To: The Commissioners of the CNSC
From: Gordon Edwards, Ph.D.
Date: December 9 2012

Re: The Unavailability of CANDU safety systems

I am writing to fulfill an obligation that I undertook during my testimony before the Commission on December 6, 2012. I promised to supply the Commissioners with data regarding the historical unavailability of the safety systems of CANDU reactors, including the fast shutdown systems.

In my testimony I mentioned that the two independent fast shutdown systems that are a feature of all operating CANDU reactors have not always been available even during operation.

I was surprised when Mr. Jammal contradicted my assertion. If I recall correctly, he declared that the fast shutdown systems are always available.

I believe this statement by Mr. Jammal to be untrue. Moreover I find it disturbing that Mr. Jammal would misinform the Commissioners on such an important topic, especially when this becomes enshrined as a matter of record in the transcript of the hearing.

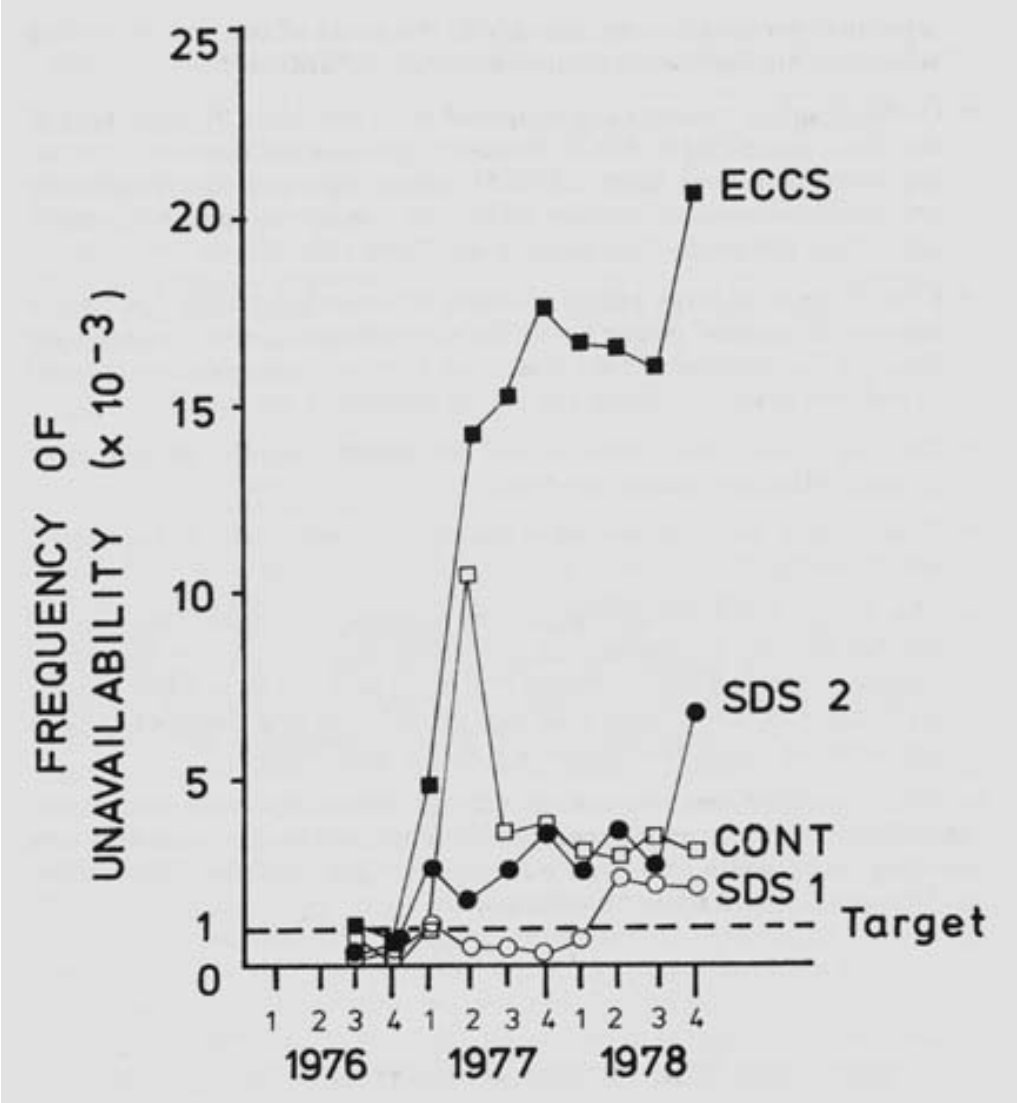
The chart reproduced below was filed as Exhibit E-71 by the Atomic Energy Control Board (AECB) on August 2 1979 during the 1979-80 Hearings on Reactor Safety – hearings conducted over a period of 15 weeks by the Select Committee on Ontario Hydro Affairs. The chart deals with the recorded unavailability of the four principal safety systems at Bruce NGS "A" during the three year period from 1976-78 inclusive.

Those safety systems are the Emergency Core Cooling System (ECCS), the two fast shutdown systems (SDS1 and SDS2), and the Containment System (CONT).

As Mr. Jammal confirmed during the December 9 hearings, the target unavailability of each of these four safety systems, as prescribed by the regulator, is 10^{-3} or 1 in 1000. In practical terms, this means that each year, each safety system is assumed to be unavailable no more than 7 hours per year, based on an 80% capacity factor.

As it happens, in the last three quarters of 1978 none of the four safety systems at Bruce "A" met this target. ECCS, for example, was unavailable for 39 hours during the fourth quarter of 1978; that is more than 22 times above the target (i.e. $^{7}/_{4} = 1.75$ hours per quarter). In addition, 3 of the 4 Bruce "A" safety systems failed to meet the target in each of the four quarters of the year 1977 (as well as each of the four quarters of 1978).

Such data have important repercussions for the credibility of any Probabilistic Safety Analysis. For example, if the probability of a Loss of Coolant Accident (LOCA) is assumed to be 1 in 100 for a small pipe break, and the probability of no Emergency Cooling is assumed to be 1 in 1000, then the probability of a LOCA with no ECCS may be calculated to be 1 in 100,000 per year. But if ECCS is unavailable 22 times more often than assumed, the probability of this accident is 1 in 4,550 per year – much higher!



The subject of unavailability of CANDU safety systems was introduced a couple of years earlier, in 1977, during my testimony before the Ontario Royal Commission on Electric Planning, presided over by University of Toronto Engineering Professor Arthur Porter.

Here are some verbatim excerpts from the 1978 Commission Report on Nuclear Energy in Ontario, entitled "A Race Against Time", directly related to the unavailability of CANDU safety systems – including the statistical unavailability of the containment system:

> *When we talk about the safety of a nuclear reactor, we are referring essentially to how effectively the fantastic amount of radioactivity contained in the reactor core can be prevented from escaping into the ground and atmosphere in the event of major malfunctions.*
>
> *Clearly, if a major release of this accumulated radioactivity occurred, as discussed in the previous section, the consequences would be extremely serious and could involve several thousand immediate fatalities and many more delayed fatalities.*

During normal operation, not only is a great deal of radioactivity created in the reactor core but also a great deal of thermal energy [heat]…. The purpose of the ECCS is to remove the heat from the core as rapidly as possible.

If, however, both primary coolant and emergency coolant fail there would probably be partial or complete melting of the reactor core. An uncontained complete core meltdown would almost certainly give rise to a large release of radioactivity, the consequences of which were discussed previously.

This would only occur, however, in the very unlikely event of the containment system – both reactor building and vacuum building – being breached. This could happen, for example, if the melted fuel were to fall to the reactor floor, melt through the floor, escape into the earth and contaminate a large area.

But both Ontario Hydro and AECL have stressed that, in their opinion, even in the highly improbable event of a core meltdown, the containment system would hold. The main reason for this high degree of confidence is the fact that the melted fuel would first fall into the large volume of cool heavy water moderator (about 400,000 litres). This would act as a heat sink – approximately four hours would be required to evaporate the water, during which period the decay heat of the fuel would be about 1 per cent of that at full power.

Furthermore, the designers contend that the cooling system embedded in the reactor floor combined with an external water source, which could be hooked up manually, would be able to cope with the residual heat.

Assuming absolute independence of the process and safety systems, the probability of a core meltdown per reactor at Pickering is said to be in the order of 1 in 1,000,000 years [once in a million years]. At Bruce, because there are two independent shutdown systems (i.e. shutdown rods and "poison" injection), the theoretical probability per reactor might be considerably lower, perhaps in the order of 1 in 1,000,000,000 years [once in a billion years].

However, two well-informed nuclear critics who participated in the hearings, Dr. Gordon Edwards and Ralph Torrie, have argued that the probability of a dual failure could be about 100 times higher than the theoretical levels. This estimate is based on failure rates in the high pressure piping of the primary heat transport system being 10 times higher than has been assumed, and also on the fact that the availability of the Pickering ECCS has been demonstrated to be 10 times lower than postulated by the designers.

We believe that the Edwards/Torrie estimate [of 1 in 10,000] is more realistic than the theoretical probability, not least because the Rasmussen Report has concluded that the probability of an uncontained meltdown in a light water (U.S.) reactor is 1 in 20,000 per reactor per year (it has been suggested, moreover, that this figure could be out by a factor of "5 either way").

Assuming, for the sake of argument, that within the next forty years Canada will have 100 operating reactors, the probability of a core meltdown might be in the order of 1 in 40 years, if the most pessimistic estimate of probability is assumed.

Evidence to support the Edwards/Torrie position, which is available in the Pickering Safety Reports, indicates that there were in fact (if the commissioning period is included) six loss of regulation accidents within four years. This compares very unfavourably with the design target of one in 100 years. However, as a result of a major study, involving Ontario Hydro and AECL, several improvements have been incorporated, and there has not been a loss of regulation accident since April, 1975.

We have noted also that the emergency core cooling system has not met the design targets although there is evidence that the reliability of the system is improving.

Of more serious concern is the fact that a leak was discovered in the wall of the Pickering unit 2 reactor building in June, 1974, and may have existed for one and a half years – this leak "would have reduced the ability of the containment system to limit radioactive release after any unit 2 accident since the beginning of 1973".

Measures which have been taken subsequently have resulted in design target levels being achieved. But the concern nevertheless persists because, as Ralph Torrie has pointed out, the "Pickering unit 2 containment would have to operate within target levels for 500 years before the average annual availability would be back within the bounds of the annual regulatory limit".

In assessing the legitimacy of the above limits it should be stressed that no study similar to the Rasmussen Study has been undertaken in Canada to assess the reliability of the reactor system as a whole and the consequences of major CANDU reactor accidents.

From "A Race Against Time", pp.73-79

I have said it before, and I will say it again – I do not believe that the Commissioners are getting good advice from the CNSC staff on several matters or great importance to public safety. But this example is much worse. For the CNSC Staff to tell the Commissioners that CANDU safety systems are never unavailable during operation is unacceptable.

I ask the Commission to make available to me the data on the unavailability of safety systems at all licensed CANDU reactors over the last 15 years.

Thank you.

Gordon Edwards, Ph.D.