Comments and recommendations on IAA Guidelines for Bruce C project.

Sunil Nijhawan, PhD P.Eng

As a Canadian nuclear safety engineer with over 40 years of hands-on technical safety assessment experience working with all segments of the Canadian nuclear industry (AECL, OPG, CNSC) and a number of reactor designs, I firmly believe that the IAA has a unique opportunity and a legal obligation to ask the proponent the right questions as Canada is sleep-walking towards a nuclear power reactor related disaster of historic proportions with dishonesty in regulation and technical incompetence has taken hold of the power reactor licensing, design evaluation and risk assessment processes. It is alarming that utilities like Bruce Power, the leaser of its reactors - the Ontario Power Generation and the national regulator CNSC have acted in serious collusion for years and almost never solely in public interest. CNSC have not only accepted faulty submissions by the industry, they have also created and propagated their own lies (e.g. consequences of a severe core damage are a mere 100 TBq of Cs-137 as opposed to about 30,000 TBq estimate by others). Granting any green signal to Bruce Power by accepting their preliminary environment assessment based on some ill-suited for purpose 'plant parameter envelope' to start working towards the construction of a new nuclear station at Bruce C, would be an irresponsible act that certainly will have historic and nation destroying consequences because the juggernaut so created could never be stopped. Without a technically capable designer whose qualifications, history of success in reactor design and capabilities to do honest safety assessments must form part of the questionnaire, the current parties to the project striving to get various approvals – including the one from the Impact Assessment Agency cannot be relied upon to present technically honest arguments. Consider the following:

1. CNSC management has lied brazenly about environmental impact from extreme accidents in the reactors they currently license from a severe core damage reactor. Their lies are documented in reference xx[i] and a real nuclear safety engineer's honest rebuttal in appendix A. The CNSC president is drawn from the industry the CNSC is legislated to regulate and Commission members take pride in issuing ever longer licenses to reactors as personal achievements (see member Lacroix's resume where he proudly claims having licensed 3 power reactors) . What would be unprecedented in a number of less arrogant regulatory bodies around the world , is the fact that the CNSC has never denied any application from the industry with which it shares an open revolving door for employment and most of their funds for their bloated workforce that has never published a decent technical article on risk assessment or environment impact of an actual nuclear reactor. Public input into CNSC decisions has become an unfortunate farce as evident from the last 50 decisions by the CNSC. For example, construction license was granted for construction of BWRX-300 reactors in the courtyard of the Darlington reactors inspite of the fact that the BWRX-300 reactors were not fully designed yet and they lack basic safety features such as Emergency Core Coolant or Emergency Power or Emergency Overpressure Protection on the reactor or on the miniscule containment it sports right under a vulnerable to external attack, the spent fuel pool located right on top of the reactor.

2. The guidelines must ask Bruce Power if their senior management includes past senior VPs or other managers from the CNSC and if they have any qualms about the revolving door that exists between CNSC and utilities like the Bruce Power.
3. The guidelines must ask Bruce Power if they have investigated and resolved or ignored all technical information made available to them (see appendix A) regarding the vulnerabilities in design of their 8 currently operating reactors at Bruce A and Bruce B stations that can cause environmental impacts that will severely dwarf the astronomical consequences of avoidable but severe accidents at Fukushima and Chernobyl. That will reveal their ability to actually own nuclear reactors they operate, with corresponding responsibilities consistent of their new role. Even a city permit dept would ask such a question from a new property owner contemplating construction.
4. The design organizations (remnants of AECL) likely to benefit from a go ahead to Bruce C station have demonstrated that they are technically incapable of designing a new reactor that meets the current public expectations of risk. Not only the last 5 'new' rector designs by AECL were commercial failures, their staff are unable to comprehend even basic engineering facts as stated in appendix A and just feign ignorance or disagreement without presenting a single technical argument. Guidelines must ask Bruce power to demonstrate that they are capable and willing to look for alternate suppliers with competent technical staff who are not proposing a rehash of the 50 year old design now at Bruce and Darlington reactors with a minor change like a real containment building that is currently absent in Bruce A and B reactors.
5. The guidelines must emphasize that there is no such thing as a technology neutral risk assessment or project impact assessment. Overall 50 odd reactor design parameters in a PPE rarely define risk from its operation or accident, it is the detailed design (and ability to control and manage) that does. Why was that lost on CNSC when they supported the Darlington SMR and now on Bruce Power ? Is is because to them public safety has no meaning? Just one wrong choice of metal in feeders at Bruce A and B makes those reactors susceptible to double the production of hydrogen and an early explosion caused not only by excessive hydrogen but by the design of PARS used to mitigate hydrogen (Korea is already junking their PARS that cannot withstand 8% hydrogen, a fact that escapes the genius MBAs that run safety in our Canadian nuclear institutions). So please ask Bruce Power to withdraw that approach for risk classification or reject it pending development of an actual design that represents public expectations of risk in 2025. Only someone who does not care for my country will approve such an approach or be taken by the empty jargon that calls it an enverlope.

6. The draft regulations must ask Bruce Power if the potential reactor designer for Bruce does has qualified personnel to undertake the task of designing a new, safe reactor. A good test will be a demonstrated ability of their chief engineer to understand some basic engineering facts as outlined in Appendix A.

APPENDIX A

DESIGN ISSUES WITH CANADIAN MULTI UNIT CANDU REACTORS AT BRUCE & DARLINGTON AND THE VULNERABILITIES IN THEIR DESIGN THAT BRUCE POWER AND OPG SHOULD FIX

Sunil Nijhawan, Ph.D, P.Eng.

11 JULY 2025

SUMMARY

One sees eerie similarities here in Canada to the cozy relationship between regulator and utilities in 'pre-Fukushima' Japan.

The chronic degradation of real commitments to continued improvements in reactor safety systems and a decline in overall safety culture that discourages critical design reviews and willfully ignores well justified, safety critical hardware upgrades, has created alarming conditions that are likely inching us towards another nuclear disaster. Operating CANDU reactors at Darlington, in spite of the expensive 'refurbishments' are now close to being obsolete but have barely seen any substantive severe accident related risk reduction upgrades fourteen years after Fukushima, hoopla in Canada around some minor improvements and premature closure of even otherwise sparse and what were really weak regulatory *'Fukushima Action Items*', notwithstanding.

With a number of common barriers to fission product releases to environment missing or weak, one would expect the regulator to be extra vigilant in promoting prevention and encouraging delays in onset of core damage. On the contrary, it has only made matters worse by its collusion & obfuscation as long summarized in [ii] and even denying the additional burden of age related degradations as in long operating licenses 50% longer than design life at Pickering [iii]. Whether the regulatory actions are out of ignorance, inability or intent is debatable but equally disturbing.

At 2%/hour design leakage (against the international practice of 0.1% per day; and a design pressure of less than 0.9 bar, the Darlington CANDU station sports some of the weakest and leakiest containments in the world. With no reactor pressure vessel to isolate the overheating channel and debris, these leaky containments will directly see un-attenuated fission products releases from the fuel. They will trap combustible D_2 gas in interconnected from below inverted cup like crowded reactors vaults to an increased gas explosion potential. The reactor units have high steam and air oxidation potential on both sides of over 10 km of low carbon steel feeder piping with over 1800 m^2 hot surface areas exposed for each of internal steam and external air oxidation and copious amounts of core Zircaloy (> 50,000 kg, twice of that in a BWR of similar power).

Combustible gas detection and mitigation systems are designed for Hydrogen (H_2) instead of Deuterium (D_2) gas in these D_2O cooled and D_2O moderated PHWRs. At the last hearings some OPG senior manager claimed that 'research' showed there was no difference between the heavier isotope D2 and H2, an alarming claim that is indicative of the reason for my request to the Commission to deny the OPG request for a 30 year license, a focal point of making this submission. The pressure relief systems in primary cooling and moderating systems are dangerously inadequate, resulting likely in potential pressure boundary ruptures and early containment bypass, accelerated onset of core damage and vessel failures. Backup diesel generators are located low and close to water as in Fukushima. Spent fuel pools are overcrowded with horizontally stacked fuel bundles akin fish in fish-baskets. Yet, the emphasis has shifted to passing wishful thinking of low off-site releases [iv] and convenient half-truths assumption of an early core collapse terminating further core degradation and releases into containment as facts and ignoring [v] known design vulnerabilities that amplify risk actively denying [vi] even the basic science on high temperature oxidation of carbon steel [vii].

Even more dangerous are the unsubstantiated claims being made of near impossibility of off-site releases of long lived species from these multi-unit reactors by utility management [viii] without any a challenge by the regulators who are now being asked to rubber stamp a 30-year license extension request and thus lose any viable control over the safety aspects of the reactor. The life management issues of ageing, elongating, thinning, hydriding, embrittling and deforming CANDU Pressure Tubes is yet to be resolved but these obsolete reactors keep getting ever longer license extensions (e.g. for 10 more

years, over 50% beyond original Pickering pressure tube design life - ignoring their own data [ix] that suggests that safe operation cannot be guaranteed due to elongation. There are loud, ambiguous references to compliance with un-named IAEA documents and standards. No IAEA document has yet identified or discussed the PHWR design vulnerabilities that may lead to disastrous outcomes and this paper is repeating in forums akin ICONE for the n^{th} time. Of equally great harm to risk reduction are the IAEA team of experts missions (Integrated Regulatory Review Service (IRRS) follow-up missions - for example [x] that issue oversight certifications / seals of approval to the Canadian regulator CNSC without anything resembling a technical evaluation of CANDU design elements that contribute to risk.

Many critical vulnerabilities and proposed engineering fixes that can be undertaken to overcome also been highlighted routinely [xi] but are groundlessly rejected as in [xii] which begs for an international impartial scrutiny in ingrained obdurate industry intransigence against changes and investments into substantive safety improvements and risk reduction. Emergency preparedness by civil authorities has been illogically conditioned for the smallest possible 'Large Release' source term (of e.g. 100 TBq of Cs-137) and available response time for mitigation measures have been exaggerated baselessly. Both acts are irresponsible and dangerous to public and first responder safety. A number of early mitigation measures to externally replenish boiler inventory (a measure common to all PWRs) will not work due to an unusually low, below core, placement of pressurizer that will gradually gravity drain much primary coolant from boiler tubes. So, the most important emergency measure to restore core cooling by reflooding boilers to induce natural circulation flows will go to waste. Operators will never know why the core never cooled.

Inability of the utilities to accept responsibility for reactor upgrades and inability of the regulatory management to act independently are the signs of impending implosions in our nuclear industry. It is likely because the regulatory body CNSC is critically dependent upon the licensees financially in a 'cost recovery' plan. Not likely, but perhaps if we get lucky, an impending disaster can be avoided by a return to the first principles, and not mere slogans, of 'safety first'. Right now, an unmitigated station blackout in a CANDU multi-unit station will make the Fukushima disaster look like a walk in the park.

INEXPERT REGULATORS & DESIGN OBSCELENCE

The long ignored severe accident related design deficiencies, inability to safely, successfully withstand a simple accident such as a station blackout for a reasonable amount of time are amongst many unmet challenges that multi-unit CANDU reactors pose to public safety and very directly to the utility corporate health as well. It is not just that the reactors are now obsolete and were not designed with severe accidents in the design basis so as to make severe accident management predictable and severe accident consequences manageable; it is also that the utilities will do only the minimum they are required to do and that the regulatory body is also neither independent nor technically competent, especially in the field of severe accidents. As a result, a strong culture of privately or silently agreed obfuscation has emerged. Public safety has become secondary to corporate need for uninterrupted power production & regulator's need to exist in significant denial of lessons of Fukushima.

Almost none of the operating 400 odd nuclear power reactors incorporated severe accidents within their design basis. So, all multi-unit CANDU reactors, just like their single unit counterparts and most all operating LWRs share some of the same vulnerabilities to onset of severe core damage accidents. They also share their inability to adequately avoid severe core damage early, incorporate enough passive systems to delay its onset, provide adequate means of early arresting their progression, provide ample opportunities to successfully apply external resources to accident management, include enough design margins to reduce releases into the containment and have strong and tight enough containments to keep the accident source terms from releases by leaks, over-pressurization or explosive outcomes. While LWRs also are of a vintage design and vulnerable to severe core damage, not all have taken the path of denial. Many LWR utilities, like with NRC's State-of-the-Art Reactor Consequence Analysis Project, are doing a much better job of critical self examination and risk reduction. Overseas CANDU utilities cite Canadian CNSC actions to justify their inaction and apparent lack of technical expertise.

Detailed technical analyses including sophisticated computer simulations reveal that many of the severe accident related vulnerabilities of multi unit CANDU PHWR design at Darlington (4 units) reactors are common with single unit CANDU reactors in Canada , Korea, Argentina, India, Pakistan, Romania and China. A number of inadequacies in severe accident mitigation capabilities are also shared with LWR designs of the same vintage. As discussed in a number of earlier papers on the same issues [xiii], an evaluation of a station blackout (SBO) accident at the multi-unit Darlington station reveals significant challenges to accident management options. There, however, are easily identifiable indicators and sources, instigators of potentially unacceptable off site radiological consequences as well as engineering fixes to reduce risks. It is unfortunate that only another severe core damage accident will likely force the required change. Right now the Canadian utilities have the regulator CNSC in a firm capture and are in no mood for a serious dialogue on the topic, irrespective of risk or consequences. It is hoped that professional forums such as ICONE and public awareness will propel the regulators and/or utilities into action.

Design analyses and numerical simulations reveal that opportunities for design improvements and alternate mitigation measures are abundantly clear for certain challenges and not so much for others. But in all cases regulators and utilities reject them in their preference for wild and untrue claims of easy operator actions to bring the reactor under control and benign severe accident consequences even without any operator actions. The regulator have put out glorifying videos

without doing any analyses and accepted utility submissions without any meaningful critical technical reviews. These evangelical pronouncements of eternal and near absolute safety in the presently operating, albeit of obsolete design reactors, portray severe core damage accidents in a distorted positive light in defiance of engineered realities (by claiming physically impossible long times to bring in emergency equipment - [xiv] that claims 5 hours for boilers as heat sinks instead of likely 1 hour when an engineering analyses is undertaken [xv] and in defiance of expected professional integrity in ensuring public safety (by claiming extremely low releases of ~ 100 TBq of Cs-137 instead of likely 30,000 TBq from leaky, weak containments without ever doing any numerical analyses or modelling - [iv]).

The CANDU PHWRs concept started in 1950s with a 22 MWe Nuclear Power Demonstration (NPD) going critical in 1962 and a first full scale power plant at Douglas Point (220 MWe) in 1966. The 600 to 800 MWe units first entered commercial operation as multi unit power plants in 1971. The basic design of twelve or so, 10 cm diameter 50 cm long fuel bundles in about three to five hundred horizontal Zircaloy pressure tubes within a thermally isolated low pressure, low temperature D_2O moderator has not changed much over these 60 years. Improvements in rolled joints, end fittings and pressure tube materials have increased their reliability but the degradation of Zircaloy pressure tubes has required previously unforeseen 'mid-life' replacements and extensive 'refurbishments' which involve removal and replacement of very radioactive core structural materials and have typically cost more than the original plant did. All units are at the end of their design life, under 'refurbishment' to replace degraded core components (pressure and Calandria tubes, feeders and boilers) or already rebuilt back to the original specs of 1960s and 1970s.

Further development of the CANDU technology has since been almost abandoned in Canada with the design organization AECL, into which literally billions of dollars were invested by the Government of Canada to develop the CANDU reactor concept, was sold with most all its assets minus the liabilities to a private company SNC-Lavalin for the price of a well used corporate jet and all future plans have now shifted to commercializing the so called Small Modular Reactors with renewed promises of riches and safety. The national regulator CNSC is playing the bandleader once again. Attention has shifted away from the high risk obsolete multi unit reactors at Bruce, Darlington and Pickering with their long term licenses in the utility pockets with risk reduction opportunities of no immediate interest to anyone. Unless of course if CNSC members recognize the disservice this does to our future & force them to act in public interest alone.

What has changed over these 60 years is our understanding that these reactors, like all others of that vintage, were more complex than other power reactors and were certainly not designed with core damage accidents within the design basis. Some have been thankfully taken off service at the end of their life (Gentilly-2) or earlier (Gentilly-1, Pickering A units 2,3) while one at Wolsong 1 was removed from service after it was refurbished with new reactor internals at great expense but did not satisfy safe operating envelope expectations. In Canada, Gentilly-2 single unit CANDU was wisely retired after its' design life. It was not the regulator that initiated its closure, it was the utility that did not particularly need the associated risk.

CONTRIBUTIONS BY THE NATIONAL REGULATOR

The challenge to public safety is further exasperated by a diminishing safety culture at the regulatory body CNSC that glorifies the obsolete designs, disregards known safety issues and discourages real public discourse and input from outside the regular payroll of the industry [ii]. It also spends inordinate times in self adulation and is looking more like a public relations arm of the utilities it is supposed to regulate.

The Canadian regulator CNSC has taken the lead in producing misleading information about CANDU severe accident progression [xiv] and its consequences [iv]. Reactor vulnerabilities have been ignored in defiance of basic science by siding with corporate interests that have had the regulators in firm capture for over a decade. This behaviour is in stark contrast to the practices south of the border where rule based regulations are more the norm; rules are scientific fact based and comprehensive analyses and supporting research are routinely commissioned. A comparison of CNSC generated claims in [iv], [xiv] is instructive with reports such as 'The State-of-the-Art Reactor Consequence Analyses' (SOARCA) project [xvi] that were undertaken by NRC to systematically summarize accident progression pathways and mitigation strategies with actual numerical analyses using state of the art computational aides without resorting to hyperbole on one hand and artificially generated fog as in [iv], [xiv] on the other.

The continuing insistence by the regulator to be the bugler for support an obsolete technology that it explicitly says need not be comprehensively, systematically rejuvenated before its further exploitation and claims in its reports that severe accident consequences are nothing more than benign - are all appalling facts. When the issue of high oxidation potential of feeders, the carbon steel pipes downstream of hot fuel, their first reaction was that feeders cannot get warm and hence any issues of carbon steel oxidation were humbug. The regulator has even told the local emergency management organizations that the worst off-site releases after a severe accident are expected to be as minimal as total releases of 100 TBq of Cs-137 (and other species in proportion) which is from about 0.15% of the fuel and that health effects of a severe accident would be benign. This pronouncement was not based on any analysis but was camouflaged under words deceptively implying that specific analyses for the worst accident without operator intervention were undertaken. This has emboldened the utilities to do practically nothing meaningful to reduce residual risk and push for even longer operating licenses well beyond the original design life of plants whose materials degrade faster than in any other reactor with age (Zircaloy pressure tube thinning, elongating, thinning and increasing in diameter with creep, hydriding and being replaced prematurely at exorbitant costs) and normal exploitation (e.g. thinning of carbon steel feeder pipes that connect the fuel channels to pumps and boilers).

Given the unexpected nature of any accident and severe potential for extreme damage to the environment if the accident results in severe core damage as in a sustained loss of heat sinks after a station blackout as in Fukushima, one would imagine that the regulators would be insisting and utilities would be installing proper measures to reduce the likelihood of occurrence of multiple failures that can lead to severe core damage; and incorporating measures to identify, control, manage and arrest the progression of the accidents early; and ensuring measures to contain the consequences to within the reactor units and most of all, accepting the limitations of the technology and their understanding of it to invest in fundamental research. None of that has happened to a degree consistent with needs. As a result the reactors today are not much better able to mitigate

severe accidents than they were before Fukushima and before the shiny pumper fire trucks were bought to provide low pressure heat sinks, filtered containment venting systems installed and a few symbolic but dangerous hydrogen recombiners scattered around the plants. These measures are poorly thought out and even more poorly executed with the large number of other vulnerabilities largely unaddressed. Of course such a behaviour has consequences. The official report of The Fukushima Nuclear Accident Independent Investigation Commission concluded in part that :

"The TEPCO Fukushima Nuclear Power Plant accident was the result of collusion between the government, the regulators and TEPCO, and the lack of governance by said parties. They effectively betrayed the nation's right to be safe from nuclear accidents. Therefore, we conclude that the accident was clearly 'manmade.' We believe that the root causes were the organizational and regulatory systems that supported faulty rationales for decisions and actions, rather than issues relating to the competency of any specific individual."

It has become very clear that the situation in a number of countries is exactly the same as summarized above for Japan in 2011. While this paper concentrates on the issues arising out of multi unit CANDU PHWR operation in Canada, the path taken by the regulators in other countries with CANDU reactors is not much different. After 3 decades of severe accident progression and consequence assessment evaluations and trying to get the industry to recognize that the reactors do not meet the evolving public expectations of risk, it has become apparent to me and many others that a combination of design weaknesses, corporate intransigence, and regulatory weakness has come together in a form that is detrimental not only to public safety but also to the future of nuclear power. The regulators have recently bestowed on the multi unit reactor utilities unprecedented 10 year license extensions, in some cases in defiance of overwhelming evidence that these reactors pose large risk under SBO accident conditions not dissimilar to Fukushima.

I will make my point by first discussing the design specifics that have cried out for new and innovative mitigating measures as our understanding of severe accidents have matured and then pointing out the specific decisions made by specific people in the Canadian nuclear industry to put the issues under the rug. As a nuclear safety engineer with over 45 years of work in nuclear safety and as one who has developed a dozen computer codes to model accident progression in CANDU reactors, including the CANDU specific parts of the now obsolete MAAP-CANDU code that the industry still uses to analyze severe accidents, I consider it my ethical duty to present the arguments in favour of stepping our game up to meet the unmet challenges to successfully mitigating severe accidents in Darlington multi unit CANDU reactors or shutting them all down in interest of public safety and security. In interest of clarity I will use the multi unit reactors at Darlington and Bruce in Canada as examples, although the malaise of poor severe accident mitigation permeates to all CANDU / PHWR units in all countries. I will demonstrate that giving OPG's Darlington station a 30 year license is an exercise like driving on a highway with eyes closed on a with erratic brakes and no fenders.

DARLINGTON CANDU DESIGN VULNERABITY IS NOT A NEWLY DISCOVERED PROBLEM

A number of red flags have been raised over the years and a systematic design evaluation has uncovered a long list of vulnerabilities that make severe core damage accident consequences from multi unit reactors alarmingly unacceptable. The response of the Canadian nuclear industry has varied from silence to outright lies and bullying. The Canadian national regulator has taken the lead in spewing technically impossible positions on severe accident consequences [iv] and the collusion between the industry and the regulators has deteriorated progress in resolution to such an extent that the latest position from a utility Bruce Power VP during relicensing hearings is that they will soon see no conditions under which these reactors will release any long lived isotopes following a severe core damage accident [viii] and hence a reduction in planning zones is to be in order . This for a design that has a containment unable to be tested above 0.45 atmospheres and a leak rate at design pressure of 2% per hour (500 times more than at a light water PWR such as at Surry), not to mention the other design features that make these multi unit reactors un-licensable in any other jurisdiction in the world. The same VP smugly claimed that Bruce Power adopted new standards faster than others and in special contrast to overseas utilities that would do so only every 30 - 40 years on relicensing. The regulator CNSC similarly makes claims of being the 'world leader' in safety regulation. Their mutual admiration is evident in transcripts of public meetings where the two practically finish each other's sentences. CNSC has also quietly sidestepped its own already watered down regulations to allow the utilities to pressure test their containment every 12 years [xvii] instead of the already unusual for a nuclear reactor containment leakage test frequency at full design pressure of every 6 years per the CNSC regulatory guide R7 [xviii].

In this time of strained relations, a severe accident at Darlington having contaminated lake Ontario after a core damage accident, may invite swift response from the US against Canada. The CNSC members need to be more responsible and deny OPG their unprecedented request for a 30 year license in a reactor that essentially is an obsolete design void of any design enhancements after Fukushima.

CANDU REACTOR DESIGN VULNERABILITIES TO UNSATISFACTORY OUTCOMES AFTER STATION BLACKOUT

CANDU PHWRs suffer from a number of vulnerabilities to unacceptable outcomes after severe accidents and a number of design features that accelerate failures or exasperate the accident consequences and hence risk to public. Some of these are specific to the D_2O cooled and moderated horizontal fuel channel concept just as the RBMK is with its vertical boiling light water cooled, hot graphite moderated fuel channels. While utilities and the national regulators have long sung the CANDU design praises, some fundamental CANDU vulnerabilities cannot be rectified for existing reactors. For example, absence of a pressure vessel around the core will always directly expel activity into the containment once the channels experience structural damage. Thus the leaky containment becomes the only barrier to release of activity.

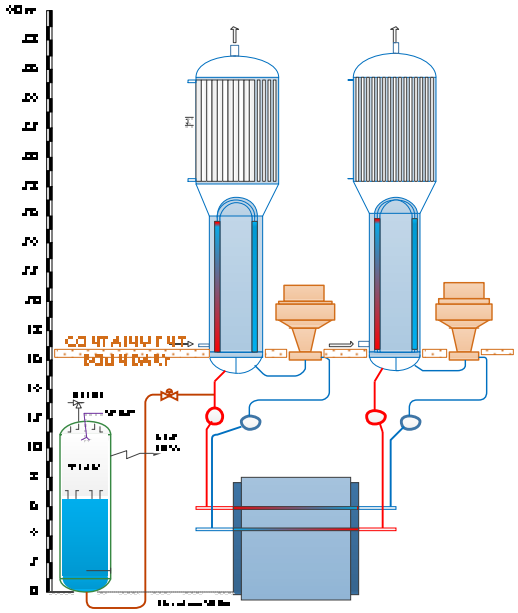

Figure 1 : Lower than core placement of pressurizer that will drain boiler tube inventory at Darlington reactors in a station blackout scenario (not a low frequency event)

The strange choice of pressurizer location below the boilers and reactor headers (in 12 reactor units at Darlington and Bruce stations) will cause draining into it of primary coolant from boiler tubes in a SBO to an extent that boilers will become useless as heat sinks and no amount of emergency measures to add water to boilers will restore cooling to the reactor core unless the primary cooling system was replenished as well, something that cannot be done after an SBO in the present design and presently configured SAMGs.

The low pressure retention capacity (<<0.9 bar) of the rectangular slab industrial buildings that surround the reactor cores and their design leak rate at 2%/hour which is 480 times greater than the 0.1%/day in modern PWRs will always make the containments ineffective repositories of fission and activation product activity put unfiltered into them from the disassembling fuel channels and also make them traps for combustible Deuterium that will come out of the same path into inverted cup like inter-connected rooms called reactor vaults that surround the reactors. Gas explosions in any one reactor vault will cause a huge containment bypass.

What is fundamentally disturbing is that certain long well known design features that may cause an unwarranted pressure boundary failure (*because the primary heat transport system (PHTS) overpressure steam relief capacity is too low*) or accelerate onset of core disassembly (*such as an un-necessary, forced expulsion by flashing of a critical amount of moderator upon onset of boiling because rupture disks actuate instead of a controlled relief through relief valves*) or a lack means of direct depressurization of PHTS or cause the containment to leak profusely at relatively low pressures have not been accepted or rectified. Certain challenges to the containment integrity, such as from high amounts of hydrogen and deuterium produced by oxidation of outside and inside surfaces of feeders after a core damage accident of LOCA+LOECC have been ignored for even design basis accidents without the regulator ever highlighting the omission or recognizing that Carbon steel is more oxidation reactive than Zircaloy at all temperatures.

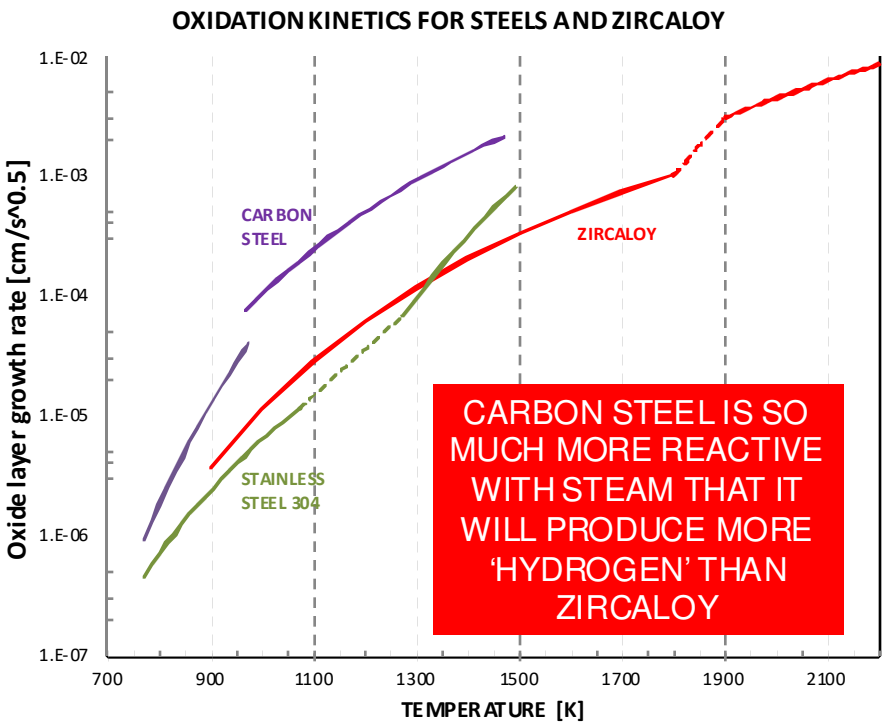

Figure 2: Oxidation kinetics for Zircaloy, carbon steel and stainless steel

Potential for steam and air oxidation to produce copious amounts of combustible Deuterium and Hydrogen from the large amount of Zircaloy and carbon steel associated with the fuel channels during a severe core damage accident is easy to see. There is about 50,000 kg of Zircaloy with an oxidation surface area of over 12000 m^2 and over 120 tons of low carbon steel piping over 10 km long with a surface area greater than 1800 m^2 in a Darlington CANDU PHWR associated with fuel channels where a loss of cooling can elevate fuel temperatures such that rate of oxidation of feeder carbon steel will always be greater than that for Zircaloy (Figure 2) and the amount of Deuterium produced by oxidation of steel will exceed that from Zircaloy very early (Figure 3).

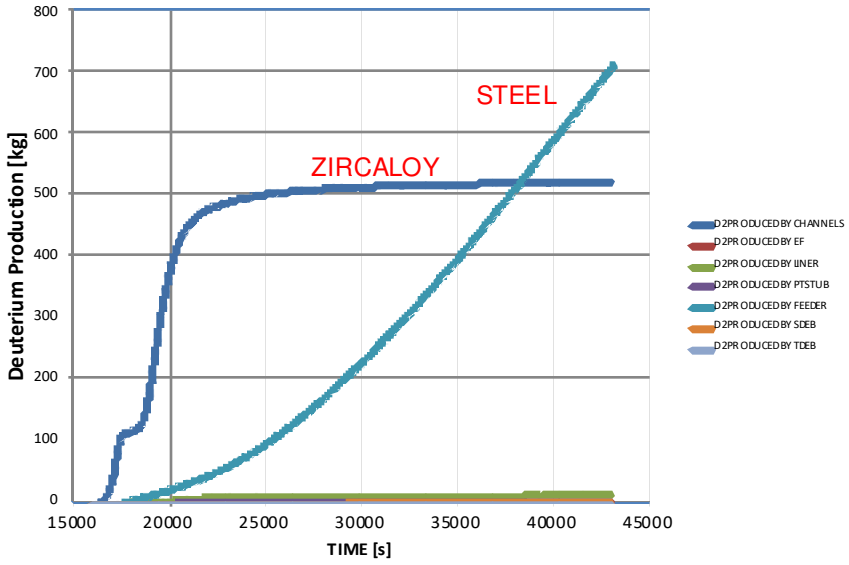

Figure 3 : Sample results for the first 12 hours of combustible gas production in a 600 MWe single unit CANDU

A station black out (SBO) scenario which with its sustained loss of engineered heat sinks represents a large number of accidents with other initiating failures and is a representative scenario undertaken for all reactors worldwide to assess effectiveness of engineered passive systems that may come into play and of opportunities for emergency mitigating measures.

Engineering analyses reveal that reactor risk profiles are in the alarm territory for a number of very obvious reasons. Early passive heat removal by steam generators after a station blackout is not only short lived (~1.5 hours as opposed to claimed 5 hours) but can also be compromised even earlier by primary coolant from boiler tubes getting drained into a large cooling pressurizer located well below the boilers and the reactor core. (Figure 1, for Darlington). Thus any delay in restoring secondary heat sinks and primary inventory drained by gravity into pressurizer may make the boilers irrelevant and ineffective.

Over-pressure protection systems on main core cooling system is indirect (goes through another vessel and requires two sets of valves in series to successfully actuate) and functionally inadequate to satisfy the heat load. On a loss of boilers as heat sink, a steam relief through relief valves is the only heat sinks for decay heat but the PHTS steam relief capacity is only ~20% of decay heat equivalent, let alone for other anticipated severe accident loads [[xix]]. This can likely cause an early over pressure failure and hence a containment bypass by steam generator tube ruptures or another uncontrolled pressure boundary rupture, something that the ASME code or common engineering sense would require that not ever happen. This very fundamental error in design has been known to the utilities for 20 years without resolution or nay an understanding of its consequences. When an industry starts accepting a pressure boundary failure as an acceptable outcome rather than re-engineer the safety valves, it is time for that industry to shut operations or as an ex NRC chairman Gregory Jaczko put it 'is Going Away' [[xx]]. As a nuclear engineer with great confidence in my peers, I find such a direction and such an outcome for my industry also likely but otherwise unacceptable.

Inability to manage a loss of heat sinks accidents is exacerbated by handicaps like no external emergency means of high pressure water addition to the heat transport system. Any addition of emergency coolant requires that boilers be manually depressurized successfully first for the PHTS to be hopefully, indirectly depressurized. A manual depressurization of boilers is actually an operator assisted process of forcing the relief valves to stay open in a process that forcibly removes a third or so of the boiler liquid inventory by flashing and dumps it into the atmosphere without a foolproof guarantee that any subsequent action to replenish the same inventory would be successful. A high pressure makeup feedwater injection with a passive steam driven turbine would have easily solved both problems without breaking a sweat. This has been the logical backup solution at a number of PWRs but the CNSC brass totally trashed the idea a number of times citing some unrelated steam turbine failures at Fukushima. A steam driven auxiliary feedback system is as passive as they get. In fact one has been at the single unit CANDU at Pt. Lepreau forever. The issue is really not the merit of this or that solution to the various vulnerabilities in multi unit CANDU stations; the issue is the attitude and a collusive decision to do absolutely nothing more than what little they have done, even if the decisions such as low pressure pumper fire trucks to add water to the boilers is now recognized in private conversations to be not the wisest one.

The current SAMGs erroneously credit gravity feed of water into the boilers after their depressurization through the feedwater train from de-aerator. This will really not work. Flashing of the ~160^{o}C water inventory and unavoidable high pressure back leakage of boiler inventory through the check valves would vapour bind the feedwater flow path. In addition, there will not be enough driving force to open and then keep the feedwater check valves open.

With more and more channels losing their heat sinks and dumping their decay and chemical heat into the moderator, onset of moderator boiling causes the rupture disks on the Calandria vessel to open up, creating a direct path for release of steam, fission products, hot and combustible gases into the inverted-cup reactor vault over the common duct in the containment.

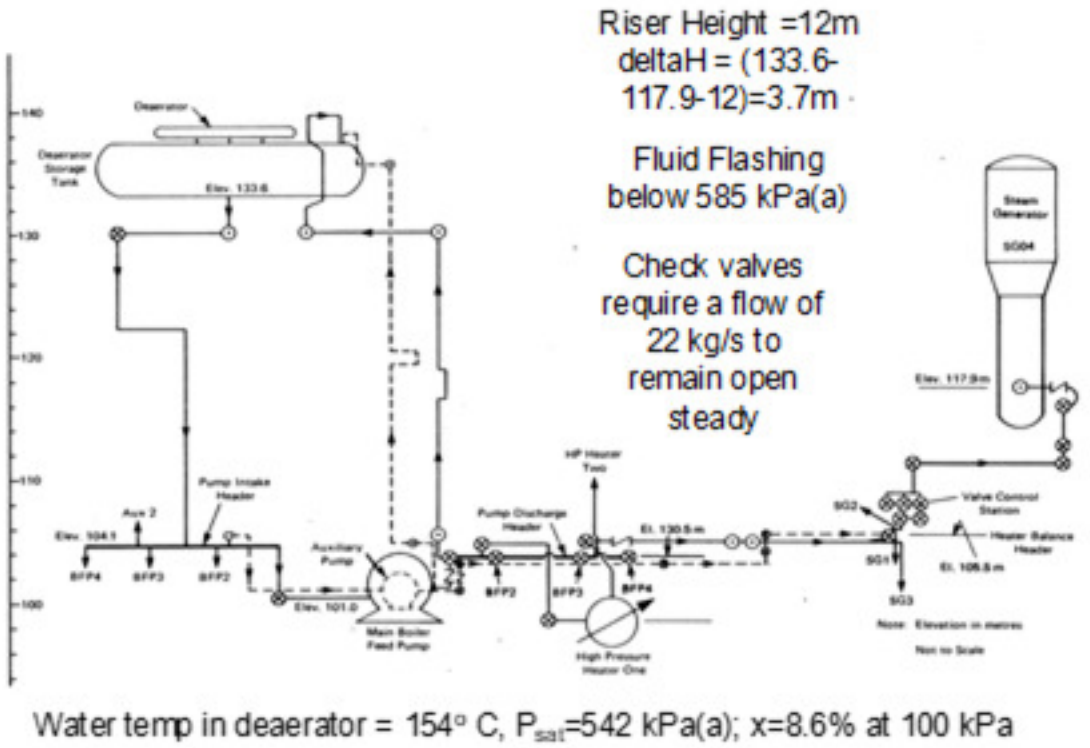

Figure 4 : Looking into gravity feed into the boilers from de-aerator

This happens as a lack of a decay heat level controlled steam relief on the Calandria vessel (which contains the moderator) accelerates severe core damage by ejecting a significant amount of moderator when it becomes the dominant heat sink for fuel channels, boils and causes the rupture disks on its large piping to burst to eject water by flashing and carryover. By ignoring the extra 30-60 min such a design omission subtracts from time to onset of severe core damage, the industry reinforces its intransigence and inability to think through that public safety supersedes all other considerations .

An important claim by the industry on debris creation and potential retention of 'melt' in the Calandria vessel is examined below:

Disassembly of a reactor fuel channel is its partial breakup into single or multiple bundle length pieces and in some cases even separation from the rolled joints at end shields. Breakup into pieces can occur when both the primary coolant from inside of the fuel channel and the moderator coolant from outside the fuel channel are depleted and the pressure tube perforates with it being unable to sustain the weight of fuel within or above it. Fuel channels begin to heatup individually once they are devoid of coolant and the moderator becomes the sole heat sink. A widespread core damage accident in a CANDU would only occur gradually because of the large variability in the inventory of water associated with each channel, variability in channel powers and variability in time at which the moderator outside each channel may drain or be boiled off. In all cases a fuel heatup to temperatures high enough to cause the pressure and Calandria tubes to deform and perforate are required and disassembly of different channel segments would take a finite time and with a finite stagger between channels.

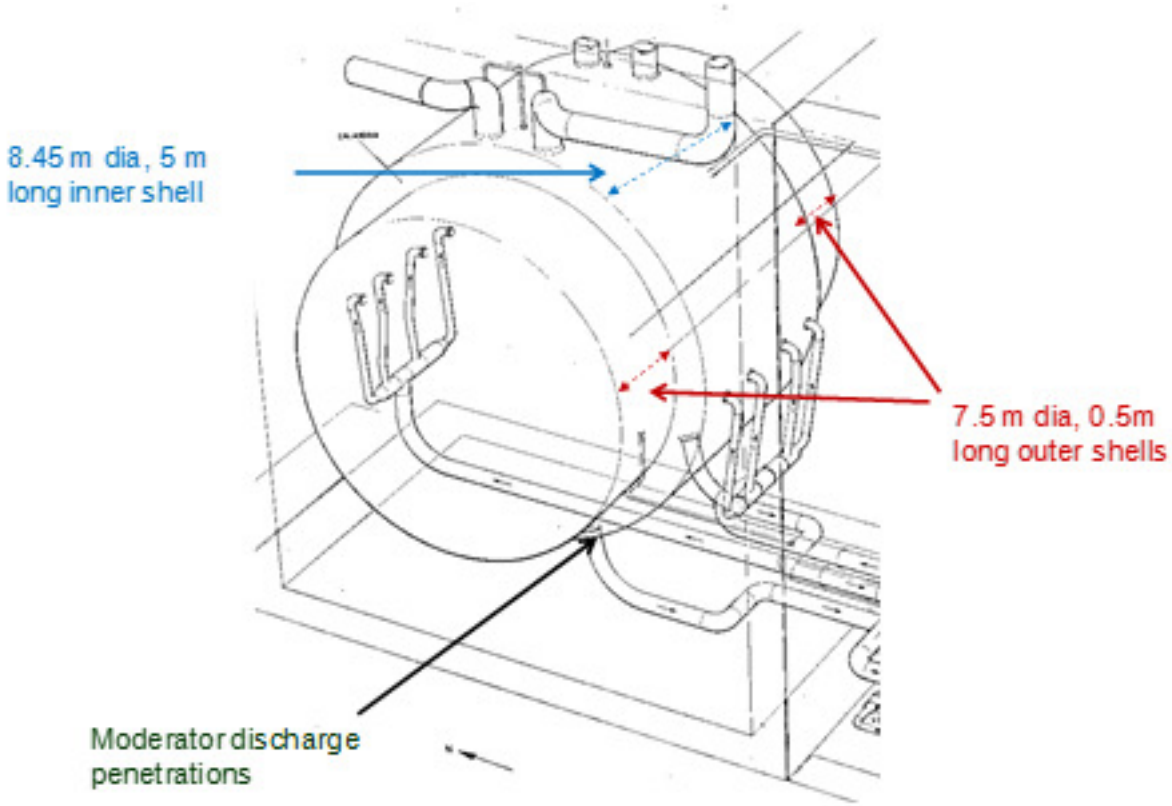

Figure 5: Calandria vessel, a stepped stainless steel vessel with welded annular plate

Accident termination by retention of molten core debris in a vessel have been adopted from PWRs without consideration of the design specifics of the stepped low pressure and thin CANDU moderator vessel. The debris formation in a CANDU reactor is in solid chunks of fuel channel and its eventual retention upon Zircaloy melting in the Calandria vessel cannot be guaranteed as the relatively thin walled stepped and welded vessel (wall thickness varying between 19 and 28 mm) may fail at welds by thermal loads long before any gross melting thus violently introducing water from the shield tank onto hot debris.

Any claims of an LWR like in-vessel retention of molten uranium debris are not credible or consistent with the gradual core disassembly of CANDU cores in case of a station blackout scenario with a sustained absence of heat sinks. The Calandria vessel has a wall thickness that varies between 19mm at annular plates to 28 mm in main shell. The weld failure upon differential expansion of the two shells, with outer shell constrained, is easy to demonstrate (Figure 6 and Figure 7).

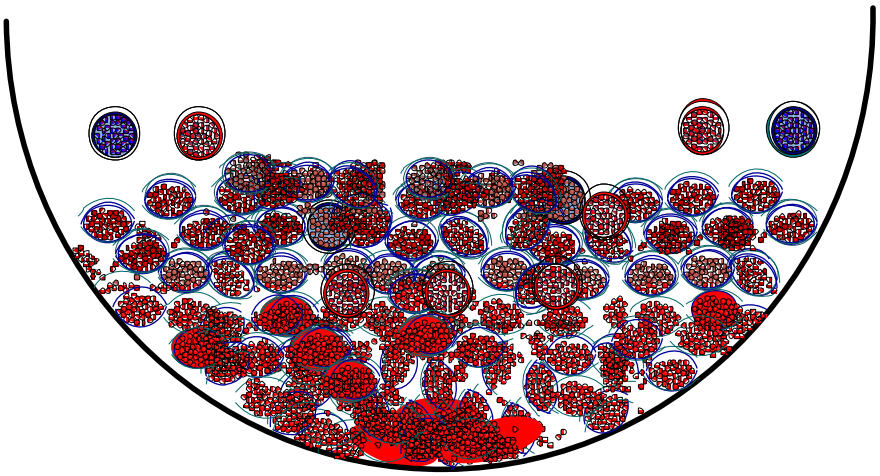

Figure 6 : Likely state of debris upon Calandria weld failure

The effect of Calandria vessel weld failure can vary from additional hydrogen production, accelerated fission product releases as one mode of outcome for small weld cracks and slow leaks, to catastrophic vessel failures by energetic interactions of incoming water with the hot and molten solid-liquid debris at the bottom of the Calandria vessel as the other mode.

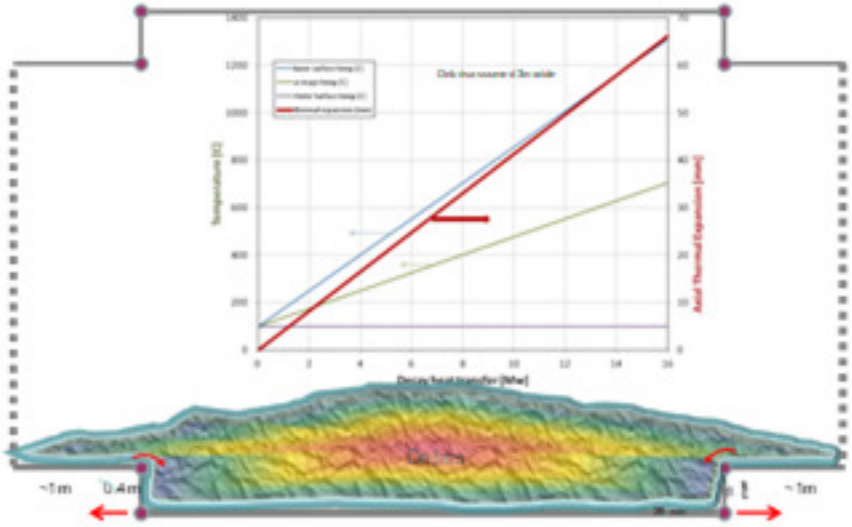

Figure 7: Calandria shell elongation as an indicator of stresses that will cause weld failure

As a result of absence of a retaining vessel, direct un-attenuated releases into the containment, weak containment structures and significant likelihood of energetic interaction of hot debris with water and Deuterium burns /explosions causing challenges to containment integrity, large releases of radioactivity from failed containment structures are inevitable.

WEAK AND LEAKY CONTAINMENT STRUCTURES

In all cases in absence of a retaining LWR like pressure vessel, the disassembling channels would continuously and over many hours release fission products without attenuation through the rupture disk pipes and directly into the box like containments (Figure 9) that are at 48% per day design leak rate at design pressure very leaky and at less than 1 bar design pressure, structurally

weakest of all operating reactor containments (typical PWR building design pressure is 5 times higher and leakage at design pressure is 480 times lower).

Another containment bypass potential is in high temperature disassembly of in-core devices along with hot channels. Recall that the in-core device controllers and drives are outside the containment on the reactivity deck. So certain release of fission products onto the reactivity deck cannot be avoided once these devices heatup and melt.

The reactor buildings around each individual reactor core are inverted cup like traps for combustible gases (Figure 8). A large number of safety significant components like the steam generators, pumps and the reactivity control devices are all outside the containment envelope and vulnerable to failures by external impact or otherwise of the weak structures on top of the reactivity decks. These are some of the vulnerabilities that can be fixed.

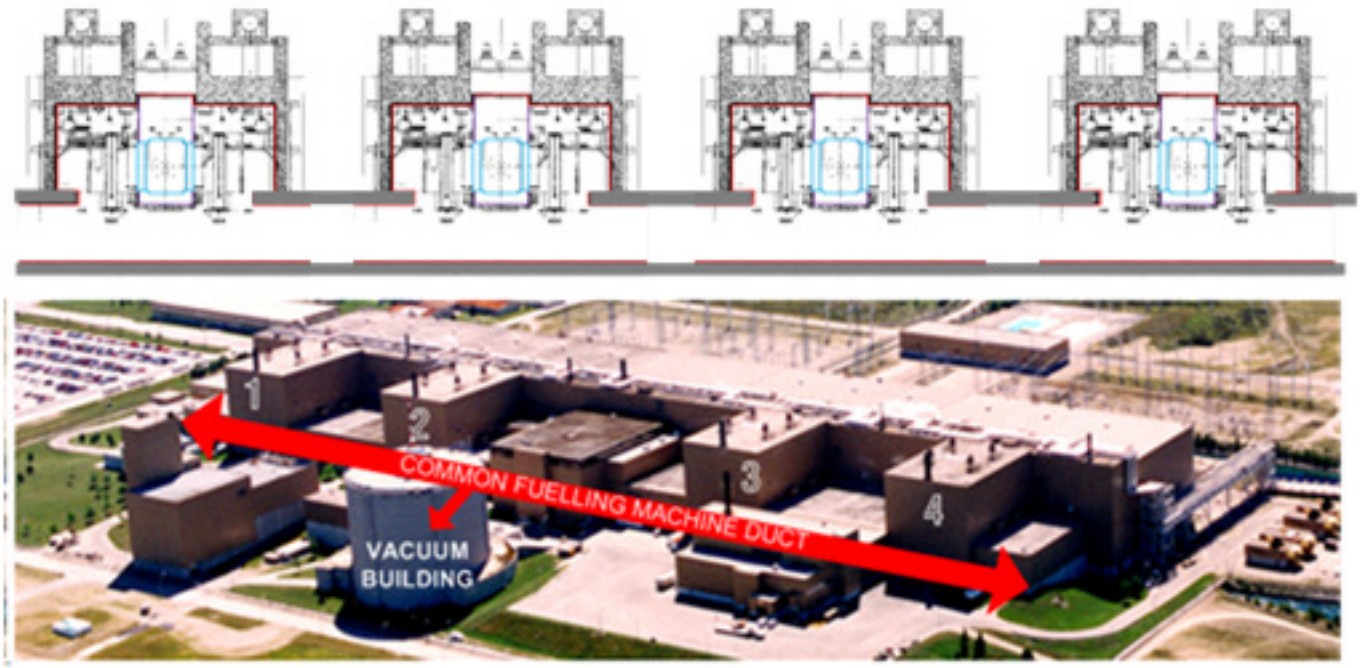

Figure 8: Multi unit layout at Bruce station; Darlington is similar

REACTOR VAULT A TRAP FOR HYDROGEN

The containment layout is such that even a 1% oxidation of any of these materials will cause stagnated and explosive pockets of combustible Deuterium and Hydrogen in reactor vaults shaped like interconnected inverted cups. The reactor vault is the direct recipient of products of reaction with hot fuel as the moderator relief pipes vent into the reactor vault.

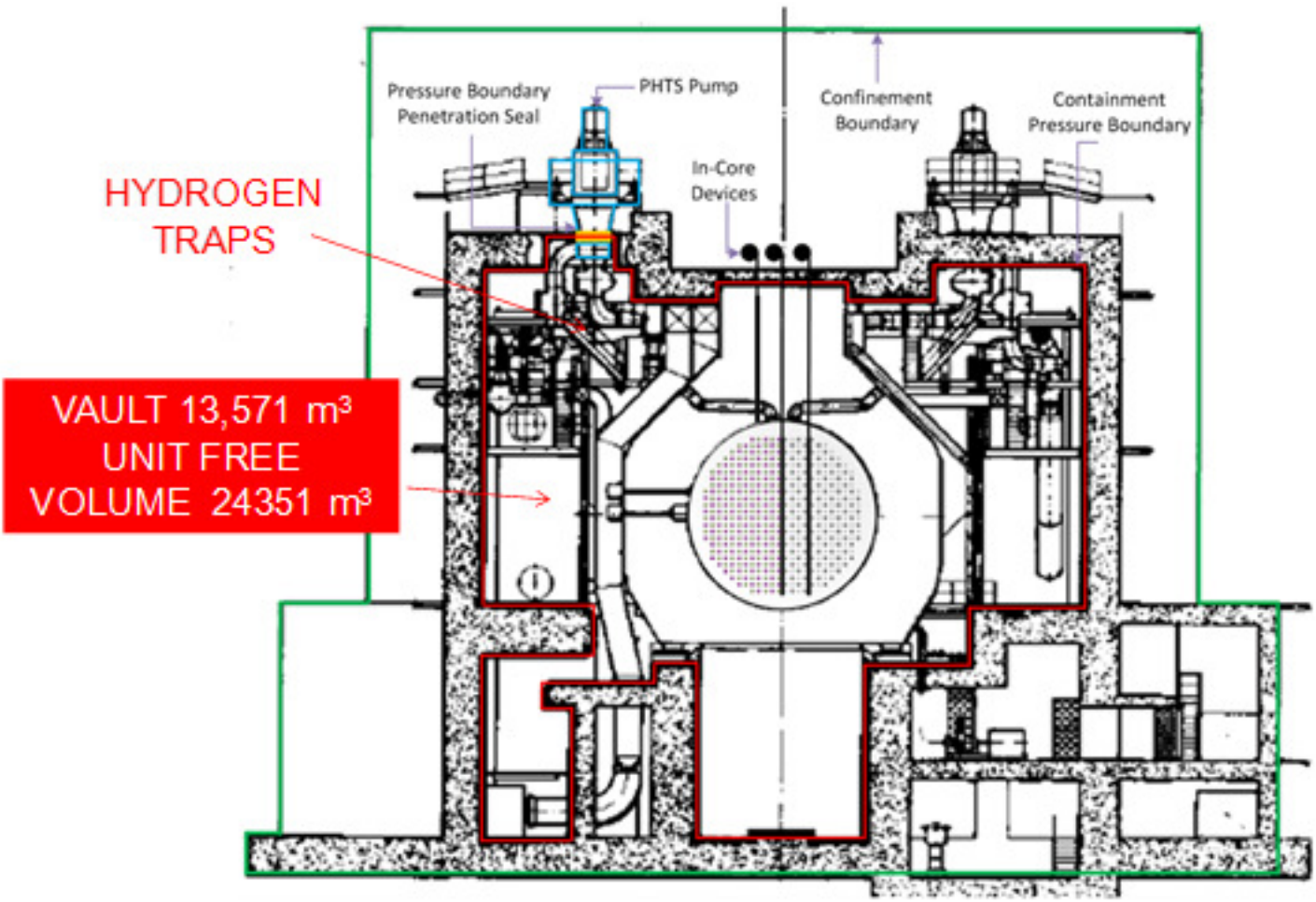

Figure 9: Single unit reactor assembly in a crowded vault with common fuelling machine duct below

The production of combustible Deuterium gas from over ten km of carbon steel piping and over 50 tons of Zircaloy in each Darlington unit can be extremely high with steel oxidation more problematic over the longer term; making the installed numbers and types of PARS not only inadequate but as early ignition sources also dangerous.

These conclusions are based on forty years of working on severe accident related issues at CANDU reactors, conducting extensive design reviews and developing integrated computer codes (MAAP-CANDU [xxi] and ROSHNI [xxii]) and supporting numerous analytical methods for PHWR accident progression and consequence assessments.

It was hoped that open discussions by professional engineers would foster change in name of public safety. That has not happened for a number of reasons, allegiances and self-interests. It is now feared that nothing will change unless an accident occurs and an ensuing national inquiry unveils a naked collusion between the regulator and the utility as in Japan prior to Fukushima. A lax and uninformed regulatory regime blindly supporting an intransigent industry resisting basic design enhancements has further exasperated, like it did in Japan, the severe accident related risk from continued operation of these reactors.

It is unfortunate that assumptions in evaluations of accident progression are made by the industry and the regulatory bodies acting in unison that make the accident consequences look benign. One such assumption of a 'core collapse' due to disassembly of higher elevation channels is essentially a numerical trick that gives a false impression of the whole core suddenly falling into cold water in the moderator and ceasing to emit radiation for 8 hours or so. As a result the accident consequences can actually be engineered to look benign.

Actual improvements after Fukushima are perfunctory and the analytical methods in support of severe accident management procedures are outdated and incomplete. A widely used computer code MAAP-CANDU (developed 25 years ago by this author based on the non CANDU specific components from MAAP LWR code) is incapable of providing the source terms required to evaluate containment response, design mitigation equipment or off-site releases. I developed that code over 25 years ago integrating CANDU specific models with the LWR code MAAP at a time when we used Pentium 286 machines and have made public [xiii] a large number of limitations that make it ill suited to meet today's post Fukushima requirements.

A PHWR WILL PRODUCE DEUTERIUM - NOT HYDROGEN : D_2-H_2 DIFFERENCE

Given that the reactor is cooled and moderated with D_2O, one would expect the mitigation measures and detection measures designed for D_2, but almost all research and development and implementation has been for H_2. On top of public denial of the almost two fold difference in transport properties between D_2 and H_2, differences in recombination rates have been loudly professed by the regulator and the utilities to be negligible, in defiance of hosts of research papers that have shown that except for chemical reaction of formation, the two gases are really not identical in any meaningful way that would allow the utilities to treat them as one and the same. In addition to differences in transport properties differences in recombination on metallic catalysts has also shown to be different for the two gases [xxiii, xxiv]. In addition, there are scenarios in which H_2 would also be produced by external surface air oxidation of carbon steel feeders. This also has to be considered in design of systems for mitigation and detection. It is interesting that the senior OPG managers claim to the CNSC Commission in hearings to see no difference between the 2 gases.

MANAGEMENT CLAIMS OF NO FUTURE RELEASES

Meanwhile the largest of multi unit reactors continue to operate with 5 to 10 year license extensions in the middle of the most densely populated parts of Canada with almost no new systems in place to retard the progression of a severe core damage accident with the management claiming publicly [viii], to the horror of those who understand these reactors that the improvements made so far will make the chances of long lived radioactive species escaping from these reactors after a severe accident an impossibility. A 30 year license extension is a license to go ruin my country.

A 'HOLISTIC' APPROACH TO SAMG

Utilities have recently touted a new and bizarre 'holistic' approach to severe accident management. For example, Bruce Power say that by claiming in-vessel retention of core melt and a filtered containment venting it needs to not install adequate hydrogen mitigation systems or over pressure protection systems or rectify any one of the dozens of design deficiencies [xi]. In denying the risk reduction capability of such simple measures such as adequate safety relief valves for over pressure protection of the primary and the moderator cooling loops, it is acting against public interest, forgetting that according to good engineering practices and IAEA guidelines probabilistic analyses should not be considered as a substitute to a design approach based on deterministic requirements but as a part of the process to identify potential safety enhancements and to judge their effectiveness.

STATION BLACKOUT AT A MULTU UNIT CANDU

Let us go back to a Station Blackout scenario with an unmitigated loss of all AC power in a multi-unit CANDU plant at Darlington or Bruce station. This scenario implies that no AC power is available for a specified recovery period, usually taken at 12-24 hours for consequence analyses.

As the reactor trips, turbines trip and feedwater flow ceases, nuclear steam discharges to the atmosphere through Main Steam Safety Valves (MSSVs). Necessary condition for the atmospheric discharge of steam to remain a heat sink is that fluid inventory in maintained both within the boiler tubes and outside the boiler tubes. Early passive heat removal by thermo syphoning flows from core to the steam generators is maintained as long as the primary fluid inventory can be carried over the U tubes. It is unfortunately jeopardized early at Darlington and Bruce multi unit stations by the low elevation positioning of the large pressurizer vessel. It's free steam volume a couple of minutes after a reactor trip is about equal to the volume of the coolant in the boiler tubes (65 m^3) upon a loss of power to the pressurizer heaters [xxv]. So the pressurizer can slowly swallow the volume of the heat transport coolant in the boiler tubes. As a result, the boilers stop being a heat sink even before they run out of water on the secondary side. No further addition of water to the boilers by AFW pumps or any other means will restore a heat sink for the core decay heat.

Even if the lost water inventory in the boilers tubes can be replenished by a major change in emergency management procedures, with no passive steam driven auxiliary feedwater pumps or a method to easily replenish the steam generators with a high pressure emergency water injection the boilers stop being an effective heat sinks after less than 2 hours. Back leakage through the feedwater line check valves will cause vapour binding in the feed pumps and only alternate paths for water addition to the boilers will be effective.

With no effective heat sinks, the primary cooling system re-pressurizes and with an inadequate steam relief capacity of the safety relief valves on the degasser condenser vessel in path of the relief, an uncontrolled over-pressurization leads to a pressure boundary rupture. There neither are any provisions for passive or manual depressurization of the reactor loops after a loss of steam generator heat sinks nor a capability for a high pressure coolant injection into the pressurized heat transport loops and an uncontrolled rupture becomes an unnecessary inevitability with a potential for an early containment bypass as the most atypical of any reactor overpressure protection system fails to provide adequate relieve steam through dual valves in series qualified only for liquid relief. In absence of a retaining pressure vessel like in LWRs, an ensuing gradual onset of fuel channel

heatup and disassembly upon loss of moderator coolant puts energy, radioactivity and combustible gases directly into the relatively weak reactor buildings. These structures are quite different from a traditional PWR cylindrical dome building and are rectangular structures built to old industrial standards. There are significantly high sources of combustible Deuterium gas ('heavy hydrogen') from large amounts of carbon steel in feeders and Zircaloy in fuel and fuel channels. Given the layout of the reactor units mimicking four inverted volumes interconnected at the bottom by a common duct, separation and accumulation of combustible gases in these unventable, inverted-cup like geometries makes for impracticable combustible gas control. The small number of Passive Autocatalytic Recombiners planned and/or installed are neither quantified / qualified for severe accidents nor for the actual gas (Deuterium) they must recombine and can become early ignition sources. There is an enhanced potential for energetic interactions of fuel debris with bodies of water enveloping the hot fuel channels. Pressure relief in relevant reactor systems (PHTS, Calandria, Shield Tank, and Containment) is inadequate for anticipated severe accident loads. With the reactor units directly attached to the containment pressure boundary and a significant number of reactor systems outside the containment, a containment bypass, as for example from reactivity device failure following fuel and debris heatup, is a likely outcome after a severe core damage. The Calandria Vessel, long heralded as a core catcher, is a thin ~1" thick stainless steel welded low pressure vessel that has been assessed to fail catastrophically at welds and not able to contain hot molten debris. This failure can not only lead to enhanced combustible gas production but also severe energetic explosions leading to failure of structures at the containment pressure boundary. The Shield Tank also cannot contain pressure upon boiling and can fail.

Given that unmitigated expulsion of hot gases and fission products targets the small reactor buildings, there is potential for poor equipment survivability. The in-reactor instrumentation for monitoring and control is neither adequate nor qualified for conditions after a severe accident. Severe accident simulation methods are outdated, crude and in dire need of upgrades. There are no dedicated simulators for severe accidents and the perfunctory desktop exercises with high-level Severe Accident Management 'Guidelines' are inadequate. No significant design changes have been implemented since Fukushima that may prevent a severe core damage scenario and some well known design problems like inadequate over pressure protection have been ignored. Yet, there are opportunities for engineered upgrades that can substantially eliminate a large number of vulnerabilities. However, the regulatory regime in Canada is lax and regulatory staff does not have the technical capability or guidance to independently verify assessments and analyses presented by the utilities not motivated to invest in design upgrades for low probability events they want to ignore. As a result, a continued exploitation of an outdated design with refurbishments that extend the life by another couple of decades is not only a risk to public but also to the utilities.

CONTAINMENT STRUCTURE VULNERABILITIES

The multi unit CANDUs at Darlington and Bruce house four reactor units in an interconnected slightly sub-atmospheric containment attached to a normally isolated vacuum building maintained at about 7 kPa(a) and of about 75% of the containment volume. Each reactor sports a containment structure that is common and contiguous to 4 relatively large reactor power units. Each reactor is capable of putting un-attenuated fission products from the ~2700 MW(th) fuel fission sources as well as combustible Deuterium from over 50,000 kg of Zircaloy and 2000 m^2 of the 120,000 kg of carbon steel. As a result, any accident that results in activity releases into the containment, whether

within the design basis or not, is likely to contaminate and disable from service all four reactor units.

With an over pressure retention capability of less than a bar (at design and significantly deteriorated after 20+ years such that all containments are no longer tested at design pressure or at the required frequency of 6 years) and a containment structure made up of rectangular concrete slabs and about 500 times leakier than the 1%/day leakage at design pressure for PWRs, a number of critical equipment are outside the containment and some critical equipment like pressurizers are placed below the mid elevation of the reactor core inside the containment. A common Fuelling Machine Duct underlying the 4 reactors connects the containment volume via a Pressure Relief Duct to a Vacuum building whose volume is deemed adequate for most design basis accidents in a single unit but its effectiveness to mitigate a severe accident in all 4 units is very obviously lacking as the effective volume per reactor unit is less than half of that for a typical PWR and the structures are weaker and with greater likelihood of trapping combustible gases . The containment is built to the National Building Code as are the access requirements, fire protection, smoke detection, etc. It is not built to modern nuclear containment standards.

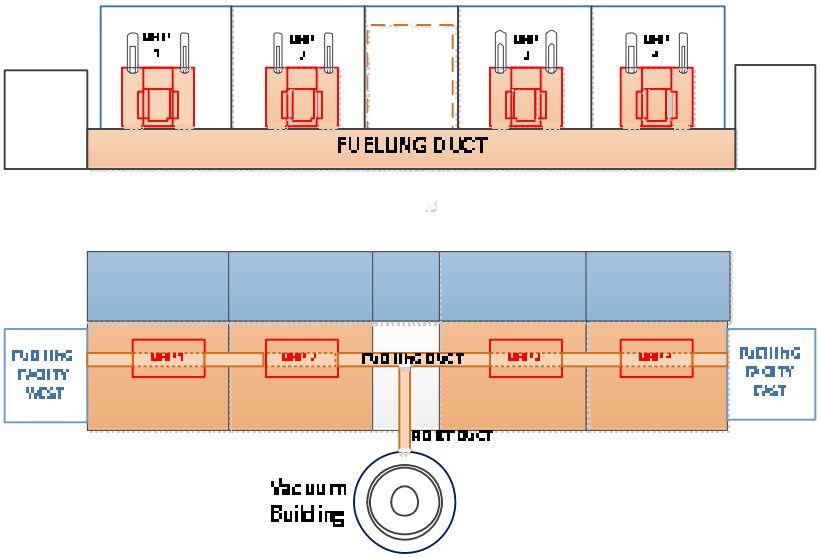

Figure 10 : Darlington station layout for 4 units with common containment

A number of reactor systems including the reactivity control mechanisms, primary pumps and steam generators are located outside the containment boundary above the reactor cores. The reactor core related structures themselves are within a tank attached at the containment pressure boundary. Critical structures essential for maintaining core cooling being outside the containment are likely vulnerable to certain externally induced challenges. The stations have not considered reactor building reinforcements to avoid building failure or added additional reinforcements with special emphasis on confinement space on top of reactivity decks to mitigate external impact hazards. While a PWR containment may be expected to withstand an aircraft impact, there is such no protection in a multi unit CANDU.

There are no new improvements to pressure suppression system in reactor building as the vacuum building is an inadequate volume supplement to avoid building failure after a multiunit core damage accident or even due to pressurization caused by hydrogen burns. Measures to

reinforce the confinement pressure boundary (space occupied by safety and process systems outside the containment) are missing.

The basement of the reactor buildings (fuelling machine duct and the pressure relief duct) is located below the level of the water in the lake. To the credit of the utilities, new portable Emergency Diesel Generators have been to be located at elevations higher than the original backup Diesel Generators that are at lower grade elevations, about 3m higher than the water, not dissimilar to what sank Fukushima. They are yet to be relocated to higher elevations. If that was done a failure similar to that at Fukushima could be avoided.

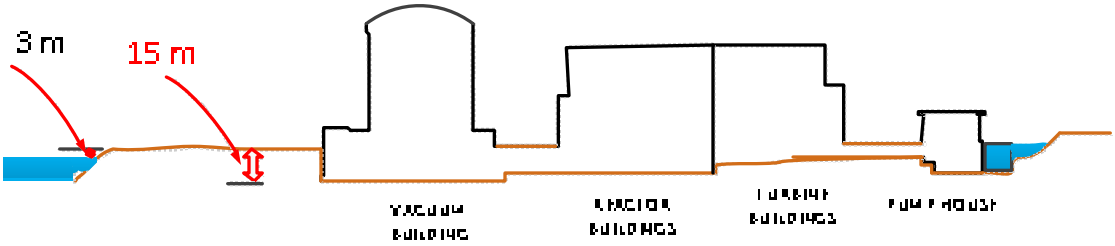

Figure 11 : Building basement layout below Lake water level. The emergency power supply generators are at grade level with cable tunnel 6m under.

The containment structures are rectangular slabs different significantly from typical cylindrical PWR containments and have a relatively weak design pressure (0.6 to 0.9 bar) with relatively high design leakage at design pressure (up to 2% volume per hour or up to 48% per day comparing very unfavorably to a typical PWR with 0.1% leakage per day (Figure 4) at a design pressure that is typically 5 times higher).

The containments are tested for pressure retention most infrequently of any power reactor in the world. Darlington now tests containment for pressure every 12 years while the regulations under which it was originally licensed required a 6 year test interval. The last pressure test was described as a difficult and arduous process that took 6 months of planning.

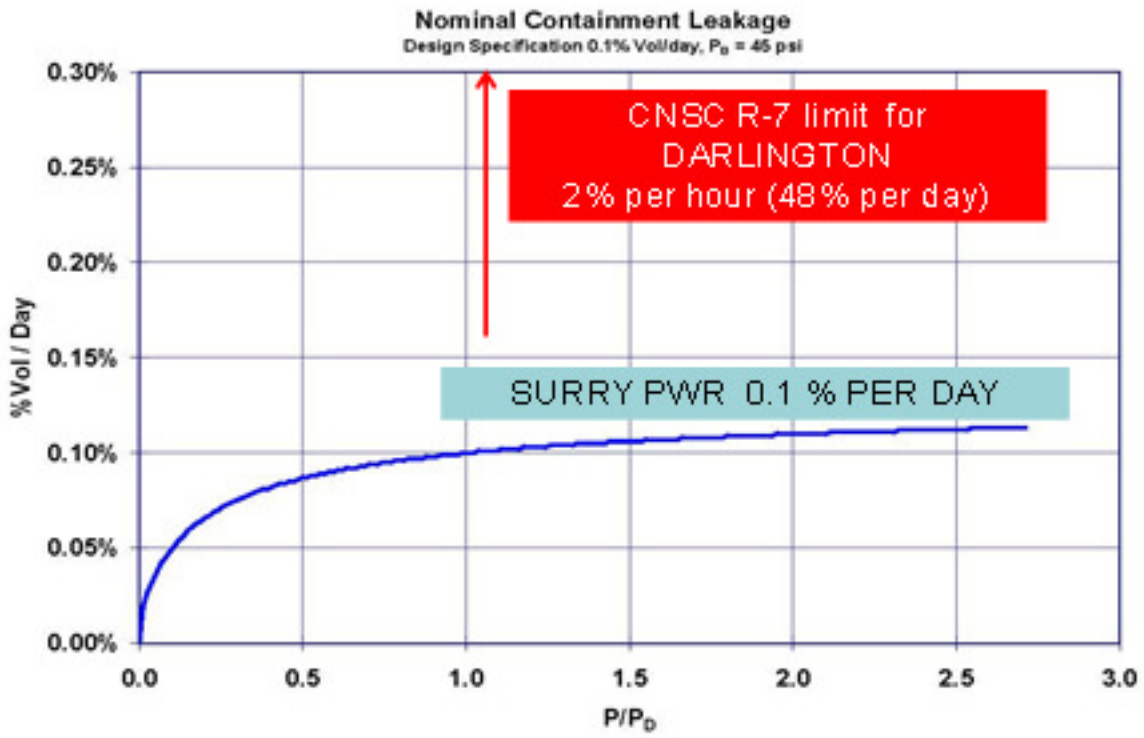

Figure 12 : Comparison of a PWR containment design pressure leakage with that for a Multi unit CANDU.

The individual reactor buildings can be envisioned to be inverted cups on top of a common duct such that retention of flammable gases and fission products after the vacuum building becomes ineffective is a concern. The reactor building volumes are about 14000 m^3 each with a combined volume of the 4 unit reactor buildings and the common fuelling machine and pressure relief ducts of about 120,000 m^3. The normally isolated vacuum building is an additional 95,000 m^3 and it is maintained originally at an isolated pressure of 7 kPa(a) with the main containment volume slightly sub atmospheric. For a multi unit severe accident, the containment volume per unit power is among the smallest of any other similar power reactor in the world.

SUMMARY OF DARLINGTON SEVERE ACCIDENT PROGRESSION & MITIGATION CHALLENGES

Containment

- Low containment design pressure (<0.9 bar) and high design leakage at design pressure(48% per day)
- Reactivity devices, steam generators, pumps and other equipment critical for long term heat removal are outside the containment and located under an industrial building .
- Containment bypass from over-pressure and thermal creep induced steam generator tube ruptures and from reactivity device failure a likely outcome after a severe core damage.
- Reactor vaults shaped and arranged to be highly likely traps for combustible gases.

Poor Overpressure Protection Design

- Safety relief valves not directly on the main cooling circuit (ASME section III , NB-7141 (b) requires a direct and unobstructed relief path) and require another pair of downstream valves to open. All valves designed for liquid relief.
- Only two safety relief valves (called 50% capacity valves but the 'capacity' is misrepresented) - contravenes single failure criteria
- Undersized over pressure protection with steam relief capacity of the 2 safety relief valves by a factor of up to 10 - contravenes common sense - relief capacity must exceed anticipated loads, which will always exceed decay heat.
- Inadequate primary cooling circuit relief inherently forces reactor damage by uncontrolled over-pressurization even before an ECC is given a chance to avoid severe core damage. An uncontrolled relief through a rupture in pressure boundary is an unacceptable outcome.
- Accelerated depletion of moderator inventory due to expulsion through pressurized Calandria rupture disks upon channel voiding and fuel heatup to cause moderator boiling.
- Shield Tank cannot contain anticipated pressurization upon boiling and can fail. Restoration of cooling after water depletion problematic as pump flow inlet at the top of vessel that can be voided.

Poor Pressure and inventory control

- No provisions for direct manual depressurization of the Primary Heat transport system.
- Pressurizer located well below the core can drain water from primary coolant system upon cooling upon loss of power and inhibit thermosyphoning flows.
- No systems for high pressure ECC or any emergency measures for high pressure primary makeup intervention / injection.

Lack of a pressure vessel causes direct containment contamination

- Onset of severe core damage puts activity directly into the containment. There is no isolation of damaged core and its activity in a closed vessel like in a PWR pressure vessel.

Poor Deuterium Hydrogen mitigation systems

- Significantly higher sources of hydrogen from large amounts of carbon steel and Zircaloy.
- Currently planned hydrogen mitigation systems (igniters + a small number of PARS) inadequate and potentially dangerous. Poor combustible gas mitigation measures. Small number of Autocatalytic Recombiners inadequate for severe accident scenarios and will cause explosions.

Moderator vessel an unlikely core catcher - poor

- Energetic interactions of disassembling core debris with underlying boiling moderator water in the low pressure Calandria vessel can cause vessel structural failures.
- Calandria vessel failure by weld failures is a likely outcome even before debris melt. There are a number of pipe penetrations at the bottom of the vessel that can fail by thermal interactions with hot debris.

Should the Calandria vessel fail, interaction of hot debris with Shield Tank water also similarly challenging to integrity of structures holding the reactor vessels connected to the reactivity deck at the containment pressure boundary pressure relief in ALL relevant reactor systems in inadequate (PHTS, Calandria, Shield Tank, Containment) to remove decay heat

- Calandria vessel likely cannot contain melting reactor core debris and can fail catastrophically at welds causing energetic interactions with potential for gross structure failures.

Spent Fuel storage

The spent fuel medium term storage in spent fuel pools is poorly designed and highly susceptible to Zircaloy fires.

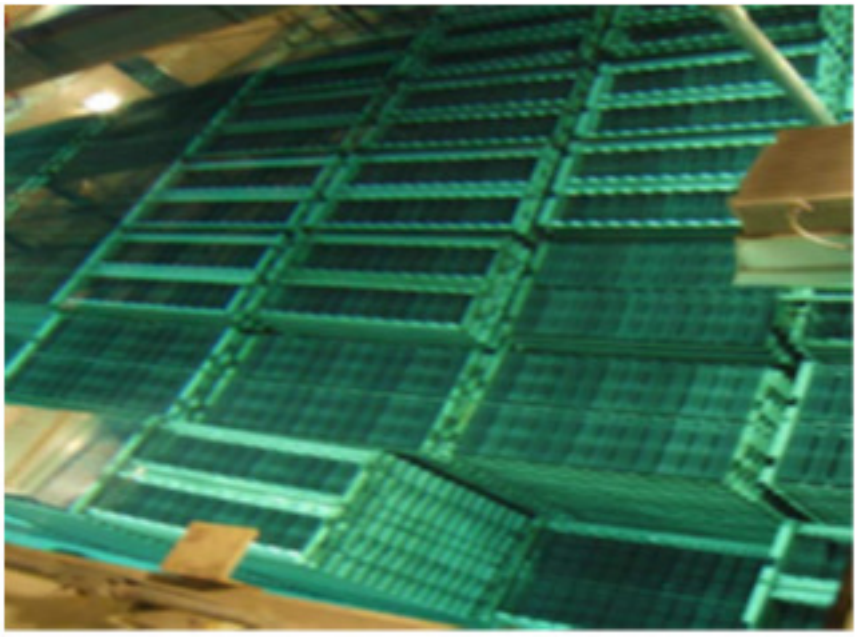

Figure 13: Spent fuel bundles stacked like fish in a fish basket, 16 or more trays high

Backup Diesel Generators

These are located at the lowest grade elevation in the plant and are no more than 3m above the water line at Darlington The tunnel carrying the cables is below the water line by about 4m and can get deluged with water. Pickering station has seen its basement level flooded in the past from water swell in the lake. Location of backup diesel generators has been pointed out as the single most critical error at Fukushima; something that has escaped the CNSC despite repeated warnings. In fact, CNSC staff provided misleading information as to the actual location of the diesel generators in Bruce reactor relicensing public hearings in 2018 by claiming that they were located 40-50 feet higher than the lake water.

In Bruce the diesel generators are at 591' elevation while the grade varies from 614.5' at the north side to 590.5 ft at the south side. So the diesel generators are at lowest grade in the station grounds and certainly below the average grade. The tunnel carrying the cables from the water treatment plant (where the generators are) is at 569' with the water line higher by 10' at 579'. So the tunnel is below water line. The tunnel can be flooded by a deluge or a flood or a seismic activity. So if the grounds which are at 591' in that area ever get flooded by a wave, a tsunami, ice dam or whatever, the diesel generators will get flooded at Bruce, just like at Fukushima. The cables from the diesels are in the trench at a much lower elevation, below water line. Design of structures housing backup diesel generator at Darlington is a copy of the one at Bruce.

And…

- Inadequate instrumentation and control for severe accidents
- Poor equipment survivability due to poor containment layout
- No dedicated operator training / simulators for severe accidents.
- Severe accident simulation methods are outdated, crude and inadequate.

- No significant design changes implemented. Known problems ignored for decades.
- Current SAMGs are unrealistic and inadequate. Many potentially favorable emergency hookups not implemented.
- Environmental assessments for off-site releases after a severe accidents performed with a source term that represents barely 0.15% of the total core inventory

The lessons learned from Fukushima disaster have been poorly accepted despite the hoopla surrounding development of Fukushima Action items by the National Regulator. Risk to public can only be reduced by much needed design upgrades, starting with an open discussion of the severe accident related vulnerabilities, and an acknowledgment that the reactors not designed with consideration of any severe accidents within the design basis; cannot be expected to provide mitigation measures necessary to meet the newly emerging understanding of progression and consequences of a severe accident and current public expectations.

SUMMARY MAJOR AVENUES OF DESIGN UPGRADES THAT SHOULD REVISITED EVERY 5 YEARS IN RELICENSING HEARINGS

Following is a partial list of design improvements that require serious and immediate consideration to meet some of the vulnerabilities of the multi-unit CANDU design.

1. Passive makeup by steam driven auxiliary feedwater pumps for high pressure water addition to boilers
2. PHTS overpressure protection enhancements for avoidance of uncontrolled ruptures (replace PHTS relief valves)
3. Emergency power hookups to pressurizer heaters for early re-establishment of pressure control, or Relocate pressurizer to higher elevation
4. High pressure makeup of PHTS inventory loss (high pressure emergency water injection pumps)
5. Pressure relief valves on Pressurizer for manual PHTS depressurization
6. Calandria vessel overpressure protection enhancements for avoidance of deliberate voiding (relief valves with decay heat capacity in addition to rupture disks)
7. Calandria vessel structural design enhancements for better likelihood of retention of core debris
8. Shield tank overpressure protection enhancements for avoidance of structural failure
9. Shield tank heat removal capacity enhancements for retention of debris in Calandria vessel
10. Containment penetration reinforcement for avoidance of overpressure failures
11. Containment pressure suppression improvements: local sprays and external support to coolers
12. Instrumentation enhancements for detection of important accident parameters
13. Filtered containment cooling for avoidance of imminent structural failures
14. Emergency hookups for water and power to safety critical systems at appropriate pressures
15. Improved Class 1 batteries., better definition of anticipated loads over prolonged periods of loss of AC power.
16. Combustible gas detection, measurement and recombination systems calibrated for Deuterium
17. External water makeup to a stranded fuelling machine after a LOCA
18. External water makeup and heat removal from the spent fuel bay
19. Off-site measurements of activity magnitude and energy for identification of radioactive species in releases and correlating them to source terms;
20. Upgraded consequence assessment codes dedicated for PHWRs (current codes are not entirely fit for intended use)

UNEXPLORED AVENUES OF RESEARCH OR THINGS WE DO NOT KNOW / UNDERSTAND WELL ENOUGH- A 30 YEAR LICENSE WILL RETARD ANY IMPETUS TO PROMOTE RESEARCH

There are a number of phenomena associated with accident progression that require separate effect quantification with research and have not been addressed properly. These include:

1. Effect of uncontrolled pressurization of the heat transport system before core degradation. With over-pressure relief valves unable to remove decay heat an uncontrolled re-pressurization of the PHTS is inevitable. Typical design failure pressures in a CANDU reactor for level C conditions in Table 1 indicate that the ever so vulnerable boiler tubes have the lowest pressure retention capacity and are thus are prime candidates for failure. However, the degradation of feeders by thinning (~0.1 mm/yr) and of pressure tubes by hydriding, creep - thinning, elongating etc. makes the issues more complex.

2. Reflux condensation holdup of water in boiler tubes on feedwater recovery. This becomes important in case of boiler recovery after PHTS is voided and can lead to early channel heatup of voided channels and their failures at high pressures when natural circulation flows cannot be re-established.

Table 1: PHTS COMPONENT PRESSURE RETENTION CAPACITY

CANDU 6 REACTOR COMPONENT	**Level B**	**Level C**	**Level C with Seismic**
Inlet Header	14.81	18.96	18.96
Outlet header	12.49	17.58	17.58
Pressure Tube Outlet	11.81	22.22	15.10
Rolled joint outlet	12.46	21.65	10.14
thickness	12.11	16.52	13.71
SG tubing	13.43	14.34	12.72
Pressurizer	12.13	16.00	16.00
Degasser Condenser	11.77	15.51	15.51
header interconnect	17.46	30.99	11.68

3. Core and Channel thermal hydraulics under loss of forced circulation - during PHTS blowdown, voiding by boiloff and depressurization ; intra channel fluid interactions

4. Mechanisms of high temperature fuel bundle deformations and quantification of bundle geometry parameters

5. Fuel bundle oxidation with air, oxygen at various stages of its disassembly.

6. Mechanisms of high pressure rupture failure of CANDU channels by hot fuel and melt interactions with pressure tubes

7. Channel failures by their deformations; melt through to channel disassembly at low pressures

8. Gross core disassembly, debris retention, displacements, interactions and collapse of individual columns of channels

9. Effect of recovery actions to reflood fuel channels

10. Steam explosion potential during debris and melt relocation to underlying water in Calandria vessel

11. Solid debris behavior in Calandria with accumulation over many hours and without water ingress

12. Solid debris interactions with air drawn from Calandria overpressure relief ducts

13. Thermo-mechanical behavior of stepped welded Calandria vessel under load of hot debris

14. Response of boiler tubes following core heatup (consequential boiler tube failure) at high pressures and at low pressures with boilers dried out

15. Component and system failure modes for interfacing systems, in-core device failures that may create a containment bypass.

16. Interaction of debris with an intact loop in case of coolant loss and core damage restricted to one loop.

17. Oxidation of end fittings, feeders, Calandria by steam and air

18. Fission product release mechanisms under different fluid conditions from fuel pins in bundles, debris, corium

19. Effect of recovery actions in Calandria, shield tank, fueling machine duct in presence of debris

20. Effect of Calandria vessel weld failures including interaction of water ingress on solid and molten debris

21. Containment response to sharp pressurization loads (energy, mass addition ; hydrogen combustion)

22. Hydrogen / Deuterium distribution in reactor vaults and rest of containment

23. Hydrogen / Deuterium burns, detonation, deflagration in reactor vaults and failure modes of structures

24. Effectiveness and adverse effects of recombiners, igniters (auto-ignition and explosions)

25. Containment response to sharp pressurization loads (energy, mass addition ; hydrogen combustion)

26. Potential and effects of consequential floods, fires in containment

COMPUTER CODES USED FOR SEVERE ACCIDENT PROGRESSION & CONSEQUENCE ASSESSMENTS

The currently used computer code MAAP-CANDU suffers from the following errors and deficiencies (a complete list contains 52 entries) :

1. No consideration of heavy water, deuterium gas (light water and H_2 properties used)

2. No momentum equation for PHTS

3. Channel degradation during channel boiloff before dry steam/D_2 heatup not modelled - Initial fuel temperatures at onset of heatup are arbitrary

4. Channel hydraulics based on assumed header to header Δp and no overall core thermal hydraulics. No intra channel flows. No consideration of fluid discharge paths.

5. A limited number of channels modelled.

6. No explicit fuel sheath modeling.

7. No modeling of out of flux pressure tube lengths.

8. No modeling of water retention in end fittings after boiloff or blowdown

9. No thermal modeling of feeders and end fittings

10. No consideration of differences in burnup and power profiles between various channels

11. No modeling of in-core devices and their effect on individual fuel bundle displacements.

12. No modeling of piping into Calandria vessel.

13. Crude modeling of core disassembly & a physically impossible model of 'core collapse'

14. Primitive modeling of suspended solid debris

15. Solid debris interactions with air not modelled

16. Deuterium / Hydrogen generation by steel oxidation and Uranium-steam oxidation ignored.

17. Fission product releases from debris crudely modelled.

18. Fission products do not decay.

19. As 'engineered' codes with specific accident progression pathways – many scenario paths not considered.

20. Difficult I/O; primitive post processing

It is incomprehensible that above deficiencies have not been rectified in the 25 years since the control of code development left Canadian hands. No SAMGs, design assist or other accident management or training measures are possible without properly modeling the reactor, its phenomenology and all potential accident progression pathways. Without modeling the behaviour of each fuel channel individually, for example, the erroneous conclusions drawn from models such as for a total, global core collapse can give misleading and dangerously inaccurate results.

REFERENCES

[i] Study of Consequences of a Hypothetical Severe Nuclear Accident and Effectiveness of Mitigation Measures, CNSC, Sept 2015, http://nuclearsafety.gc.ca /eng/resources/health/ hypothetical-severe-nuclear-accident-study.cfm

[ii] Sunil Nijhawan, Regulatory Actions That Hinder Development Of Effective Risk Reduction Measures By The Nuclear Industry For Enhanced Severe Accident Prevention And Mitigation Measures After Fukushima, ICONE24-60700, Proceedings of the 2016 24th International Conference on Nuclear Engineering ICONE24, June 26-30, 2016, Charlotte, North Carolina, USA

[iii] Submissions to the CNSC Public Hearing on Ontario Power Generation's Application to Renew the Reactor Operating License for Pickering A & B. In particular Sunil Nijhawan submission CMD-H6-38 from http://www.suretenucleaire.gc.ca/eng/the-commission/hearings/ documents_browse/results.cfm?dt=25-Jun-2018&yr=2018

[iv] Study of Consequences of a Hypothetical Severe Nuclear Accident and Effectiveness of Mitigation Measures, CNSC, Sept 2015, http://nuclearsafety.gc.ca /eng/resources/health/ hypothetical-severe-nuclear-accident-study.cfm

[v] CANDU Owners Group, Final Report on Post-Fukushima Questions, COG-JP-4534-02-R0, October 2016

[vi] Bruce Power Relicensing Hearings Transcripts, 2014, page 306, April 15, 2014, page 306, 2015-04-15-Hearing-Transcript-edocs4744683-e.pdf, Canadian Nuclear Safety Commission.

[vii] Review of the High-Temperature Oxidation of Iron and Carbon Steels in Air or Oxygen, R. Y. Chen and W. Y. D. Yuen, Oxidation of Metals, Vol. 59, Nos. 5/6 (2003.6)

[viii] Bruce Power Relicensing Hearings Transcripts, 2018, page 227, May 29, 2018. 2018-05-29-HearingCorrected.pdf . Canadian Nuclear Safety Commission.

[ix] Submissions to the CNSC Public Hearing on Ontario Power Generation's Application to Renew the Reactor Operating License for Pickering A & B. In particular Sunil Nijhawan submission CMD-H6-38 from http://www.suretenucleaire. gc.ca /eng/the-commission/hearings/documents_browse/ results.cfm?dt=25-Jun-2018&yr=2018

[x] Integrated Regulatory Review Service (IRSS); Followup mission to Canada, Ottawa, Canada - 28 Nov to 9, Dec 2011, Department of Nuclear Safety and Security, IAEA-NS-IRRS-2011/08 from http://nuclearsafety.gc.ca/eng/pdfs/irrs/2011-IRRS-Follow-up-Mission-to-Canada-Report-IAEA-NS-IRRS-2011-08-eng.pdf

[xi] Challenges In Multi-Unit CANDU Reactor Severe Accident Mitigation Strategies, Sunil Nijhawan, Proceedings of the 24th International Conference on Nuclear Engineering ICONE24-60689, June 26-30, 2016, Charlotte, NC, USA

[xii] CANDU Owners Group, Final Report on Post-Fukushima Questions, COG-JP-4534-02-R0, October 2016

[xiii] Improved Regulatory Oversight And Immediate Retrofits For Operating Pressurized Heavy Water Reactors , Sunil Nijhawan, Proceedings of the 20th International Conference on Nuclear Engineering, ICONE20-POWER2012, Paper-54387, July 30- August 3, 2012, Anaheim, California, USA

[xiv] Severe accident progression without operator action, Canadian Nuclear safety Commission, Oct 2015, http://www.nuclearsafety.gc.ca/eng/pdfs/Reports/Severe-AccidentProgression-without-Operator-Action.pdf

[xv] http://nuclearsafety.gc.ca/eng/the-commission/hearings/cmd/pdf/CMD18/CMD18-H4-144.pdf

[xvi] State-of-the-Art Reactor Consequence Analyses (SOARCA) project,https://www.nrc.gov/about-nrc/regulatory/research/soar.html; NUREG/CR-7110, vol1, 2, NUREG/BE-0359, US Nuclear Regulatory Commission.

[xvii] Bruce Power Relicensing Hearings Transcripts, 204, page 378, April 14, 2014, page 378. Canadian Nuclear Safety Commission, 2015-04-14-HearingTranscripts-edocs4743165-e.pdf.

[xviii] Requirements for Containment Systems for CANDU Nuclear Power Plants, Atomic Energy Control Board (*now CNSC*), 1991

[xix] Importance Of Reactor Heat Transport System Overpressure Protection System Under Severe Accident Conditions With Special Reference To CANDU Reactors, Proceedings of the 20th International Conference on Nuclear Engineering CONE20 & POWER2012 , July 30-August 3, 2012, Anaheim, CA, USA Paper 54301

[xx] https://spectrum.ieee.org/tech-talk/energy/nuclear/former-nrc-chairman-says-us-nuclear-industry-is-going-away

[xxi] Modular Accident Analysis Program for CANDU Reactors,C.Blahnik, C.Kim, S.Nijhawan, R.Thuaisingham, ANS 1992

[xxii] ROSHNI - a new integrated severe accident simulations code for PHWR level 2 PSA applications and severe accident simulator development, Proceedings of ICONE-23, Paper ICONE23-1054,23rd International Conference on Nuclear EngineeringMay 17-21, 2015, Chiba, Japan

[xxiii] Hydrogen and Deuterium in Pd-25 Pct Ag Alloy: Permeation, Diffusion, Solubilization, and Surface Reaction, E. Serra, M. Kemali, A. Perujo, And D.K. Ross, Metallurgical And Materials Transactions A Volume 29A, March 1998—1023

[xxiv] Gaseous transport properties of hydrogen, deuterium and their binary mixtures from ab initio potential, Bo Song, Xiaopo Wang and Zingang Liu, Molecular Physics, Vol 111, No. 1, 49-59, 2013

[xxv] RELAP5 Simulation of Darlington Nuclear Generating Station Loss of Flow Event (NUREG/IA-0247), D. Naundorf, J.Yin, Feb 2011.