HOW SAFE IS SAFE ENOUGH? THE CANADIAN ANSWER

by Fred Boyd

Consultant (former AECB)
9 Sandwell Crescent, Kanata, Ontario, K2K 1V2 Canada
e-mail: fboyd@sympatico.ca

Abstract

Since the beginning of the nuclear power program safety has been a major concern. The basic question has been "How safe is safe enough?"

An accident to the NRX reactor in 1952 prompted much introspection about safety, especially for the power reactors then being considered. As a result, Canada approached the question from a fundamental basis. This contrasted with the arbitrary rules applied by most of the other countries involved in the beginning of the nuclear power program in the 1950s and 1960s.

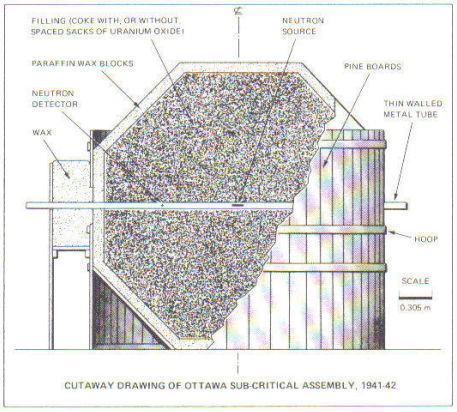
This paper reviews the safety concepts that evolved in Canada based on that fundamental approach and the resulting design and operational requirements that ensued. Some comparisons are made with current proposed" international standards".

1. Background

Even the earliest researchers of nuclear fission were aware of the potential hazards. Consequently, safety has been a prime concern from the beginning of the nuclear program. Therefore, to provide an appropriate context for the evolution of safety concepts it is necessary to review the early evolution of nuclear science internationally as well as in Canada. (If you know your nuclear history you can skip the next sections.)

Fissioning of uranium was only identified in late1938, less than a year before the outbreak of the Second World War. By late 1939, with the war already begun, scientists were aware of the possibility of a nuclear weapon. Many European nuclear scientists managed to escape to the United Kingdom with some bringing the limited amount of heavy water that had been produced in Norway.

There was a Canadian connection. George Laurence, then head of radiation physics at the National Research Council, was aware of the work on uranium fission. In 1941 – 1942, with the assistance of Bernard Sargent, he built a sub-critical assembly of coke and uranium. The impurity of the materials precluded criticality but much information was obtained about neutron multiplication and diffusion. With additional help and purer materials they might have built the first reactor, a year before Enrico Fermi and team did so in Chicago in December 1942.



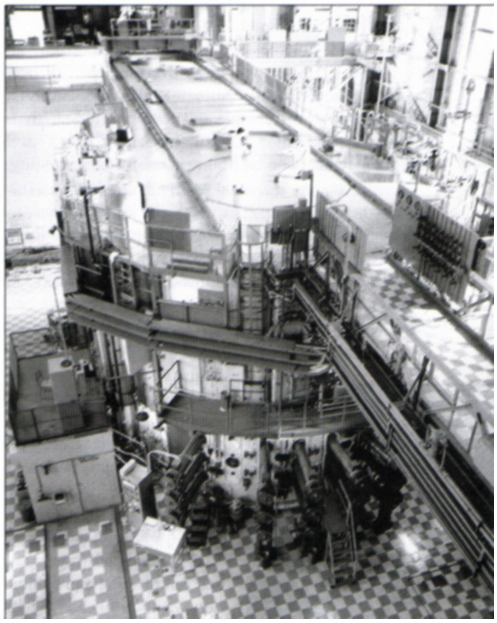
CUTAWAY DRAWING OF OTTAWA SUB-CRITICAL ASSEMBLY, 1941-42

Following Fermi's achievement, the USA began a huge program (later called the Manhattan Project) with the objective of creating a nuclear explosive, which, as is well known, resulted in the attacks on Hiroshima and Nagasaki in August 1945.

With the UK being under attack it was difficult to pursue nuclear research there. A joint British-Canadian laboratory was proposed to be established in Canada, with, initially, the blessing of the USA. Laurence's work was one factor in the decision. The objective was research leading to the construction of a heavy-water moderated reactor for the production of plutonium. The Montreal Laboratory was set up at the end of 1942 and in early 1943 moved into a new building of the University of Montreal.

2. The Canadian beginnings

Canada's nuclear program can be considered as beginning with the Montreal Laboratory, making Canada the first country outside the USA to have an organized nuclear program.



NRX

Starting from first principles, the team at the Montreal Laboratory developed the theories and applied them to create the basic design of a large heavy-water moderated research reactor that became known as NRX. At the same time a site was sought for the location of the reactor and the associated laboratories. Safety and security were major factors but it also had to be accessible for the delivery of heavy equipment. In 1944, on the recommendation of Laurence (who had become the senior Canadian at the Montreal Laboratory), the Chalk River site was chosen and the construction of the Chalk River Nuclear Laboratory was begun.

Indicative of the concern for safety a senior scientist described NRX as having 900 devices to shut it down and only one way to start it. Also, radiation scientists at the Montreal Laboratory established dose limits that preceded international ones.

While NRX was being built it was decided to build a simple, zero energy, pool reactor to check calculations. It was called ZEEP, and when it started in September 1945 it was the first reactor outside the United States.

NRX achieved criticality in July 1947 and reached its original rated power of 20 MW(th) later that year. Five years later, during a test on December 12, 1952, the reactor suffered a power excursion causing significant damage to the fuel. It was rebuilt in just fourteen months, and, in early 1954, the reactor was started again, this time achieving 40MW(th). For many years it was the most powerful research reactor in the world and Chalk River attracted many international as well as Canadian scientists. Indicative of the quality of the research Bertram Brockhouse won the Nobel Prize for his work on neutron diffraction at Chalk River in the 1950s and 1960s.

3. Early organizational structures

Two years after the creation of the Chalk River Nuclear Laboratory, the federal government, in 1946, passed the very succinct Atomic Energy Control Act (AEC Act), one of the first nuclear legislation in the world. That Act stated that the Canadian program would be for peaceful purposes only, making Canada the first nation to make such a declaration, and created the Atomic Energy Control Board. Initially the AECB had total responsibility for control of all "atomic energy" activities, including CRNL, which it delegated to NRC. Since it was assumed that all atomic energy activities would be by the federal government the AECB was primarily a "figurehead" organization with just one scientific staff member.

In 1952 the government decided to create a crown corporation, Atomic Energy of Canada Limited, to take over the operation of CRNL and the AEC Act was modified to make the AECB primarily a regulatory organization. The regulatory powers of the AECB stemmed primarily from one paragraph in the Act that stated that no [defined atomic energy] activity could be undertaken without permission of the AECB. It was still assumed that all nuclear activities would be by the federal government.

In the mid 1950s McMaster University decided to build a research reactor and an agreement was reached between AECL, Ontario Hydro (the comprehensive electrical utility in the province) and Canadian General Electric company to design and build a 20 MWe "demonstration" nuclear power plant, called the Nuclear Power Demonstration (NPD).

To assist in regulating these projects the five-members of the Board of the AECB established a Reactor Safety Advisory Committee (RSAC) with George Laurence as chairman and members drawn primarily from CRNL and federal government departments. Following a practice that had developed in the USA the proponents of the McMaster Research Reactor and NPD were required to submit "Hazards Reports" describing the safety features of their facilities and the consequences of potential failures. Meetings ensued between the RSAC and proponents of the two reactor projects.

The Canadian nuclear power program grew rapidly. In the 1960s the electricity demand in Ontario was growing and the integrated provincial utility, Ontario Hydro, chose to go nuclear. Before NPD started in 1962 the 200 MWe prototype, Douglas Point was committed. Then, before it started in 1966 the first two units at Pickering were committed. That pattern continued with Bruce A, Pickering B and Bruce B during the 1970s. In addition, single units were committed in Quebec and New Brunswick in the early 1970s

With a small support staff the RSAC reviewed all of these projects focussing on the essential safety features. Construction was typically begun before the design was completed. (This caused problems later because the utility did not, as promised, assemble the "as built" plans and the regulator never required them to do it. Consequently when it became time to do upgrading or changes the documentation was not available.)

Plant	Begin build	Start-up
NPD	1958	1962
Douglas Point	1960	1966
Pickering A	1966	1971
Gentilly 1	1966	1970
Bruce A	1970	1976
Pickering B	1974	1982
Gentilly 2	1974	1982
Point Lepreau	1975	1982
Bruce B	1978	1984
Darlington	1981	1989

The pattern was that proponents would submit information on the design and safety analyses. The RSAC and its support staff would review the material and then hold meetings with the proponents. These meetings often became animated despite the professional attitude of both sides.

4. Beginning of Canadian safety approach

The 1952 NRX accident was the subject of considerable inspection and review that led to many improvements in the reactor's control and shutdown systems. It also triggered many at the Chalk River Laboratory to think about the safety of nuclear power reactors that were beginning to be considered.

In a seminal paper in 1954, Ernest Siddall examined the fatal causalities from accidents in a number of different large industrial activities on the premise that society accepted that level of safety. Based on the economic benefit of a postulated "large" nuclear power plant compared to other industrial activities and, arbitrarily applying a factor of 10 relative safety he came up with a figure of 1 death per hundred years as a criterion for a large (200 MWe) nuclear power plant.

George Laurence, then the director of the division at Chalk River responsible for the design of the larger NRU research reactor and subsequently of the conceptual design for a nuclear power reactor, accepted Siddall's target, and set out to determine how to achieve it. Over the next decade and a half he devoted much of his efforts to the question of reactor safety and wrote a number of papers.

In 1955, a report from the United States Atomic Energy Commission, WASH 740, called the "Brookhaven Report", estimated that the consequences of a release of 25 per cent of the volatile fission products from a "large" (200 MWe) reactor could be thousands of deaths. This caused much reaction including the requirement for a "hazards" report for any proposed large reactor. (These have now evolved into the massive "safety reports" required throughout the world for any major nuclear project.)

Although WASH 740 was simplistic in its assumptions it did draw attention to the source of the greatest potential hazard of a nuclear reactor – the immense amount of radioactive elements

created within the uranium fuel from the fission process. It emphasized that the primary hazard of a nuclear reactor was the potential release of significant quantities of these fission products.

Using the assumption of WASH 740 that a major release of fission products from a large reactor could kill 1,000 persons and accepting Siddall's target of 1 death per 100 years, Laurence proposed a target of one severe accident (resulting in a major release of fission products) of 1 in 100,000 years or a probability of 10^{-5} per reactor-year. The challenge was how to achieve this

Given that focus, those concerned began to look at the mechanisms that could lead to the fission products being released from the fuel. This quickly focussed on the over-heating, or even, melting, of the fuel. For this to occur, the fission energy in the fuel would have to exceed the capacity of the cooling medium. This led to two scenarios – which are still the focus of reactor safety studies today – loss of cooling (or of the coolant), and excess fission energy in the fuel (loss of control). All reactor safety analyses begin with these two scenarios.

A couple of years later, in 1957, an accident in one of the reactors at the Windscale site in England put a major focus on radioiodine, a major fission product which is volatile.

The Windscale reactor was a large graphite moderated, air-cooled, assembly, designed to produce plutonium. It so happens that, when irradiated with neutrons, graphite absorbs energy (called the Wigner effect), which can cause it to heat up. When this was recognized a procedure was developed to "anneal" the graphite. On the occasion of the accident an annealing process was under way but because of inadequate temperature monitors it was believed that the annealing was not taking place. The reactor was increased in temperature and radiation alarms on the stack sounded. It was discovered that parts of the reactor had actually been heated too much and the graphite caught on fire.

The result was extensive damage to the fuel and the release of large quantities of radioiodine that contaminated much of the surrounding farmland. For several years thereafter, not just in England, radioiodine became a major focus of reactor safety studies.

Back in Canada, Laurence was examining ways to provide assurance, at the level of his target (10^{-5} per year), that the fuel would not become over heated. This was long before modern computers with their ability to do probabilistic evaluations of complex designs.

He concluded that the operating systems of a reactor could be designed, built and operated to provide assurance that the probability of a significant failure (one that could potentially threaten the integrity of the fuel) could be kept low.

Safety systems were needed to ensure cooling of the fuel and control of the nuclear reaction. In addition a confinement system was desired to prevent radioactive material that might be released from the systems from being released to the environment.

Laurence concluded that if the safety systems designed to maintain cooling of the fuel and to shut down the reactor were completely separate from the operating systems and from each other his desired target could be achieved with practical designs.

The assumed frequency of a serious accident of the operating systems (one that could lead to fuel failure) was initially chosen as 1 per 10 years then later as 1 per 3 years. By designing the safety systems to be tested while the plant was operating it was finally assumed that their unavailability could be $10^{-3.}$ Further, the safety systems had to be designed that the failure of two would have to occur along with a serious failure of the operating system for a major release of fission products to occur. Assuming sufficient separation and variation of design (to avoid common mode failure) this could provide a likelihood of $1/3 \text{ X } 10^{-3} \text{ X } 10^{-3} = 3 \text{ X } 10^{-6}$.

To provide criteria for the effectiveness of the safety systems, design dose limits for an individual at the boundary of the exclusion zone were stipulated for "single" failures (operating system) and "dual" failures (failure of the operating system combined with failure of any safety system)

All of this developed within the circle of the RSAC and the proponents. The first public presentation was in a paper by D. G. Hurst and F. C. Boyd in 1972. The following table provided a summary.

OPERATING DOSE LIMITS AND REFERENCE DOSE LIMITS FOR ACCIDENT CONDITIONS

Situation	Assumed Maximum Frequency	Meteorology to be Used in Calculation	Maximum Individual Dose Limits	Maximum Total Population Dose Limits
Normal Operation		Weighted according to effect, i.e. frequency times dose for unit release	0.5 rem/yr whole body	10^4 man- rem/yr 10^4 thyroid
Serious Process Equipment Failure	1 per 3 years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete	3 rem/yr to thyroid[3]	rem/yr
Process Equipment Failure plus Failure of any Safety System	IperSxlO[3] years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete	25 rem whole body 250 rem thyroid[b]	10^6 man-rem 10^6 thyroid-rem

[1] For'other organs use 1/10 ICRP occupational values

' For other organs use 5 times ICRP annual occupational dose (tentative)

Other jurisdictions, principally the USA, the regulatory approach was to develop a massive set of deterministic requirements similar to the many engineering codes. Although there was a number of individuals and groups that favoured a "probabilistic" approach similar to that of Canada the diverse nature of their nuclear industry precluded that route. It has been stated that no two of the

100 or more nuclear power plants built in the USA in the 1960s and 1970s had the same combination of reactor designer, balance of plant designer and owner.

A further development evolved when the Bruce A design was proposed. Because there was uncertainty about the ability of the smaller containment to withstand a "runaway" accident it was eventually decided to require two shutdown systems. These were each to be considered a separate safety system. To achieve the independence assumed in the approach these had to be equal in effectiveness, different in mechanism and physically separate.

About the same time as this problem was being addressed there was considerable debate in the USA about ATWS (Anticipated Transient Without Scram) because of similar concerns. The designers of the LWR reactors being built in the USA argued against a similar requirement because they did not know how to incorporate a second shutdown system. That situation continues until today, with the designers contending that PSA evaluations of their combined operating and shutdown systems show that they are adequate.

5. Summary

Long before PSA evaluations became feasible Canada adopted a "probabilistic" target for the safety of nuclear power plants. The target figure adopted in Canada over four decades ago for a significant release is now essentially the same as current proposed "international" standards.

The Canadian approach achieves this target through separated systems that can be shown to have the requisite (practical) reliability. In contrast, the international "standards" depend on interconnected systems whose reliability can only be determined through probabilistic evaluations.

6. Postscript

In its recent draft regulatory document RD-337, the Canadian Nuclear Safety Commission has continued the requirement for two independent, equal and different shutdown systems. Areva and the Canadian nuclear utilities, together with Westinghouse, are protesting this, primarily on the basis that it is not required in recent IAEA documents, not on any technical facts. The CNSC document does allow an applicant to argue against any particular requirement if they can show an equivalent result. It would appear that the PWR proponents doubt they can do so.

7. References

1. ------- "Theoretical Consequences of an Accident in a Nuclear Power Reactor" Brookhaven Laboratory for USAEC WASH 740 (1957)

2. E. SIDDALL "Statistical Analysis of Reactor Safety Standards" "Nucleonics 17, No. 2 (1959)

3. G.C.LAURENCE "Required Safety in Nuclear Reactors" AECL - 1923 (1961)

4. F. R. FARMER "Reactor Risks IAEA symposium (1967)

5. D. G. HURST & F. C. BOYD "Reactor Licensing and Safety Requirements" AECB - 1059 (1972)

ANNEX: PUBLIC PERCEPTION

It must be acknowledged that “safety” is a subjective concept and no amount of mathematical arguments will convince most people of the safety of any particular activity.

Nuclear energy still evokes visions of Hiroshima and Nagasaki from 60 years ago and more recent memories of the Chernobyl accident of 1986.

There is still widespread phobia about radiation. Even though people readily have X-ray examinations and accept radiation treatment for cancer they, or at lest the media, become excited about miniscule releases of radioactive material.

The "problem" of the management or disposal of nuclear fuel waste still looms large. Here the nuclear community is partially to blame. By spending hundreds of millions of dollars on "research" associated with waste disposal the industry is, essentially, admitting that it is a very difficult problem.

The basic fact is that the public does not accept the nuclear industry's claim of the very low risk associated with nuclear power plants.

The nuclear industry must acknowledge that mathematical talk will not convince the public nor, in fact, even be understood. Therefore means must be found to express our confidence of the safety of nuclear power plants that the public can understand and, hopefully, accept.

The nuclear industry has, itself, caused the public to be concenrned.

- We should discard the unsubstantiated linear-dose-effect concept of radiation protection. This theory has been grossly misused, especially in the widely publicized exaggerated predictions of millions of deaths from Chernobyl. It continues to fuel the media's obsession with minor releases of radioactive material.
- A more rational approach is needed for the management of spent nuclear fuel. There is no justification for spending billions of dollars to develop burial grounds good for tens of thousands of years. It is unlikely that civilization as we know it will exist that far into the future. The fact that some of the radioactive components of spent fuel have long half-lives should be put in context with toxic materials such as mercury and arsenic which have infinite half-lives and are disposed into dumps with little or no control.

Then we must demonstrate that we can operate plants safely and that we have personal confidence in them.

- Operating plants must be run extremely well. The longer plants operate without any incident and continue to supply reliable and economic electricity the more the public will learn to accept them. Any significant failure in any nuclear power plant will set back this acceptance for many years.
- An excellent method of demonstrating confidence, which is actually happening in may areas, is to have employees of nuclear plants live close near-by.

The public may never love nuclear power but it is possible that it will accept it.

* * *