments done in the United States (by the Department of Energy) and in the United Kingdom, and by the Soviet Union (Reference (7)).

2.1 How and Why It Happened

2.1.1 A Test for Safety Sets it Off

It is one of history's ironies that the worst nuclear accident in the world began as a test to improve safety. The events of April 26 started as an experiment to see how long a spinning turbine could provide electrical power to certain systems in the plant. The reason for the test? Well, the Soviets, in common with most of the rest of the world, design their reactors not only to withstand an accident, but also to cope simultaneously with a loss of electric power. This may seem a little strange — to run out of power at a generating station — but in an accident the reactor is shut down right away, so can't generate its own power directly. It would normally get power from the electrical supply *to* the station or from the other reactors at the same site. To ensure an extra layer of defence, it is considered that there is a possibility that these sources have also failed. The normal backup is to provide diesel engines at the site to drive emergency generators, just as hospitals do in case of a power failure. These diesels usually start up in 30 seconds, and for most plants this is a short enough interruption to keep important systems going. For the Chernobyl reactor, the Soviets felt this was *not* short enough, and they had to have almost an uninterrupted supply. Now even with the reactor shut down, the spinning turbine is so heavy, it takes a while to slow down, and the Soviets decided to tap the energy of the spinning turbine to generate electricity for the few seconds before their diesels started. The experiment was to see how long this electricity would power the main pumps which keep the cooling water flowing over the fuel.

The test **had** been done before, on unit 3, with no particular ill-effects on the reactor. However the electrical voltage had fallen off too quickly, so that the test was to be redone on unit 4 with improved electrical equipment. The idea was to reduce reactor power to less than half its normal output, so all the steam could be put into one turbine; this remaining turbine was then to be disconnected, and its spinning energy used to run some of the main pumps for a short while. At the meeting in Vienna the Soviets were at some pains to point out that the atmosphere was not conducive to the operators performing a cautious test:

1. The test was scheduled to be done just before a planned reactor shutdown for routine maintenance. If the test could not be done successfully **this** time, then the people would have to wait another year for the next shutdown. Thus they felt under pressure to complete the test this time.
2. Chernobyl unit 4 was a model plant - of all the RBMK-1000 type plants, it ran the best. Its operators felt they were an elite crew and they had become overconfident.
3. The test was perceived as an electrical test only, and had been done uneventfully before. Thus the operators did not think carefully enough about the effects on the reactor. There is some suggestion that in fact the test was being supervised by representatives of the turbine manufacturer instead of the normal operators.

2.1.2 How the Trap Was Set

The accident really began 24 hours earlier, since the mistakes made then slowly set the scene that culminated in the explosion on April 26. Table 1 shows a summary of all the things the operators did and how the plant responded; here we describe the key events.

At 1 a.m. on April 25, the reactor was at full power, operating normally with steam going to both turbines. Permission was given to start reducing power for the test, and this was done slowly, with the reactor reaching 50% power twelve hours later at 1:05 in the afternoon. At this point only one of the two turbines was needed to take the steam from the reactor, and the second turbine was switched off.

Normally the test would then have proceeded, with the next step being to reduce power still further to about 30%. However the people in charge of distribution of electricity in the USSR refused to allow this, as apparently the electricity was needed, so the reactor stayed at 50% power for another 9 hours. At 11:10 p.m. on April 25,

Table 1 — Event Sequence

TIME	EVENT	COMMENTS
April 25		
01:00	Reactor at full power. Power reduction began.	As planned.
13:05	Reactor power 50%. All steam switched to one turbine.	As planned.
14:00	Reactor power stayed at 50% for 9 hours because of unexpected electrical demand.	
April 26		
00:28	In continuing the power rundown, the operator made an error which caused the power to drop to 1%, almost shutting the reactor off.	This caused the core to fill with water & allowed xenon (a neutron absorber) to build up, making it impossible to reach the planned test power.
01:00-01:20	The operator managed to raise power to 7%. He attempted to control the reactor manually, causing fluctuations in flow and temperature.	The RBMK design is unstable with the core filled with water — i.e., small changes in flow or temperature can cause large power changes, and the capability of the emergency shutdown is badly weakened.
01:20	The operator blocked automatic reactor shutdown first on low water level, then on the loss of both turbines.	He was afraid that a shutdown would abort the test. Repeat tests were planned, if necessary, and he wanted to keep the reactor running to do these also.
01:23	The operator tripped the remaining turbine to start the test.	
01:23:40	Power began to rise.	The reduction in flow as the voltage dropped caused a gradual increase in boiling leading to a power rise.
	The operator pushed the manual shutdown button.	Canadian (and other) calculations show that, because of the shutoff rod design, this had exactly the opposite effect to what was expected. The power increased rapidly instead of dropping.
01:23:44	The reactor power reached about 100 times full power, fuel disintegrated, and excess steam pressure broke the pressure tubes.	The pressure in the reactor core blew the top shield off and broke all the remaining pressure tubes.

the Chernobyl staff got permission to continue with the power reduction. Unfortunately the operator made a mistake, and instead of holding power at about 30%, he forgot to reset a controller and the power fell to about 1% — the reactor was almost shut off. This was too low for the test. Now in all reactors, a sudden power reduction causes a quick buildup of a material called xenon in the uranium fuel. Xenon is a radioactive gas, but more important it sucks up neutrons like a sponge, and tends to hasten the reactor down the slope to complete shutdown. As well, the core was at such a low power that the water in the pressure tubes was not boiling, as it normally does, but was liquid instead. Liquid water has the same absorbing effect as xenon. To try to offset these two effects, the operator pulled out almost **all** the control rods, and managed to struggle back up to about 7% power — still well below the level he was supposed to test at, but as high as he could go because of the xenon and water.

It was as if you were trying to drive a car with the accelerator floored and the brakes on — it's abnormal and unstable.

Indeed it is a very serious error in *this* reactor design to try to run with all the control rods out. The main reason is that some of these same rods are used for emergency shutdown, and if they are all pulled out well above the core, it takes too long for them to fall back into the high-power part of the reactor in an emergency, and the shutdown is very slow. The Soviets said that their procedures were very emphatic on that point, and that "not even the Premier of the Soviet Union is authorized to run with less than 30 rods!"

Nevertheless, at the time of the accident, there was the equivalent of only **6 to 8** rods in the core. At any rate, the operator had struggled up to 7% power by 1 a.m. on April 26, by violating the procedure on the control rods. He had other problems as well — all stemming from the fact that the plant was never intended to operate at such a low power. He had to take over manual control of the flow of water returning from the turbine, as the automatic controllers were not operating well at the low power. This is a complex task to do manually, and he never did succeed in getting the flow correct. The reactor was so unstable that it was close to being shut down by the emergency rods. But since a shutdown would abort the test, the operator *disabled* a number of the emergency shutdown signals.

After about half an hour of trying to stabilize the reactor, by 1:22 a.m. the operators felt that things were as steady as they were going to be, and decided to start the test. But first they disabled one more signal for automatic shutdown. Normally the reactor would shut down automatically if the remaining turbine were disconnected, as would occur in the test, but because the staff wanted the chance to *repeat* the test, they disabled this shutdown signal also. The remaining automatic shutdown signals would go off on abnormal power levels, but would not react immediately to the test.

Let us pause briefly to see what the state of the reactor was. Most of the shutdown signals had been disabled. The control/safety rods had mostly been removed, and the power was abnormally low. As well, the core was filled with water **almost** at the boiling point, but not quite. We mentioned that liquid water is a good absorber of neutrons. So if it boils suddenly (water being replaced with steam), fewer neutrons get absorbed and the power goes up. In normal operation, this is not a problem as the reactor is designed to cope with this change. But at low power, with the core filled **completely** with water, sudden boiling would cause a rise in power *at a time when the shutdown systems were abnormally slow*. The Canadian analysis of the accident by Chan, Dastur, Grant, and Hopwood of AECL and Chexal of the U.S. Electric Power Research Institute (EPRI), (Reference (6)), showed that this effect by itself would be too small to **start** a bad accident, but it would **accelerate** a rise in power that had **already** started.

The Canadian/EPRI analysis in fact points to a more fundamental weakness in the shutdown system design. The control rods (which are also used for shutdown) travel in vertical tubes, and are cooled by flowing water. Normally the control rod moves in and out of the reactor to control the power — moving in (adding more neutron absorber) to reduce power and out to increase it. So as the control rod moved in, it would replace the water, and as it moved out, it would be replaced by water. The trouble with this scheme is that water **also** absorbs neutrons, so the effect of moving the rod would be small. To enhance its effect, at the bottom end of most of the rods, there is attached **another** rod, made of graphite — called a displacer. Graphite as we have said does **not** absorb neutrons very well. So

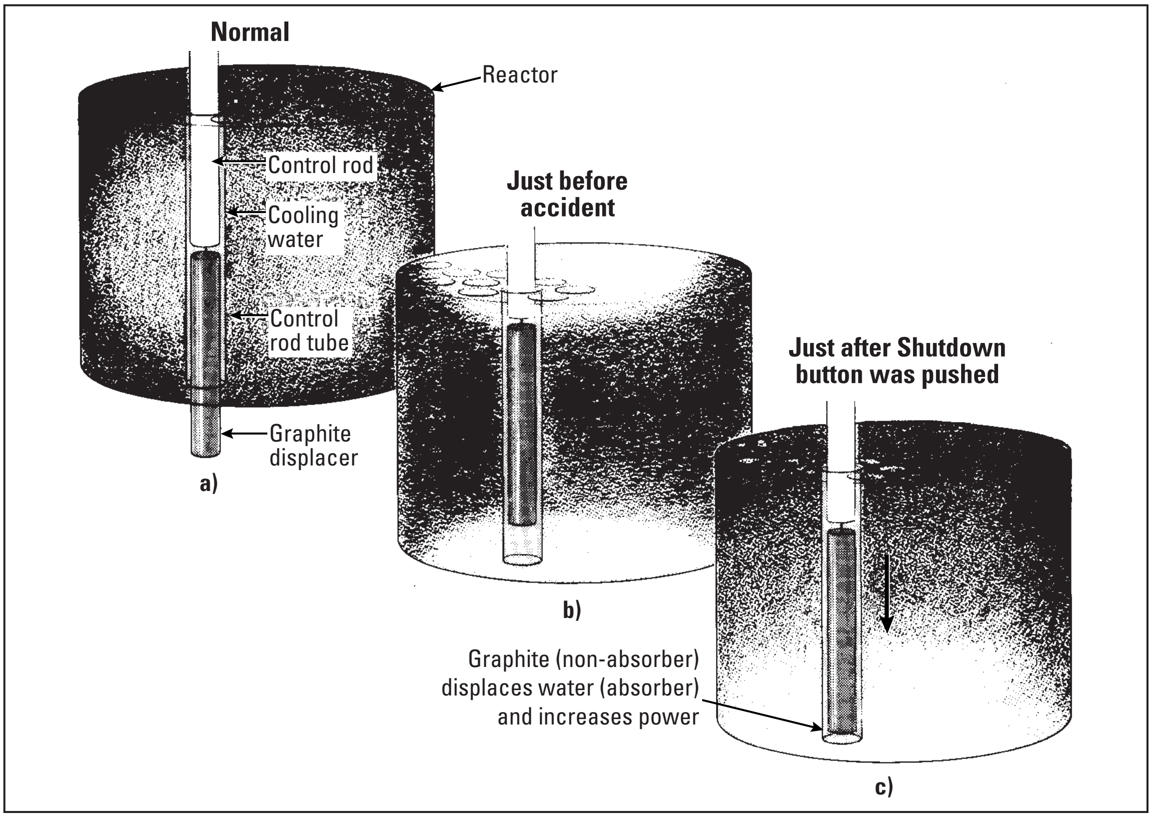


Figure 8
Role of shutdown rods

now when a control rod moves in, it replaces not water but graphite — so its effect on the number of neutrons is larger. And similarly when it moves out (Fig. (8a)).

So far so good. The weakness lay in the way this scheme worked if the reactor was **not** operating normally. Just before the accident, most of the control rods were pulled out of the reactor, so far out in fact that even the graphite section was **above** the bottom part of the reactor — the control rod tubes at the bottom contained only water (Fig. (8b)). Even this would not normally matter, because very little power is usually generated at the bottom. But Canadian simulations and the pattern of damage to the reactor suggest that just before the accident, most of the reactor power *was* being generated near the bottom. If the control/shutoff rods were then driven slowly in, the **first** effect would be to replace water (which absorbs neutrons) by graphite (which does not) (Fig. (8c)).

In other words, driving in the control/shutoff rods, which was supposed to shut down the reactor, would have precisely the *opposite* effect — it would cause a fast power **increase** instead. With this in mind, let us return to the sequence of events.

2.1.3 The Test Begins

At 1:23:04, the turbine was disconnected and its energy fed to 4 of the 8 main pumps. As it slowed down, so did the pumps, and the water in the core, now moving more slowly over the hot fuel, began to boil. Twenty seconds later the power started rising slowly, then faster, and at 1:23:40 an operator pushed the button to drive in the emergency rods and shut down the reactor. We do not know for sure why he did it — the individual was one of the early casualties — but likely he saw either the power begin to rise or the control rods start to move slowly in to overcome the power rise. The shutdown rods began to move in slowly. Our analysis (Reference (6)) shows that this attempt to shut the reactor down in fact caused a *large, fast* **power rise**. It is acknowledged as plausible by a Soviet paper, presented at a public conference in October, 1987 (Reference 7)). Within **four** seconds, the power had risen to perhaps 100 times full power and had destroyed the reactor.

2.1.4 The Test Ends Disastrously

The power surge put a sudden burst of heat into the uranium fuel, and it broke up into little pieces. The heat from these pieces caused a rapid boiling of the cooling water, and a number of pressure tubes burst under the strain. The steam escaped from the pressure tubes, burst the metal container around the graphite, and lifted the concrete shield on top of the reactor. This broke all the remaining pressure tubes.

2.2 Damage to the Plant

2.2.1 The Same Day

The power surge destroyed the top half of the reactor core, the building immediately above the reactor, and some of the walls on either side (Figure 9(b)). The Soviets commented somewhat ironically that the leak-tight compartments below the reactor survived intact.

Burning fragments of fuel and graphite were thrown out in the explosion, and landed on the roof of the adjacent turbine building, causing about 30 fires on the asphalt roof and elsewhere. The Soviets' first priority was to put these out, so the damage would not spread to the reactors operating nearby. Local firefighters had extinguished all fires by 5 in the morning, but at a terrible personal cost: many of them were overexposed to radiation and were among the early casualties.

The destruction was not, of course, caused by a nuclear explosion but by steam and perhaps chemical explosions, so the damage was confined to unit 4. Indeed, unit 3 was kept generating electricity for several hours, and the other units for somewhat longer, until they were all shut down in a controlled manner because of the increasing radioactive contamination of the area.

2.2.2 The Next Ten Days

The next step was to try to cool off the damaged core. The water pipes had been broken in the explosion, so an attempt to flood the core with water didn't work. The graphite, meanwhile, had been exposed to air by the destruction, and was being heated by the small amount of heat coming from the fuel, which although broken up, was still in the reactor and piping compartments. By the second day, the graphite had begun to burn in places, as clearly seen in a film taken from a Soviet helicopter. Eventually about 10% of it was consumed. The burning was not altogether bad — it caused an air draft through the damaged core that kept the fuel cool, but the same air was reacting chemically with the fuel and causing it to release radioactive particles. So the Soviets decided to smother the core, and from April 28 to May 2, flew hundreds of helicopter sorties over the reactor, dropping 5000 tons of mainly lead, sand, clay, and limestone — the idea was that these materials would trap radioactive particles before they could escape.

The materials **did** shield the core, but like putting a tea cozy over an electric kettle, also trapped the heat, so the fuel began to heat up again. The Soviets solved **that** by pumping nitrogen into the bottom of the core. That really did the job — cooling off the core and putting out the graphite fire.

The Soviets **were** worried about the possibility of the core collapsing into the water pool below, causing a burst of steam. So they sent courageous divers *into* the pool to open some valves and empty it. Indeed, recent observations on the remains of the reactor showed that fuel had melted and flowed out of the core, later solidifying again as it cooled down. In the end, between 2% and 8% of the significant radioactive species of material escaped from the plant, much of it being deposited as dust or particles close by, and the rest being carried by wind over the Ukraine and Europe.

2.2.3 The Long Term

With the situation stabilized, the Soviets' next jobs were to remove radioactivity from the site so the other three units could be restarted, and to shield the damaged reactor more permanently. Remotely-controlled bulldozers were used to scrape off contaminated soil, buildings were washed down with special chemicals, concrete was poured on the ground to keep down radioactive dust, and deep concrete walls were built in the ground around the site to prevent contaminated groundwater from spreading. The damaged reactor itself has been surrounded by a concrete "sarcophagus", as the Soviets called it, which shields the radiation sufficiently that working near it is possible. The fuel will continue to generate a small amount of heat for a long time, so fans blow cooling air through the core, and filters remove radioactive particles from the air on its way out. Figures 9 (a, b, c) show the state of the buildings before and just after the accident, and the burial of the damaged reactor six months later.

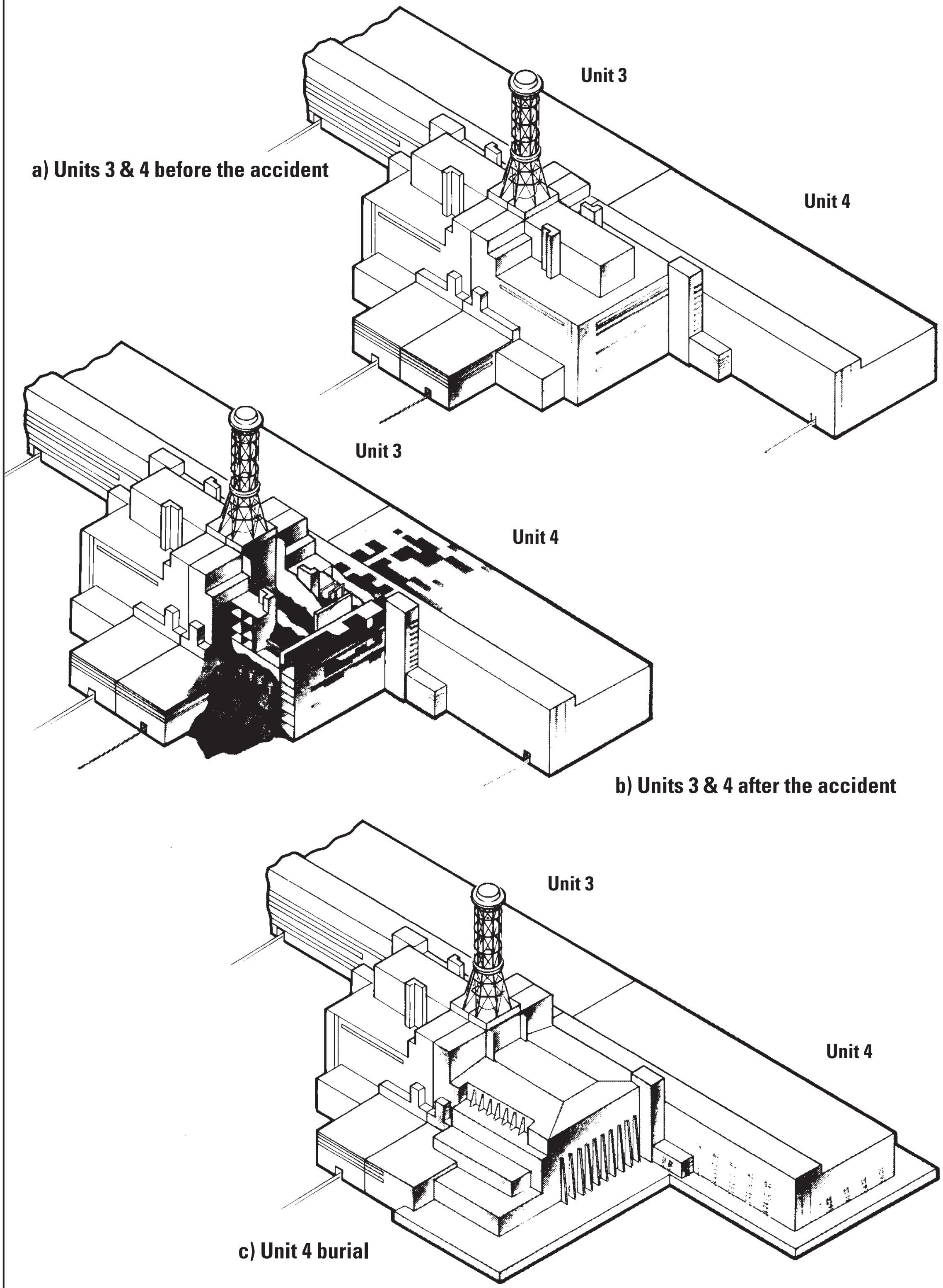


Figure 9
Damage from the accident

2.3 Effects on People

2.3.1 Immediate Effects

The brunt of the accident, in human terms, was borne by the station staff and the firefighters — no member of the public received lethal doses of radiation or even became ill from radiation. Two station staff were killed almost immediately — one was trapped by falling masonry, and the other was badly burned in the fire. Twenty-nine others died over the next few weeks — many from severe skin damage. The combination of ordinary skin burns from the fire, and radiation damage to the skin, proved particularly difficult to treat. Bone marrow transplants, which featured so prominently in the early days after the accident, were reported as counterproductive for some patients, because the surgery exposed the patients to increased risk of infection and to complications resulting from rejection of the transplant. In the end the Soviets felt that the most effective treatment was Tender Loving Care — meaning individual nursing, antibiotics, very sterile surroundings, and as little dramatic intervention as possible.

2.3.2 Longer-Term Effects

As the scale of the accident became apparent, and the direction of the wind veered toward populated areas near the plant, the Soviets ordered first that people in Pripyat and other nearby towns should stay indoors (to reduce their exposure to the radioactive cloud) and then decided to evacuate them. On April 27, 45,000 people from Pripyat were evacuated, followed over the next few days by 90,000 people living within 30 km of the plant.

In order to appreciate the significance of radiation effects, we should remember that we live in a natural seal of "background" radiation (from cosmic rays, soil, food, water and air). From it, if we live in Canada or Europe, we get a **radiation dose** of about 200 units (called millirem) a year. In some places in the world, it is much higher — in Kerala, India, the natural dose is about 1000 millirem/year, because of natural radioactivity in the soil. There are no obvious effects from this increase — in that area, poverty, for example, has a much larger effect on life expectancy than radiation.

For the people evacuated from the 30 km zone, the radiation dose they received before evacuation was, on average, equivalent to 60 years' worth of natural radiation in Europe; a few were as high as 200 years' worth. The effect fell off quickly with distance, as the radioactive material became more and more dilute: in the regional population of 75 million in the Ukraine, the average dose was equivalent to 4 to 16 years' worth of natural radiation, and in most of

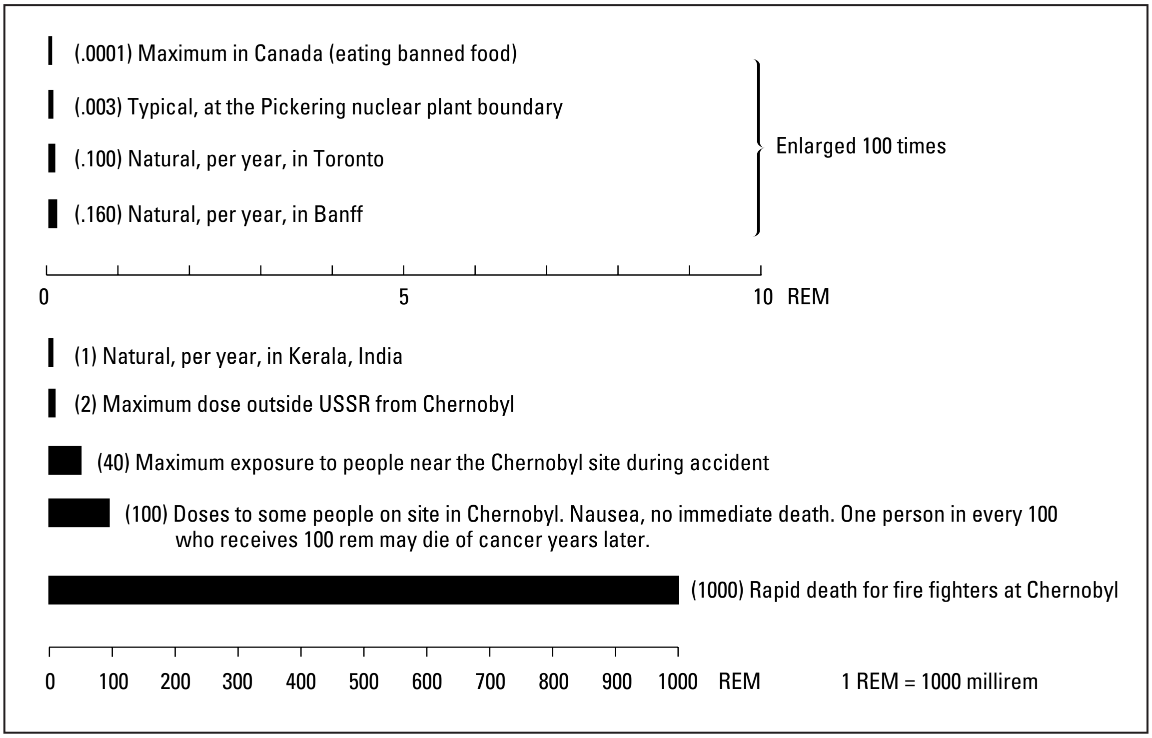


Figure 10(a)
Examples of radiation dose

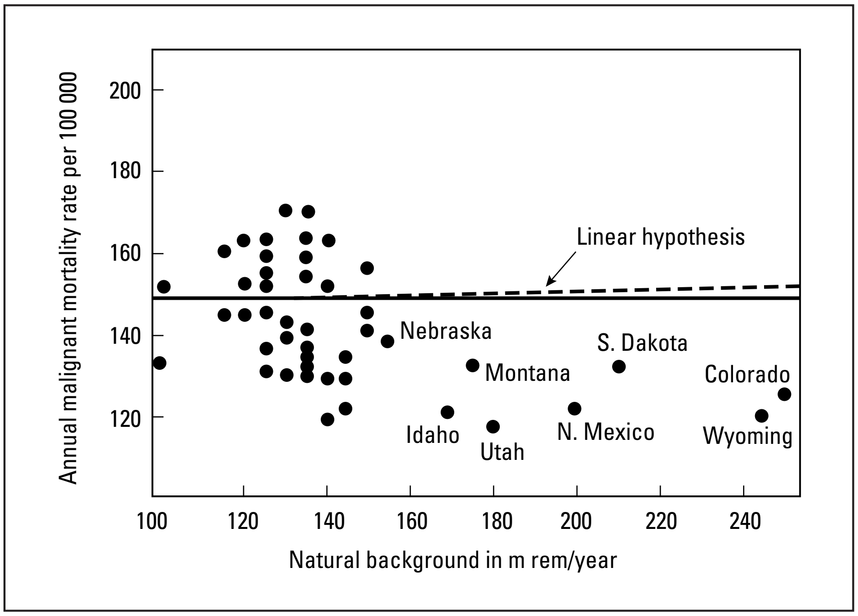


Figure 10(b)
Cancer deaths versus natural background radiation levels in the U.S. states

Western Europe, the dose to people was less than one year's worth (Figure 10 (a)). The extensive coverage of the accident caused widespread concern among people who thought they could have been exposed. In addition to the stress on these people, what do we expect to happen to them as a physical effect of the radiation?

We know that radiation can lead to a small increase in the normal chance of getting cancer many years after the original exposure — but the tests which show this effect are for doses much *higher* than almost all people received in the accident. How does one interpret these tests at lower doses? The technique used by almost all scientists is to assume that the **effect** of a dose of radiation is **proportional to** the dose — i.e., if the dose is halved, the effect is halved — even down to very small doses. The effects of small amounts of radiation are difficult to quantify because they **are** small. Figure 10(b) quoted in Reference (3) shows the incidence of cancer deaths versus background radiation in the various U.S. states. The states with the *higher* natural background have the *lower* rate of cancer fatalities. Does this mean radiation is good for you in small doses? More likely the effect of radiation is swamped by other factors. Nevertheless, the predictions of cancer fatalities from Chernobyl, which we present below, are for doses **in this range** — the dose to the average population of the Ukraine from Chernobyl is similar to the increase in dose that you get by spending your life in Banff rather than Toronto, because of the increase in natural radiation exposure with altitude.

The Soviets' dose figures suggest that in the evacuated population of 135,000, over the next 30-40 years, about 200 people would die of cancer from the accident — or about 1% of the 17,000 people who would die of cancer from other causes. In the regional population of 75 million, the accident would increase the number of fatal cancers by about a fifth of a per cent. The effects on the rest of Europe will be much less than this.

At the Vienna meeting, there was considerable debate over the Soviets' calculations — many experts felt that their modelling of how radioactive material got into the food chain was a large overestimate, and the Soviets conceded that the results of their calculations could be ten times too high. Indeed more recent estimates are lower (Reference (9)). However, all the predictions are small enough that direct observations of the effects are difficult — thus a continuing follow-up of the health of the exposed people is planned. The follow-up itself could affect the results — if people see the doctor more often, illnesses which normally go undetected until too late will be caught and cured — a phenomena which was found in the follow-up of the Hiroshima bomb survivors.

3. Why Things Went Wrong — Ideas of Safety

What went wrong? To be sure, the operators made some mistakes. But a mistake should not lead to such disastrous consequences. The problem was that the design was not **forgiving** of mistakes. Let's explore that a bit, by looking at a household tool that almost every Canadian has used — the power drill.

3.1 A Simple Analogy

Let's assume, narrowly, that our safety concern with a power drill is electrocution — we'll ignore drilling holes in one's hand or getting hit by broken metal. To achieve this safety goal, the first thing an informed consumer does is buy a *quality* product — the better the drill is built, the less chance there is that it will short out. **Accident prevention** is the most effective way of assuring safety.

But it is not enough. Most of us want to be protected even if an accident occurs. Modern power drills are able to protect you from electrocution by means of a ground plug (which ensures the housing is grounded) or by double electrical insulation — so even if a wire does short out, you do not get a shock. This is **accident mitigation**.

You can go even one step further, and buy a ground-fault-interrupter — this plugs into the wall and the drill plugs into it in turn. It works by measuring the **difference** in current between the hot and neutral wires, and if there is a difference, concludes the missing current must be passing through you, and cuts it off (Figure 11). This level of safety assumes *the drill has failed* and accommodates that failure — **accident accommodation**.

In order for these to work well, they have to be **simple** and **powerful**. **Simple** in the sense that they shouldn't depend on the *type* of fault in order to work — e.g., **which** wire shorts out shouldn't matter. **Powerful** in the sense that they have to be designed to do the job — a ground fault interrupter has to cut off the current *fast* enough that you are not injured.

3.2 Nuclear Safety

In a nuclear power plant, although it is much more complex, the same basic ideas apply. In fact, we introduced them early on in the context of a pipe break. The safety goal is to avoid the release of dangerous amounts of radioactivity. Since almost all the radioactivity is in the fuel, and can only get out if the fuel overheats, the need is to control the power and keep cooling water on the fuel.

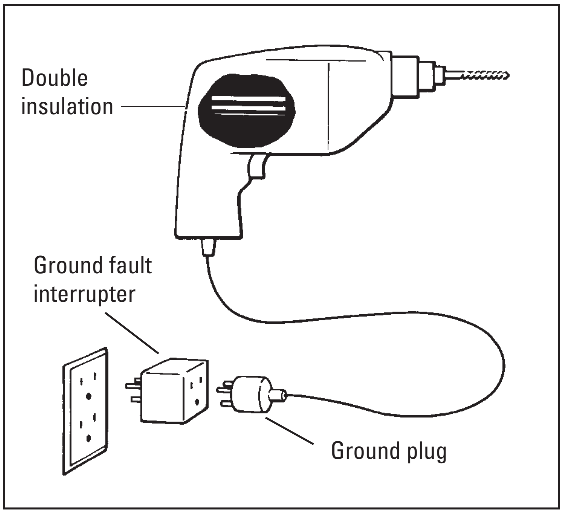


Figure 11
Power drill safety

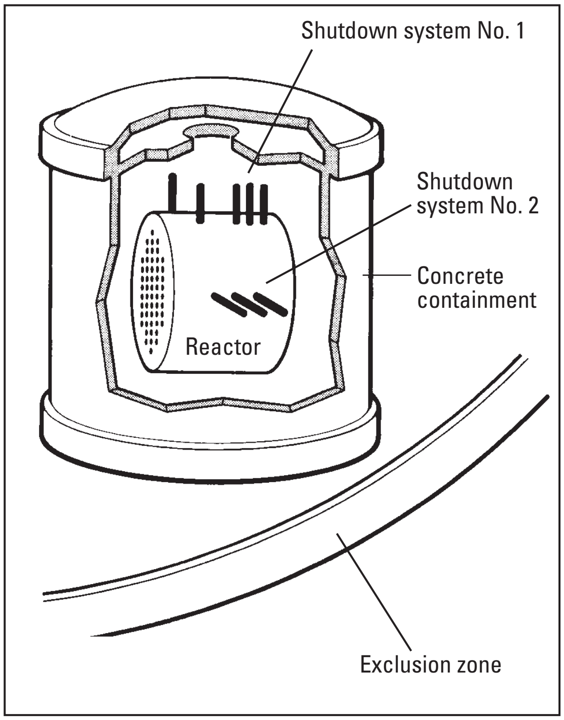


Figure 12 CANDU reactor containment of radioactivity

Again, accident **prevention** is the most important thing to do, and it is done by strict quality control in manufacture and construction, by inspecting the plant while it's running, and by using operating experience to fix up small problems before they become large ones.

If an accident starts, the next step is to arrest it before it damages the plant. In CANDU reactors, the normal control systems are powerful enough to do this for most accidents. They are backed up by separate systems dedicated *only* to safety — shutdown systems to turn off the power if it starts to go up higher than it should (Figure 12), and emergency core cooling, to replace cooling water if it should be lost from a pipe break. These are the CANDU **mitigating** systems.

The CANDU goes one step further and allows for the possibility that fuel is damaged regardless, and so it has an **accommodating** system — containment — also a safety system, but whose role is to contain radioactivity released from the fuel. There is also a one-kilometer ring of land around the reactor — called the exclusion zone — which allows *dilution* of any radioactivity released in an accident before it can get to where people live (Figure 12).

Let's now look at Chernobyl, and CANDU, in this light.

4. How CANDU Stacks Up

We are going to compare CANDU and Chernobyl in three areas:

- control systems
- shutdown systems
- containment systems

to see how the ideas of **simplicity** and **power** were applied in both cases (Reference (8)).

A thumbnail comparison to the Chernobyl design is given in Table 2. For a description of CANDU safety, see Reference (4), and for a general description of CANDU, see Reference (5). Like Chernobyl, the CANDU uses pressure tubes to contain the fuel. But that's where the similarity ends. In CANDU, the tubes are horizontal rather than vertical; the fuel is natural uranium rather than enriched; the coolant is a special form of water, called heavy water, rather than ordinary water; the moderator is also heavy water rather than graphite; and the steam from the reactor goes *not* directly to turbines, but to boil ordinary water in a **second** cooling system. While the differences in design concept are interesting, what is more important is how safety was approached. There are differences between various CANDU reactors — here we use the CANDU 600, as it is in operation both in Canada and in other countries.

Table 1 — Event Sequence

FEATURE	CHERNOBYL	CANDU (typical)
Design		
Coolant	Ordinary water	Heavy water
Steam Cycle	Direct (steam & water from reactor are separated and steam goes directly to turbines)	Indirect (hot water from reactor boils ordinary water in a boiler to steam, which then goes to the turbine)
Fuel	~2% enriched uranium oxide	Natural uranium oxide
Moderator	Graphite bricks (max. temp. 700°C)	Heavy water (max. temp. ~88°C)
Fuel channels	Vertical, pressure-tube, no calandria tube	Horizontal, pressure tube with calandria tube
Safety Systems		
Containment	No upper containment — lower containment is concrete cells surrounding high pressure piping, & connected to water pool, to reduce the building pressure.	Concrete building, or multi-unit negative pressure containment, surrounding all major piping, with water spray (dousing) to reduce the building pressure.
Shutdown	One mechanism: — absorber rods	Two complete systems: — absorber rods — liquid injection
	10 seconds to be effective	2 seconds to be effective
	Effectiveness depends on state of plant	Effectiveness independent of state of plant
Emergency Core Cooling	High pressure injection driven by gas and pumps, then pumped flow	High pressure injection driven by gas or pumps, then pumped flow

4.1 Controlling the Power

Figure 13 shows the two power control systems schematically.

Chernobyl is a physically large core — 12 m in diameter by 7 m high. It is also large in a **physics** sense — that is, one part of the core can be going up or down in power without the rest of the core feeling the effect. In fact, it takes only 2% to 10% of the reactor to form a mini-reactor which behaves almost independently of the rest of it. Thus the control system has to be able to handle both the bulk power, and the spatial power, i.e., to ensure that the power is in step across the core, and that the *mini-reactors* are acting together. This difficult job is done by a mixture of computers, ordinary control circuits, and people — *but* the computers in Chernobyl are used for **monitoring** only, and a combination of ordinary control circuits and people does the day-to-day, hour-to-hour controlling based on the information the computers present. The Soviets mistrusted the reliability of direct computer control, apparently based on some bad early experience they had.

In case the mini-reactor concept seems academic to you, we are fairly certain that in the accident the reactor really behaved as two independent reactors — one at the top and one at the bottom. We believe that the shutoff rods probably succeeded in shutting down the "top" reactor but never reached the "bottom" one in time — in fact they *raised* its power.

CANDU is a smaller core physically — less than half the size (6 m diameter by 6 m high) of Chernobyl. It is also a more tightly-coupled core: specifically, it takes at least 65% of the core to form a mini-reactor, so if there is a higher power in one region of the core than another, the regions are large and easy to detect. Routine control is through two independent computers, one always operating and the other on standby. The operators tell the computers what power they would like, and the computers process all the power measurements, and operate all the control rods, to achieve that. They also provide information to the operators on the state of the plant. The CANDU designers and owners felt that although the CANDU can be controlled manually, the computers were faster in response

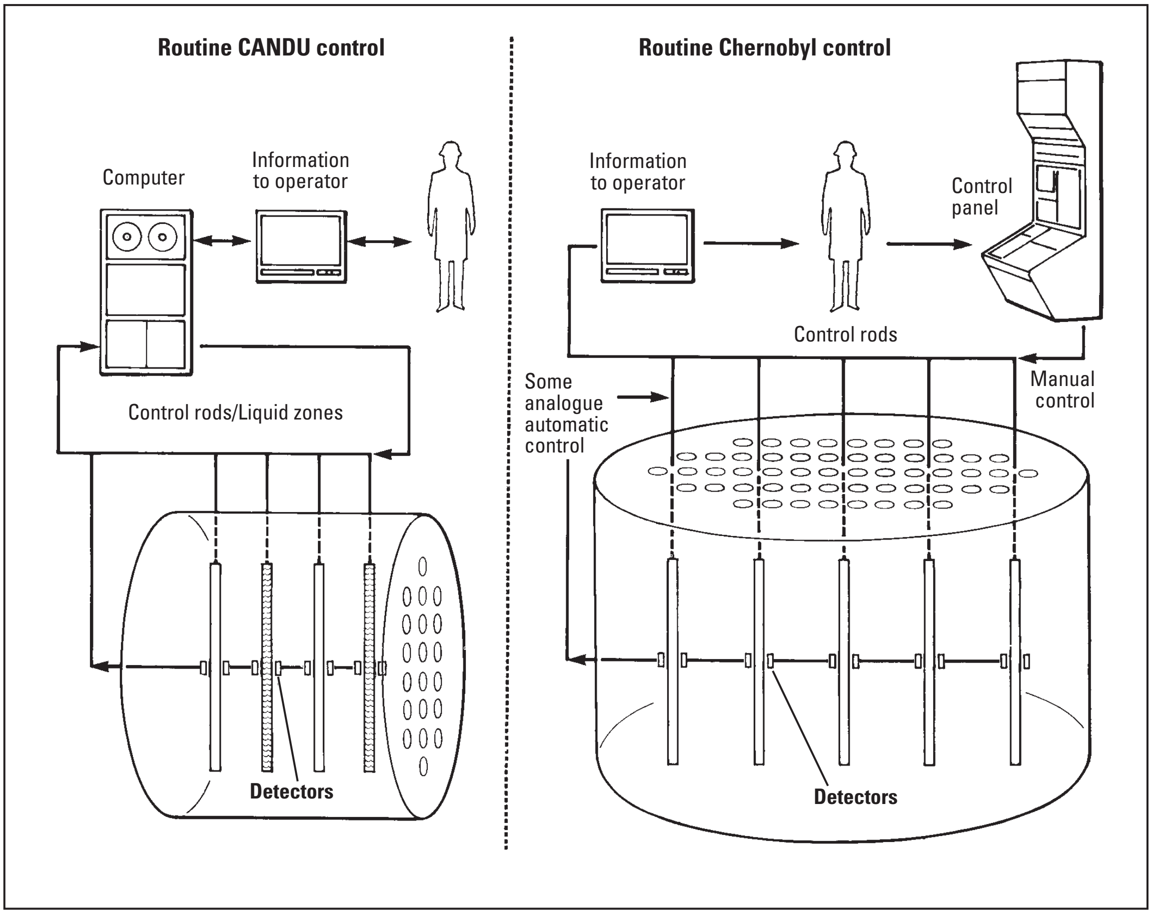


Figure 13
Controlling the power

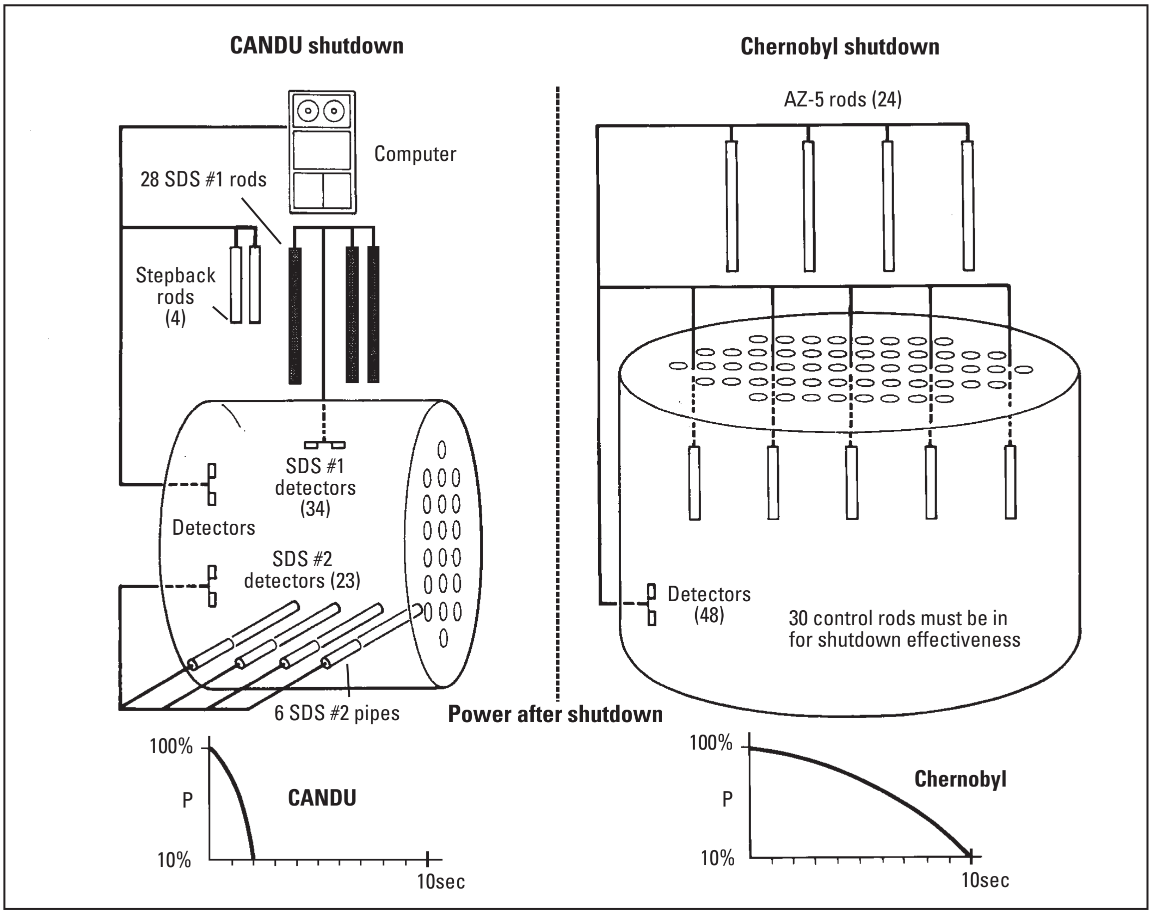


Figure 14
Shutting down the reactor

to off-normal conditions and less likely to make mistakes, than a human. Our experience has borne that out — if **both** computers do fail, that station is designed so that it will shut down immediately, and in practice double computer failures account for an insignificant fraction of the downtime of the station.

In short, Chernobyl, which is more difficult to control, relies much more on operators for that control. This is one reason why the Soviets were so critical of their operators for making mistakes in the events leading up to the accident — Chernobyl is more *unforgiving* of such mistakes.

4.2 Shutting Down the Reactor

Perhaps no area is more dramatically different than emergency shutdown of the two reactors. In Chernobyl, emergency shutdown relies on 24 rods, held in the upper parts of the core, and driven in, in an emergency (Figure 14). The Soviets are reluctant to shut down these reactors completely, probably because of the length of time it takes to restart them, so emergencies are classified into five groups. For four of these groups, the reactor is not shut down completely, but the power is reduced until the abnormal condition can be controlled. For the fifth group, the reactor is shut down **slowly** — the power goes from 100% to 20% in about 10 seconds.

In fact the shutdown rods are part of the control system, rather than being a separate emergency system. This means there is a risk of a fault in the control room **also** disabling emergency shutdown. Even more important, **the shutdown effectiveness depends on the reactor being operated properly**. There **must** be a least 30 (other) control rods in the core for the emergency shutdown to work properly, and the reactor should not normally be run at low power. If these requirements are violated by the operators, as they were in the accident, then emergency shutdown can be slowed down considerably or work exactly opposite to the way it is supposed to.

In CANDU 600 (Figure 14), the closest equivalent to the Chernobyl emergency shutdown is something we call stepback. This is what the control system does in an abnormal condition — it drops 4 control rods partially or fully into the core, and can shut the reactor down for most, but not all accidents. In addition, there are **two, independent shutdown systems**. These are there *only* for safety reasons — they play no part in the day-to-day control of the plant, and in fact each system has its own power detectors, logic, and shutdown mechanism. **Each system** is capable of shutting down the reactor for all accidents. And they are fast — either can take the power from 100% to 10% in less than 2 seconds. They are shown schematically in the figure — the first system consists of 28 rods, which are shot by heavy springs down into the moderator, and the second consists of 6 pipes with over 200 nozzles which squirt a liquid neutron absorber, at high pressure (about 75 times tap-water pressure) into the moderator.

Why such a dramatic difference for CANDU? Perhaps the simplest reason is that Canada had a severe accident in a research reactor in Chalk River in 1952. The reactor (NRX — an experimental model from which the CANDU eventually evolved) was much smaller, there were no injuries, and the damage was not nearly as severe (in fact the core was replaced and the reactor operated continually until 1987 and still runs periodically in a back-up role to another research reactor, NRU). The causes of the accident were operator errors in incapacitating the shutdown rods, followed by a rise in power they could not react to. The operators did manually fire another shutdown mechanism — quickly draining the heavy-water moderator — although too late to prevent damage to the reactor core.

The biggest effect was on the safety philosophy of CANDU. We learned some hard lessons then and made sure the same mistakes were not repeated in the Canadian power reactors. The lessons were:

- keep the control and shutdown systems independent
- keep the mechanical design simple and powerful
- ensure the shutdown systems can be tested on-power to meet stringent reliability targets.

Canada has had a unique emphasis on shutdown capability since then. Indeed the Pickering ‘A’ units put into operation in the early 1970s (near Toronto, Ontario) have two separate shutdown mechanisms (shutoff rods, and quickly draining the heavy water moderator). The shutdown is fully independent of the control and, unlike Chernobyl, capable under any accident conditions of shutting the reactor down. The logic of each shutdown mechanism is not as separate as in later CANDU designs. Offsetting this, the measured reliability of shutdown in Pickering ‘A’ is much better than called for in the original design requirements, and shutdown is not impaired even if a number of the rods (~6) do not work.

We mentioned that, in the Chernobyl design, increased boiling in the core increases the power (this is called a *positive void coefficient*). The same is true of CANDU, although the effect is much smaller. Other reactors (such as U.S. water cooled reactors) have the opposite effect — the

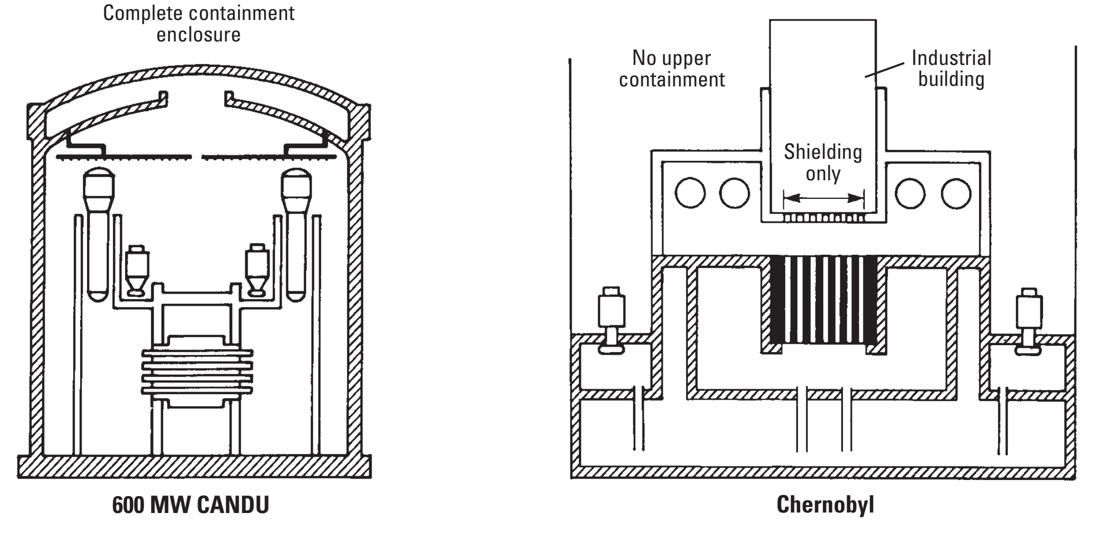


Figure 15
Containment

power goes down as the boiling increases. Is that safer? Not necessarily — it means that there is just a **different** accident where the power goes up. For example, in a Boiling-Water Reactor (one of the two main types of U.S. reactors), if the steam valves on the boilers close by mistake, the reactor starts behaving like a pressure cooker with the valve closed — the cooling water to the fuel heats up, the pressure rises and compresses the water, and since compression is the opposite effect to boiling, the power goes up. So U.S. reactors must have shutdown systems to be able to handle this. The general rule is quite simple: the shutdown systems must be **powerful** enough to overcome *all* sources of a power increase so as to shut the reactor down in an emergency. The **larger** the effect of boiling (whether positive or negative), the harder this is to do — it's better to have a small coefficient than a large one.

4.3 Containing Radioactivity

We have already mentioned that Chernobyl had a partial containment. The accident bypassed this partial containment, with the releases all going out through the burst-open top of the reactor core into the region of the building where there were *no* leak-tight boxes.

The CANDU 600 design (Figure 15) surrounds **all** major cooling piping with a concrete building designed to take the pressure of **all** the steam released in an accident. The pressure in the building is controlled by a spray of water coming from a huge (500,000 gallon) tank in the roof of the building — the equivalent of the water pool in Chernobyl. There is a rather subtle advantage of enclosing all this water in a building. The atmosphere in the building after an accident will be like a rain forest during a tropical storm, and the water will dissolve almost all the radioactive iodine and cesium released. The iodine and cesium, so trapped, will not escape even if the containment leaks. This chemical reaction did not occur in Chernobyl because the hot fuel and graphite were exposed to air, and there was no containment on top of the reactor.

4.4 The End Result

Chernobyl need not have been an unsafe design. However it had sensitive characteristics that required a sophisticated control and emergency shutdown design to keep the chance of an accident sufficiently small. As we have seen, its safety depended very heavily on operators staying within certain limits. If the operators went outside these limits, the safety systems could be ineffective in an accident, and in a very real sense, the operators would be operating blind. In a CANDU, the capability of the safety systems is independent of the operating state; as well, we have more backup systems, especially for shutdown. In that sense, CANDU is a much more **forgiving** design.

5. Lessons Learned

The world will continue to study Chernobyl for years to come. Each country with a nuclear power program has scrutinized the accident to see what lessons apply to its design and operation. In the meantime, the Soviets have drawn certain conclusions for their own program (Reference (7)).

1. They recognize how important their operators are. On the positive side, they are installing improved displays of information in the control room; improving operator training; improving procedures; and making it much more difficult to disable safety systems. On the negative side, the importance of procedures will be reinforced — violating one will be a **criminal** offense, and the designers and operators of Chernobyl Unit 4 have already been tried and sentenced.

2. On the hardware side, in the short term the Soviets first mechanically prevented control rods from being withdrawn too far in the RBMK reactors. This caused a misshapen power distribution so the reactors had to be run at reduced power. They are now redesigning the rods so that the graphite cannot be lifted above the bottom of the core even if control rods are fully withdrawn. They also required more rods to be inserted — in fact, the plants will now shut down automatically if the operator tries to pull out too many rods. The motors of the shutoff rods have been changed to speed up shutdown — from 20 seconds to 10 (compared to 2 seconds in CANDU). A new fast shutdown design is being developed. Finally the composition of the fuel is being changed (more enrichment). These changes reduce the **size** of the positive void coefficient, and increase the effectiveness of the emergency shutdown.

In Canada, we have shown that these problems have already been addressed. In particular, we checked, again, to see if there was any possible operating state in which the shutdown systems could be ineffective; and electrical utilities also reviewed the operational aspects of their nuclear power plants.

6. References

(1) USSR State Committee on the Utilization of Atomic Energy, *The Accident at the Chernobyl Nuclear Power Plant and Its Consequences*, presented at the International Atomic Energy Agency Post-Accident Review Meeting, August 25-29, 1986; Vienna.

(2) A. Dastur, R. Osborne, D. Pendergast, D. Primeau, V. Snell and D. Torgerson, *A Quick Look at the Post-Accident Review Meeting (PARM)*, Atomic Energy of Canada Limited Publication AECL-9327, September, 1986.

(3) Frigerio, N.A., Eckerman, K.F. and Stowe, R.S., *Argonne Radiological Impact Program (ARIP): Part I, Carcinogenic Hazard from Low-level, Low-rate Radiation*, Argonne National Lab. Publication ANC/ES-26, September, 1973. Also see J. Jovanovich, *World Energy Choices: Malthusian Catastrophes, Climactic Changes or Nuclear Power*, University of Manitoba Department of Physics preprint, February, 1986.

(4) V.G. Snell, *Safety of CANDU Nuclear Power Stations*, Atomic Energy of Canada Limited Publication AECL-6329, January, 1985.

(5) *CANDU Nuclear Generating Station Technical Summary*, Atomic Energy of Canada Limited Publication 901212PA, AECL CANDU, Mississauga.

(6) P.S.W. Chan, A.R. Dastur, S.D. Grant, J.M. Hopwood, and B. Chexal, *The Chernobyl Accident: Multidimensional Simulations to Identify the Role of Design and Operational Features of the RBMK-1000*, paper presented to the ENS/ANS Topical Meeting on Probabilistic Risk Assessment, Zurich, Switzerland; August 30 – September 4, 1987.

(7) V.G. Asmolov et al., *The Accident at the Chernobyl Nuclear Power Plant: One Year After*, translation of principal Soviet paper presented by N.N. Ponomarev-Stepnoj to the International Atomic Energy Agency International Conference on Nuclear Power Plant Performance and Safety, Vienna; September 28 – October 2, 1987.

(8) For a detailed technical evaluation, see: J.Q. Howieson and V.G. Snell, *Chernobyl – A Canadian Technical Perspective*, Nuclear Journal of Canada, Vol. 1, No. 3; September, 1987. A technical executive summary of this is in: V.G. Snell and J.Q. Howieson, *Chernobyl – A Canadian Technical Perspective – Executive Summary*, Atomic Energy of Canada Limited publication AECL-9334S, January, 1987.

(9) International Advisory Committee report to the International Atomic Energy Agency, *The International Chernobyl Report – An Overview*, June 1991.