# Chapter 2 - Design Basis Accidents

## Introduction

This chapter shows how accidents in nuclear power plants are identified and classified. The purpose is to describe the methodology, so the examples are illustrative and not complete.

## Accident Identification

First - a disclaimer. In Chapter 1, we pointed out that the term Design Basis Accidents is not a very complete concept. Notwithstanding, it is used by most countries in the world, and now in Canada. We shall therefore use it, in the following sense: Design Basis Accidents are the set of accidents for which the designer makes explicit provision (defence)[a], while remembering that more severe or peculiar accidents can occur, and ensuring that his/her design has some capability to deal with them. Design Basis Accidents are often defined as those which the regulatory body requires you to analyze - but that just shifts the responsibility of making sure the list is reasonable from the designer/operator (where it belongs[b]) to the regulator. The Canadian regulator (CNSC - Canadian Nuclear Safety Commission) has traditionally had it both ways: their regulatory documents gave long lists of Design Basis Accidents for CANDUs but then require the designer to do a systematic review and add back in any they have missed. This has now changed to accommodate non-CANDU designs.

We start by stating baldly that there is no way of identifying possible accidents beforehand that is guaranteed to be complete. The history of any technology is replete with unpleasant surprises, especially at the beginning - just think of the Hindenburg disaster, the Flixborough cyclohexane explosion, and of course the Titanic. Technologies - if we are fortunate - have their accidents early on, when the scale is small and lessons learned can be applied to the commercial

---

[a]We shall see later on that the most recent requirements in Canada and other countries ask the designer to make specific provisions for severe accidents - and in order to do so, he/she must choose some sort of representative sequences, or “design basis”, for “beyond design basis” accidents.

[b]One of the fundamental principles of nuclear safety is that the designer (or operator, once the plant is committed) is responsible for nuclear safety - *not* the regulator. The regulator sets the overall safety requirements and does an audit - i.e., provides the safety goals and ensures there are checks and balances to the designer’s ideas. If this seems strange to you, think of flying in an aeroplane. Whom do you want to be directly responsible for your safety *at that instant* - the pilot, the aircraft designers, or the bureaucrats who make the rules?

application as it becomes widely used. Although this chapter gives several methodologies for identifying accidents 'from scratch', the influence of the early accidents in research reactors has been profound in setting the safety approach of modern power reactors. We will cover this experience in a later chapter. The best way to get a 'nearly complete' list of accidents is to use more than one technique. We shall cover some of these techniques at an overview level in this chapter.

Recall from Chapter 1 that there are really three ways of designing against accidents - deterministic, probabilistic and standards- or rule-based. The first two seek to identify lists of accidents which the designer must:

- first, try to prevent;
- second, provide protection against (to stop their progress); and
- third, provide mitigation for (to reduce their effects if they occur).

Deterministic analysis is based largely on experience, and basically says to the designer, "Regardless of whether you think this accident is likely or not, you *shall* provide protection/mitigation for it, and here are the assumptions you will use". Probabilistic analysis says "Develop fault trees and event trees to find out a large list of possible accidents in a systematic way; select those above a certain frequency; and provide protection/mitigation for them". The standards-based approach says "If you design this component to these rules, and maintain it properly, you don't have to worry about it failing". As we noted, the last approach is most commonly used in designing pressure vessels. Very few reactor designs can withstand the sudden rupture of a pressure vessel[c]. In a light-water reactor, the sudden massive failure of the reactor pressure vessel would almost instantly destroy all barriers to release of radioactivity - the fuel, the primary coolant system, and the containment (which is not designed to withstand the force of a pressure vessel rocket propelled by the discharging coolant). Therefore earnest efforts are made to prove, based on a combination of experience and very sophisticated mechanical analysis, that the failure frequency of a pressure vessel is something less than $10^{-6}$ per year. Some analyses claim it is as low as $10^{-8}$ per year. Such a low number for a single event *cannot* be derived directly or by extrapolation from experience and therefore should be viewed with some skepticism. One can best say that the frequency is "low enough".

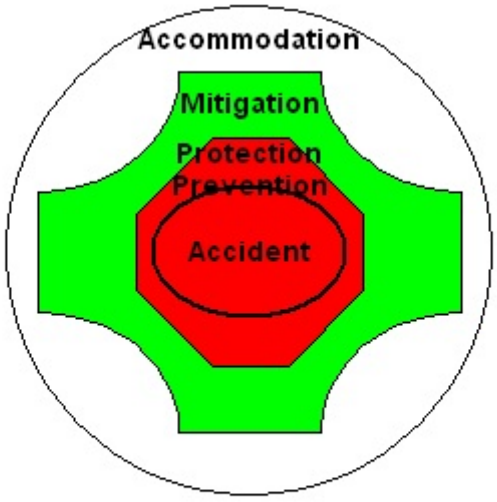
Indeed, pressure-vessel integrity became a huge issue in the introduction of a Westinghouse-type PWR - Sizewell B - into Great Britain, which until then had designed and operated gas-cooled reactors (plus one vertical pressure-tube, heavy-water-moderated reactor at Winfrith). Part of the

---

[c]One of the authors (Snell) was asked a few years ago to review the safety of a moderately-sized (500 MW(th)) Russian district heating reactor. It was a pressure-vessel design, and to cater for vessel failure, the designers surrounded the vessel with another pressure vessel - the 'guard' vessel. For large electricity-producing power reactors, this is prohibitively expensive.

difficulty is that unlike thin-walled pipes, pressure vessels have such a thick wall that they may not 'leak before break'. That is, a growing defect in a pipe will normally lead to observable leakage before the pipe fails catastrophically. In a pressure vessel this may not occur, as the crack may grow to critical length[d] before it penetrates the wall, so great emphasis must be placed on quality of manufacture and ultrasonic in-service inspection.

Finally we have used the terms "prevention", "protection" and "mitigation". We will add a fourth - "accommodation". These terms are one manifestation of the 'defence-in-depth' concept, which states simply that plant safety should not depend on only one physical barrier or system. Its origin is military, containing the idea that a single line of soldiers should not be the only barrier between you and defeat. For example: say your regulator requires you to include a large Loss of Coolant Accident (LOCA) as a Design Basis Accident. You provide an Emergency Core Cooling (ECC) system which *mitigates* the accident once it has occurred, by pouring water into the heat transport system fast enough to re-cover, and keep covered, the reactor fuel. Have you done your job? Not according to defence-in-depth. You should have first tried to *prevent* the accident (e.g., by designing to high quality standards and installing leak detection - since, as stated earlier, pipes can be designed and manufactured so that they leak (in most cases) before an impending rupture, and if you detect a leak you could shut down and depressurize the plant before the pipe broke). Still not enough - you could have provided, at least for small breaks, some *protection*, which could **stop** a small LOCA from - say - a stuck-open relief valve, by providing piping and valves to return the discharge to the heat transport system. And you should also have provided some *accommodation* in case ECC is not effective - e.g., in CANDU, by surrounding the fuel channels by a moderator which can remove decay heat - and in all reactors, by a containment building which prevents the release of radioactivity (Figure 2.1). We shall return to defence-in-depth in Chapter 9.




One Model of Defence-in-depth

**Figure 2.1**

[d]At which an unstable fast fracture occurs.

**Example**

Consider a simple example. We have just invented a new technology - called an automobile.

What could go wrong?

Well, we could start by saying that the main thing we wish to avoid was death or injury to the human occupant. This is called the "top" event. We now look at all the ways which could be the *immediate* cause of this top event. Here are a few:

- the sudden deceleration of the human occupant caused by the car's impacting a heavy object
- fire in the car
- carbon monoxide in the car

Think of some others. Remember they have to be immediate causes.

Now we take each of these events and once again ask what the immediate causes could be. For the first one:

- collision of the car with an object resulting in collision of the passenger with the car
- ejection of the passenger from the car resulting in collision of the passenger with the ground

Again we take each one in turn and ask what the immediate causes are, eventually working our way down to basic failures (e.g., failure of the headlights while driving at night). Once we have reached a reasonable level of resolution, we sort the events into design basis and non-design basis, using likelihood, and possibly consequences, as criteria. So collision with another vehicle is the design basis for the seat belts; but there is no particular design provision to protect you if you drive the car into a lake (except for old Volkswagens, which were reputed to float).

This is called the "top-down" approach. Figure 2.2 shows the first few steps for a nuclear reactor using this approach.

Another approach is to look at each component of the car and ask: What is the consequence if this component fails? If there are systems which are supposed to protect the car (or you) against such a failure, what are they, and what happens if they also fail? Eventually, if the car is well-designed, one gets to a very low frequency and draws the boundary between design basis and non-design basis again. For example, if there is a leak in the brake line, can the car stop? Yes if the emergency brake is activated and works; if not, can the car be put into low gear, etc. Typically one ends up with a lot of redundancy on braking systems (dual hydraulic cylinders, hand brake using mechanical linkage), reflecting their higher failure rate, but not on steering

systems.

This is called the “bottom-up” approach. Another term is FMEA, standing for “Failure Modes and Effects Analysis”, although that tends to be more limited, stopping after the first failure..

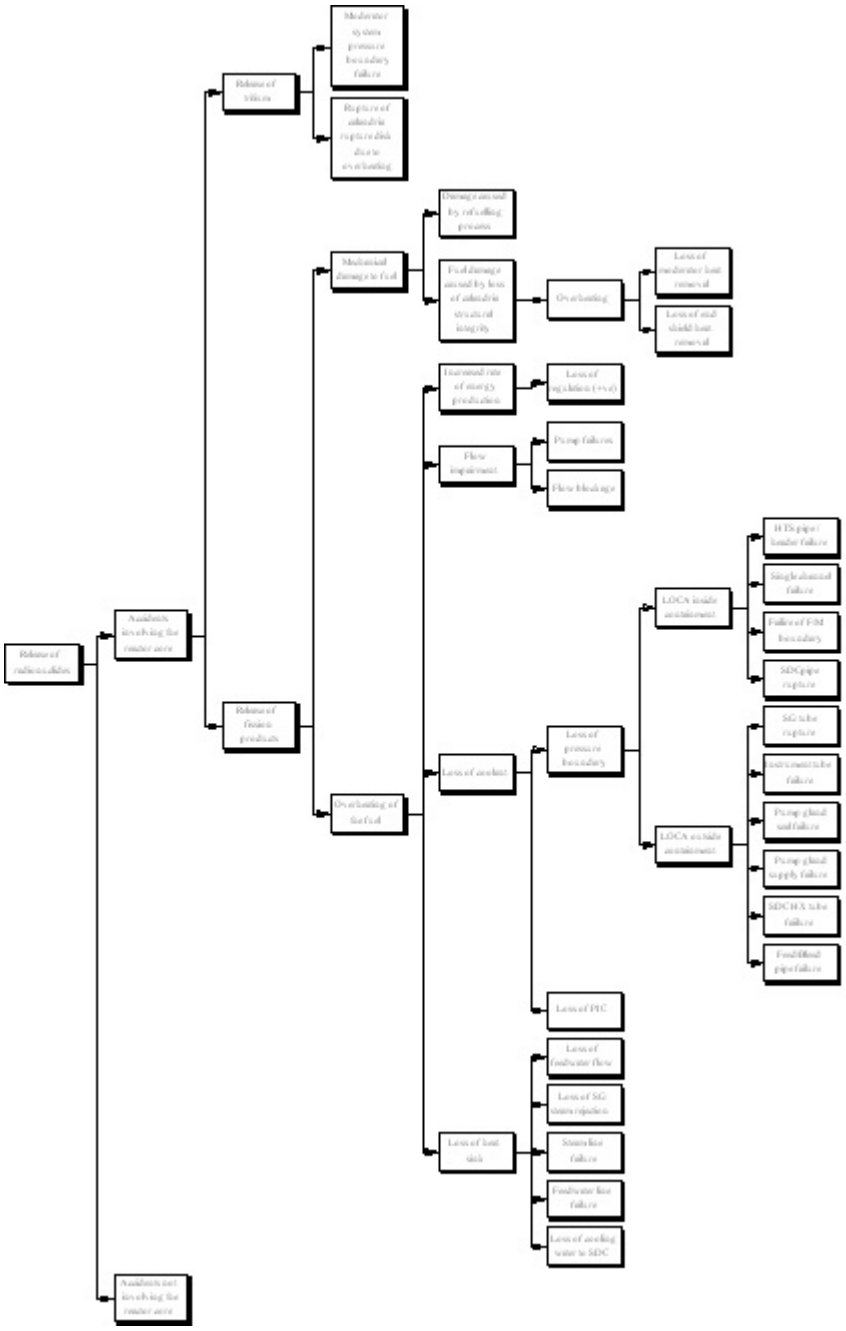


**Figure 2.2** "Top-Down" Accident Identification

**Nuclear reactor application**

The same approach is taken in trying to get a reasonable list of nuclear reactor accidents. In the "top down" approach, the top event could be taken as "unwanted movement of radioactive materials". Since most radioactive materials are either in the fuel, the coolant, the moderator, or the spent fuel bay, we can then ask how in each of these cases they could become mobile - i.e., airborne or waterborne[e]. Radioactive material could be released from the fuel by overheating or mechanical damage; from the coolant and moderator, by pipe breaks or overheating (released through relief valves); from the spent fuel bay, also by overheating. Fuel overheating in the core (power-cooling mismatch) can be caused by a loss of heat removal from the coolant (loss of heat sink), a loss of the coolant itself, coolant flow impairment, or a loss of reactor reactivity control causing the power to rise. And so on. Figure 2.2 illustrates the event generation sequence graphically. It should be noted that although the tritium branch is not developed therein, moderator tritium can pose a significant hazard to workers in the plant.

A combination of the top-down and the bottom-up methods will give a large number of accidents which, if the developer of the trees is knowledgeable about the design, cover most possible events.

We mentioned that Probabilistic Safety Analysis (PSA) is a rigorous tool for identifying accidents and assigning frequencies to them. PSA uses a bottom-up approach to generate failure frequencies of operating systems and failure probabilities of safety systems; it then combines failure of each operating system with successive failures of the required safety systems, to get a large list of accidents and their frequencies. One can then select Design Basis Accidents from this list using the criteria mentioned.

---

[e]One could also consider a loss of shielding accident, where the radioactive material stays in place but the shielding around it is lost or inadequate, exposing people near it to "shine" from gamma rays or neutrons. Inadvertent criticality could be one cause of loss of shielding even if the fuel is undamaged. Another could be loading radioactive material from a reactor into an unshielded flask designed for rehearsing such a task but not actually for doing it - this has happened at Ontario Hydro. For nuclear reactors, loss of shielding poses occupational risks but the public risk is determined by airborne or waterborne radioactivity.

Finally some Design Basis Accidents are added just because of history, even if they would be very low frequency. Canadian practice requires that each accident be analyzed assuming complete failure of one shutdown system, no matter how low the frequency. The reason goes back to 1952, when the core of the NRX research reactor in Chalk River, Ontario, was damaged in an accident. We shall discuss this accident later on, but one of the causes was a complex shutdown system design; the rods were hydraulically driven and were sensitive to dirt in the system. The accident resulted in an large subsequent emphasis on shutdown system reliability, testability and robustness, to the extent that, even though the shutdown systems in CANDU bear no resemblance to NRX (lessons having been learned about shutdown system design), the CANDU reactor had to be designed to survive an accident even if the shutdown system failed. Although one could show that the most severe accident without shutdown (large LOCA) would not release enough energy to break containment, the analysis was speculative and the designers decided (eventually) to add another, fully independent shutdown system.

By contrast, Light Water Reactor (LWR) Design Basis Accidents include the combination of a frequent event with unavailability of their shutdown system - so-called Anticipated Transient Without Scram[f] (ATWS). Such a sequence can be 'stopped' even without a shutdown system because of large inherent negative reactivity feedback, or by operator action if the accident is slow enough, or by use of another process system. Thus Light Water Reactors generally have one shutdown system, whereas CANDUs have two. However LWRs do not generally include rarer accidents with assumed loss of a shutdown system in the Design Basis - e.g., steam-line break plus failure to shutdown[g]. Conversely, the design basis for the containment system in LWRs was

---

[f]There is an apocryphal story of the derivation of the word "scram", which means shutting down the reactor quickly. The world's first reactor consisted of uranium and graphite in a "pile" in a squash court at the University of Chicago. A single control rod was suspended by a rope and a pulley over the core, the idea being that in case the power started to rise out of control, someone - doubtless a graduate student - would run and seize the axe that was fastened to the wall, and cut the rope. He was called the Safety Control Rod Axe Man (SCRAM), the world's first shutdown system.

[g]Some recent PWR designs have a second shutdown mechanism - addition of boron to the coolant - but it is slow and may be manually operated. Sizewell B, however, has a fairly powerful redundant shutdown mechanism (the Emergency Boration System), automatically triggered, consisting of four large tanks of boron solution, connected to the RCS upstream and downstream of the main RCS pumps .

(until recently) more stringent than for CANDU - regardless of the reactor design, a prescribed fraction of the core radioactive inventory is assumed to be released inside containment and the pressure is held at design pressure for 24 hours. For existing CANDUs, an accident-dependent calculation was permitted, the most severe of which served as the basis for containment design. This sort of physically-based calculation is still performed for new plants in Canada, but in addition a severe accident source term must be postulated as a test of containment.

A complete list of Design Basis Accidents includes external hazards - meaning earthquakes, fires, tornadoes, tsunami, floods, etc. The magnitude and frequency of the hazard are site-dependent. The unique aspect of these hazards is that they can affect more than one system at the same time.

Design Basis Accidents also include man-made hazards, both internal (operator error, sabotage) and external (explosions from nearby industrial or transportation facilities, and terrorism). The last has been given much prominence following the attacks on New York and Washington in September 2001 by terrorists in aeroplanes. Defining what should be the "design basis" for malevolent acts is the responsibility of the federal government..

## Evolution of Canadian Safety Philosophy - Early Beginnings

Having got a list of possible design basis accidents, we now have to decide what to do with them. Which are 'credible' and which are not? What limits apply to each one? What confidence must we have that the limits are met? These are not simple questions to answer, and the answers have evolved over any years. As an illustrative example, we trace the historical development of Canadian safety philosophy. Other countries have different approaches, shaped by their own history and the peculiarities of their dominant reactor design.

Canada's approach to accidents starts, as mentioned, with the accident to the NRX research reactor, in 1952[1,2]. This spurred an early interest in both the frequency of accidents, and the nature of protective systems, particularly their separation from the process systems which normally control the station.

These ideas (a review paper[3] summarizes them) were enunciated in 1959 by Ernest Siddall[4], then with the Reactor Research and Development Division at Chalk River Nuclear Laboratories (CRNL). He took as a safety goal that the risk from nuclear power should be five times lower than the risk from coal power, which was then the alternative in Ontario for future electricity

generation. He compared the two power sources on the basis of prompt fatalities, including the front-end fuel cycle for both. From this he derived a target for a remotely-sited nuclear power station of 0.2 deaths/year on average. This risk was felt at that time to come mainly from the catastrophic accident, as described in the U.S. WASH-740 report[h]. Assuming these results applied equally to a Canadian reactor, he produced a set of maximum event frequencies and safety system unavailabilities to be used as design targets, as follows:

| | |
|---|---|
| **LOSS OF COOLANT** | **One in 50 years** |
| **LOSS OF POWER CONTROL** | **One in 16 to one in 160 years, depending on severity** |
| **SHUTDOWN SYSTEM UNAVAILABILITY** | **One in 500 tries** |

In simple terms, a catastrophic accident such as postulated in WASH-740 could only occur if a process system failed (e.g., pipe break or loss of power control) *and* the shutdown system failed *and* the containment was absent or ineffective. One could estimate the frequency of the catastrophe by multiplying the initiating event frequency by safety system unavailabilities (e.g., initial failure frequency of 1 per 50 years times shutdown system unavailability of 1 in 500 tries, for a combined failure frequency of one in 25,000 reactor years). Now this is only possible if the systems are sufficiently independent, or in modern terminology, if there are no major cross-links between the initiating event and the mitigating system. This philosophy of separation (logically and physically) between process and safety systems has been one of the hallmarks of CANDU design from then until today. It was achieved by prudent design practice, and until the mid-1980s was hard to verify in a systematic manner. Fault-tree/event-sequence analysis in a PSA is now

---

[h]This was a study by the U.S. to look at the public health consequences of a massive un-contained reactor accident. Because of the extreme assumptions (energetic release of about half the reactor fission products to atmosphere, no containment) it predicted large numbers of casualties and has often been used as evidence of the 'danger' of nuclear power. However the assumptions were extreme - even the Chernobyl disaster had zero offsite prompt deaths - so the work was misleading. The analogy is the worst case backyard swimming pool disaster - there is enough water in the pool to drown hundreds of people - what saves us is the lack of a credible mechanism for delivery of the right amount of water to each person.

one of the tools used to verify that this required reliability is achieved.

A similar approach to Siddall was followed in a paper in 1961 by G. C. Laurence[5], who was then director of the Reactor Research and Development Division at CRNL, and who later became President of the Atomic Energy Control Board (AECB), the nuclear regulatory agency of Canada at the time. He took as a **safety goal** $10^{-2}$ deaths per year from nuclear power plant accidents, a factor of 10 lower than Siddall's, with the justification that this was far better than in other industries. With remotely-sited plants, which were then the only locations being considered, a disastrous accident would cause fewer than 1000 early deaths, so the frequency of such disasters must be held to less than one per 100,000 years. Such a disaster could occur if we had a simultaneous failure of **all** of the following: one of the normal process systems (such as the reactor power control system), plus one of the protective systems (emergency core cooling[i] or shutdown) plus containment. From this he derived the following design targets:

| | |
|---|---|
| **Process failures** | **One in 10 years** |
| **Protective System Unavailability** | **One in 100 demands** |
| **Containment System Unavailability** | **One in 100 demands** |

The frequency of process failures seems rather undemanding - for example no utility would tolerate a plant with a predicted large LOCA frequency of one every 10 years. The numbers should be looked at minimal requirements for public safety, not risk estimates. There is no point setting targets if they can't be shown to be met. Thus the numbers were chosen **large enough to be demonstrable individually by experience or testing in a few years of reactor operation**. Similarly if the target was *not* met, one would know early.

These ideas were applied in the design of Canada's first demonstration power reactor - the Nuclear Power Demonstration (NPD) Reactor. Its 1961 Hazards Report used higher

---

[i]The author (vgs) views ECC as a mitigating system rather than a protective system - unlike shutdown, it cannot stop an accident but can prevent it from progressing. However when summarizing history, we stick to the terms used by the pioneers.

unavailability for shutdown, and did not credit containment[j]. It also assessed the dose to the public from less severe accidents than disasters, using as a figure-of-merit a "once-in-a-lifetime" emergency dose. For Iodine-131, for example, this was 0.25 Sv (originally, 25 rad).

The Safety Report for the 200 MWe Douglas Point nuclear reactor, in 1962, was perhaps the fullest flowering of the overall risk-based approach. The safety goal, proposed by the designers, was that the risk of death to any member of the public be less than $10^{-6}$ per year, a factor of 10 less than that for NPD. The target risk for injury was taken to be 10 times larger, in the same ratio as experienced in other industries. The breakdown by frequency was similar to that for NPD, with some allowance for the lower frequency of large pipe breaks. Included in this risk evaluation was a quantification of the effects of a major accident on the operating staff. The Safety Report consisted of a systematic listing of all identifiable events, an evaluation of their frequency, and a calculation of their consequences in terms of dose. Again, separation was assumed to be achieved by careful design practice[k]. Note in addition the increasing requirement for nuclear not just to be safer than coal, but to be orders of magnitude safer. This was partly due to the fact that it was a new technology and the "increased safety" seemed achievable, and partly to cover uncertainties. However this did result in an erosion of the rationale for optimizing safety across industries.

## The Single/Dual Failure Approach

In 1967, F. C. Boyd of the AECB laid the ground rules for the deterministic licensing guidelines, under which all large operating CANDU plants up to but excluding Darlington have been licensed. They showed evidence of their risk-based origins, but collapsed the spectrum of possible accidents into two broad categories: **single failures**, or the failure of any one process system in the plant; and **dual failures**, a much less likely event defined as a single failure coupled with the unavailability of **either** the shutdown system**, or** containment, **or** the emergency

---

[j]The NPD containment was a "pressure-relief" containment - the initial blast of steam from a LOCA was released outside containment, then a door would be triggered to fall shut under gravity and close containment. This was felt to be practical because the low rating of fuel in NPD meant that any fuel failures would take some time to develop after the pipe break.

[k]Later use of PSA showed that the separation of control and shutdown systems was excellent, but some dependencies - notably on shared systems such as electrical power and process water - still existed.

core cooling system - the so-called *special safety systems*. (This single failure, by the way, is an assumed *system* failure, and is not related to the same term used originally for Light Water Reactors, and now internationally, to describe a random single active component failure additional to the initiating event). For each category, a frequency and consequence target was chosen that designers had to demonstrate were met. In addition, to deal with the siting of a reactor (Pickering A) next to a major population centre (Toronto), *population* dose limits were defined for each category of accident. For whole body doses, these were:

| | **INDIVIDUAL** | **POPULATION** |
|---|---|---|
| **Single Failure** | **0.005 Sv** | **$10^2$ Sv** |
| **Dual Failure** | **0.25 Sv** | **$l0^4$ Sv** |

with additional limits for thyroid dose. These limits were chosen as follows, based on the knowledge at the time:

- The single failure individual dose was consistent with international annual limits for normal operation.
- The dual failure individual dose was the threshold of observable cell damage at the microscopic level.
- The $10^2$ person-Sv would cause a negligible («l%) increase in the number of cancer deaths relative to those from other causes.
- The $10^4$ person-Sv would cause a number of leukaemia cases comparable to the normal incidence for one year.

The single/dual failure guidelines were finalized in 1972 by D. G. Hurst and F. C. Boyd of the AECB[6]. They were similar to Boyd's 1967 guidelines, with two key clarifications:

- The status of the containment system was changed. Failures of containment subsystems (such as failure to isolate ventilation dampers) would now be included as part of the full accident matrix, as opposed to containment being treated monolithically as available or unavailable.
- If the designer provided two capable independent shutdown systems, he would not be required to postulate a total loss of shutdown capability.

The guidelines were as follows:

**TABLE 2.1 - DOSE/FREQUENCY GUIDELINES**

| ACCIDENT | MAXIMUM FREQUENCY | INDIVIDUAL DOSE LIMIT | POPULATION DOSE LIMIT |
|---|---|---|---|
| Single Failure | 1 per 3 years | 0.005 Sv<br>0.03 Sv thyroid. | $10^2$ Sv<br>$10^2$ Sv thyroid |
| Dual Failure | 1 per 3000 years | 0.25 Sv<br>2.5 Sv thyroid | $10^4$ Sv<br>$10^4$ Sv thyroid |

The dual failure frequency was too small to be observed directly. The inference that the dual failure frequency was less than the rates above came from the observed single failure frequency after a few years of operation, and the safety system availability demonstrated through continual in-service testing of the safety systems. Multiplication of such numbers could be done only after one was reasonably sure that no significant cross-links remained between the initiating event and the safety system. Note the risk aversion implied above, with the frequency × consequence of dual failures being about an order of magnitude less than that for single failures.

Although the single-dual failure approach was a movement away from the early risk-based days, it still retained some risk roots (event classes and dose limits based on frequency). We can plot the upper bound of the implied risk in Figure 2.3.

**Probabilistic Safety Assessment**

As a safety design tool, the single/dual failure approach gave a basis for design of the four special safety systems (assuming there were two shutdown systems), but had several deficiencies:

1. It did not provide a way of treating multiple process failures, even if these could be more probable than single or dual failures, or could be induced by a single common cause. This is particularly true of failures of safety support systems, such as electric power, instrument air, etc. As well, there was no way of putting into

perspective any events which were well beyond the original design basis of the plant, but for which the regulatory body wanted to know the consequences (e.g. an accident occurring at power with the main airlock doors inadvertently left open).

2. In terms of assessing design changes, it did not factor in realistic frequencies, so that a small power excursion, a large loss-of-coolant, and multiple low-frequency failures were all treated on an equivalent footing.

   By the same token, because events were analyzed with conservative[l] assumptions on plant performance, safety analysis could give a misleading picture to the operator of the expected plant response to an accident.

3. Safety system failures, while explicitly identified and analyzed, were treated simplistically, particularly for safety systems, such as containment and emergency core cooling, which had redundant components and subsystems which were highly reliable.

4. There was no framework for looking at long term equipment reliability, once the initial phase of the accident was over.

For these reasons, a probabilistically-based design review was undertaken starting with the Bruce-A plant, and later extended to all subsequent CANDUs. We shall cover this methodology later.

---

[l]We will hear this term many times. “Conservative” means that the systems assumptions and/or models and/or input data are chosen so as to give a pessimistic answer (over-predict consequences). It is not an unalloyed ‘good thing’. Why?

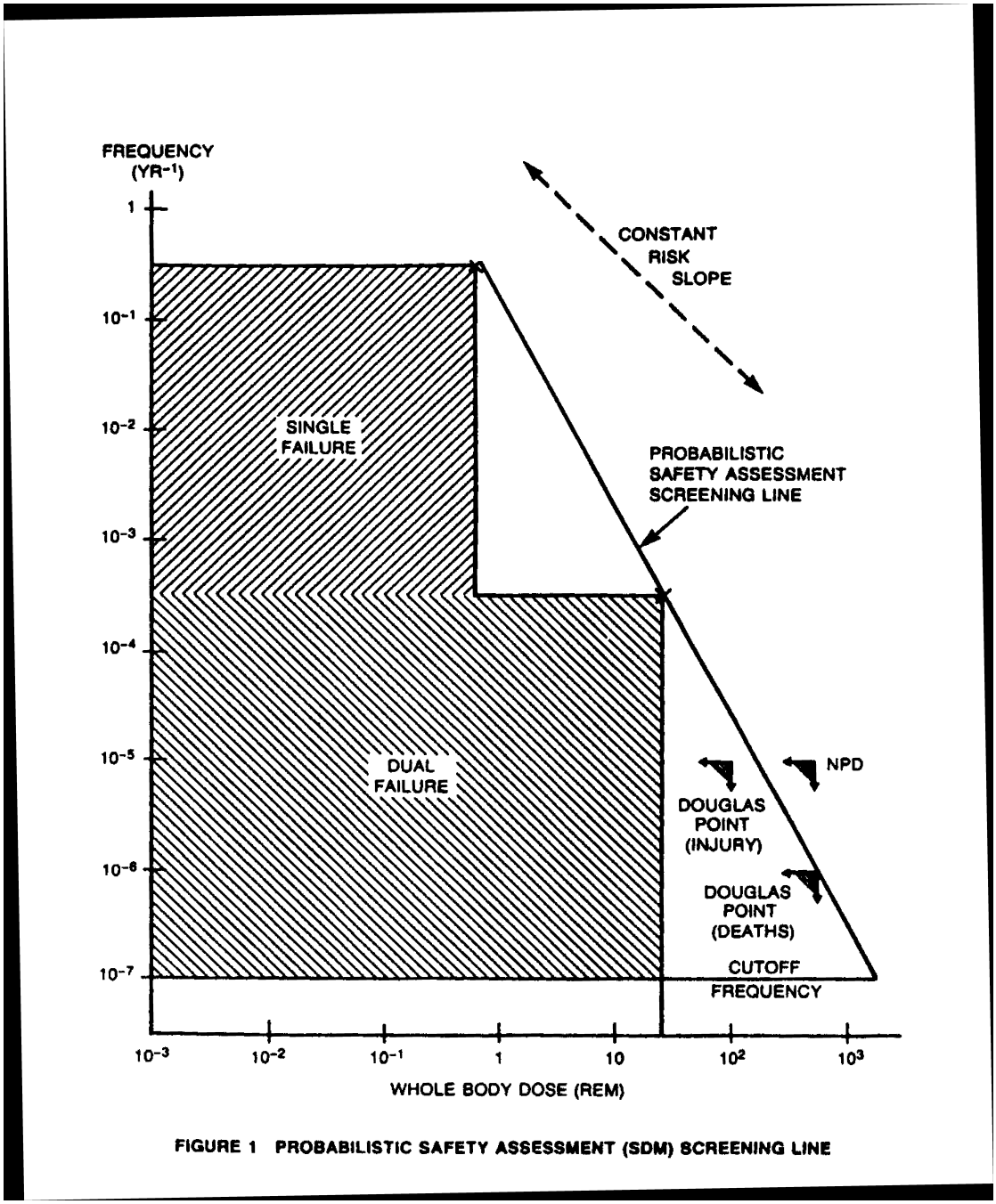



**Figure 2.3** Consequence Plot of Canadian Safety Criteria

## Consultative Document C-6

To address some of the deficiencies in the single-dual failure methodology, *but still in the design-basis accident approach*, the AECB[m] issued document C-6 in June 1980[7]. This retained the concept of several classes of events, five in this case, but with important differences:

1. Although the classes represented decreasing event frequency, assignment of events to the classes was done *a priori* by AECB staff, based on their belief as to the likelihood of the event. This was done with a conservative bias, so that an analysis done in the framework of C-6 could give a distorted picture of 'real' safety. Also by assigning events to a class, the document removed from the designer some of his incentive either to show that an event was indeed less frequent, or to make changes to decrease the frequency. Indeed, the list of events is highly design-specific, and might not be sensibly applied to future plants - a significant limitation as new generations of CANDU were being developed.

2. Because of the sensitivity to appearing to increase the maximum "permissible" dose, the AECB set the maximum dose for the most infrequent class at 0.25 Sv whole body: in other words, events *less* frequent than the traditional dual failure were not recognized in terms of increased allowable doses.

3. Since each event was required to meet a given dose, there was no need to sum to get a risk estimate. The limits were as follows:

[m] AECB underwent a name change to CNSC with the passage of the Nuclear Safety & Control Act. We shall use the names which were correct at the time of reference.

**DOSE/FREQUENCY LIMITS FROM AECB DOCUMENT C-6**

| | REFERENCE DOSE LIMIT, Sv | |
|---|---|---|
| **EVENT CLASS** | **WHOLE BODY** | **THYROID** |
| 1 | 0.0005 | 0.005 |
| 2 | 0.005 | 0.05 |
| 3 | 0.03 | 0.3 |
| 4 | 0.1 | 1 |
| 5 | 0.25 | 2.5 |

Examples of events in each class are:

Class 1: failure of reactivity or pressure control, failure of normal electrical power, loss of feedwater flow, loss of service water flow, loss of instrument air, and a number of other events that one might expect to occur occasionally.

Class 2: feeder pipe failure, pressure tube failure, channel flow blockage, pump seal failure, and other events that would not be expected to occur more than once (if that) in a plant lifetime.

Class 3: large LOCA, earthquakes and other events that are rare and could damage the fuel or portions of the plant.

Class 4: dual failures: Class 1 events + unavailability of a special safety system

Class 5: dual failures: Class 2 or 3 events + unavailability of a special safety system, e.g., LOCA plus ECC impairment

In short, C-6 can best be viewed as a deterministic approach, despite its growth from two to five classes. Recognizing that it is *not* a risk curve, we can plot it on the same scale as the single-dual failure criterion to see how they compare, in Figure 2.4. C-6 was revised[8] (C-6 Rev. 1) and issued for public comment. The framework is similar to C-6 Rev. 0, but an Appendix acknowledges that events can be reclassified based on strong probabilistic arguments. At this point C-6 will never be developed further.

## Recent Developments - RD-337

Darlington will be the last and only plant licensed in Canada according to C-6. For the last few years, AECL has been developing the Advanced CANDU Reactor, or ACR™; other vendors are likewise developing modern designs. As the nuclear industry has become more international and more competitive, the CNSC has understood the need to align its requirements, especially for new build, more closely with international ones - albeit the latter tend to reflect the predominant international experience, which is LWR. The CNSC have therefore been developed top-level design requirements, which replace C-6, and more closely reflect IAEA standards and are less technology-specific. For example there is more emphasis on severe accidents and less on rigid separation of safety and process systems. The CNSC officially issued its top-level design requirements[9], entitled "Design of New Nuclear Power Plants", in November 2008.

These new requirements merit a course in themselves. For this chapter, we shall focus on the dose limits. Events are now divided into three classes: Anticipated Operational Occurrences (AOOs), which are expected to occur at least once in the pant lifetime; Design Basis Accidents, which we have already discussed; and Beyond Design Basis Accidents (BDBAs), including event sequences that may lead to a severe accident. For the first two classes, dose limits are set for average members of the critical groups who are most at risk, at or beyond the site boundary - in short, individual dose limits. Population dose limits have been dropped. The limits are:

| Event | Dose Limit |
|---|---|
| Anticipated Operational Occurrence | 0.5 mSv |
| Design Basis Accident | 20 mSv |

There are no dose limits for BDBAs but there are numerical safety goals and system requirements - see Chapter 6.. RD-337 is *very* close to the top level IAEA design requirements report[10], on which it is based.

## Other Countries

We have not even scratched the surface of what other countries use. Almost all take a partly or

fully deterministic approach to safety analysis for the purpose of licensing. The influence of risk in the development of this deterministic approach varies widely. The approach in the U.S., until recently, was almost entirely deterministic - specifying in great detail not only how the safety analysis was to be done, but also how the design was to be done. At the other end of the spectrum, Argentina's approach to licensing (and originally that of the United Kingdom) was almost entirely risk-based. Recently most countries have moved towards the 'centre', combining both deterministic and probabilistic approaches. For example the U.S. has placed more emphasis on 'risk-informed' regulation, tempering its deterministic rules with probabilistic considerations (the term 'risk-informed' is used to distinguish the decision from being purely 'risk-based'). The U.K. on the other hand, had to develop more specific rules for the licensing of Sizewell B, and has published (and revised) a set of several hundred Safety Assessment Principles, to supplement its risk-based licensing[11].

## Other Designs

To make things more complex, the requirements and the design basis accidents cannot be developed in the abstract - they depend on the reactor design and its use. It is often argued that the allowable risk from a nuclear (or any) installation should be related to its benefit. So one might demand greater safety for, say, a small reactor producing a few tens of MW for district heating, than for a large one producing a GW of electricity. But what if the small reactor produces radioisotopes for medical diagnosis and treatment? What if a similar small reactor was located in uninhabited areas of northern Canada and used to provide power for military installations? What if it was on a military submarine? On a civilian icebreaker?

We will cover this topic of *safety goals* in Chapter 6.

Similarly for design basis accidents: rupture of any large coolant pipe is a good design basis for the emergency core cooling system, and almost all power reactors adopt it. But what about rupture of a pressure vessel? We stated that it would be very difficult (expensive) to design a containment to withstand such a rupture and the resulting missiles. So Light Water Reactor designers try to show that such a rupture is incredible ($<10^{-6}$ per year). The same is true for other pressure vessels within a CANDU containment building, such as the pressurizer or (in some cases) the steam generators. By the same token, many small reactors are pool reactors, with either no coolant piping, or very low pressure piping. Does it make sense to design for rupture of the pool? If not, what should the designer do to prevent it?

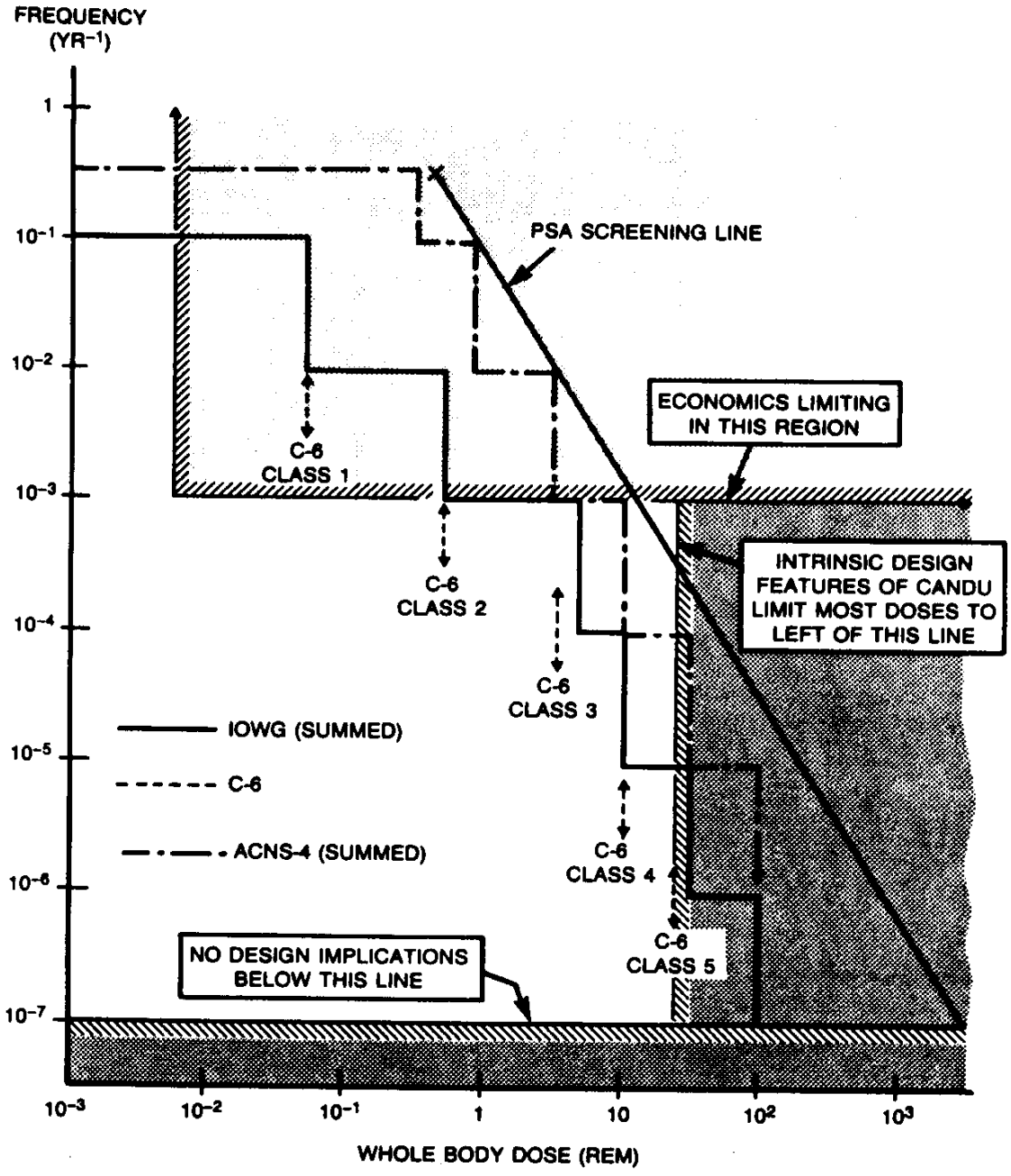



**FIGURE 2 COMPARISON OF SAFETY GOALS AND "NATURAL" RESTRICTIONS**

**Figure 2.4** - Consultative Document C-6 Limits

## Exercises

1. A laboratory experiment (this is in the 1940s) is set up to determine the critical mass of enriched uranium. Two hemispheres of $U^{235}$ metal are supported in an unshielded facility. A screwdriver is used to slowly push one hemisphere closer to the other, while a neutron

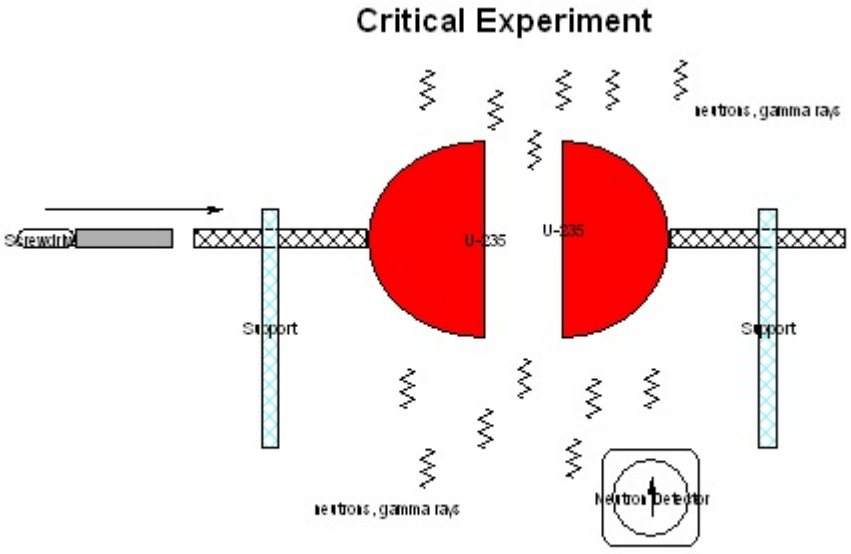



**Figure 2.5** Critical Experiment

detector measures the increase in neutron flux as they approach each other (Figure 2.5). Develop a safety approach using the concept of design basis accidents as follows:

a. Use both 'top down' and 'bottom up' approaches to define a set of accidents. Specifically: What is the "top event' that is to be avoided? What could cause the accidents?
b. How fast do they occur (i.e. what physical process determines the time-scale)? What inherently limits the consequences (why don't you get a nuclear bomb)?
c. Compare the nature of the hazard to the scientists with that to the public?
d. How could the consequence of an accident be prevented or mitigated:
    i. Without any further equipment - i.e., just after it has occurred?
    ii. With equipment installed beforehand?

2. Develop the arguments for and against having population dose limits. Hint: consider what aspects of design or siting they may influence.

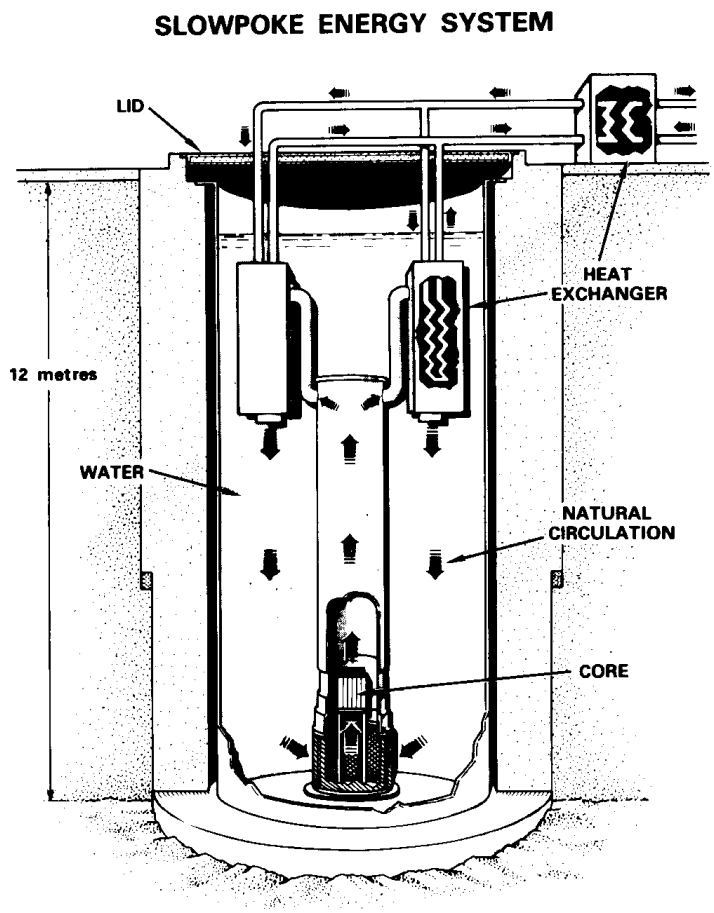
3. Calculate the "risk" in Sv/year to an individual at the site boundary from a (not very good) reactor designed and operated so it *exactly* meets the dose limits in:
   a. The two classes of accidents in the single/dual failure approach
   b. Event classes 1 to 5 inclusive from Consultative Document C-6
   c. The AOO and DBA limits from RD-337.

   What conclusions can you draw (if you think the comparison is not meaningful, explain). What contribution do the more severe accidents have to the risk?

4. Consider a small reactor for urban district heating as shown in Figure 2.6. It is intended to be located in urban areas in buildings such as hospitals or universities. Salient safety-related characteristics are:

   a. pool reactor, natural circulation, atmospheric pressure
   b. double-walled pool (350,000 litres) with a purification system (small pump and ion exchange resins, outside the pool)
   c. 10 MW(th) output
   d. forced-flow secondary side, heat exchanger immersed in the pool
   e. tertiary heat exchanger connected to heating grid (why?)
   f. negative reactivity feedback from fuel temperature, coolant temperature, coolant void (e.g., an increase in coolant temperature decreases the reactivity)
   g. active reactor control devices (rods) with limits on rate (a few mk/hour, compared to say, CANDU, which can go up to several mk/minute) and worth (no rod in excess of a couple of mk).
   h. low fuel temperatures, such that there are no free fission products in the fuel
   i. two shutdown systems - one active (drops the control rods) and one passive (rods within the core which are thermally activated: the absorber material inside the rods, normally above the core, melts and fall into the core on high temperature)
   j. a confinement boundary (not shown in the figure) covering the pool top, but the building is conventional
   k. no Emergency Core Cooling System (why?)
   l. a licensed operator is *not* required to be in the control room. Any upset sounds an alarm which notifies a local attendant (who can shut the reactor down, but not restart it). Licensed operators can remotely monitor the reactor but not control it.

Develop a set of design basis accidents for this reactor. It is important that you show *how* you did this, not whether you get the same answer as AECL did (there is not really enough information given in the exercise to get the "right" answer - it's your thinking process that counts). If you are getting design basis accidents which seem inconsistent with an urban location, how could they be made impossible?




Schematic Diagram of the SLOWPOKE Energy System

**Figure 2.6**

5. Consider a low-energy research reactor used to determine fundamental physics parameters. It consists of a vertical cylindrical heavy water tank in which are suspended fuel assemblies (Figures 2.7 and 2.8). Salient safety-related characteristics are (I have simplified a bit):

- pool reactor, natural circulation, atmospheric pressure
- nominal zero energy (a few watts), no engineered heat removal systems
- low fuel temperatures, very little fission products in the fuel
- fuel rods suspended from hangars, can be arranged manually to different lattice pitches and geometries. Fuel rods are stored beside the pool.
- capability to use fuel with a large range of enrichment (but not highly irradiated fuel)
- provision for insertion of a few channels consisting of fuel inside a pressure tube containing electrically-heated coolant at high pressure and high temperature, inside a calandria tube (but still nominally ~zero nuclear power)
- control via moderator level (pump-up and drain), pump-up speed limited by pump capacity
- manual start-up and shutdown
- three redundant dump valves open to trigger a heavy-water dump on high neutron power or high log-rate
- no emergency core cooling system, no containment. A cover provides shielding of operators when the reactor is critical.

a) Develop a set of design basis accidents for this reactor. It is important that you show *how* you did this, not whether you get the same answer as AECL did (there is not really enough information given in the exercise to get the "right" answer - it's your thinking process that counts). Start from a large list developed using *at least two* of the techniques discussed in this Chapter and then suggest which accidents you would consider too rare to design against, and why. Provide details - e.g., it is not enough to say "increase in power" - list all the ways this could occur.

b) If you wanted to reduce the risk from this reactor (based on your list of design basis accidents and a judgement about probability), what design changes would you do first?

c) What elements of defence in depth are present in this design? What are missing?

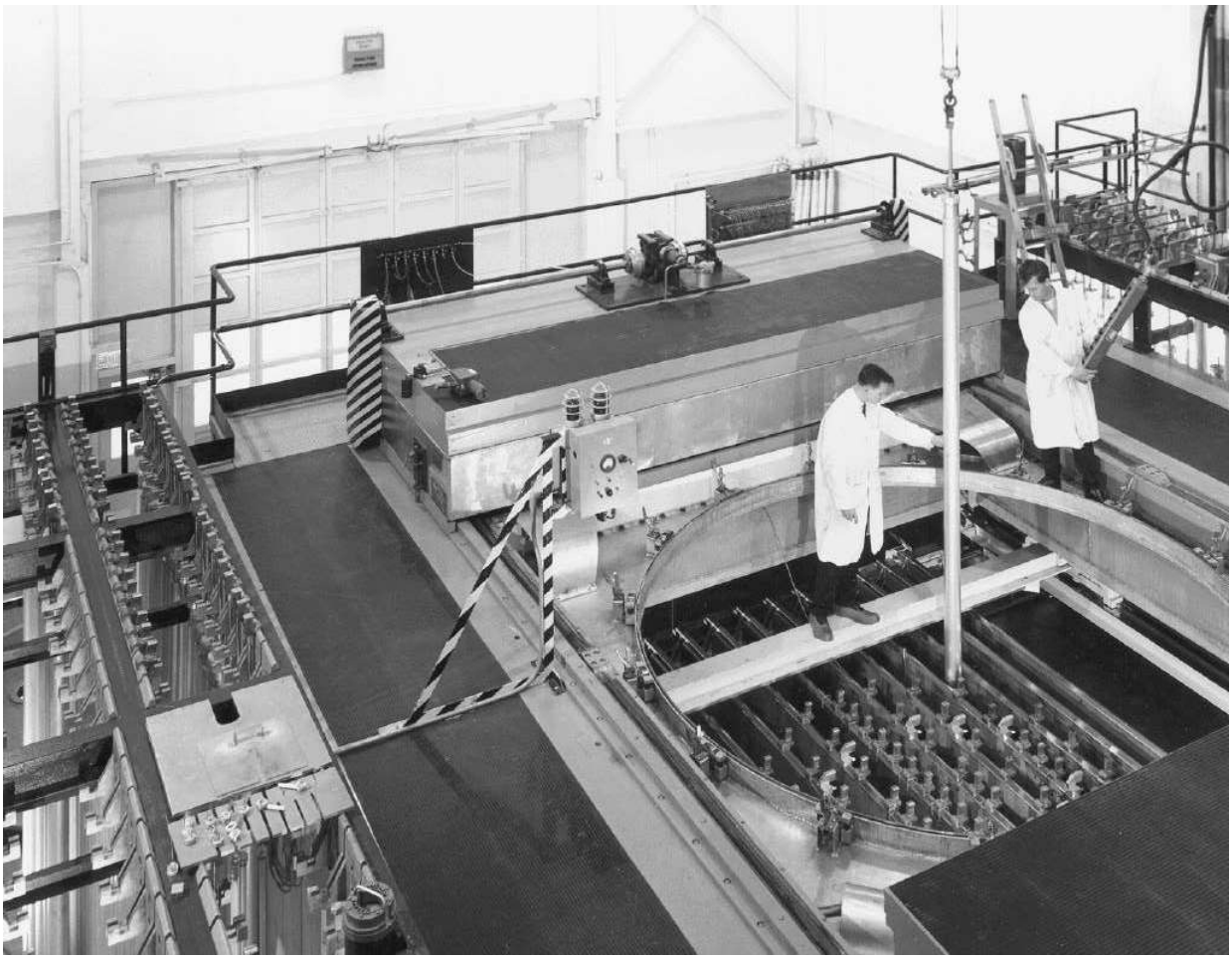


**Figure 2.7** ZED-2 Top View

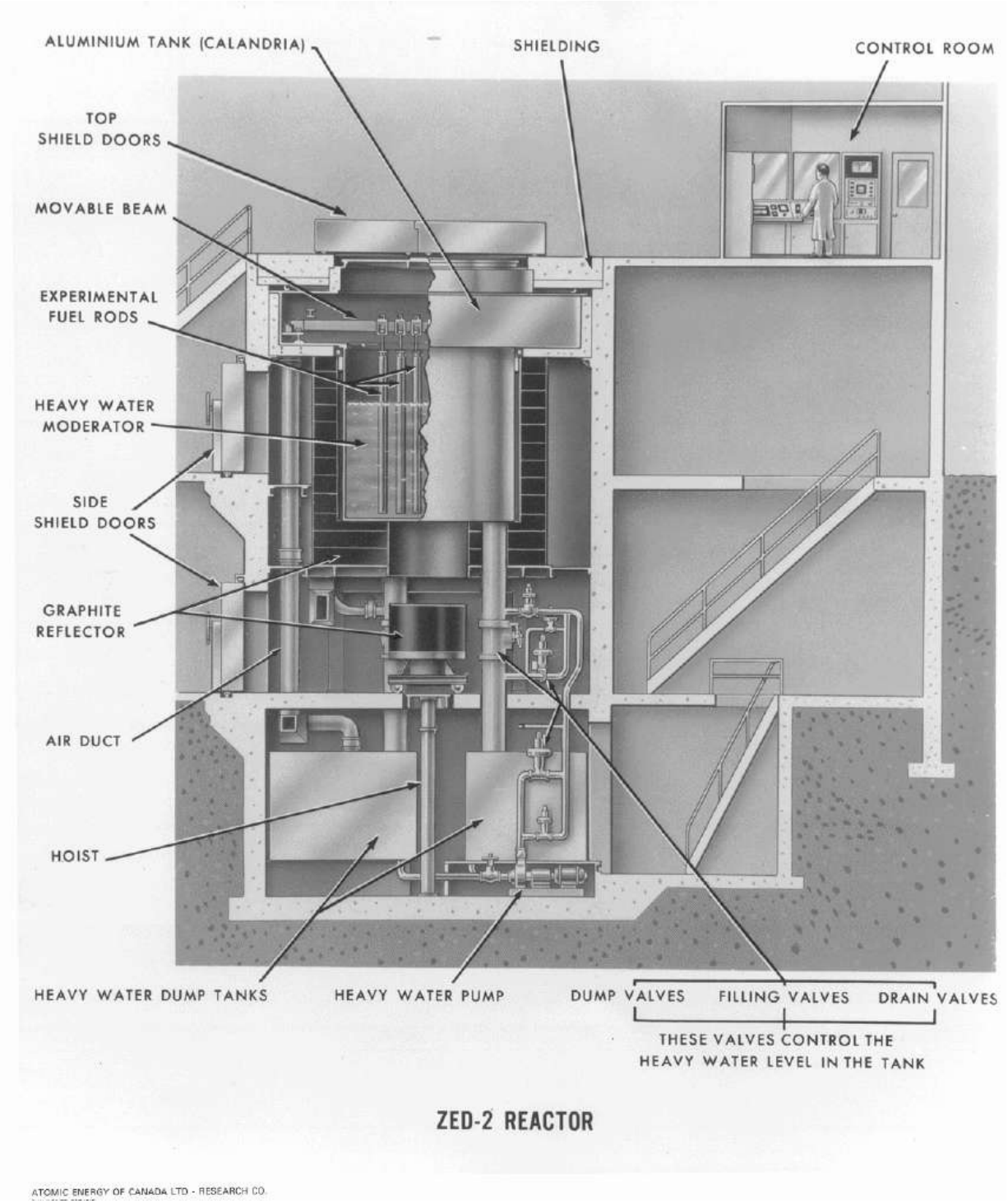

ALUMINIUM TANK (CALANDRIA)
SHIELDING
CONTROL ROOM
TOP SHIELD DOORS
MOVABLE BEAM
EXPERIMENTAL FUEL RODS
HEAVY WATER MODERATOR
SIDE SHIELD DOORS
GRAPHITE REFLECTOR
AIR DUCT
HOIST
HEAVY WATER DUMP TANKS
HEAVY WATER PUMP
DUMP VALVES
FILLING VALVES
DRAIN VALVES
THESE VALVES CONTROL THE HEAVY WATER LEVEL IN THE TANK
ZED-2 REACTOR
ATOMIC ENERGY OF CANADA LTD - RESEARCH CO.

**Figure 2.8**

## References


1. W. B. Lewis, “The Accident to the NRX Reactor on December 12, 1952", Atomic Energy of Canada Limited, Report AECL-232, July 1953.

2. D. G. Hurst, “The Accident to the NRX Reactor, Part II”, Atomic Energy of Canada Limited, Report AECL-233, October 1953.

3. V.G. Snell, “Evolution of CANDU Safety Philosophy”, Proceedings of the Canadian Nuclear Society Symposium on CANDU Reactor Safety Design; November, 1978.

4. E. Siddall, “Statistical Analysis of Reactor Safety Standards”, Nucleonics, Vol. 7, pp 64-69.

5. G. C. Laurence, “Required Safety in Nuclear Reactors”, Atomic Energy of Canada Limited, Report AECL-1923, 1961.

6. 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, 1972.

7. “Requirements for the Safety Analysis of CANDU Nuclear Power Plants”, Consultative Document C-6, Atomic Energy Control Board Proposed Regulatory Guide, June 1980.

8. “Safety Analysis of CANDU Nuclear Power Plants”, Draft Regulatory Guide C-006 (Rev. 1), Canadian Nuclear Safety Commission, September 1999.

9. “Design of New Nuclear Power Plants”, CNSC report RD-337, November 2008

10. “Safety of Nuclear Power Plants: Design”, International Atomic Energy Agency report NS-R-1, 2000.

11. “Safety Assessment Principles for Nuclear Facilities”, U.K. Health and Safety Executive, 2006.